DSCI Reference Architecture Series

VIRTUALIZATION | CLOUD COMPUTING | MOBILITY/BYOD

Architectural Ideas and Capabilities

NETWORK IN THE CONTEXT OF SECURITY

INDUSTRY COLLABORATED REPORT

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CISCO

About DSCI

DSCI was setup as an independent Self-Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same. DSCI is engaged with the Indian IT/BPO industry, their clients worldwide, Banking and Telecom sectors, industry associations, data protection authorities and other government agencies in different countries. It conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cyber crimes in the country and towards this; it operates several Cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.

Public Advocacy, Thought Leadership, Awareness & Outreach and Capacity Building are the key words through which DSCI continues to build and enhance trust in India as a secure global sourcing hub, and promotes data protection in the country.

About Cisco

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. At Cisco (NASDAQ: CSCO) customers come first. An integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success. Founded in 1984, Cisco has been a leader in the development of Internet Protocol (IP)-based networking technologies since the company's inception. John T. Chambers is the Chairman and Chief Executive Officer of the $46 billion company which has over 72,000 employees globally. Cisco India Commenced operations in 1995 and has seven Sales Offices in the region-New Delhi, Mumbai, Bangalore, Chennai, Pune, Kolkata and Hyderabad. The Cisco Global Development Center is in Bangalore and is the largest outside the US.

For further information about Cisco India, please visit http://www.cisco.com/in

For more information on Security Thought Leadership Program contact - thoughtleadership@dsci.in

Published in September 2013

Designed & Printed by
Swati Communications
+91 11 41659877, +91 9213132174

Disclaimer

The DSCI-Cisco report on 'Architectural Ideas and Capabilities on Virtualization, Cloud Computing and Mobility/BYOD' is produced as part of the DSCI Reference Architecture Series. The study is part of the industry consultation process and is an Intellectual Property of DSCI. No part of this document in whole or its any part thereof may be reproduced, stored in a retrieval system, published, circulated, transmitted, or copied in any form or by any means, without the prior and explicit permission of DSCI. DSCI expressly disclaim to the maximum limit permissible by law, all warranties, express or implied, including, but not limiting to implied warranties of merchantability, fitness for a particular purpose and non-infringement. DSCI disclaim responsibility for any loss, injury, liability or damage of any kind resulting from and arising out of use this material/information or part thereof. Views expressed herein are views of DSCI and /or their respective authors and should not be construed as legal advice or legal opinion. Further, the general availability of information or part thereof does not intend to constitute legal advice or to create a Lawyer/Attorney-Client relationship, in any manner whatsoever.

DSCI-Cisco Security Thought Leadership Program

In its endeavor to strengthen cyber security and data protection ecosystem in the country, DSCI has undertaken various studies and surveys to develop reports on facets of Data Security and Privacy in India. DSCI has engaged the security community & leadership in India to contribute in reports that DSCI has published so far. Taking this initiative one step forward, DSCI in collaboration with Cisco launched the **Security Thought Leadership Program**. The program titled **"Re-Inventing the network in the context of security"** has been successful in connecting the security community in India and has provided multiple platforms for deliberations around evolutions in security.

DSCI, as a focal body on data protection in India, has leveraged this collaboration with Cisco to provide insights into the rapidly changing threat landscape and bring focus on the next generation capabilities available to effectively counter the ever growing dynamic and advance persistent threats.

The program focused on **Next-Generation Security,** based on the emergence of *Virtualization, Cloud computing, and Mobility/BYOD* changing the threat perception/ landscape in the Indian context. It further dealt with topics such as evolution of network security; capability to gather intelligence based on content, context and application awareness; self-healing and policy governed networks amongst others. As part of the program, DSCI in collaboration with Cisco released a survey report, findings of which were validated with the CISO community across major IT hubs in India. We further engaged the community by organizing webinars, hosting meetings and discussions, conducting a technical paper presentation competition, in addition to collaborating with several organizations for development of the Reference Architecture. The Reference Architecture will be a resource for the utilization of the security community to evaluate and analyze gaps in their existing security architecture.

Role of Reference Architecture - Ideas & Capabilities

The role of reference architecture was to provide an exposure to security leadership and professionals in the country around the architectural evolution with respect to technological innovation in the area of virtualization, cloud computing and mobility/BYOD and how they are changing the security response to scalability, diversity, complexity, extensibility, and granularity of business requirements, rules and service delivery expectations.

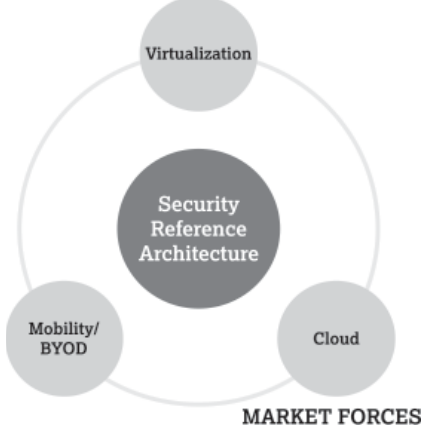
The increasing adoption of these technologies has not only resulted in proliferation of endpoints, but also blended the use of device for both personal and corporate use. Add to that, the challenges with respect to providing access through multiple mediums and provisioning services through the cloud has added to the complexity of IT security landscape. Businesses today, are dealing with **"Any-to-Any"** problem essentially meaning access provided ***to Any User*** *from* ***Any Device at Any Location*** *through* ***Any Application*** *via* ***Any Infrastructure (Physical/Virtual).***

Further, the overall state of traditional security methodology is considered restrictive & incompetent primarily because of following aspects:

- Conventional governance policies directing configuration, operating environment and choice of brand are no longer valid
- Expansionary, and extending nature of business makes the access map more complex
- Rationality of traditional model of DMZ based security enforcement is challenged by mobility and distributed environment
- Managing and enforcing policies is increasingly becoming difficult in the age of mobility and BYOD
- Prevalent approach of enforcement based on IP, protocol and services is becoming increasingly irrelevant
- Ability of current capabilities in the context of mobility, BYOD, virtualization, and APTs are getting challenged

The survey conducted as part of the program provided interesting revelations about the perception of the industry with respect to challenges the industry may encounter as they look towards adoption of these technologies. The findings from the survey acted as the foundation for development of the reference architecture. The focus of reference architecture was to depict architectural considerations while taking into account the trends that are increasingly influencing attributes for network security, content management and security of infrastructure transformation due to Virtualization, Cloud, and Mobility & BYOD.

The reference architecture reflects the interactions and engagement with security professionals along with their challenges, viewpoints and approaches which have been incorporated to support rationales and arguments. Architectural considerations on different deployments aspects within the three areas of Virtualization, Cloud and Mobility/ BYOD are presented in this report. The report aims at providing key considerations with respect to each technology and compiles architectural, technical, and implementation aspects by presenting sample architectural scenarios with industry use cases. These are further supported by security considerations for IT/Security architects, implementing these technologies within the enterprise.



Contents

Virtualization

Introduction

JOURNEY

- Mainframe Application
- Server Consolidation
- Desktop, Application, Network Virtualization
- Grid, Utility and Cloud Computing

Virtualization is the construct of Information Technology (IT) assets that hides the tangibility of physical assets and boundaries from end users. An IT asset may either be a server, a client, storage, networks, applications or Operating Systems (OS). Fundamentally, any IT building element can be abstracted from end users. Virtualization as a concept is dated back to 1960s when it was utilized in order to effectively tap the power of mainframe computers. The dilemma is how a five decade old technology is becoming pertinent in today's dynamic IT environment. If we look closely it is not the same set of technology elements which are again rising but it is the technical architecture which has found its place or application in today's IT infrastructure. The pendulum is swinging as its application varies from allowing a single server to act as many (server virtualization), to making a single piece of hardware look like multiple machines from multiple OS (desktop virtualization), application interacting with its own virtualized OS, user interacting with applications not running on their desktops (application virtualization) etc. This also includes 'Grid Computing' where computing clusters are designed to operate as one virtual IT asset, 'Utility Computing' where a virtualized platform is used to deliver on demand and metered services and 'Cloud Computing' which is believed to be the extension of virtualization in which desired IT resources are accessible on demand basis with no rich investment in its procurement, setup and maintenance.

Virtualization: Benefits and Challenges

In spite of the existence and diverse applicability of virtualization over several years, it is quite new in the galleria of various business ecosystems. Business categories ranging from small medium businesses (SMB) to large enterprises are yet to kick start their virtualization engine. Although there are proven use cases in the industry citing major benefits of virtualization such as cost optimization, agile business delivery, reduced power consumption, hardware consolidation, enhanced resiliency, expedited organization technology deployments etc; however, the dice is not rolling due to certain apprehensions.

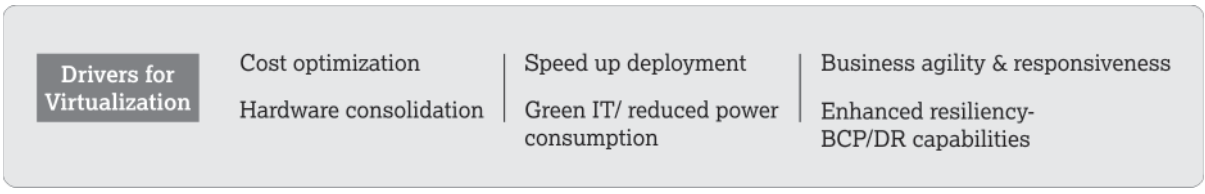
In case of virtualization, some of the challenges stated by technology analysts and implementers are such as 'network is not competent enough to execute virtualization, virtualization integration with storage architecture, back up issues, visibility of security posture, application support requirements changing, new skill set needed for effective functioning etc'.

The need is to incorporate strategic elements in the organization virtualization strategy which may include, but not limited to:

- Preparing organization architecture for the change
- Identification of spots which may undergo major changes
- Making sure that virtualization is right for your organization by referring use cases
- Breaking the myth that virtualization is a project only
- Training the right people
- Putting required governance and technology policies in to place

Virtualization Drivers

Proven industry case studies advocate that virtualization helps in controlling cost as the business grows, but most importantly, it brings flexibility which provides an organization with an added advantage. It helps to adjust swiftly and respond to dynamic market ecosystem. Virtualization not only supports IT but enables businesses as it influences new forms of applications and is also used as an enabler of cloud computing and helps in building mobility. It helps in redefining boundaries between IT components, platforms and operational processes and supports business agility by empowering IT to enable components across all platforms from mobile, desktops, servers and storage. It helps in adoption of contemporary applications, trends and platforms at a greater speed, and does more with limited resources. The imperatives of virtualization are summarized as below:



1.	**Cost optimization:** Virtualization significantly reduces cost by enhancing productivity of IT administration, reclaiming network ports, sizing data center capacity for effective utilization, etc. 'Hardware Consolidation', as enabled by virtualization, is an important driver in reducing the cost.
2.	**Green IT/Reduced power consumption:** IT assets consolidation, as facilitated by virtualization not only takes care of physical resources, but also scales down the requirement of resources leading to significant saving of power.
3.	**Business agility and responsiveness:** Virtualization is changing traditional, rigid, complex infrastructure comprising of physical servers, storage, and networks into a virtual ecosystem that IT can utilize dynamically to tackle new challenges, and open gates for new business opportunities. Major business organizations have been able to enhance IT scalability, manageability, and responsiveness exponentially by consolidating multiple IT physical assets into a fewer assets.
4.	**Speed up deployment:** Less hardware implies less infrastructure elements on which newer deployments need to be carried out. This is achieved by replicating deployment on virtualized IT assets with the help of host and guess operating system concept.
5.	**Enhanced resiliency:** Beyond tangible benefits such as cost optimization, organizations are also adopting virtualization for improved business continuity and disaster recovery (BC/DR).

Industry Use Cases

Case 1 – Large financial institution, looking to consolidate IT Infrastructure for Testing and Development

BACKGROUND

A leading PSU bank offering a wide variety of banking services, including corporate and personal banking, industrial finance, agricultural finance, financing of trade; serving over 3.5 crore customers through 4000+ branches and 450 extension counters. The bank is at the early stages of virtualization and is taking steps to consolidate its IT Infrastructure specifically for testing and development and non-critical applications

CHALLENGES

- Server consolidation for testing and development environment.
- Access issues in upcoming virtualized environment template based provisioning is being explored
- Enhance IT assets and workforce productivity by focusing on business needs rather than maintenance of Testing and Development application
- Security hygiene elements such as firewalls, IPS, IDS, encryption and antivirus capabilities had been implemented

BUSINESS BENEFITS

- Virtualization would shorten the deployment time of IT assets, enhance infrastructure resiliency, avoid service disruptions and also aid in better compliance demonstration
- Reducing the number of servers in the branch offices

SOLUTION

- The Bank identified the IT architectural touch points where virtualization can be carried out
- It achieved resource utilization particularly through server and workload consolidation
- It started focusing on reducing the number of servers by virtualizing the non-critical systems and moving development and testing application in the virtualized environment
- The bank, making use of virtualization for infrastructure consolidation focused on resolving issues arising from the effects on networks, security and software licensing
- It is also focused on simplifying high availability and recovery infrastructures, which are complex and can be a big cost centers for organization

SECURITY CHALLENGES

- Resolving security issues arising from the effects on networks, security and software licensing
- Issues related to access provisioning to resources
- Threat and vulnerability management of virtualized assets
- Security of development and test environment

Case 2 – Large IT Services Company Virtualizing Application to enable mobility

BACKGROUND

A leading IT solutions organization, with operations in 16 countries, provides services in application development and maintenance, enterprise solutions including managed services and business process outsourcing to enterprises in the financial service and government sectors. It is an IT partner to over 220 clients and has a talent pool of about 8000 professionals across the globe. Its internal and external workforce requirements are changing dynamically. Organizations employees spend a considerable amount of time in local travel on daily basis to client and partner locations. The workforce requested access on basic applications such as emails, calendars, time sheets etc on their smart phones and other mobile device, in order to effectively utilize their commute time for productive activities.

CHALLENGES

- Data should not be stored in personal device and should be accessed through virtualized environment
- Integration issues with various VM environments as most database and storage vendors do not support all virtual environments
- Virtualized environment can be quite vulnerable with the issues related to patch and upgrades leading to a single point of failure
- Compatibility issues with oracle & SQL databases even after following VMware guidelines
- Readymade data to support configurations and test labs was not available

BUSINESS BENEFITS

- Enhanced employee productivity as it enabled mobility/BYOD for the workforce
- Better utilization of employee travel time as they could utilize business applications on the move

SOLUTION

- Desktop virtualization was implemented for IT assets such as helpdesk machines only to enhance productivity and to save on infrastructure cost.
- Leveraged application virtualization for enabling mobility requirements of the workforce. However, application virtualization is confined only to non-critical applications with basic security hygiene such as firewalls, IPS, Antivirus etc in place
- Non critical applications like application performance monitoring were the first to be migrated on to a virtualized environment
- Care was taken by use of additional security consideration such as deploying software firewalls on VM machines so that they do not talk to each other

SECURITY CHALLENGES

- Mixing of traffic from virtual machines challenges segmentation & enforcement of policies
- Lack of visibility over virtualized assets
- Access to virtualized applications lead to complexity
- Securing data on end point devices is an important goal which was achieved by implementing capabilities such as data leak prevention, content filtering and end point encryption etc.

Case 3 – Large IT Solution Integerator leveraged Virtualization for Mobility

BACKGROUND

A leading IT services organizations operating in 14 countries with 18 offices in India, having a 2500+ strong work-force, and diverse customer base including fortune 500 companies. They cater to clients spread across a broad spectrum of industry verticals, and require executives and staff to travel to client locations for discussions and other interaction. The organization was looking to adopt virtualization in order to provide access to enterprise applications and setup collaboration tools for conferencing, IM and document editing for executives on the move. This will enable the organization to cope up with today's competitive environment and to deliver business services with greater agility and reliability.

CHALLENGES

- Data confidentiality is of prime importance from the organizations perspective
- Restriction on data which cannot be stored on an endpoint device
- Video traffic segregation as organization prefers videos conferences to physical meetings internally
- Should be able to enable monitoring, general administration and patch management

BUSINESS BENEFITS

- In their IT architectural approach the organization treated virtualization as an enabler to integrate contemporary trends such as mobility and bring your own device (BYOD) in the organization IT environment.

SOLUTIONS

- Segregation of IT environment for creating zones with different levels of security requirements, through the use of virtual switches
- In order to enable mobility, they evaluate the most used application which were emails and journals and segregated the same with audio/video traffic
- Isolation of virtualized operating systems through the use of firewalls and evaluated software firewalls for restricting P2P traffic
- Two sessions allowed from virtualization environment with a restriction of enabling parallel sessions only from office network

SECURITY CHALLENGES

- Network traffic from virtualized asset needs segregation
- Conflict between the operating systems residing on the same physical machine
- Access to virtualized asset
- Seamless access over devices

Case 4 – Large Insurance company looking for Data Center Virtualization

BACKGROUND

A 160 year old insurance company which caters to automotive, residential, and commercial insurance, focusing on the needs of rural areas. The company has more than 150 field offices scattered around large geographical spread which vary from single home offices to 100-person sites. As majority of work was carried from remote locations, in rural areas, the field agents had to travel large distances to branch offices to submit customer records and information. Further, the company needs to address issues related to setup of more than 150 field offices and ensure that the data collected at these centers is uploaded to its central servers.

CHALLENGES

- To secure data & applications residing in remote offices and focus on saving from storage, hardware & software and support cost
- Enable scalability and enhance network performance
- Space constrains & uncontrolled spend on power & cooling systems
- Productivity issues with respect to server downtime due to maintenance delays
- Agents unable to access systems from the field

BUSINESS BENEFITS

- The explicit benefits of virtualization which they have realized over the years are '300% gain in storage & scalability, critical applications & data residing in head offices assuring security,
- 50 % gain in support time, 200 % saving on hardware, software & support cost, 200% improvement in network performance, significant power savings etc

SOLUTION

- Consolidating of IT Infrastructure and data centre virtualization
- Virtual desktop integration was enabled across enterprise architecture
- Deployment of Virtual network switches deployment, which are contextually aware of virtual machines & at the same time provide virtual network services
- With the help of virtualized servers branch office applications enabled IT staff to virtualize multiple applications and services in one box at branch offices
- Sharing of elements such as I/O memory, virtual NICs & CPU for which a hypervisor environment was introduced

SECURITY CHALLENGES

- Local storage of data at remote location
- Varity applications of applications and platform, no uniform security posture
- Security of virtualized branch network
- Provisioning of access to applications & resources, complex business rules for it
- Enforcement of security policy in virtual environment
- Virtualized traffic flowing over the network

Case 5 - Global network & security equipment supplier looking for server farm virtualization

BACKGROUND

A global network & security equipment supplier has been a leader in the development of Internet Protocol (IP)-based networking technologies since the company's inception. A $46 billion company which has over 72,000 employees globally provided premier support, network & security equipment's to their clients and to drive internal workforce had implemented 11000 servers and 4000+ applications in their IT environment. The dynamic changes in the IT landscape brought a challenge of managing the gigantic IT architecture located physically across the globe.

CHALLENGES

- The business directions were clear and concise to save cost of hardware, limiting space & optimizing power & cooling requirement for IT assets
- The focus was on avoiding delays in provisioning servers, optimizing project cycles, develop service oriented data centre that fosters innovation & productivity etc.
- Segregating access requirements based on need to know services
- Challenges of application outages/failures because of migration

BUSINESS BENEFITS

- Reduction in number of servers from 11,000 to 1,500 resulting in a saving of about US $10 million
- 30 % saving of power due to removal and virtualization of unwarranted IT assets.
- Virtualized LANs deployment for application access resulting in saving considerable network bandwidth
- Reduction in provisioning of servers from 11 to 3 days

SOLUTION

- IT architecture overhaul by deploying virtualized servers in server farms which provided flexibility & redundancy
- Access maps were built for virtualized assets & virtual LANs were deployed for application access
- Traditional capabilities such as IDS and IPS were integrated with virtualized environment to monitor performance of security
- Design application maps to establish visibility on critical applications which were virtualized
- A data service oriented data center was also developed using virtualization, which resulted in improving client support services
- The hypervisor environment deployment enabled sharing of software & hardware resources from a single IT asset pool

SECURITY CHALLENGES

- Security of mission critical applications while ensuring consistency security measures across variety of applications
- Monitoring performance of virtualized security services
- Encryption of traffic and connections
- Issues with respect to Firewall, IDS, IPS, etc. which are sensitive to virtualization
- Mapping of servers with application/system for better security incidents & response

Case 6 - Leading Telecom Service Provider (TSP) utilizing the benefits of Virtualization

BACKGROUND

A TSP based out of Italy offers technological infrastructures and platforms in which voice and data are converted into advanced telecommunications services - as well as the latest ICT and Media solutions. These tools cater for the Group's as well as the country's growth. The current IT infrastructure comprised of 4000+ servers, with multiple network connections which resulted in different middleware & switching dependencies. As a leading TSP in the country, a high level of security was required that is adaptive in nature, provides firewalling & VPN intelligent threat defence to secure the infrastructure from emerging cyber threats.

CHALLENGES

- Consumer and business end demanding secure communication services
- Segregation of sensitive data to satisfy the compliance requirements of the customers respectively
- Providing robust & secure telecommunication architecture to end users, to overcome middleware and switching dependencies in its IT architecture
- Establish visibility on compliance requirements
- Building a single IT assets & resource pool, optimization of bandwidth etc.

BUSINESS BENEFITS

- The explicit advantages such as savings on hardware and software cost
- Cost savings resulting from virtualization, which allowed multiple applications & operating systems within a single resource pool.
- Enhancement of infrastructure and workforce productivity
- Savings on utilization of network bandwidth
- Security areas such as session resiliency & policy driven networks were introduced to deliver robust telecom services

SOLUTION

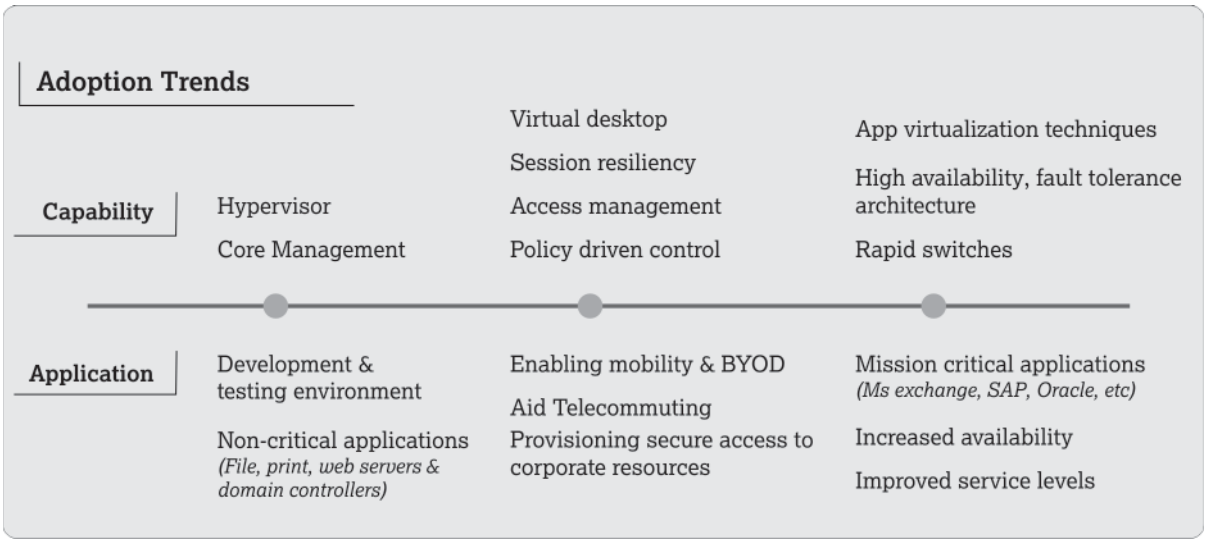
- The servers, networks and applications were virtualized within their IT architecture environment to achieve the end objective of running multiple applications & operating systems within a single resource pool
- Selection of varied server families for virtualization was carried with the help of an IT consolidation and rationalization framework
- Deployment of virtual LANs & switches & creation of zones were prioritized for network virtualization
- They deployed server virtualization in conjunction with intelligent network switching
- Selection of IT security services which will be virtualized was planned in parallel to server virtualization
- Virtual port channels were implemented for optimum utilization of uplink bandwidth
- The storage virtualization was completed with deployment of Virtual SANs (Storage Areas Networks)

SECURITY CHALLENGES

- Context based provisioning of access
- Delivering highly secure virtualized services
- Segregation of traffic from virtualized asset
- Requirement of advanced level of network level encryption
- Offering segregation of sensitive data to satisfy the compliance requirements
- Expectation of high level of security, adaptive, intelligent & self- healing

Adoption Trend

The initial trends of virtualization are more focused on deployment of hypervisor and the ability to manage the core for setting up a dynamic development and testing environment. The configuration of multiple operating and service instances suit dynamic requirements of development and testing as it has to deal with variety of configurations for development and testing. Organizations also look at non-critical applications, such as file, print and web servers for initial deployment of virtualization. Telecommuting, aiding mobility & BYOD and securing access to corporate information are generally taken up as a next step of implementation of virtualization. This is enabled by virtual desktop interfaces, techniques such as session resiliency, and fine grain access management. Virtualization also offers policy driven controls, which are widely used for managing devices, users and access.



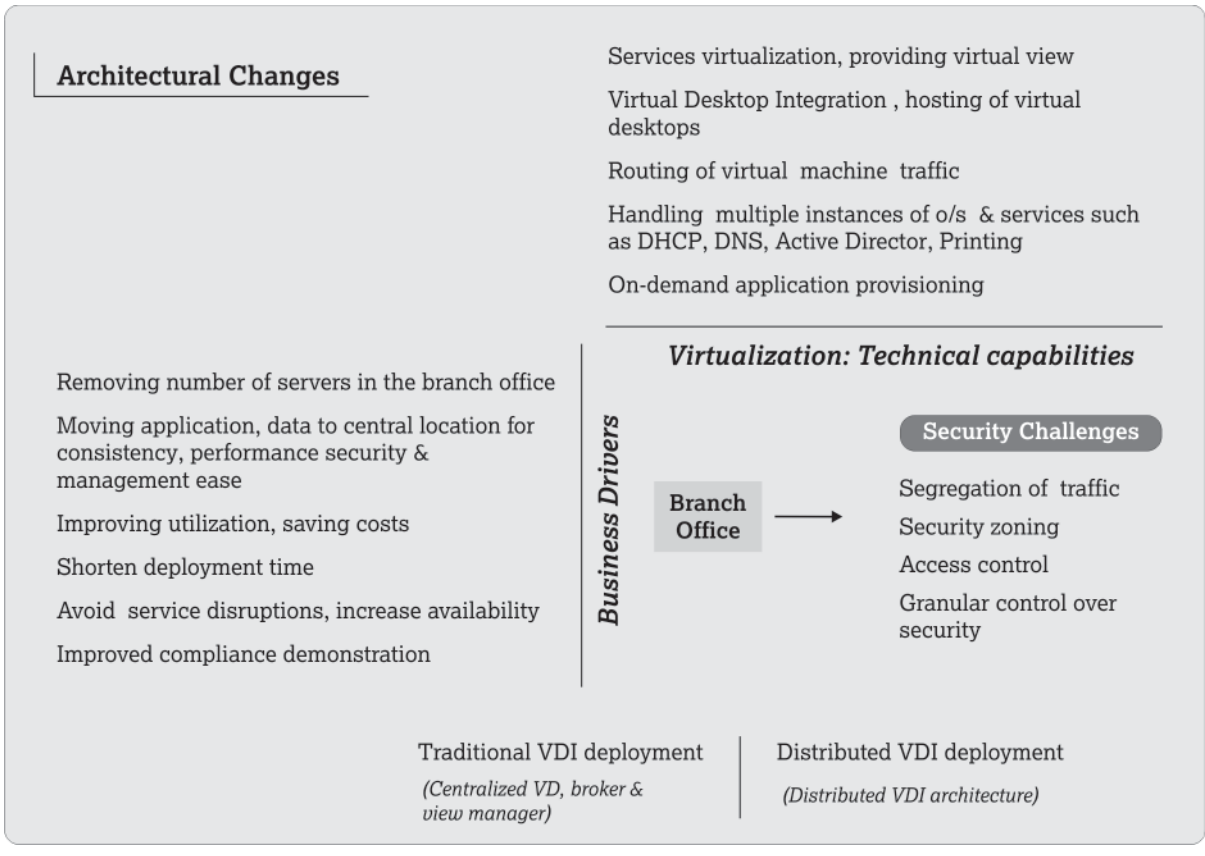
Over the years, virtualization has matured and is gradually becoming more relevant to mission critical applications. It is also been used as a means of enhancing availability. Organizations can rely on virtualization for improved service levels and in a way that it makes the business ready for cloud computing. Application virtualization techniques, high availability, fault tolerance and rapid virtual switches also contribute to the advanced use of virtualization.

- The trend is to start virtualization with non-critical applications and moving on to mission critical applications once reaping the success of previous implementations
- The implicit operational drivers to adopt virtualization are to enhance the availability of IT architecture and improve service levels. These demands from business are driving security architects to design and implement highly available and fault tolerant IT architectures. They are trying to achieve this by implementing capabilities such as session resiliency, policy driven networks, stringent access management rules etc.
- The trend is shifting towards the implementation of virtualization 'to enable the deployments of mobility, BYOD, telecommuting etc'.

Architectural Scenarios

Branch Office

The primary business drivers to adopt virtualization in a branch office are - reducing the number of servers in the branch offices, moving application and data to central location for achieving consistency, to achieve performance, improve utilization of IT assets, saving cost on IT infrastructure etc. Moreover, virtualization shortens deployment time of IT assets, enhances infrastructure resiliency, helps avoid service disruptions and also aids in better compliance demonstration.



When an organization decides to virtualize its IT assets in a branch office scenario, following technical capabilities play a pivotal role:

- The first stage is to virtualize services that provide virtual view of applications
- Next, a host environment is created to run various guest operating systems which will be accessible to the workforce of branch offices
- The third stage is to route the virtual network traffic via segregated zones to a centralized location for its effective monitoring and management

Ability of branch office to handle multiple instances of operating systems or the ability to provide on demand application provisioning to workforces may be used as few parameters to measure the success of implementing virtualization.

Organizations further need to deal with the challenge to choose between a traditional and distributed Virtualized Desktop Integration (VDI) environment, where the former advocates a centralized virtualized environment with a unified view of all IT assets, while the latter focuses on virtualization at different levels.

Technical capabilities that aid branch virtualization

(i) **Service virtualization:** Resource utilization in the virtual environment needs to be structured, scientific and consistent. Virtualized environment has to serve multiple requests of resources and each of the request demand specific set requirements, to be fulfilled. Unless the delivery resources and performance of services is streamlined it will be difficult to achieve the desired result. Virtualization of services, defines attributes such as performance norms, desired behaviours and publishes them to deliver desired resources and performance;

(ii) **Handling of multiple instances of services:** Network's capability to allow multiple instances of service helps consolidation of services such as DHCP server, DNS server, Active Directory Domain Services, and print services;

(iii) **Virtual views:** Virtualize the operating system, applications, and user data, which help in provisioning, managing and troubleshooting desktops;

(iv) **Virtual desktop integration and hosting of desktops:** Adds a layer of virtualization between server and desktop PCs. VDI hosts the desktop images in the data centres which not only enhances the speed of desktop deployment but adds to overall user experience;

(v) **Routing of virtual machine traffic:** A specific routing protocol for separating virtual traffic makes it possible to handle multiple connections originated and directed towards a physical asset;

(vi) **On-demand application provisioning:** Automated provisioning of applications, delivery of applications in the virtual environment and control of access makes it possible to provision on-demand application

Security challenges and architectural capabilities

(i) **Security of virtualized services:** Depending upon the customer, environment and trust domain, security measures may vary. This requires the capability of defining security mechanism, parameters and attributes while virtualizing services. This will ensure integration of security in the type of virtualized services and state what kind of protection mechanism it will use, what security parameters it should conform to and what attributes of security it should publish for integration with other solutions;

(ii) **Segregation of traffic:** As one virtual machine will initiate multiple connections and participate in the associated traffic flow, segregating traffic is critical for ensuring desired security behaviour of each connection. The routing and switching device should be able to recognize the traffic originating from and towards physical assets. It should perform routing and switching of the multiple connections originating from a source;

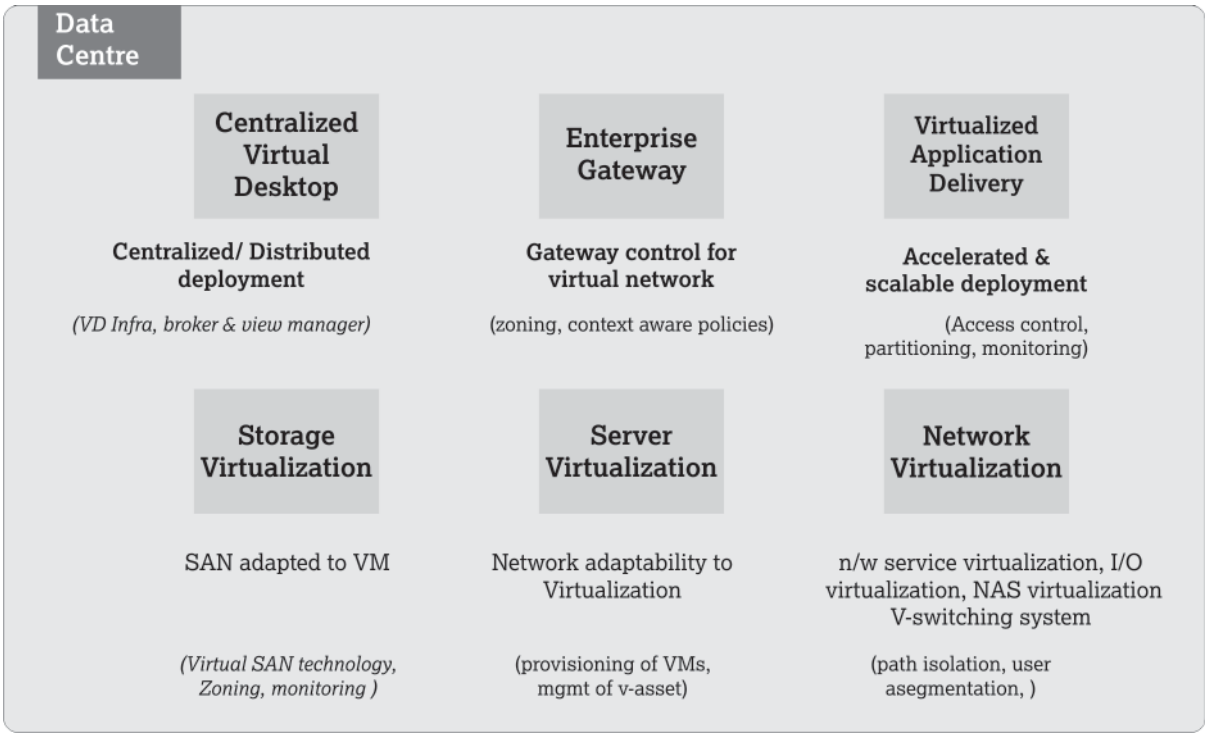
(iii) **Security zoning:** Each service instance created on a physical resource may have different security requirements. Zoning based on traditional attributes like IP address, ports and services may not be sufficient; hence, specific consideration for creation of security zones for virtualization must be given. The policy options of routing and switching for virtualized traffic would be more detailed, granular and specific;

(iv) **Access control:** Multiple resources, ability to create multiple service instances in each of the resources and innovations in providing access to users and devices make the access map significantly complex. Attributes, considerations, conditions and business rules of governing the accesses will add to that complexity;

(v) **Granular control over security:** Complexity introduced by virtualization is rising rapidly, while, on the other hand, there is requirement of a very granular approach which determines the security behaviour of the IT infrastructure and operation. Networking devices should have provisions for configuring and enforcing granular policies for effective delivery of security

Data Center

Data center virtualization embraces an array of virtualization activities aimed at creating a virtualized computing environment by unifying compute, storage, networking, virtualization, and management into a single platform. At a high level, these can be classified in six different areas as depicted in the figure.

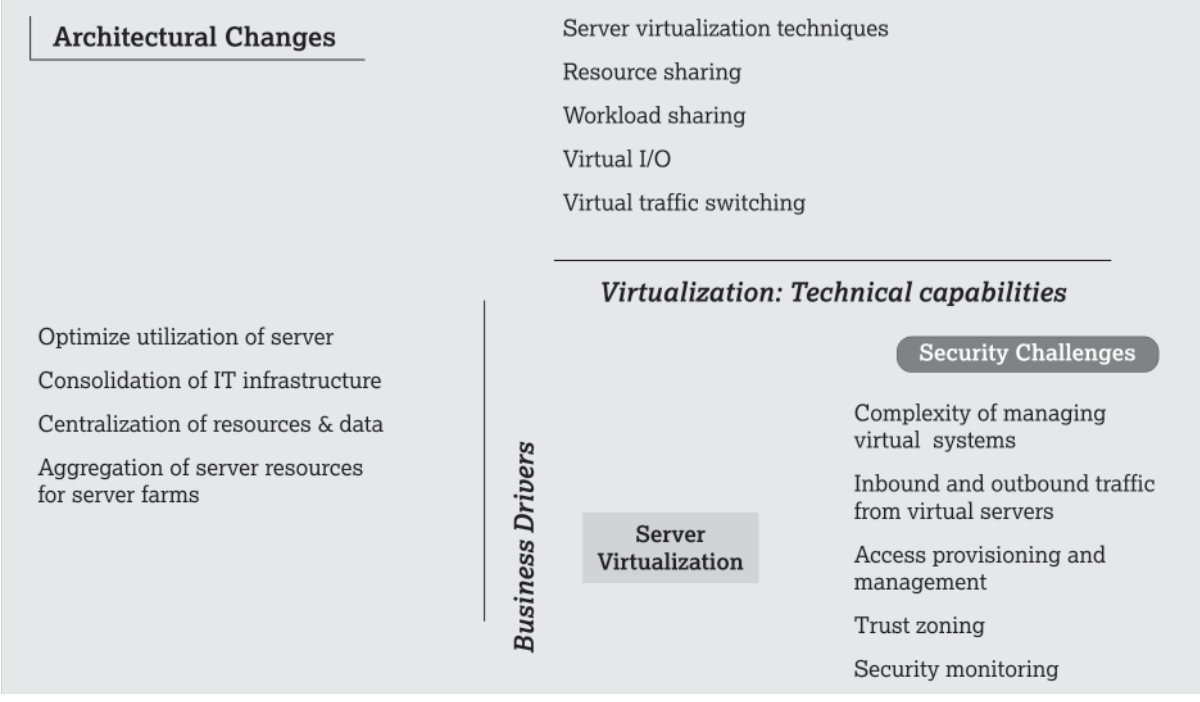


While Centralized Virtual Desktop is covered in the architectural scenario above, the other five architectural scenarios are explained below separately to give a comprehensive view of a Data Center Virtualization.

- **Server virtualization** is critical for driving consolidation of data center. Server farm employs multiple application and infrastructure servers
- Storage virtualization allows optimized utilization of storage capabilities
- **Virtualized application delivery** is enabled by stringent deployment of access controls, proper partitioning of storage for applications and its integration with security monitoring devices
- **Network virtualization** offers the required dynamism at the network to cater different aspects of virtualization. It also offers virtualization of its services, NAS & various switching systems. The requirement is to isolate network paths and segment users.
- **The network adaptability to virtualization** is reflected with proper provisioning of VMs and by establishing unified view of virtual assets on network level
- ***Enterprise gateways*** need specific capabilities to manage virtual traffic such as creation of virtual zones and context aware policies

Server Virtualization

Server virtualization masks the physical identity of servers from the users; it allows dividing one physical server into multiple isolated virtual environments. Techniques of virtualization incorporate both hardware and software. Server farm matures the virtualization technology by aggregating computing power of thousands of servers. Technical capabilities such as resource scheduling, workload balancing, virtual I/O, and virtual traffic switching enables data center architecture which is based on server virtualization. The network has to deal with increased density of identities, with the possibility that each identity may have multiple instances created on the servers. Resources utilized for facilitating establishment of multiple connections, traffic flow and availability should be considered for optimum utilization during the resource planning stage.



Security Challenges and Architectural Considerations

(i) **The complexity of managing virtual systems:** Virtualization introduces a fair level of complexity as utilization of servers is enhance significantly for serving multiple resource requirements. The Security complexity increases tremendously, with the increase in number of virtual systems.

(ii) **Managing inbound and outbound traffic from virtualized server:** The density of connections rises significantly due to virtualization. The network should have the capability to manage these connections, configure business and security rules for each type of connections and help enforce them;

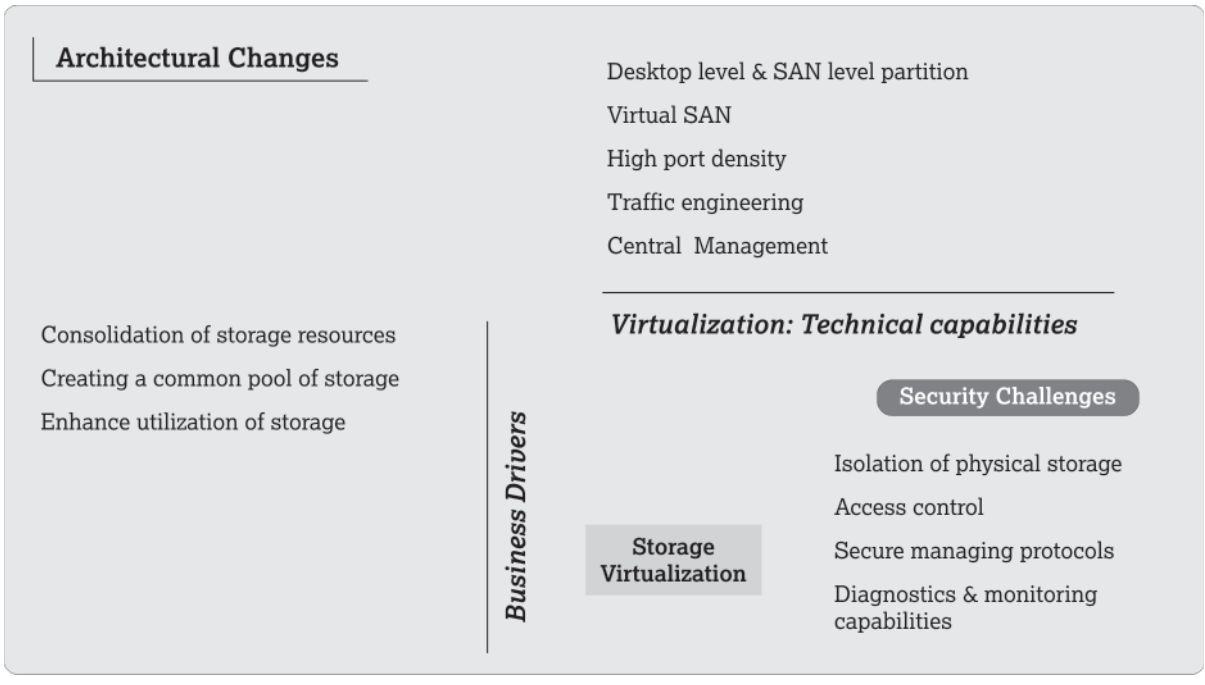
(iii) **Managing access:** As multiple instances allow access to resources, the access requests may increase multi-fold. In addition, users demand flexible and seamless access over new channels - from devices of their choice. This requires network to have the ability to configure and enforce access policies, at a granular level. In such scenarios, identity awareness of the network is a crucial attribute to ensure security;

(iv) **Trust zoning:** Multiple instances originating from virtual server may result in mixing of the trust zones, as conventional zoning policies are primarily based on IP, port and services. The potential of overlap of trust levels is much higher in a virtual environment. Hence, the network should able to understand and gain visibility over such complexity and provide policy options for creating trust zones in a virtual environment;

(v) **Security monitoring:** Network administrators struggle to gain visibility over or control inter-VM communication. Inter-VM traffic monitoring, policy based inspection and filtering are key challenges, which require consideration in the virtual environment as it may allow an attacker to compromise an application which may run in a VM. This may further be exploited to penetrate deeper into the infrastructure. Without packet inspection or filtering, an attacker may get access to other VMS

Storage Virtualization

Technology solutions such as SAN volume controller provide control and consolidation at SAN as well at disk level. However, the network brings the capability of large scale virtualization across both disks and SANs. This creates a single storage pool, which can be administered by a centralized console, paving ways for moving existing SANs to the storage pool. Higher port density, performance and traffic engineering are the key drivers for virtualizing SANs. Virtual SAN technology, offered by the network, partitions single physical SANs into multiple VSANs. Service orchestration and provisioning help abstraction of applications from the storage and streamline assigning storage to the applications. This boosts utilization of the storage by 50 to 100%.



Insulation of servers from storage, single point of management and consolidation of storage into one pool are the benefits of storage virtualization.

Security challenges and Architectural considerations

(i) **Isolation of physical storage:** Common pool will bring all data together from different applications. Data may be visible to other applications or users. Security isolation of physical storage should be the key consideration while designing security;

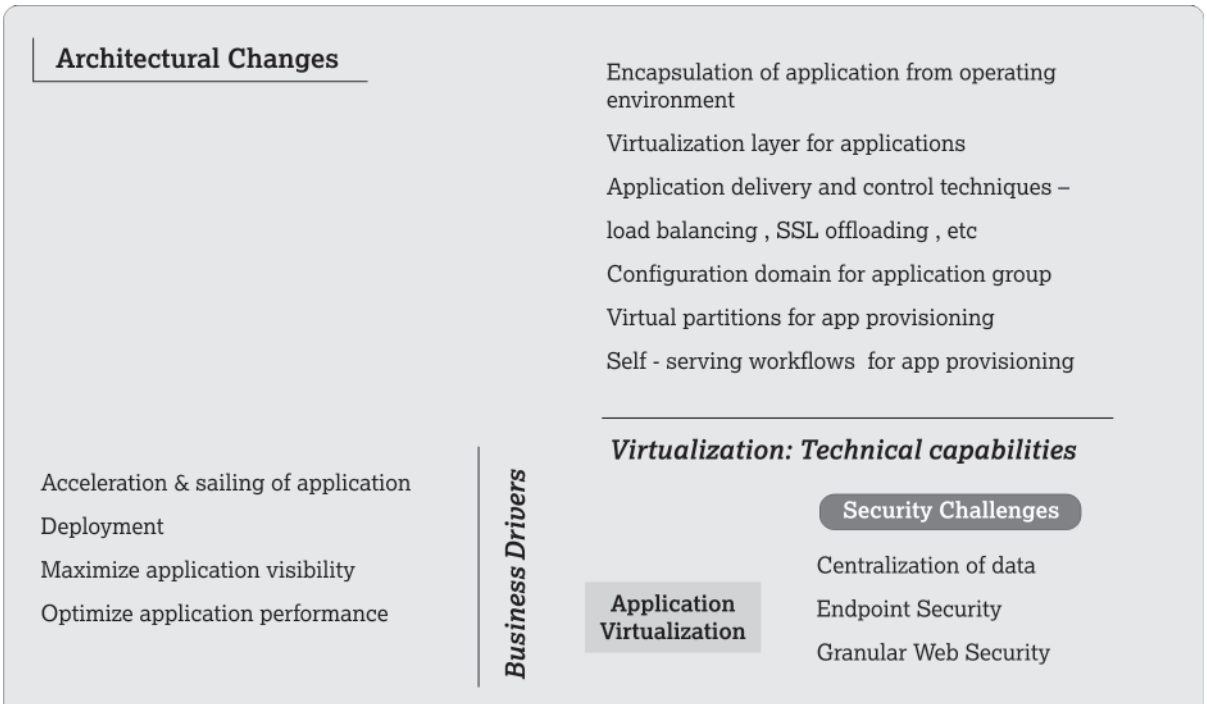
(ii) **Access control:** Data and data files stored in the common pool may not adhere to the access limitations, unless storage Virtualization provides granular role based access control;

(iii) **Secure management:** Protocols used to manage virtual SANS may not be secure. Protocols such as SSH, SFTP, SNMPv3 should be used for managing virtual SANs. Management of SAN should get specific consideration in the architectural arrangement;

(iv) **Diagnosis and monitoring:** Virtualization affects monitoring and diagnostic capabilities as existing arrangements may not be competent to withstand multiple connections from physical assets, increasing density of ports and user access and multiple traffic paths. Security architectural arrangements should provide a solution to this problem

Application Virtualization

As businesses are critically dependent on applications, enterprises and service providers need to accelerate and scale the deployment of applications. Businesses also require maximized application availability and optimized application performance. Application virtualization encapsulates application software from the underlying operating environment. The operating platform provides application virtualization capability through the virtualization layer through a runtime environment. From network operation point of view delivery of application is a critical aspect.



The network is evolving to perform the task of application delivery and control. Application delivery services such as advanced server load balancing, secure socket layer (SSL) offloading help achieve the same. Rolling out a new application or adding application support for another department is a simple task of adding a new virtual partition, as offered by the application delivery platform offered by the network. Application delivery services enable a network administrator to create a configuration domain for an application group. Assigning configuration privileges within a single isolated virtual device to the application group, the network administrator can stay out of the workflow. This creates a self-service model where an application group can independently test, upgrade and deploy applications faster.

Security challenges and Architectural considerations

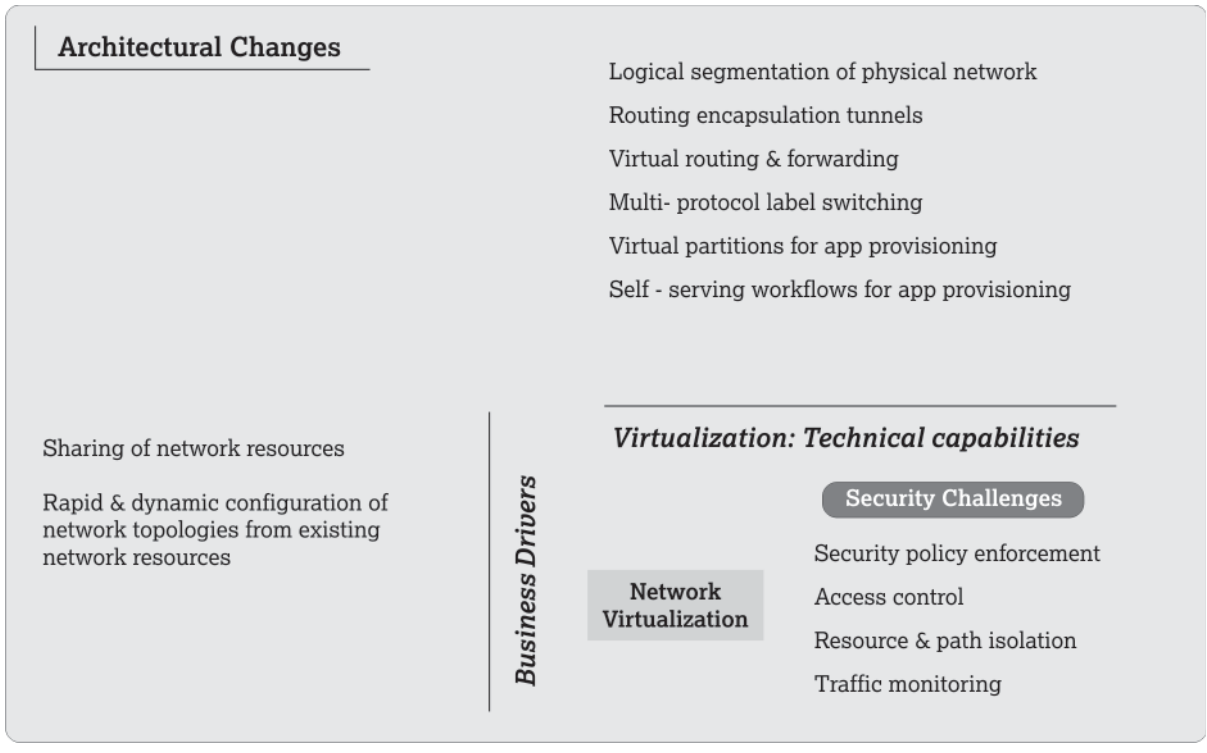
(i) **Isolation of applications, business users and customers:** Consolidation of applications may lead to confusion on delivering applications and provisioning access to users and customers. The application delivery and control isolate virtual instances of applications based on the access requirements

(ii) **Access Control:** An application can use its multiple instances for different purposes and user groups. An increasing number of devices and users seek access while the application is deployed over the virtual environment. As a result, access provisioning and management is getting complicated and requires greater control over applications and delivery capability of the network;

(iii) **Application security measures:** Increasing awareness over application usage, deep packet inspection, controls for provisioning and deployment, protection against protocol violation and defending against the malware are the challenges before the network for securing applications. Architectural arrangement should provide necessary considerations for this.

Network Virtualization

Network virtualization allows efficient use of network resources through logical segmentation of physical network. Multiple logical networks over a common infrastructure could be configured for different organizational units or departments on a single company wide network. This helps in significantly reducing associated cost. Techniques such as routing encapsulation tunnels, virtual routing & forwarding and multiprotocol label switching help network virtualization. Access control, path isolation and services edge are the three important aspects of network virtualization. Network virtualization helps creating network topologies for virtual environment and helps in rapid and dynamic reconfiguration of network topologies. Each logical network provides users with a custom set of protocols and services.



Security challenges and Architectural considerations

(i) **Security policy enforcement:** Factors such as different virtualized network entities, multiplicity of computing resources participating in a network instances and increasing density of identities make it difficult to drive the expected security behaviour from the network. The network should help identify policy decision points and the policy enforcement points for effective conformance and results;

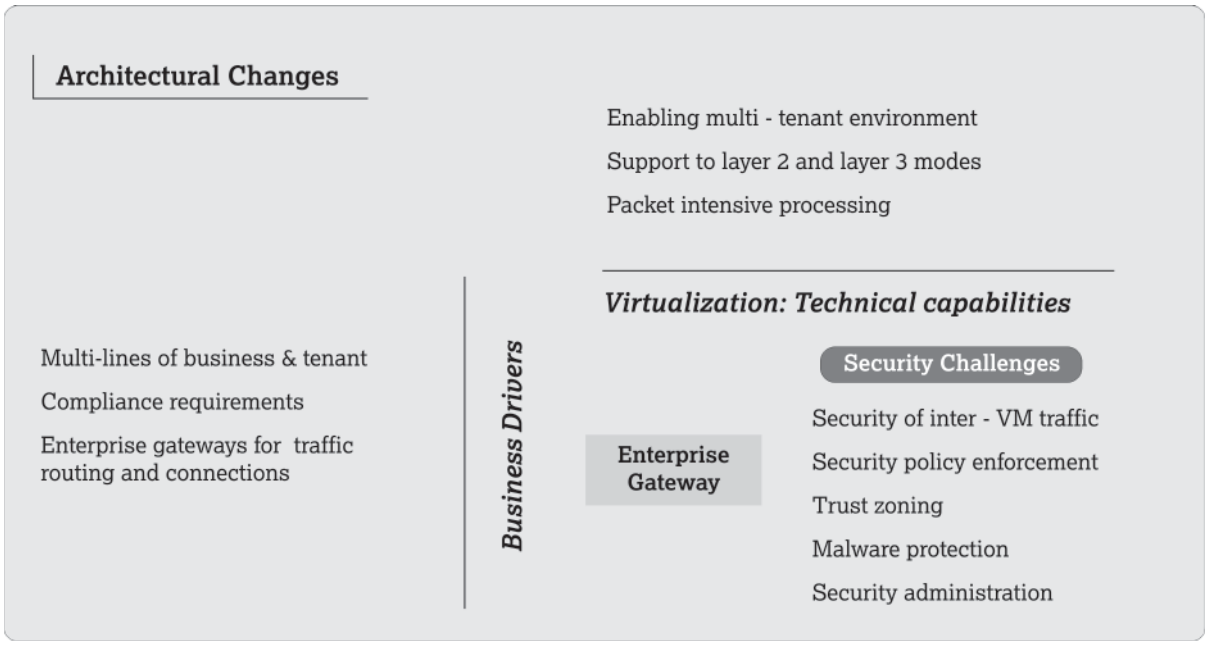
(ii) **Access control:** Enhanced density of entities, network paths and overlaying network zones makes the tasks of managing access daunting;

(iii) **Resource isolation:** Resource isolation is an important aspect. The underlying resources should be divided and isolated from hosted virtual networks;

(iv) **Traffic monitoring:** Traffic monitoring capabilities may be hampered because of network virtualization

Enterprise Gateway

Virtualization enables multiple operating systems to share a single physical server. This leads to collision between multiple lines of business, each requiring protected and trusted virtual computing environment for its data. As with the physical environment, virtual environments also needs specific arrangement at the gateway level for security.



Security requirements and Architectural considerations

(i) **Security for inter-VM traffic:** Security monitoring of communication between VMs is an important challenge. New deployment of VMs should be secured and live migration of VMs should be done without disruption. This requires special considerations at the gateway level;

(ii) **Security policy management:** The policies should be granular, zone-based, and context-aware along with providing multi-tenant access. They should maintain consistency of security across both physical and virtual environments. The task of policy management should be simplified and productive to enable comprehension of complexity while providing a high level understanding in drilling down to specific issues;

(iii) **Governance of virtual environment:** Provisioning of security policies and trust zones during virtual machine (VM) instantiation and policy portability during virtual machine (VM) movement is an important aspect of governance of virtual environment. Secondly, it should able to address each minute issue which may have ramification to the security posture of an organization. Policy based management of the network significantly improves the governance of virtual environment;

(iv) **Malware protection:** Ensuring malware protection for virtual machines is an important task. Virtualization adds significant opportunities for malware to propagate. Security hardening and patching of virtualized asset is still a challenge that can limit anti-malware capabilities

(v) **Security administration:** As virtualization multiplies traffic paths and connections, it increases density of identities and ports and increases workload of IT operations while demanding significant efforts for security. Security administration should be given specific attention and architectural arrangement should also be considered to facilitate administration

Security Considerations

1. **Insecure connections:** If the virtualized asset traffic is not segregated from physical IT asset traffic, then there lies a possibility of establishing 'n' number of insecure connections resulting in data leakage or infrastructure IT security incidents. It emerged in the use cases that organizations sooner or later were able to identify open ports in a virtualized environment that can be used to establish insecure connections.

2. **Un-patched virtual assets:** Un-patched virtual assets may lead to severe security vulnerabilities or incidents which may go unidentified. Patching of virtualized assets is a challenge. There are very few solution providers in the market which are providing patching of virtualized assets in an offline state as cited by majority of the organizations in their use case descriptions.

3. **Complicated access rules:** The shift to a virtualized environment brings with it a complex map of provisioning 'n' number of access for end users and resources. Organizations in the use cases have shared their experience in managing the challenge of complicated access rules.

4. **Conflicting operating environments:** The biggest advantage of a virtualized environment for an organization is that they can combine any set of operating environments to work together. However, there is a high possibility of conflict between the operating environments. Use cases show that organizations are facing issues in integrating one set of storage environment with another set of operating systems residing on a virtualized environment

5. **Insecure SDLC environments:** Application development and testing is best fit for virtualization. However, in design of security, development and testing environment is neglected.

6. **Granular security required:** Virtualization complicates the access, traffic and utilization of resources. The business rules governing them, hence, become more complex. Security conditions, scenarios and requirements have to deal with multiplicity of traffic, connections and instances. It has to handle and manage distinct virtual network segments, address security concerns of on demand provisioning and respond to security issues on real-time basis.

7. **Delayed incident response:** Conventional Incident Management approach is not always effective in a partially or completely virtualized environment. Complexity of virtualized environment, location or attribution of issues to virtualized assets and inadequate visualization may delay response to the incidences. There are instances due to which organizations are unable to respond to an incident in time with respect to a virtualized environment such as VMs managed by the same hypervisor instance might share information without having to send it out onto the physical network; VMs are either manually or automatically moved to react to changes in resources or workload; there is limited physical access to the intra-partition pathways from outside the host; direct host memory access capabilities can prevent quickly moving a complete partition from a compromised platform to a recovery host etc. If an administrator is equipped with better visibility on virtualized assets and granular access similar to DC physical access in traditional deployments. This can enable swift response to security incidents faced by organizations.

8. **Lack of visibility** - In the industry use cases it emerged that after the virtualization of any IT asset, organizations struggle to visualize the virtual assets to do effective monitoring and management

9. **Mixing of traffic** – Virtualized instances tend to scale the network traffic significantly. These instances create connections and direct traffic flows. The conventional switching, routing and security means may be confused with the mixing of traffic. The mixing of traffic results in ineffective monitoring of virtualized assets from both IT and IT security perspective. In one of the use cases it was noted that if separate zones are created with the help of virtual switches, an organization can be in a better position to overcome the challenge of traffic mixing due to a virtualized environment

10. **Insecure provisioning:** One of the important derivations out of the use cases is 'mobility is intertwined with virtualization'. Providing flexible and secured access to a virtualized environment via mobile devices is emerging out to be a major challenge. Some organizations believe that the same IT security controls will suffice for a virtualized environment as in case of physical IT assets i.e. they are unable to identify the unique security requirements of a virtualized environment.

11.Unauthorized access: Virtualization warrants specific attention for managing accesses. Virtual file systems, virtual instances, arrangements for resource pooling and management and challenges in enforcing controls may affect ability to govern accesses.
12.Traffic/ data exposures: In a virtualized IT environment, location is a challenge. Discovering and classifying sensitive information hosted on virtual machine are also important aspects. Virtualization traffic, if not managed properly, may expose data.
13.Inconsistent security: Shift to virtualization significantly changes the traffic patterns, adds multiple connections and creates multiple parallel instances on computing machines. It complicates and granulizes security. This will lead to inconsistency in performance of security.

Cloud Computing

Introduction

Businesses demands innovation, agility and flexibility of operations by reducing excessive processes, technology overhead, IT overheads and maintenance operations. Cloud computing, emerged as a key technology which enabled convenient, on-demand access to pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned. The foundation layer depends on the datacenter technologies and hardware, which make use of virtualization. Cloud offers benefits for all type of business requirements i.e. *(a) consolidation of hardware & software, servers, storage, networks and operating system through its Infrastructure as a service* ***(IaaS) model;*** *(b) availability of platform to businesses through sets of tools and services designed to offer development and deployment of applications through Platform as a service* ***(PaaS) model;*** *(c) ability to offer applications designed for consumers/end user delivered over the web through Software as a service* ***(SaaS) Model****.*

> Cloud computing is considered as an extension to virtualization, where the hardware used to deliver the virtualized instances is not owned by organization but by a third-party and the instances are accessed through a service model.

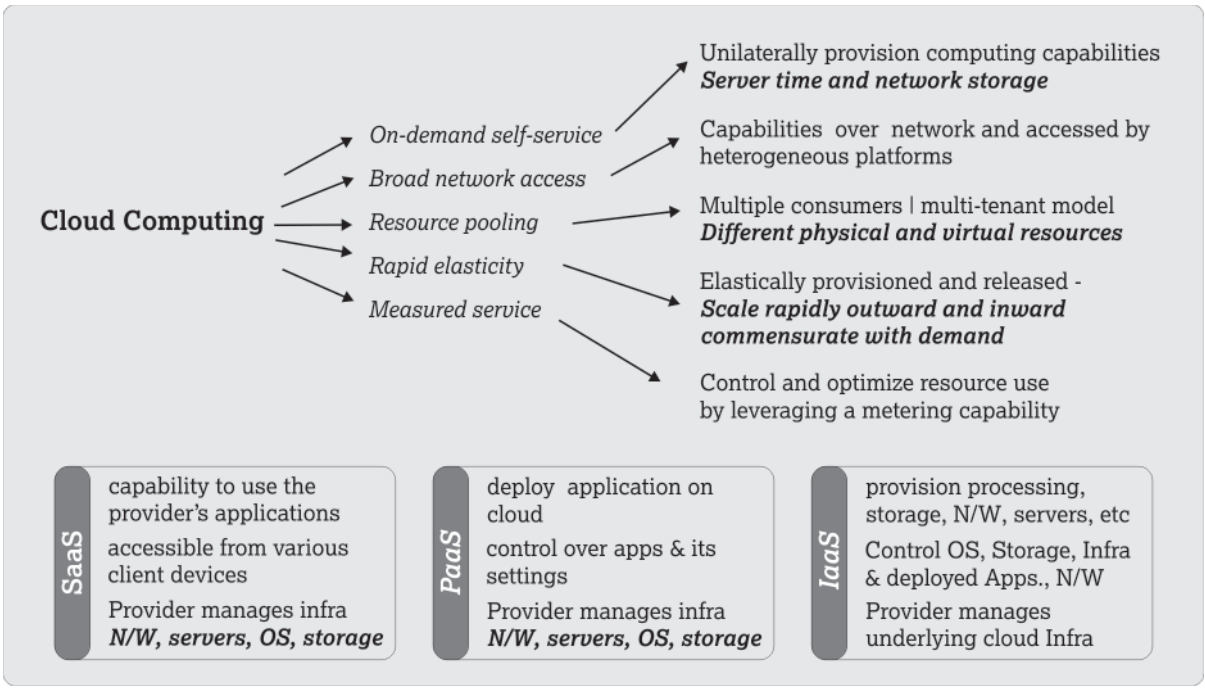
A recent report from Gartner states that by year 2015 half of all CIOs expect to operate majority of their applications and infrastructure via the cloud, and that by 2016, global spending on public cloud services will grow to more than $200 billion. Gartner also talks about how emerging countries are spending more than the mature countries for example enterprises in India allocate roughly 25% of their IT budget for cloud computing. One major fact is that emerging countries do not carry the burden of legacy systems, whereas organizations with traditionally large infrastructures generally suffer as their networks are not set up to take full advantage of the cloud, resulting in poor application performance or exposing themselves to security risks when migrating to the cloud.

The network has played a key role in the delivery and performance of cloud-based services as it is the only asset that touches every IT resource, making it one of the most useful components to overcome the challenges of managing and securing the cloud. Thus, it is essential that organizations which are transitioning to the cloud effectively architect their network with the appropriate routing, application performance, and security technologies.

What cloud offers

The network today has become pervasive with the combination of corporate networks, home networks, 3G/4G, WiFi, etc. allowing users the flexibility of all time access from any location using a multitude of devices.

The cloud has utilized the strength of the broad network access capabilities to provide on-demand self-service, which unilaterally provisions computing capabilities such as servers, network, OS and storage; allows resource pooling where multiple users through multiple tenant model can access different physical and virtual resources. Virtualization has been a key enabler for cloud services as it allows applications, compute, network resources, to reside anywhere, which may then be accessed through network. The network ties these resources together to ensure rapid elasticity and scalability through provisioning or releasing of resources based on demand. Cloud computing also has the capability to measure the services being offered through the usage of charge back or metering capability where it can control and optimize resources usage.



Key Considerations

The usage model of cloud computing mostly depends on the requirement of enterprises.

IaaS Model

The IaaS service model is used when organizations are looking to control and consolidate OS, storage, deployed application and networks. Traditionally, organizations have used peak load as a key criteria for sizing their infrastructure needs; however, most times the infrastructure remains under-utilized (except during peak loads). The IaaS model overcomes the challenges through demand based provisioning and reduces the capex, as rather than purchasing new IT Infrastructure, businesses rely on service providers to manage underlying cloud infrastructure and provision processing, storage, servers, applications and network based on the usage models and demands by business. The key characteristics of IaaS ensures:

- Resources are distributed as a service
- Standardization through homogeneous infrastructure delivered across pools of standard hardware, to eliminate unnecessary complexity - allows faster maintenance and reduces operational overheads
- Holistic unified platform optimized for the entire data center fabric, to support any and all workloads.
- Dynamic scaling through adaptive—self-programmable infrastructure that dynamically configures and reconfigures the environment according to changing application demands
- Automated management framework with built-in intelligence for complex operations
- Resilient architectures that compensates for unprecedented resiliency at minimum cost

Key considerations where IaaS makes sense

IaaS provides tremendous benefits where scalability and provisioning are the key requirements. These include:

- Organizations having unpredictable demands/workloads on the infrastructure; or
- Lack of capital available with new organizations or business units or expanding business operations through mergers/acquisitions; or
- Trial, testing and temporary infrastructure needs; or
- During major Hardware refreshment cycle; or
- Green IT Initiatives.

Larger organizations who have charted their journey towards consolidation of IT resources through virtualization also look towards IaaS models as the next best feasible option. However, where regulations restrict the offshoring/ outsourcing of IT infrastructure, IaaS may not be the best model, in-spite of private cloud deployment, which in such cases may not be cost effective.

PaaS Model

The PaaS service model brings tremendous benefits to software development world, as it allows faster creation and deployment of applications, removes the issues of dependability and scalability, without being worried over the expense of buying and maintaining the software and infrastructure underneath it. The PaaS model allows development of custom based applications by utilizing various code libraries, custom modules and development engines. It reduces the overheads, both from underlying infrastructure as well as utilization of core developers. The growth of platforms available on web stores and mobile stores recently showcases the benefits of PaaS models which have utilized this flexibility most effectively. The key characteristics of PaaS are:

- Provides underlying infrastructure for development, testing, deployment, hosting and maintenance of applications
- Provides GUI tools to create, modify, test and deploy different UI scenarios
- Supports multi-tenancy as concurrent users utilize the same development application
- Supports agile growth through availability of methodological, analysis & design Tools
- Allows faster application development cycle through various code libraries & development engines
- Provides capability for Workflow & Integration tools
- Handles integration with web servers and databases
- Provides scalability of deployed software including load balancing and failover

Key considerations where PaaS makes sense

PaaS provides tremendous benefits through its ability to automate processes using pre-defined components and building blocks and deploy them automatically to production environments. It is particularly useful for those looking to utilize the data source for developing/ testing process workflow or utility applications such as

- Development of customer facing applications which act more as an information source, rather being interactive and transactional
- Applications for better process workflows which can utilize the existing data source and provide correlation, analytics and intelligence; for example development of online forms or database applications.
- Setting up of testing infrastructure where multiple developers work simultaneously or/and interact with external parties regularly for development purposes
- Development of test-bed for applications to ensure scalability, integration, dependency without harming internal environment

- Applications which provide utility services based on available data sources through development of applications available on web/mobile platforms

It is important to note that PaaS is not a good option for development of core business application which may be transactional heavy and may require lot of customized modules and security features. However, PaaS model loses its effectiveness where the application need to be highly portable or make use of proprietary languages or have huge dependencies on customized hardware/software

SaaS Model

The SaaS service model lies on the top-most stack of cloud and provides usage of applications based on license - service on demand; subscription – pay as you go model; or even at no charge- advertisement based model. It brings tremendous benefits to organizations which offer standard/vanilla applications across the different target audience. The SaaS model has been adopted and matured in a B2C/G2C environment; however, increasingly the adoption has been growing in B2B market majorly by distributors. Recently, larger organizations are also offering SaaS services within their business units/partners through charge back mechanisms. The key characteristics of SaaS are that it:

- Provides access to commercial software through web allowing volume business for the enterprises, as software is delivered in one to many model
- Provides agility and time to market as, Application Programming Interfaces (APIs) allow for integration between different pieces of software
- Provides cost effectiveness over commoditized offerings/ or those with standard business flows - as dependency on development & maintenance by expertise (internal/external) drastically reduces
- Reduces operational overheads as users not required to handle software upgrades and patches
- Ensures resilient architectures which can handle demand based load and also provide DR capabilities.
- Provides availability of basic security and monitoring capabilities for commoditized application

Key considerations where SaaS makes sense

SaaS is increasingly used as a method of delivering cost effective services to customers and is used where the underlying technology is standard across businesses. Email is a classic example of SaaS which is being used by consumer, businesses and governments mostly through the SaaS offerings. Although a valuable tool SaaS model is largely used in scenarios where:

- The offering is undifferentiated or is a fundamental technology available in the market
- The offering is standardized requirement within the business or for a consumer service
- Applications which have significant interaction between users and businesses such as newsletters, campaign software, marketing tools, etc.
- The single application provides different modules and interactions providing flexibility to users to subscribe, upgrade and unsubscribe based on user demands and flexibility
- Application licensing model is not lucrative as compared to pay per use
- Application requires significant web/mobile access

Although SaaS is a valuable tool, it may not be appropriate either where the application is customized desired for a unique environment or where regulatory compliance does not permit hosting of data offshore or where an existing on-premise solutions full fill organization needs.

Deployment Models

The cloud model is composed of four deployment models: Private cloud, Hybrid Cloud, Public cloud and Community Cloud which varies generally based on where the physical servers are deployed and who manages them. The table below provides a high level picture of different deployment models.

	Private Clouds	Hybrid Clouds	Public Clouds	Community Clouds
Network Consideration	*User and provider are within the same trusted network boundary*	*Defined connection between the user's and provider's networks where user network may extend to provider cloud (vice-versa)*	*Standard networking infrastructure to all users*	*Similar to Public Cloud. However, structure varies based on objective & architecture of the organizations operating the cloud*
Features & Characteristics	**Security concerns -** Organizations are not comfortable putting their workloads into a shared computing environment.	**Balancing Business requirements –** Organization uses this model to outsource non critical workload to cloud while retaining the sensitive on-premise	**Economies of Scale -** Huge volume of capacity shared across different enterprises enabling price parity, scalability for highly variable workload	**Security & Data Sovereignty –** Common set of practices & security requirements to a level of a common data center under a single jurisdiction
	Data sovereignty concerns - Organizations which want control over their data- who owns it, who accesses it	**Manages security and Data Sovereignty -** Maintain control and ownership over sensitive data/applications	**Flexibility and Agility -** Flexibility to spin up demand, use it for the purpose and turn it off repeatedly.	**Scale –** larger than private cloud however provides scale of a public cloud. Reduces capex and increases efficiencies
Trend	*Most often a first step towards cloud*	*Most common model as it allows flexibility to use different clouds on requirement basis*	*Exciting option for organization who do not worry about Data Sovereignty*	*Rare as most often organization have varied practices*

Cloud Service & Deployment Models – What it entails for the network

The network plays a key role in the delivery and performance of cloud-based services as it is the only asset that touches every IT resource, making it one of the most useful components to overcome the challenges of managing and securing the cloud. The network has to:

- **Enable infrastructure enhancements** by supporting server consolidation, virtualized environment, automated infrastructure and supporting application mobility
- **Address access requirements** emerging from thin clients or organization mobility requirements which may extend to any device at any time from any place
- **Offer application analytics** by clustering requirements and enabling remote usage or community services
- **Support varied traffic patterns** through location independent endpoints while ensuring automated provisioning and orchestration

The cloud infrastructure, be it for the organization (in-case of a private cloud) or third party (in-case of a public cloud) starts from the data centres and networks have always been at the center of the data center for the simple reason that they are the common element which connect the disparate application, server, and storage silos together.

What it entails

Infrastructure enhancement

- Server consolidations
- Virtualized environments
- Automated infrastructures
- Application Mobility

Access Requirements

- Mobility
- Any device at any time from any place
- Thin clients

Applications

- Analytics
- Clustering
- Remote usage
- Community services

Network

- Varied Traffic patterns
- Location independent endpoints
- Automated provisioning
- Orchestration

Resilience and High Availability

- Simplification of Network topology allows scale & simplicity by limiting points of management
- Optimizing bandwidth by consolidating distribution switches
- Ability to route and reroute of data destined for a virtual machine
- Improved failovers by forwarding the traffic through available links

Convergence

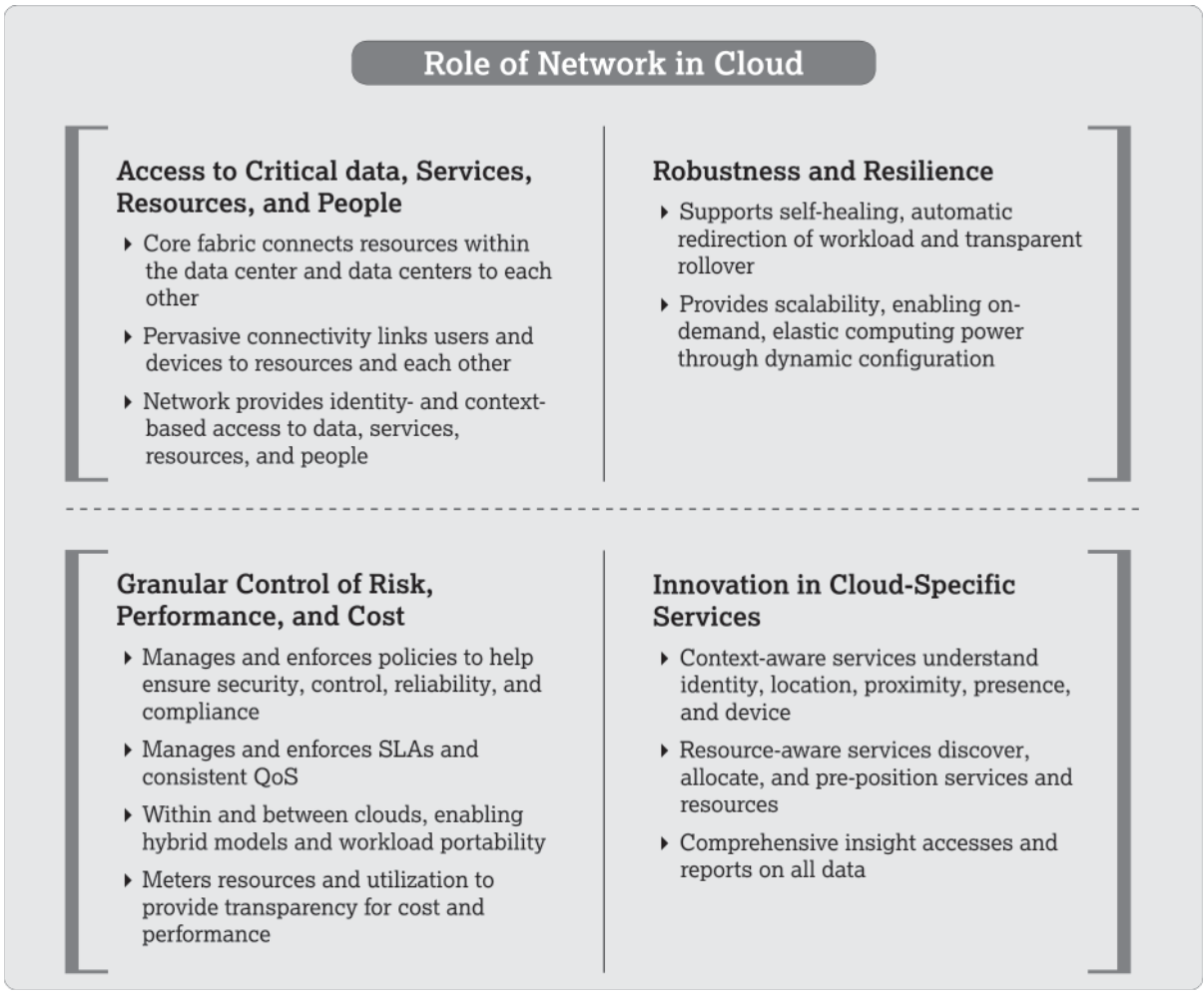
- Convergence of Ethernet switch for network and fabric for storage allowing network to be shared between different traffic types
- Common switching environment by enablement of RBAC
- Consolidated fabric which include storage

Physical and virtual Machine Management

- Ability of the fabric to provide visibility to VMs and associated policy to the N/W administrator
- Provides context-aware security, enforces policies as data is switched between virtual machines and established trust zones
- Segment networks by creating management domains enabling different security policies

Virtualization and cloud computing have changed the way the network needs to behave and interact with the broader systems in the data center. For example:

- As the number of virtual machines increases the network needs a different approach. Instead of networking servers, it needs to network virtual machines
- Unlike a physical workload, which is tied to a particular server, a virtual workload can exist anywhere on any server. This change requires the network to touch not just the edge of the server, but inside it all the way to the virtual machines
- Additionally, virtual machines have the potential to move within and between data centers. This movement can break the traditional model of how data center networks are built, so it is important to think about how modifications to the network can be implemented



Fabric based Infrastructure[1]

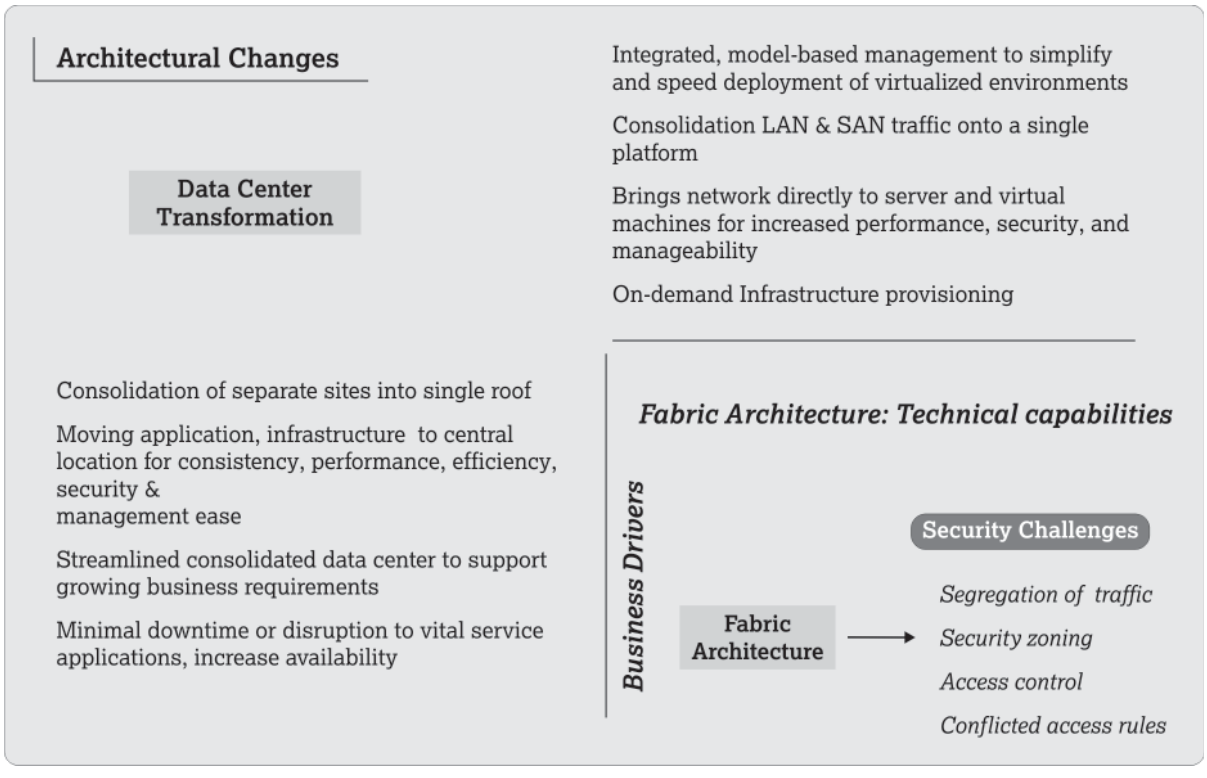
To meet these new requirements, a strong connection needs to exist between the server and the network. This is when a network and a server start becoming a fabric. The fabric based infrastructure, has the capability to reconfigure all system components - server, network, storage, and specialty engines - at the same time, the flexibility to provide resources within the fabric to workloads as needed, and the capability to manage systems holistically. A fabric provides transparency so that virtual machines are visible on both the server and the network, with capabilities to help ensure that security policies follow the virtual machine.

1 A set of compute, storage, memory and I/O components joined through a fabric interconnect and the software to configure and manage them." .Gartner

Architectural Scenarios

Data Center Transformation through Fabric Architecture

Every data center transformation begins at the physical resource domain, which includes active computing, storage, networking resources and supporting facilities, such as power and cooling equipment. Successful transformation of the data center infrastructure requires cooperation among server, network, and storage assets; these can then allow dynamic provisioning. The fabric architecture allows integrated, model-based management to *simplify and speed-up deployment of virtualized environments,* bringing the network directly to server and virtual machines for increased performance, security, and manageability. Further, the *integrated network services provide high-speed connectivity and high availability, increases application performance, and reduce security risks* in multitenant environments. Additionally, the fiber architecture allows storage networks to seamlessly extend into the Ethernet resulting in a single network with a flexibility to deploy both protocols between server and storage.



Case Study

BACKGROUND

Major public utility company wanted to consolidate its separate sites into a single roof. The organization wanted to relocate its data center IT assets from existing location to next-generation facility on shortened timetable. Data center had to support vital financial systems, asset management systems and most importantly, mission-critical components for 2000-person community of employees and partners. Apart from that the companies most vital applications are those associated with the SCADA system

CHALLENGES

- Requirement of a more streamlined consolidated data center to support growing business requirements
- The data center needed to be built with minimal downtime or disruption to vital service applications
- Quick migration requirement within 6 months
- Manage risk and avoid disruptions of mission-critical services and applications
- Increase performance, virtualization capacity, and energy efficiency of data center

BUSINESS BENEFITS

- Managed smooth data center migration of 260 servers and 60 applications
- Reducing energy consumption by up to 40%
- Improved response time and performance in customer-facing applications

SOLUTION

- The company thoroughly assessed end-to-end data center environment and identified several high-risk areas, including class of server, application logic/dependencies, and required network services, before divulging into the migration strategy
- The organization upgraded the networking infrastructure with a move to consolidate LAN and SAN traffic onto a single platform
- The networking infrastructure increased throughput to key applications, which has led to better response time, more accurate supplying, and greater performance overall by eliminating unnecessary infrastructure, increased floor space and reduced energy used for cooling
- The migration plan provided enhanced asset visibility for better investment and risk planning, while providing a simplified, stable data center for further optimization and innovation

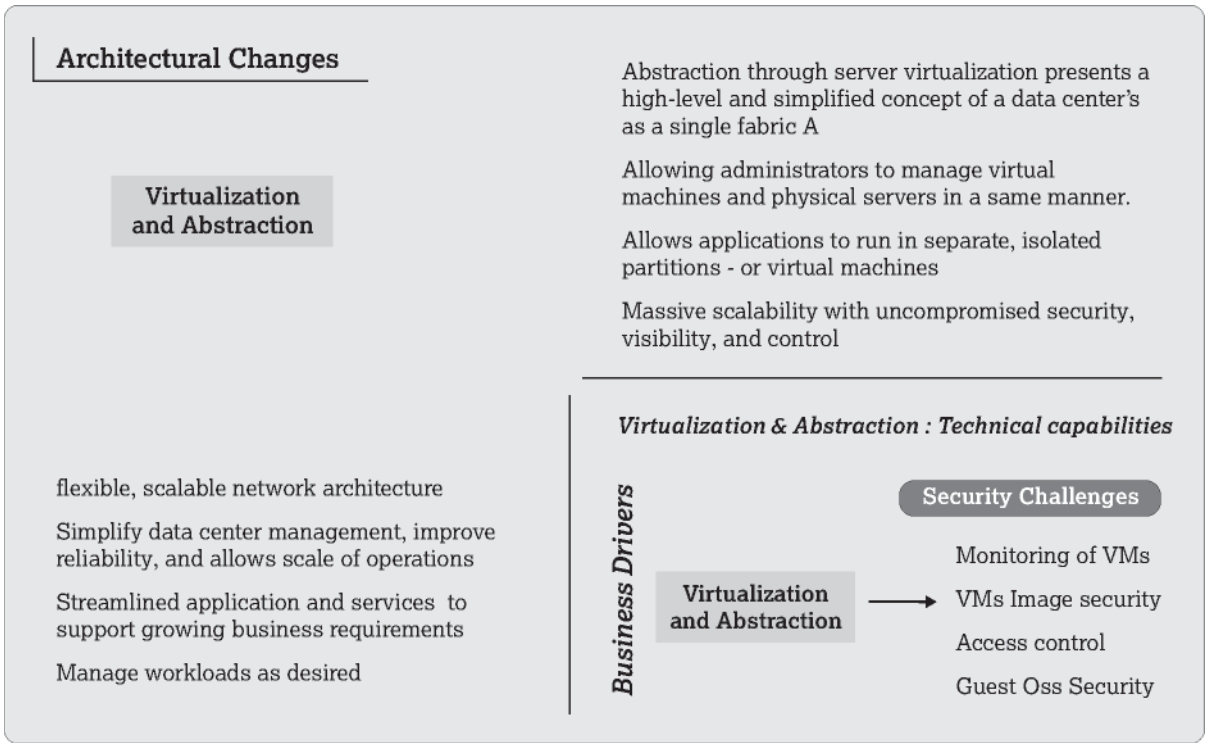
SECURITY CHALLENGES

- Segregation of network traffic from virtualized assets might lead to ineffective monitoring of virtualized IT assets resulting in insecure connections
- Complicated access rules for provision users as well as resources
- Conflicting operating environments because of integration of cross families

Virtualization and Abstraction enabling IaaS

Virtualization is the biggest trend in IT which offers separate computing functions from physical hardware and allows sharing of resources through which IT can seamlessly provide services. It fundamentally changes the way IT infrastructure is managed by focusing on server based approach to service based approach. The abstraction through server virtualization presents a high-level and simplified concept of a data center's hardware, network, infrastructure, and storage resources as a single fabric. It also allows IT managers to focus on the applications and services that they want to deploy. Additionally, virtualization must be built into network, allowing administrators to manage virtual machines and physical servers in a same manner. Workloads can be moved as desired through server virtualization as it allows applications to run in a separate, isolated partition—or virtual machines thus laying a ground work for a service oriented architecture and allows data center to move towards automation and orchestration. It provides massive scalability with uncompromised security, visibility, and control.

- Server virtualization propels storage and network virtualization, referred to as abstraction.
- Storage virtualization integrates physical storage from multiple network storage devices so that they appear as one device
- Network virtualization combines available network resources and treats all servers and services as a single pool of resources that can be redeployed in real time to meet user demand



Case Study

BACKGROUND

A large gaming service provider has six strategic business units within its organization structure. Primarily the organization has grown based on multiple mergers and acquisitions leading to heterogeneous IT environment which was bolted together with various networks managed by multitude of vendors. The company vision was to unite their various business units onto a single, highly scalable network which can be used to provide Infrastructure as a Service

CHALLENGES

- Supporting the need of six different business units with flexible, scalable network architecture
- Simplify data center management and improve reliability
- Ease integration of newly merged companies
- Providing a network infrastructure that meets the unique needs of each business while providing reliable and consistent experience.

BUSINESS BENEFITS

- Meet the primary goals of infrastructure reliability from regularity requirements; and to move capacity and performance from one business unit to another in real time.
- Increase agility and scalability; provide high visibility; and improve performance
- 80-fold increase in data center capacity and a 10-fold increase in core networking capacity
- Slashed audit time by up to 20%, lowered network maintenance costs by 30%

SOLUTION

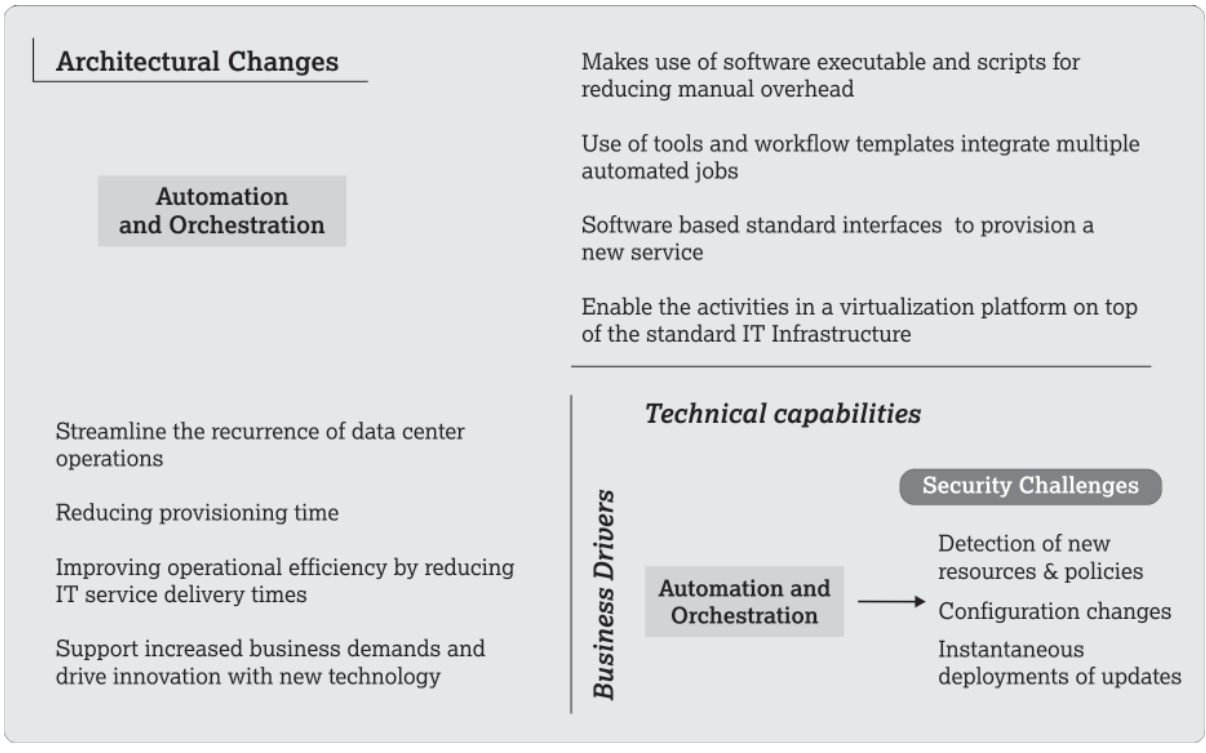
- Assessed the overall business drivers to have an architectural solution which balances security, technology, and operations
- Architectural design focused on enabling virtualization, data center interconnect, and abstraction through server virtualization.
- Key components for data center virtualization, including Virtual Device Contexts (VDC), which allows multiple instances of a device to operate on the same physical switch at the same time.
- Entirely programmable architecture to model-based management to simplify and accelerate deployment of enterprise applications & services.
- Organization used this architecture to move workloads as needed for example to support all the business virtualization needs in revenue generating and production environments.
- Streamlined management by consolidating data centers and segregating workloads through zoning of network

SECURITY CHALLENGES

- Incomplete monitoring of VMs due to abstraction, generates insufficient data to determine potential threat
- Security of VM images stored, transported, and managed in a virtualized data center or cloud
- Guest OSs can use physical peripherals available on the machine, and hence communication between guest OSs and the hypervisor must be secure
- Visibility is how much intrusion detection and prevention systems can see into a virtualized network

Automation and orchestration enabling IaaS

In order to streamline the recurrence of data center operations like applications, server OS deployment, automation software is deployed which radically reduces the provisioning time. Automation makes use of software executable and scripts and reduces manual overhead over recurring tasks such as configuring storage arrays, making network changes, continuous reviews and allocation of resources. On the other hand, orchestration through the use of tools and workflow templates integrate multiple automated jobs and actions through software based standard interfaces together to provision a new service. Together automation and orchestration enable the activities in a virtualization platform on top of the standard IT Infrastructure and promise effective benefits from the new IT model.



Case Study

BACKGROUND

A large IT service company which has seen tremendous growth and expansion in its infrastructure is facing challenges because of huge operational expenditure, and inefficiencies due to a lack of standards, processes, and tools. As the environment became complex because of innovative IT offerings with the use of social, video and mobility; it raised concern on huge IT budget and investments. The company vision was to concentrate on making its infrastructure more efficient and effective to support increased business demands. Further, it also wanted to drive innovation with new technology infrastructure which would require the ability to both securely and efficiently deploy these solutions.

CHALLENGES

- Rise in storage capacity by 300% because of Social and video traffic; bandwidth consumption by 400%; 150% rise in physical and virtual servers
- Deployment of IT budget & investment strategically
- Lowering TCO, while improving operational efficiency
- Support increased business demands and drive innovation with new technology

BUSINESS BENEFITS

- Reduced IT service delivery times from weeks down to less than an hour and five-fold decrease in support hours spent each quarter
- Reduction in TCO for infrastructure operations by more than 45% from both physical and virtual compute from the (IaaS) deployment.
- Accelerated provisioning of virtual environments through automation, reducing time from 20 hours to just a few minutes
- Streamline network testing by proactively reducing notifying potential issues freeing up the equivalent of employee job role of a week.
- Improved end-to-end service provisioning time for business system owners from several weeks to 7 minutes through self-service

SOLUTION

- Identified numerous operational capabilities that could be improved by leveraging people, processes, and technology expertise
- Conducted various design and compatibility testing that simulates its internal production environment prior to any major upgrades
- Network audit solutions performed periodic audits to report on end-of-life/end-of-sale products; this was coupled with analytical engines which provided real time analytics over a dashboard
- Deployed smart solutions which had the ability to discover all network devices, determine their movement and changes, assessed security vulnerabilities and performed remote diagnostics resulting in lower administrative costs and network risk
- Organization went ahead and conducted an application mapping exercise to determine interdependent assets to discover 5000 hosts and 1500 associated applications helping it to plan its resiliency and migration strategy
- Finally, the organization used the orchestration software to automate the provisioning of virtual environments, including network, storage, and compute resources

SECURITY CHALLENGES

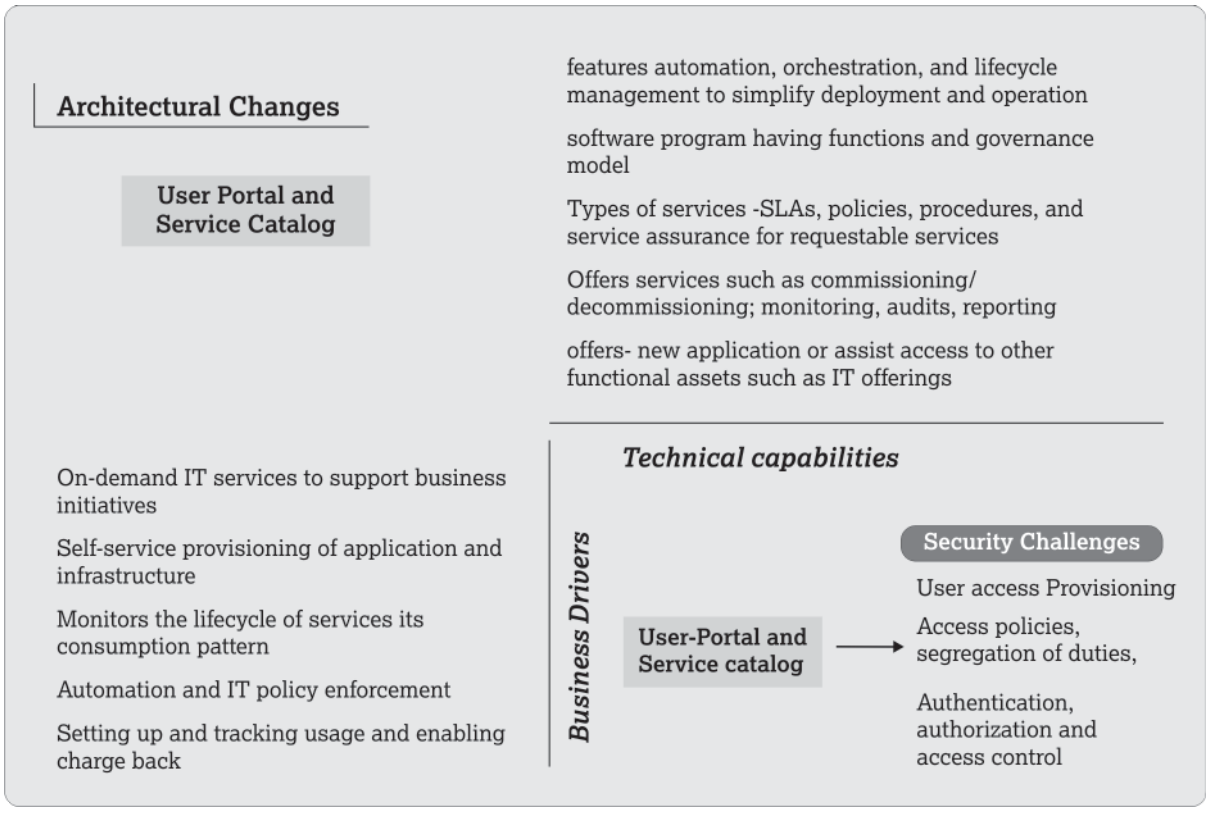
- Detection of new resources or policies; and analysis of how those changes affect security devices;
- Creation of new configuration updates that adapt to those changes; and
- Simultaneous, instant deployment of updates on a large scale

User portal and its service catalog empowering cloud | IaaS, PaaS, SaaS

The service catalog and user portal takes virtualization to a next level – Cloud; and empowers all variants of clouds i.e. IaaS, PaaS and SaaS. The portal and service catalog delivers on-demand IT services to support business initiatives The User portal is the engine which enables, self-service provisioning of application and infrastructure, monitor services and allows quicker decision making for decommissioning request and building resilient architectures. The service catalog as part of user portal is a software program having functions and governance model which monitors the lifecycle of services its consumption pattern and supports consistent ordering and delivery of processes through automation and IT policy enforcement. The service catalog helps in determining the scope of user portal like:

- Who can access the user portal - is it the IT organization alone?
- Sophistication – users only see those services they are authorized for, and connect services to the automated tasks associated with specific services
- What services are offered – commissioning/decommissioning; monitoring, audits, reporting
- What portal offers- new application or assist access to other functional assets such as IT offerings
- Types of services -SLAs, policies, procedures, and service assurance for requestable services

The service catalog features automation, orchestration, and lifecycle management to simplify deployment and operation of physical or bare-minimum, virtual and cloud infrastructure. The service catalog also allows setting up and tracking usage; enabling charge back and essentially allowing users to pay services that they use. Chargeback allows IT to justify the value of consumed services and understand the impact of consumption on costs for better Return on Investments.



Case Study

BACKGROUND

A global IT/ITeS giant offering infrastructure services to its own organization faced a challenge of multiple, conflicting, and disparate mechanisms for enabling end-users to order or request technology services for their operational needs. They spent an unwarranted amount of time responding to requests, researching requirements, validating information, and providing status updates. These requests range from complex, simple and even identical requests that have been submitted, and the hundreds of times previously. The end-user had to go through same lingering manual process of emailing to business manager for his approval taking weeks for a request to be initiated, another to be processed and delivered.

CHALLENGES

- Operations in 30 countries; 20,000 end-users receiving more than 1000 service request/day
- End-users frustrations, as request needs to be approved by managers before being processed
- Increase operational efficiency by replacing costly manual IT service request processes
- Create a scalable IT service request process to support growth globally

BUSINESS BENEFITS

- Initial roll out automated process for 100 individual requests due to architecture and flexibility of the service catalogue and the service request workflows
- More than 4000 requests were received and processed within the first two months
- Service requests, submission and approval times were reduced from 2 weeks to few days
- Calls to the service desk were down by 20%
- Better flexibility to enforce policy compliance
- Ability to identify nonstandard/ unauthorized requests and reject those immediately.

SOLUTION

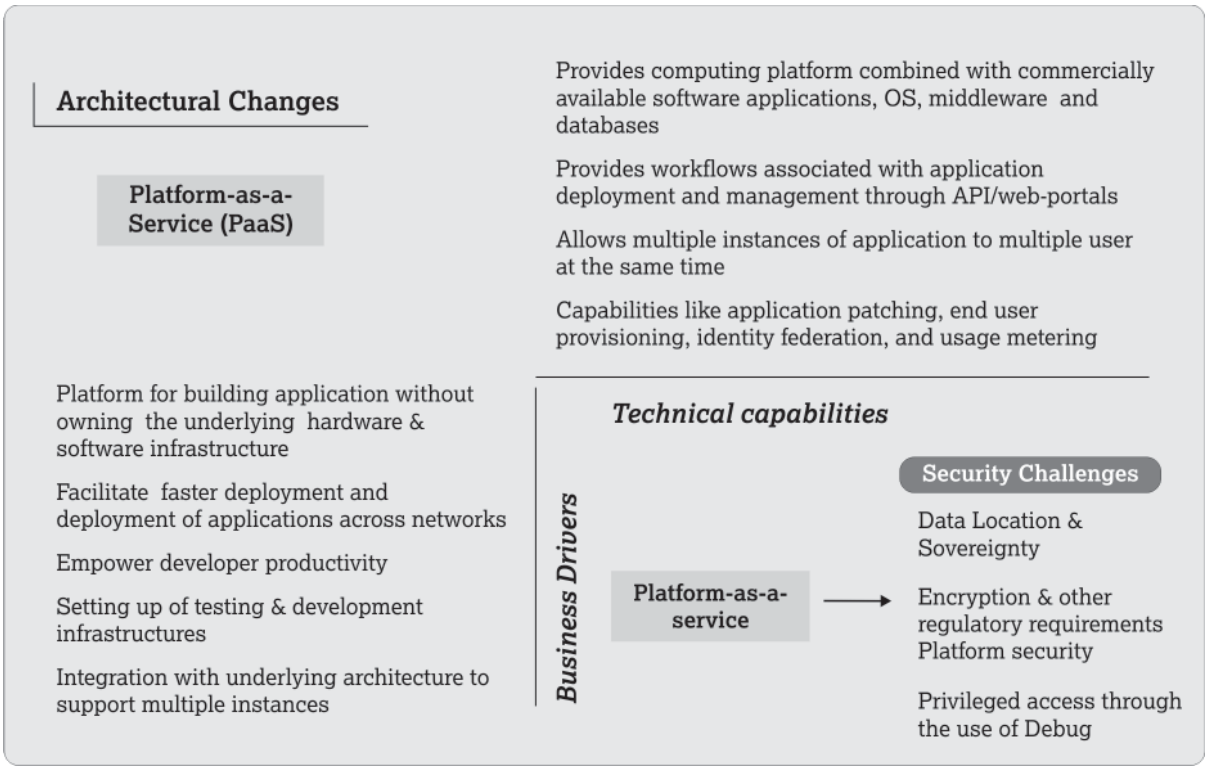
- Identified the need of integrating self-service portal, service catalogue, identity management and lifecycle management for service requests
- Focused on quick wins by automating most frequent and high volume requests, for higher visibility with line managers and users.
- The initial rollout prioritized the common service request and eliminated customized or complex request having impact on mission critical systems
- Defined the approval process, provisioning workflow and associated SLAs, which were then fed to automate tracking and reporting.
- Automated service request process not only streamlined ordering, but also allowed users access to right services which can be tracked online, thus reducing the calls to service desks
- Visibility not only allowed organization to enforce policy compliance but helped them in identifying bottlenecks with partners
- Automation of service requests provided scalability to support the company's aggressive growth plans and is being used to offer IaaS.

SECURITY CHALLENGES

- User provisioning, access policies, segregation of duties, user management
- Authentication, authorization and access control

Platform as a Service | PaaS

Platform as the name suggests provides computing platform combined with commercially available software applications and elements such as OS, middleware (codes, libraries) and databases on top of the infrastructure; enabling clients to develop, integrate or customized application for its enterprise. It exposes workflows associated with application deployment and management through API/web-portals, and abstracts number of server, OS, and networking components like load balancers into a single resource pool which are tenanted to multiple guest applications. It also has the possibility of sandboxing the application component within an OS instance and supports capabilities like application patching, end user provisioning, identity federation, and usage metering - all manageable through point and click web portals. It allows deployment of applications across the network without the need of buying or maintaining a hardware or software which are provisioned through a user portal.



Case Study

BACKGROUND

One of largest bank develops thousands of custom .Net and Java applications through support of thousands of developers and IT staff with thousands of servers posing challenges in developing, running and managing applications some of which may be core to the banking needs. These problems resulted in productivity loss, inefficient infrastructure spend and lack of agility. The bank realized that they needed an enterprise grade technology that could plug into their existing IT infrastructure and surface that infrastructure as a next generation internal PaaS cloud.

CHALLENGES

- Long lead times for application deployment due to infrastructure provisioning
- Lack of effective cost control with large up-front cost requirements and severe under-utilization of physical and virtual infrastructure
- Redundant effort between development teams that cause developers to treat application architecture patterns, security configuration, high availability and common services, such as application caching as one-off effort, rather than relying on standards

BUSINESS BENEFITS

- Application lead times and deployment reduced from weeks to fewer minutes/app
- Removed friction between developers and IT through single click application deployment
- Allocate resources to developers on an internal "Pay per use" chargeback model to keep costs in check and ensure utilization
- Empowered enhanced scale to operate at thousands of applications and yet provide for guaranteed availability
- Standardization of productivity & architecture patterns

SOLUTION

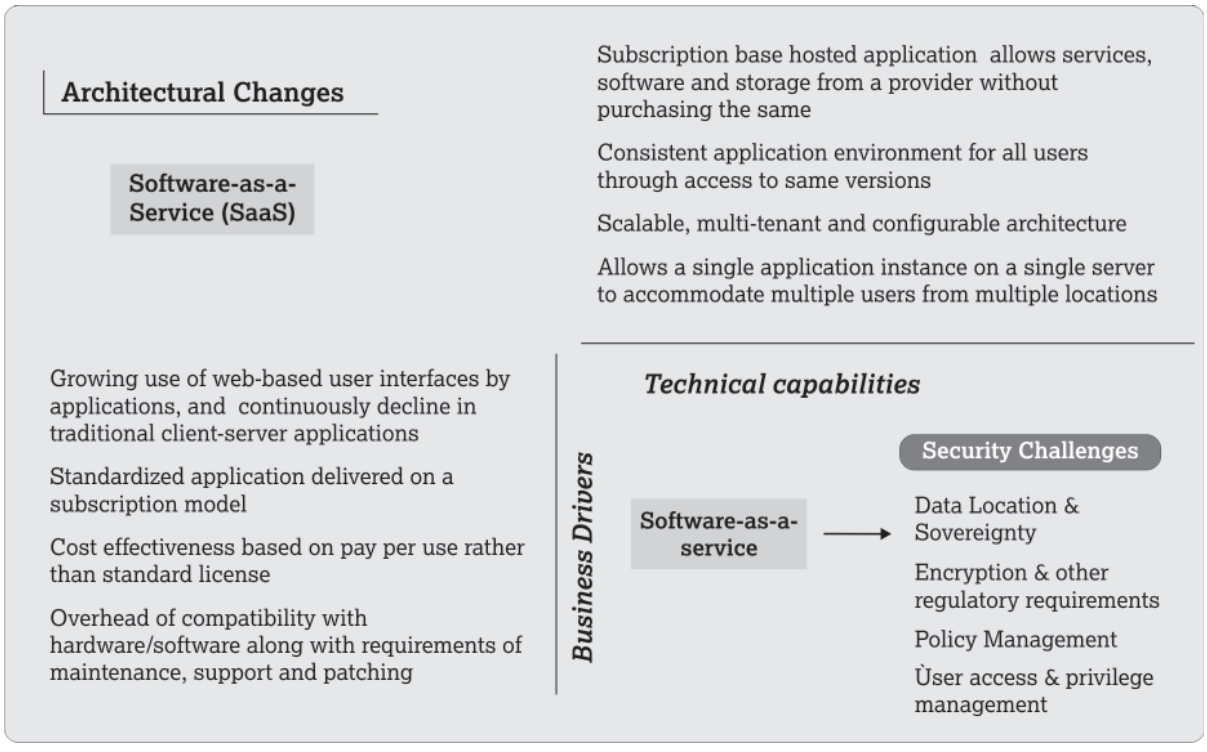
- Identified a centralized IT team as the platform owner which builds or license a PaaS layer that it deploys across cluster of servers
- Platform owner offers PaaS to internal development teams by provisioning them through individual accounts for building horizontal or Line of Business (LOB) applications
- Applications are written for internal PaaS and once ready are pushed to the PaaS or uploaded to a web portal by the development team
- Build basic configurations to the applications and publishes it, so as to dynamically deploy the application's components (web services, UIs, databases) to the underlying server cluster managed by the PaaS
- Servers are dynamically selected based on the PaaS deployment heuristics
- The PaaS monitors and manages the application at runtime, while the development team manages application lifecycle workflows through PaaS
- The platform owner never explicitly interacts with the management of an individual application, but interacts with the PaaS itself to ensure its availability, capacity, and general well-being

SECURITY CHALLENGES

- Security of the data – where it is stored, who accesses it, who controls the same
- Ability to encrypt the data whilst stored on a third-party platform and awareness of the regulatory issues that may be sensitive in different geographies.
- Security of the Infrastructure platform itself available for development of applications
- Software developers make use of Debug which grants access to data and memory locations. Equivalent to privilege access debug allows developers to step through code and modify values

Software as a Service | SaaS

SaaS is the subscription based hosted application that allows services, software and storage from a provider without purchasing the same for enterprise installation and deployment. The SaaS creates a consistent application environment for all users through access to same versions without being concerned about cross platform support. The unique characteristics of SaaS are its scalability, multi-tenant and configurable architecture which allows a single application instance on a single server to accommodate multiple users from multiple locations. While standard/non-critical application are the first which generally move on the SaaS cloud, organization must address their application environment while migrating or deploying business application for determining data location and proximity for latency requirements, profiling application for capacity and reliability, understanding their dependency with network, storage and servers, and assess the effects of DR.



Case Study

BACKGROUND

A legacy lending solution which was being offered in traditional on-premise model to financial institution and banks, faced challenges with respect to its analytical module. The module was expensive and thus adding new features for overall customization and offering of lending solution on premise, because of licensing model was no more cost effective. It also restricted the company to offer the solution to SME clients. The organization debated on SaaS or an on-premise model .Net model

CHALLENGES

- Change in licensing module of an analytical engine based on features sets, resulting in a costly model for clients
- Experience of selling software in traditional on-premise model creating bottleneck
- Restricted market positioning as the current model was not suitable for SME market

BUSINESS BENEFITS

- Phased approach to SaaS allowed cost effectiveness which was passed on to clients
- Gave visibility to customer on the various business and non-functional requirements of the application allowing customers to choose application module based on requirement and price instead of buying the complete suite

SOLUTION

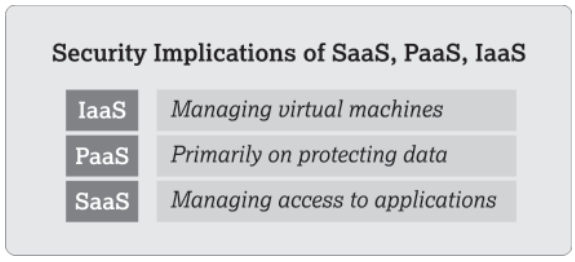
- Interviewed stakeholders to identify pain points within and in its collaborating platforms; to understand the non-functional requirements of the product; the emerging business requirements; and how competitors are able to offer the same
- Understood the current operational processes, including software development process and identified gaps to recommend a SaaS option
- New software to be built in and delivered on a web-based hosted model with multiple instances of the same software installed individually for each client evolving into multi-tenant solution
- Addressed areas from the business point of view by dividing software into functional model, framework and suite, thereby providing flexibility to choose and allowing it to market to all type of customers including large & SME clients
- Conducted operational changes required to sustain/ manage their SaaS product like SLA monitoring, product support and billing/invoicing

SECURITY CHALLENGES

- Security of the data – where it is stored, who access it, who controls the same
- Ability to encrypt the data whilst stored on a third-party application and awareness of the regulatory issues that may be sensitive in different geographies
- Policy management issues for establishing controls regarding users' access to applications
- User access and privilege management by creating mirrored users on cloud via single sign-on

Security Considerations

Cloud allows organizations to make utmost utilization of resources by provisioning infrastructure, platform and application on-demand. As users may not have direct control on the processes, infrastructure, platform or applications, they need to safeguard their data in the midst of un-trusted processes. Although, security consideration remains more or less the same as listed below, the focus changes based on different models as depicted in the figure.



1. Security challenges with respect to virtualization

Challenges of virtualization extends to the cloud for example mapping the virtual machine to physical machines securely, particularly in case of Infrastructure-as-a-service, however, there are other aspects of security which needs consideration by organizations

a. **Increasing workloads** brings issues either because number of workloads gets virtualized or when workloads of different trust levels are combined or as virtualized workloads become more mobile. Further security challenges increase because of conflicting operating environments due to integration of cross families
b. **Reduction in physical endpoints** (e.g. switches, servers, NICs) due to server and network virtualization, adds to the security challenges, as these physical endpoints were traditionally being used in defining, managing and protecting IT assets.
c. **Limited number of access points (NIC)** available to all VMs through virtualized servers presents a critical security vulnerability where compromising these access points opens the door to compromise the VMs, hypervisor or the vSwitch.
d. **Hyper-jacking** involves installing a rogue hypervisor that can take complete control of a server. Regular security measures are ineffective because the OS will not even be aware that the machine has been compromised.
e. **Incomplete monitoring** of VM due to abstraction generates insufficient data to determine potential threat. Further, there are issues with respect to visibility over how much intrusion detection and prevention systems can see into a virtualized network
f. **Communication between guest OSs and the hypervisor** needs to be secure as the guest OSs can use physical peripherals available on the machine.
g. **Compliance, update and patch management** - enforcing compliance with multiple VMs with differing environments is difficult, considering that update and patch management function might not have visibility of all the applications and OSs deployed. Further, challenges with respect to updating the VMs which are not laid.
    - Configuration management and patching of offline image
    - Restricting and auditing administrative access and management tool access
    - Lack of visibility and controls on internal VM-to-VM communications
    - Risks from combining workloads of different trust levels on the same physical machine
    - A compromise of the virtualization layer could result in the compromise of all hosted workloads

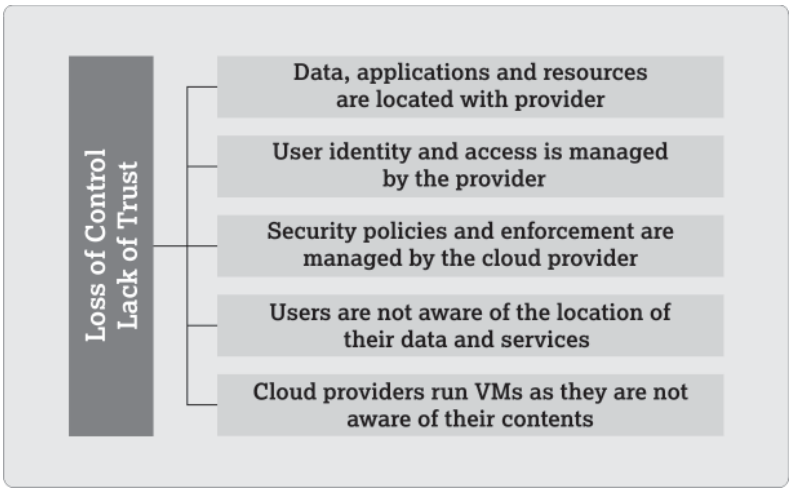
2. Multi-Tenancy

Although, multi-tenancy in a private cloud scenario is not applicable, however, it is still vital to differentiate that virtual private cloud is not a distinct system; the difference lies in strong isolation. More than half of enterprises today allow server workloads of diverse trust levels to share the same physical hardware, apart from being explicitly forbidden by a regulation

a. **Increase in Information leakage scenarios** and increase in the attack surface as multiple users within the cloud share similar infrastructure, applications and the physical hardware to run their VMs. This sharing can also enable risk of VM-to-VM or VM-to hypervisor compromise
b. **Workload Complexity** resulting due to server aggregation, which duplicates the amount of workload and network traffic that runs inside the cloud physical servers
c. **Segregation** is another important consideration to ensure that multiple tenants sharing the infrastructure are segregated and restricted to access the client data. Deployment of compensating controls such as blocking network packet capture for restricting access to the data, preventing security breaches and complying with regulators under audit needs to be evaluated

3. Lack of Control

Many security problems in the cloud arrive due to lack of control (as can be seen in the figure) or lack of trust mechanisms. In such an environment consumer relies on ***provider to ensure data sovereignty, its security and privacy, ensuring resource availability and allowing monitoring and auditability.*** The things gets complex as on one hand users might not be aware on the location of the data, while on other hand providers may not be aware of the content of the data although they run VMs, this leads to challenges with respect to lack of trust. Establishing trust mechanisms either through enforcing policy or regulation, technology measures, contractual obligations, building SLAs and enforcing monitoring and auditability capability thus becomes utmost important for the provider.



4. Privileged user access

Cloud brings inherent level of risk as the sensitive data starts processing outside the enterprise which bypasses the "physical, logical and personnel controls" resulting in complex access rules for provision users as well as resources

a. **Security implication because of privilege access** specifically in case of a PaaS platform where Infrastructure platform is made available for development of applications for example Software developers may make use of 'debug' which grants access to data and memory locations. Debug further allows developers to step through code and modify values
b. **Managing access to application** specifically in case of a SaaS platform which requires creating multiple

accounts/passwords for accessing different applications both on-premise and on cloud. Security risks and potential IT help desk costs associated with multiple passwords accessing applications or creating mirrored users or deploying single-sign-on solutions should be evaluated

c. **Logging and monitoring** to understand the security posture of data with respect to where it is stored, who accesses it, who controls the same? What is being accessed by privileged administrators? Security consideration with respect to visibility over user provisioning, access policies, segregation of duties, user management and the control measures deployed for authentication, authorization and access control
d. **Security consideration with respect to third party access** need to ascertain as the access to systems and application in the cloud is exposed to them. Mechanisms such as background checks during the hiring process and restriction on access to certain sensitive data or monitoring mechanisms should be evaluated

5. Network security

The cloud architecture is very vigorous as workloads change over time, because of creating and removing VMs. Further, the mobile nature of VMs allows it to migrate from one server to another leading to a non-predefined network topology. Thus network security becomes one of the most important considerations for the cloud.

a. **Segregation** is an important security consideration due to very nature of the cloud, and organization should evaluate the same either through virtual network isolation or through demanding individual virtual LANs (VLANs), or virtual routers and virtual switches. However because of segregation of network traffic from virtualized assets, ther might be challenges with respect to ineffective monitoring of virtualized IT assets resulting in insecure connections.
b. **Protection of network traffic** is also important consideration from network sniffing, spoofing and local denial-of-service attacks. Network security measures such as defense in depth through capability of automatic mitigation of threats such as distributed denial-of-service (DDoS) attacks, or automatically halting activity against its infrastructure that it deems malicious - such as automatic blocking of port scanning attempts, whether originating externally or internally, also are important security considerations
c. **End point security** with a basic firewall service included, allowing the customer to filter specific ports and Internet Protocol (IP) address ranges, with the default configuration offering minimal access is the most common security feature in the cloud. However sensitive systems demands more complex intrusion detection system (IDS) and intrusion prevention system (IPS) which is generally available at an extra fee.
d. **Host based Approaches** for network security is an important consideration in the cloud as most of the IaaS contracts will explicitly prohibit the use of network-based vulnerability scanning tools, as it may impact the service quality of other customers. Hence, evaluation of other options such as host-based approaches like mandating antivirus for all customers or offering host-based IDS and IPS, configuration auditing and a Web application firewall may be the only ones viable.

6. Data Center Security

Cloud has been an extension of Data Center operations from an outsourced model (in case of cloud) and a services model (in case of a public cloud). However, for each of deployment be it IaaS, PaaS or SaaS, requires a rigorous administrative and physical security controls for their data centers.

a. **Anonymous, hardened structures, with surveillance** through measures such as security guards, security cameras, and layered access with multiple authentication mechanisms (including biometrics) and access logging
b. **Software-based appliances,** typically in the form of VM, for additional security controls or **deployment of security-related hardware** in front of the customer's IaaS environment, even if that environment is shared
c. **Security within the virtualization layer** itself for stronger separation of VMs on the same physical host

d. **Security in their storage offerings,** such as data encryption
e. **Managed Security Services** such as security information and event management (SIEM), or more basic log monitoring and management
f. **Security of VM images stored, transported, and managed** in a virtualized data center or cloud

7. Regulatory and compliance

Regulatory and compliance reporting act as an important market differentiator which can be integrated into and accessible from an enterprise's own security information and risk management consoles. While many cloud providers can generate compliance reports as part of their service, consolidating provisioning reports, scanning reports, logs and the linking into a single set of documents readily accessed via a customer portal can be a key success factor in cloud governance. Some of the important consideration include the:

a. **Detection of new resources or policies;** and analysis of how those changes affect security devices;
b. **Creation of new configuration updates** that adapt to those changes; and simultaneous, instant deployment of updates on a large scale.
c. **Ability to encrypt the data** whilst stored on a third-party platform
d. **Awareness of the regulatory issues** that may be sensitive in different geographies

8. Cloud Threat Model

The success of organization security depends on it being vigilant to changing threat patterns and its approach and proactive measures in identification of zero day threat which depends on understanding the system behaviour, its interaction points and interdependencies. Monitoring protected system behaviour rather than the threat behaviour are a potentially effective approaches that enable detecting the zero-day threats with a low rate of false positives and negatives, however is pretty challenging in a cloud environment. A good picture of cloud behaviour can be developed by monitoring different components and activities inside the cloud and is an aspect which organization should evaluate with the cloud provider

Success Factors

Apart from above security considerations, evaluation of following aspects both from user and vendor assurance perspective is an important success factor

User Consideration

- Data or functionality - Is it business critical or too sensitive for the cloud?
- Data backup copy of data to ensure redundancy and restoration – where it gets stored?
- Adequacy of network connection between organization and vendor - does it provide assurance that the cloud does not weaken network security measures?
- Regulatory or legislative obligations to protect & manage data?
- Do I have the monitoring mechanism of how the data is managed, accessed on the cloud?

Vendor Assurance

- What flexibility is provided by vendor to increase/decrease computing resource based on requirements or move any data or application from one premise to another?
- What assurance is provided by the cloud on policies, technical controls, access management measures, procurement measures, logging, auditing and monitoring?
- How does it provision for strong encryption for securing sensitive data?
- What assurance is provided by vendor that it does not have access to customer data and it not only segregate different customer data but also ensures that it does not get replicated with a second vendor?
- What assurance is provided by the vendor on their security incident response plan and assist organization on security investigation and legal discovery which enabling forensics?

Mobility/BYOD

Introduction

The need for BYOD and mobility arises with the demand from users and business groups to compute and communicate using devices of their choice, in and out of the physical boundary of the office. Enterprise mobility facilitates use of mobile devices and technologies, enabling its workforce to remain connected to corporate resources, partners, clients, suppliers etc. irrespective of their physical location or access network. In recent times, mobile devices have evolved from providing access to enterprise email and data on the move, to introducing applications and services that have transformed the business landscape.

Enabling mobility requires a combination of mobile devices, wireless connectivity, applications and portals to facilitate information exchange. Further, solutions for securing this information exchange by controlling access to corporate resources and authenticating devices, or securing the device or applications are required. With mobility, the enterprise data and information will be increasingly accessed from outside its physical boundary. This adds to the challenges of IT function as they now need to secure transactions and interaction on the mobility platform. The devices used may either be purchased by the end user themselves, or be corporate owned or partly financed by the organization. However, in all cases safeguards have to be built into the mobility architecture to ensure protection against the ever-changing security landscape.

This document aims to provide guidance on the specific security concerns which arise as an organization looks forward to embracing BYOD and mobility. We explore how the landscape has evolved with examples of actual use cases in the Indian Industry and the technology available to secure corporate information and data.

Business drivers leading to adoption of BYOD & Mobility

Potential benefits of enterprise mobility

Enterprise Mobility facilitates business agility and empowers employees by enabling remote access to corporate resources and extending connectivity through mobile device. It provides users with flexibility of working away from the physical office space and greater control over planning their personal tasks without compromising on official duties. This may also enable better utilization of idle time otherwise wasted due to lack of access. Some of key potential benefits include:

- **Enhanced customer service times and delivery,** from sales staff, field agents and other customer facing executives, as they have access to product information, application access, customer information and service records on the move
- **Increase productivity** by enabling employees to access business data on the move
- **Enable larger geographical footprint,** beyond the physical office space
- **Reduced Capex and Opex** costs such as on office space, electricity charges, commuting charges etc
- **Aid business contingency planning** as employees can continue to work in case of environmental hazards such as floods or socio-political disturbances such as strikes, since they may access corporate resources from anywhere

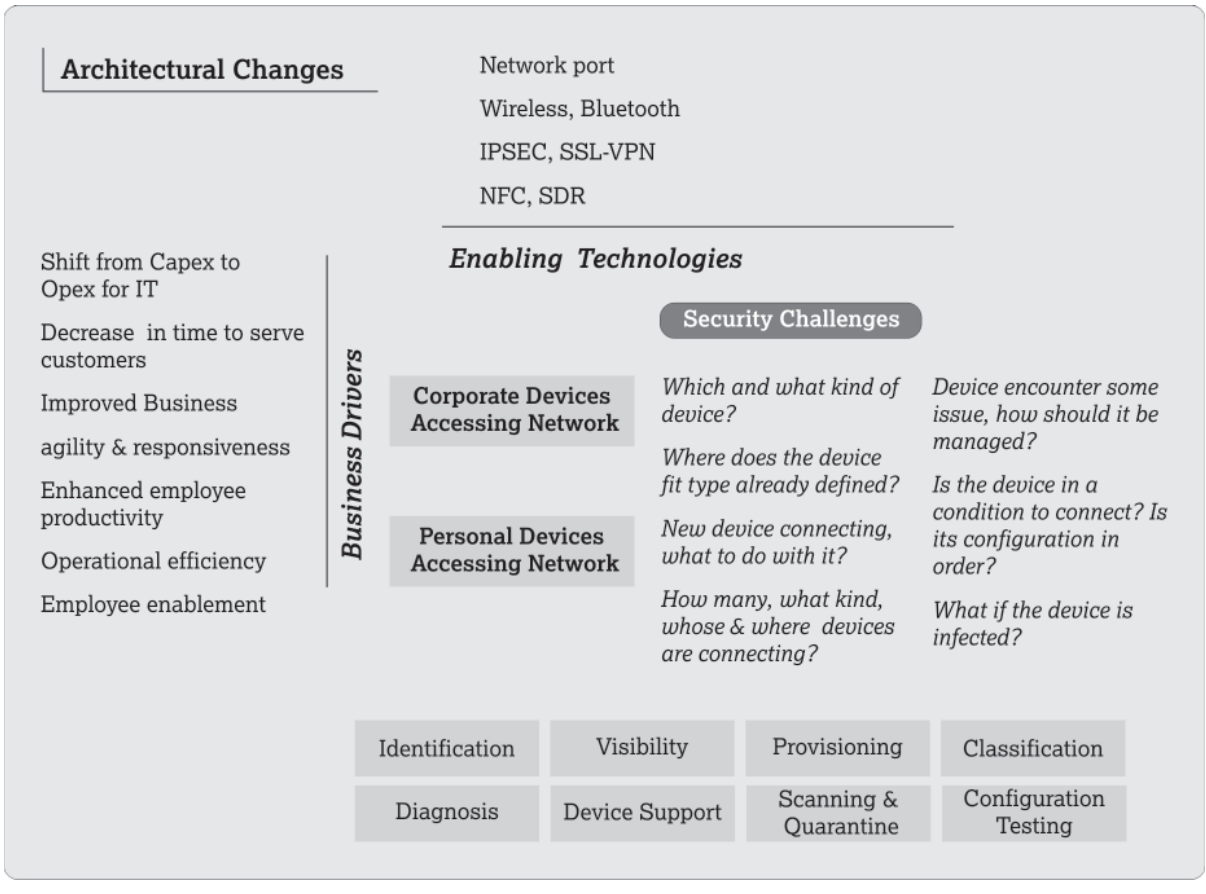
Potential benefits of using BYOD as an enabler for enterprise mobility

- **Users embracing smart computing devices** in the form of smart phones, net books, tablets, e-readers and laptops offer users an opportunity to use multi-productivity tools, as they generally have hardware resources similar to traditional computing devices used by organizations
- **Reduced cost** of hardware, by incentivizing users to procure their own endpoint device
- **Streamlining of inventory,** by reducing workflow related with management of devices, warranty updates, depreciation etc.
- **Provide flexibility** to the user to upgrade/ change their device as per their preference
- **Improve productivity** as users personal device is accessible at all instances

- **Reasonable security functionality,** such as remote wipe and encryption in addition to installing customized security features on devices, aids in the overall security design
- **Offer multi-function applications** compared to traditional computing devices such as a PC - smart phones and tablets are as powerful and capable and enable a user to use them for computing, communication and for using productivity applications
- **Support business agility,** as it allows the organization to be flexible and counter changes in business conditions. It may help organizations to build networks to support newer innovations and incorporate cutting edge technology to counter competitors

Key Considerations

The key considerations discussed below pertain to instances of adoption of BYOD and Mobility and aspects which drive the Mobility initiative. The high level architecture explains the use of enabling technologies and possible security challenges faced by organization while planning to implement BYOD & Mobility initiative.



Identification

Which and what kind of device?

IT teams may establish a device map over time which will assist in identification of the diverse devices which are allowed access to the corporate network. Further, not only do they need to establish the authenticity of the person using the device but also ascertain that access is restricted based on certain check on mobile devices. For example in case the mobile device is Jail Broken, user access should be denied

It should also be possible to provide guest access to temporary users by giving control to users to create their guest profiles. For example when a contractor comes to troubleshoot a particular application, the application owner can create a guest access with parameters such as time limit and give access to the contractor to certain resource like internet.

Provisioning

New device connecting, what to do with it?

An initial interaction between the user and IT teams may be required to ensure on-boarding of user owned device; alternatively, organizations may set-up employee self-help portals, which contain information necessary for user owned devices to be authorized. Owing to the large number of devices available in the market, IT may

- Conduct a robust posture assessment of the device capabilities to white-list certain devices based on their security functionality and features and the impact it may have on organization information/ systems
- Deploy endpoint security applications such antivirus, personal firewall or antispyware Design a system to check for compliance of user device with the enterprise security posture, prior to device being authenticated
- Use an endpoint assessment tool for automating the process of remediating non- compliant endpoint security applications
- Configure roles, applications and content automatically based on the user privileges defined in the application/ system
- Choose to restrict the number of devices enrolled per user and integrate appropriate capabilities to manage user sessions across all devices authorized per user
- Provision several users, especially from the sales or support function requiring connectivity through publically available networks or data connectivity via telecom networks
- Deploy appropriate capabilities to configure VPN; such that it remains established during IP address changes, loss of connectivity etc. and may have provision to auto-reconnect. Additionally, VPN may automatically disconnect as the user device enters the office premises and reconnect as the user move to a remote location
- Choose to partition space in the device where enterprise data may be stored while disabling the inbuilt cloud storage applications, email clients and other P2P applications from accessing this space

Visibility

How many, what kind, whose & where devices are connecting?

Traditionally a user was mapped to a specific desktop PC or laptop and could be easily identified by the IT for support or trouble shooting. With increasing adoption of mobile devices and other employee owned devices, a user may be logged in from multiple devices at the same instance. Many of these devices will deploy multiple nodes and may transition from wired Ethernet to WiFi to 3G/4G mobile networks, moving in and out of different connectivity zones. It is thus critical to be able to establish visibility over devices, both corporate and user owned, which require access to enterprise data.

Organization should monitor activity of mobile devices, the platforms used and the content being accessed from accessing the corporate environment. Once this visibility is available, capabilities may be deployed to ensure that unapproved devices are not granted access to the network and all attempts to connect to the network from such devices are tracked and monitored. This may be achieved by review of logs generated during mobile device management, network authentication, user activity and security scanning amongst others.

Important considerations for establishing visibility over access and activity include:

- Types of devices connected to the network
- Number of devices connected compared to the number of users listed in the AD/LDAP
- Location of access of users compared to the most frequently used location
- Type of connectivity used to access
- Typical amount of bandwidth consumed by user for internet usage, data storage and application access
- Number of policy violations by users
- Number of security incidents and breaches

Visibility over access and activity may be achieved by implementing context and content aware security capabilities in addition to Network traffic logging mechanism, basic internet content filters, bandwidth measurement tools and other relevant tools and capabilities

Device Support

Device encounters some issue, how should it be managed?

It may be impractical for the IT support teams to support the diverse set of devices and form factors available in the market. This is due to the widespread fragmentation of OS platforms such as Android, Windows OS, Blackberry, and iOS etc. which power mobile devices. Hence organizations face challenges of not only supporting a diverse set of OS platforms (which can further be customized), but also in ensuring that all future updates of the platform are supported. Each version of the OS may have inherent vulnerabilities, which may require specific security capability to address associated threats

The organization may otherwise decide to support a limited number of devices which are corporately – approved, with a limited set of OS platforms. As a first step, organizations need to evaluate different devices and configurations to understand which devices and OS platforms offer security aligned with the organizations expectations. The organization may mandate a list of devices that user may purchase, offer subsidies for purchase of certain device types or introduce strategic tie-ups with specific device manufacturers to encourage users to opt for a particular set of devices. Typical instances where technical support is required may include:

- Helping users configure devices to establish connectivity to the corporate network
- Assisting guest users with setting up connectivity to the corporate network
- Maintaining visibility over the number of devices connected to the network and ensuring appropriate security scanning of the same
- Updating self-help tools as and when required
- Assisting users to disable lost or stolen devices or delete/ recover data from damaged/ lost devices
- Effective monitoring and incident reporting for security breaches
- Ensure off-boarding of devices to remove organizations data, in case of user termination or even in long term overseas travel (6 months or above)

Diagnosis

Is the device in a condition to connect?

User and device authentication infrastructure scans endpoints requesting access to the corporate network and determines whether their security posture is compliant with the company's policy. This allows an administrator

to immediately remediate noncompliant endpoints. Authentication can be of various types, for example using 802.1x technologies to authenticate at the switch port level, where the user will not be provided an IP Address prior to being authenticated successfully. This may be done both at the user or a device level.

Once the user is authenticated successfully further checks on his profile may be conducted such as device antivirus status, up-to date patches, applications installed in order to determine his (device) access on to corporate network. In scenarios where the users does not pass the checks or has a non-compliant device, mechanisms to block them at the switch port level using downloadable filters on the switch/ router/ secured branch router/ Wireless LAN Controllers can be established.

Configuration

Is its configuration in order?

The diversity of devices and OS platforms makes device configuration management difficult for the organization. Apart from ensuring that employees are aware of their responsibility to safeguard device used to access corporate information, it is essential that the organization deploys appropriate mechanism to test device configuration and to evaluate the consistency of the security posture of the device. Some key focus areas are as follows:

- Check for jail-broken and OS rooted devices. Such devices may be highly vulnerable and need to be barred from access on configuration
- Configure connectivity options available in the device, such as Bluetooth, Near Field Communication, Scanning of Quick Response (QR) codes, to be turned off by default. All user owned devices may be configured to remain undiscoverable to nearby Bluetooth devices, except in case of a business requirement
- Disallow/Limit the capability of the device to install unverified third party apps as they may carry malware. Similarly, applications which seek administrative access rights or rights to access resources beyond the applications intended functionality may be barred from the device.
- Send updates to the user to install device OS updates as and when available from the manufacturer. Further, updates to corporate applications may be pushed into the user device with means of appropriate solutions.
- Other factors which may be pre-defined in the security configuration of the user device are use of camera, file sharing, and use of internet, general email security requirements and email attachments download

Scanning & Quarantine

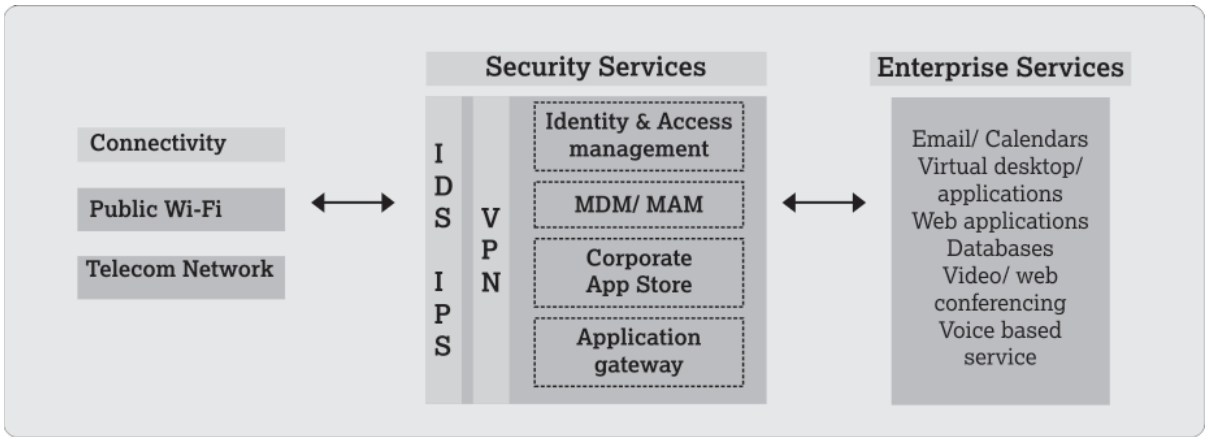
What if the device is infected?

The security teams may implement appropriate controls for scanning devices connected to the corporate network, monitoring traffic originating to and flowing from the network and scanning applications and databases for anomalies. Organization may deploy capabilities for:

- Auto-quarantine during the device on-boarding process, to maintain strict control over device which are non-conformant to the organizations security posture
- Monitoring on a real-time basis for on-device statistics, logging information and ensure availability of contextual information for analysis
- Monitoring, using flow based information to identify infected devices, for e.g. a machine may be infected by a Botnet (it might be a zero day which the device anti-virus was not able to detect when device posture was checked during initial authentication)
- Detecting corporate data on infected or non-compliant devices, which should be removed by a selective wipe and the device may be de-provisioned form accessing the network
- Reasonable web security monitoring to provide administrators granular control of hundreds of thousands of micro-applications on Facebook and Twitter, as well as many other popular platforms and streaming media. Without blocking entire websites, administrators can allow or block specific features such as chat, messaging, video, and audio

Architecture Scenarios

The mobile security architecture provides an overview of the associated risks and possible capabilities which may be incorporated to provide a secure environment for usage of mobile devices. These devices may be owned by the user or provided by the organization. However, in either case there will be associated risk which needs to be effectively countered by incorporating capabilities for securing data on the mobile, mobile device management, mobile application management and other similar technologies for deriving the security architecture for enabling mobility/BYOD. The architectural components are provided here for reference to help guide organizations with implementing safe security practices. *Security concerns with respect to network infrastructure and server's is assumed to be reasonably evaluated by organizations and are not discussed in this document. Though the security capabilities are vendor agnostic, there may be certain cases where some features may be technology or OS specific.*



Device considerations

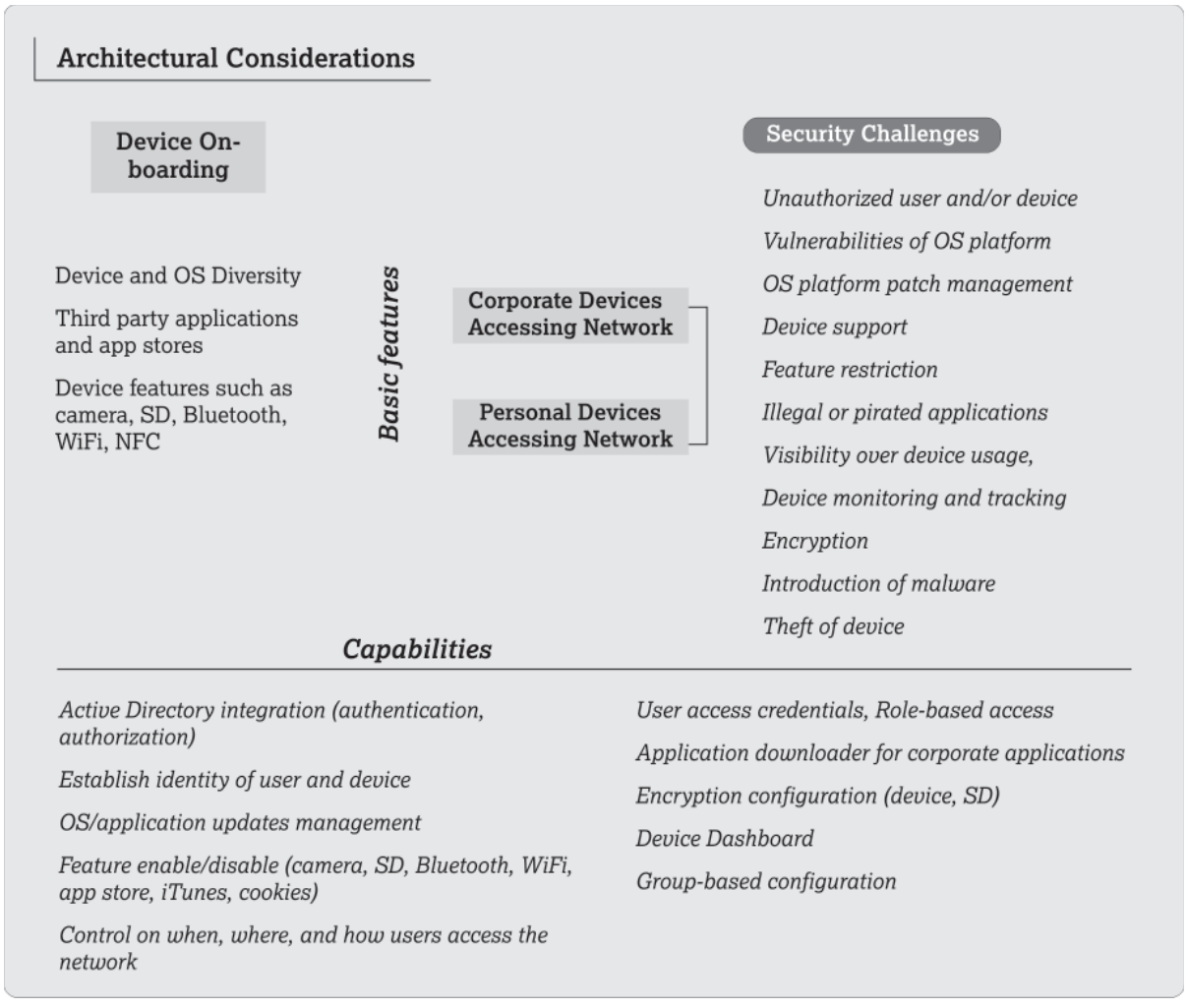
Selecting the device is an important factor and depends on the business requirements against the sensitivity of data being accessed, platform and the type of network, provides a better understanding of the opportunities and benefits versus the risks and costs to the organization. Basis the requirements of business stakeholders, a justified business case for enterprise mobility and its tangible and measured benefits to the organization, its employees and customers, may be established.

As organizations realize the benefit of BYOD and mobility, they may adopt either of the following scenarios or a combination of both, basis their business requirements.

	User Procured Device	Corporate Owned Devices
Device Considerations	Employee purchases device of own choice or from a corporately-approved set of devices	Organization procures devices and distributes to its users
	User self-help provisioned devices on the corporate network; IT assisted registration of user devices, prior to granting network access	Devices hardened by corporate IT in-line with the organizations security policy
	User needs to validate device with IT teams and install minimum set of security controls as required by the organization	Device pre-registered to access the corporate network
Challenges	Effort of validating security posture of diverse set of devices	Apart from required functionality, organization may need to focus on enhancing user experience, when offering a corporate device
	Complexity of device support due to heterogeneous nature of devices (provisioning, access, configuration and applications)	Setup mechanism to track acceptable usage of corporate device for personal use
	Complexity of creating visibility on usage of corporate resources on device	Increases burden on IT to manage mobile devices in addition to traditional office infrastructure
	Segregation of personal and business data	Issues related to securing corporate data from compromise by jail-broken or rooted devices
	Additional capabilities for securing data loss due to theft of device, such as use of Data wipe	Provision resources to assist corporate devices to establish connectivity to the corporate network
	Enforcing restrictions on installation of third party applications, wherever applicable	Involves high Capex
	Capability to gather and analyze intelligence from device monitoring for actionable use and governance	
	Ensuring adherence to legal and regulatory guidelines, while using confidential or proprietary data on user owned mobile devices	

Device on-boarding

As users introduce new devices into the corporate architecture, the IT security teams need to manage issues related with device on-boarding and provisioning. Typically, there are challenges related with respect to allowing heterogeneous systems into organization ecosystem and with identifying vulnerabilities associated with different devices and a diverse set of operating systems. Each device type and the OS platform offer features which may be desirable from a user perspective; however, the IT need counter associated security risks. Organizations may not wish to deal individually with each device and may establish processes for auto-provisioning using employee self- help.

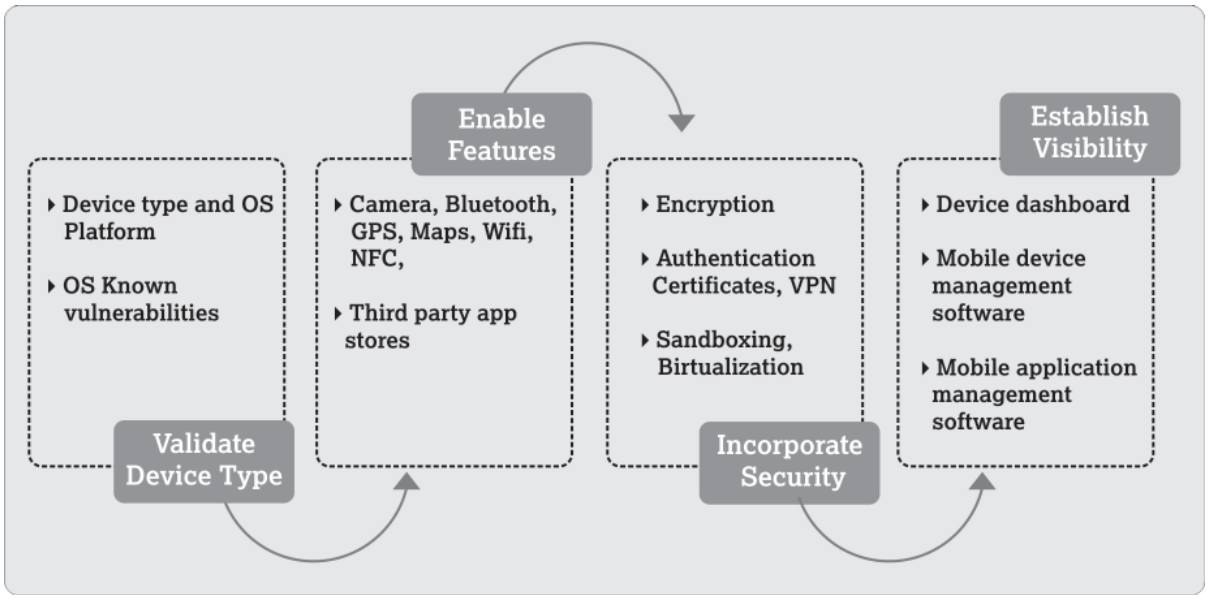


Device on-boarding may be done in either of the following ways:

Organization supported on-boarding process	User managed on-boarding process
Verify device type and OS platform	User managed on-boarding process may be managed by using appropriate capabilities, which allow users to authenticate themselves on the corporate network at first log-in.
Perform device health check	Appropriate scanning and device assessment may be performed by the network security elements prior to granting access to the device.
Installation of security features such as anti-malware, Mobile device management software, Mobile Application management software	User may be directed to a self-help page, guiding them with steps needed to be performed for registering and processes for their device to be eligible for gaining access to the corporate network.
Installation of certificates	The employee-owned devices are on-boarded and may be provisioned with digital certificates
Initiate connection with corporate applications and resources	

Key considerations

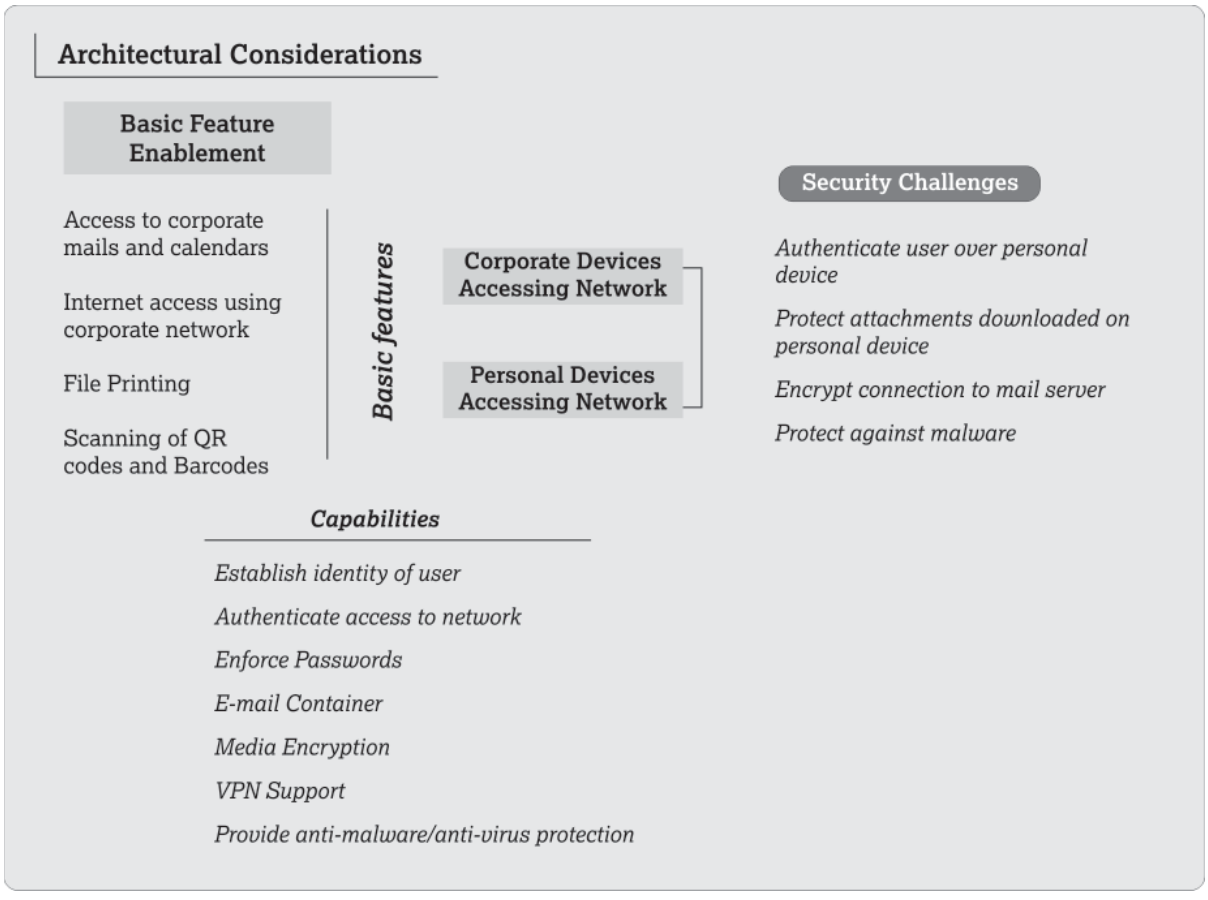
The following considerations may be incorporated into the security framework design during the device on-boarding process:



- **Validate device type,** to ensure devices with reasonable security features are allowed to be used
- **Device features** such as camera, Bluetooth, NFC etc. may be selectively enabled, depending on organization use case
- **Basic Security features** such as encryption, installation of authentication certificates etc. may be carried out
- **Device and application management capabilities** may be incorporated to help manage the device effectively, and aid monitoring of user activity over the corporate network
- **User privileges may be restricted** by specifying user profiles on mobile device, by limiting rights granted to the user to modify or access sensitive data
- **Users with administrative privileges** to access applications, systems, databases and hardware inside the organization, may be granted limited rights while accessing the same information from a personally owned mobile device
- **Other controls include,** but are not limited to
    - Disabling the use of predictive text applications or user dictionary, which stores information from the virtual session to local storage
    - Screen idle time lockout
    - Appropriate placement of firewall and intrusion detection/ prevention systems may be done to create
    - Specific zones which restrict the access of any particular device to the designated area will help aid effective monitoring and audit of information flow between the zones

Basic Feature Enablement

A cautious approach to mobility/BYOD focuses on enabling only limited access to corporate resources such as corporate emails and calendars. Some organization also allow restricted access to corporate networks, file printing and scanning of QR/Bar codes which are also considered as basic feature enablement.



Key Considerations

While establishing identity of the device and authorizing its access in the corporate network are essential capabilities, organization may look to overcome the challenges encountered for protecting data downloaded on these devices by:

i. **Establishing secure containers for corporate data,** thereby limiting exposure of corporate data to other applications and data transfer mechanisms. Example, Email may be configured so that all attachments may be downloaded inside a secure container
ii. **Selecting desirable device features,** such as the ability to scan Quick Response (QR) codes or bar codes may need safeguards to prevent scanning of malicious code onto user devices. Generally, a scanned code redirects a user to a webpage, which may lead to malicious code being downloaded onto the device.
iii. **Transferring files from the device** via file printing may also be restricted to pre-configured printers, to protect confidential information. The ability to transfer or download data to removable storage or a personal cloud may be monitored or restricted
iv. **Establishing secure channel** for communication between the device and the corporate network for example through VPN
v. **Deploying Endpoint security solutions** to secure against malware

Implementation case 1: Basic adoption of BYOD as an enabler for mobility

BACKGROUND

An emerging life insurance company, with focus on customers located in Tier 2 and tier 3 cities wanted to reduce the time it takes for their field agents to register customer information with the branch or main office, as agents had to travel long distances to the branch office to physically update the customer detail forms.

The company was additionally looking towards allowing select staff to access their corporate email and calendars in a limited set of corporate owned devices. This would help them reduce the time to serve customers and establish traction in the market for their insurance products.

CHALLENGES

- Provide access to basic mobility features to staff, while ensuring adequate security of business critical data
- Protect customer information available with field agents
- Reduce storage of business data with field staff

BUSINESS BENEFITS

- Better co-ordination amongst field and office staff
- Faster processing of customer information
- Faster communication amongst employees and with customers
- Reduced expense for travel by sales staff
- Improved response time and performance in customer facing activities
- Employee empowerment leading to increased productivity

SOLUTION

- Use of company approved device, which has been selected post comprehensive security testing of available devices
- Access to corporate email and calendars through a secure VPN connection
- Disabling Features such as Print-screen(screenshots), forwarding to personal email accounts, and uploading data to cloud
- Installing basic endpoint security, including antivirus and antimalware, remote wipe, encryption and other mobile data management solutions
- Application access is granted to authenticated users - access to an application which will enable them to transfer customer data on a real time basis to the company.
- Application does not use the device memory to store information, as all customer data is purged on a real time basis. The application works in a secure container, with very low risk of compromise.

SECURITY CHALLENGES

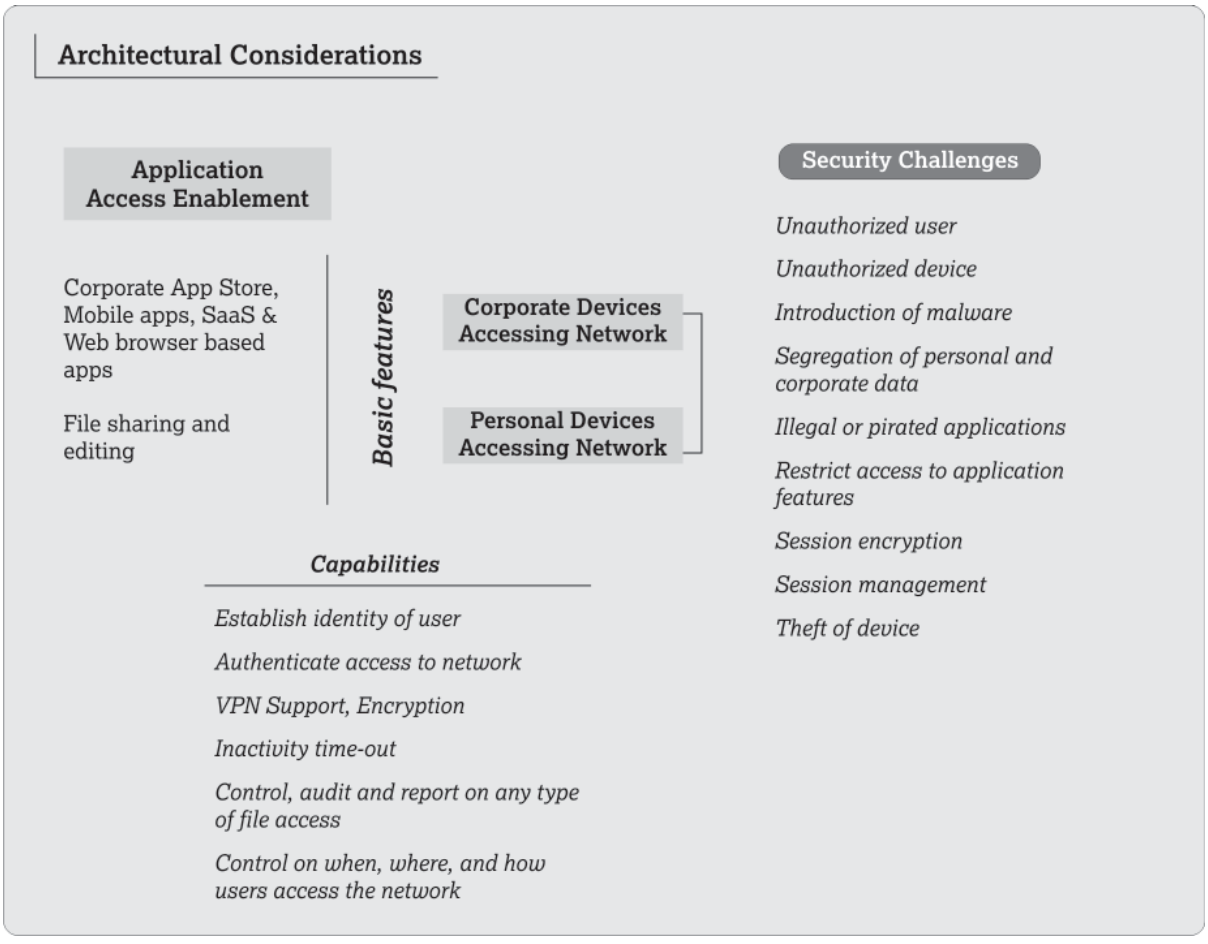
- Secure official communication such as emails, attachments and files from unauthorized disclosure
- Restricting data storage on the mobile device, while providing access to corporate Application such as CRM
- Maintain security posture of device and prevent introduction of malicious content
- Prevent compromise of customer data by means of forwarding via personal email, screenshots, upload to cloud services etc.

Application Access Enablement

As users move outside the physical boundaries of the organization, using a mobile device as a supplement to the corporate desktop becomes a necessity. Organizations also need to evolve from basic feature enablement to considering access to corporate applications on mobile devices. Some of the common methods used to achieve this are:

Virtualization: Virtualization addresses challenges posed by advent of BYOD by allowing information to be accessed on any device, as it provides a layer which sits between the device and virtualized application/ platform running in any OS. It provides remote access to computing resources so that no data or corporate application processing information is stored or conducted on the personal device. It further helps in achieving goals such as reducing cost and simplifying IT architecture. Virtualization isolates the user, delivering services to it as an end-point device. The organizations data will reside at its own IT Infrastructure as the end-user will only have access to modify it on their devices

Sandboxing: Contain data or corporate application processing within a secure application on the personal device so that it is segregated from personal data; by using techniques to sandbox data or create containers on the user device, thereby logically segregating the corporate data from the user's personal data on user owned devices. In order to access the corporate data, user may have to step out of their personal operating environment



Co-mingled data: Allow corporate and personal data to exist on the user device and/or leverage the device for local application processing. Using this approach, organizations may permit users to install application from the corporate app store, use third party applications and/or use browser based apps for performing productivity tasks. Further, corporate data may be allowed to be stored on local memory. This approach may require organizations to adopt advanced solutions, such as those utilizing context and content information, for monitoring and analysis of user activity while accessing corporate resources

While adopting this approach organization may look towards following considerations:

i. Application delivery considerations such as
    a) Use of technologies such as Virtual Desktop Infrastructure, Hosted Shared Desktops & thin clients to deliver applications
    b) Custom designing of application delivery architecture using private cloud, based on user profiles
    c) Use of browser based applications
ii. Extending application access on mobile devices requires a careful consideration into user rights and privilege management;
iii. Ensure that end users are responsible for backing up personal data; provide means for users to take backup of data on mobile devices, using either a push or pull mechanism
iv. Require employees to remove apps at the request of the organization;
v. Disable access to the network if a blacklisted app is installed or if the device has been jail-broken;
vi. Establish control over when, how and where users may access corporate data and applications
vii. Establish visibility over user activity and maintain log of information accessed and operation performed by user on corporate data

To secure the organizations resources from compromise and unauthorized access, capabilities such as Network access control (NAC) may be useful. NAC attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement. This will help in controlling access to the network and govern secure access to the operating system, application and hardware.

Implementation case 2: Advanced adoption of BYOD as an enabler for mobility

BACKGROUND

A mid – sized IT Services company, which offers IT solutions for platforms (servers and enterprise computing), storage, data center and virtualization, requires team members from Sales, Presales, Project and Delivery to keep abreast with knowledge of its solutions and technologies to offer value to customers. The company requires - providing access to business email and calendars; access to CRM applications; access to online collaboration tools. They also needed field employees to be able to access basic productivity applications from outside the organizations boundary on mobile or personally owned devices.

CHALLENGES

- Cater to unique data requirements of different functions
- Leverage device computing power, however restrict data from residing on multiple user devices
- Provide seamless transition between multiple user device

BUSINESS BENEFITS

- Tele-workers have access to productivity applications
- Reduced expense for travel by sales staff
- Improved response time and performance in customer-facing activities
- Employee empowerment leading to increased productivity

SOLUTION

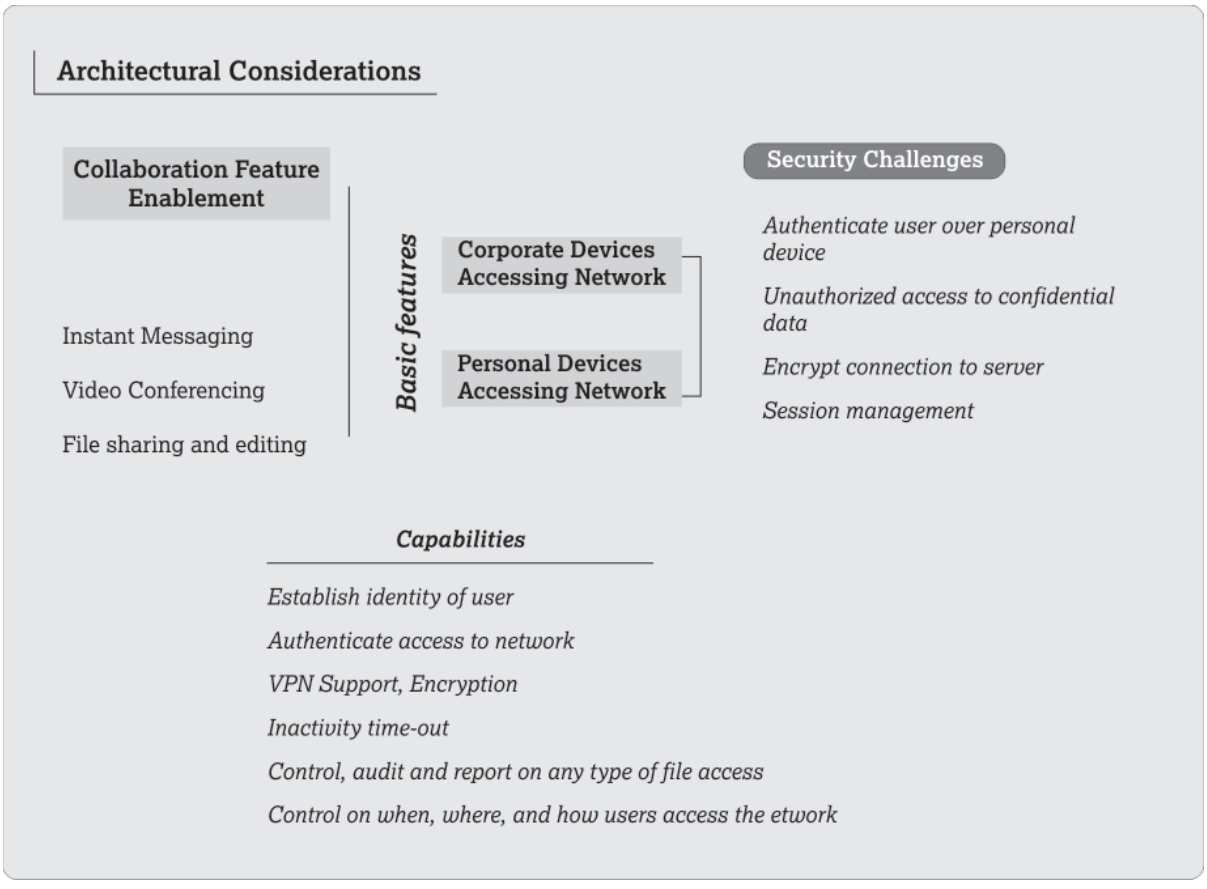
- Some application containing critical data is accessed through virtualization. The devices are used as a thin client to access the data via a citrix environment.
- Instances of some corporate apps are also available on user devices
- Native mobile apps are delivered into a secure container to maintain separation between business apps and data and the worker's personal content
- Moreover, features such as screenshot, forwarding to personal email accounts, and upload to cloud have been disabled on the user device while the user accesses corporate data
- Application access is granted to authenticated users
- Application maintains connectivity to corporate network through inbuilt VPN mechanisms

SECURITY CHALLENGES

- Authentication of users on personally owned devices such as Smartphone's and tablets
- Ensuring corporate data residing on personal devices is secure
- Application access
- Device security management – prevent malware on device from spreading to the corporate network
- Manage issues with identity as users transition between devices of create parallel sessions

Collaboration feature enablement

Although an extension of basic feature, enabling collaboration feature is generally an afterthought mainly because of data heavy transaction which consumes lot of bandwidth and also adds to data usage challenges which might have an effect on HR policy of mobile usage and its reimbursement. Collaboration allows the use of instant messaging applications, video conferencing along with ability to share files and collaborative editing using cloud services or apps on mobile devices. The use of cloud services helps in ensuring that corporate data stays off user device; and helps users collaborate in real time.



Some of the key considerations for enabling collaboration features are:

i. Appropriate usage of encryption to safeguard unauthorized access to data in transit during communication between the device and the enterprise server
ii. Monitor user sessions and enforce session time-out in-case of inactivity
iii. Establish and review logs of user activity on devices and operation performed on corporate data in the cloud
iv. Provide seamless connectivity for users to leverage benefits of video conferencing and collaboration on cloud services

Implementation case 3: Enhanced adoption of BYOD as an enabler for mobility

BACKGROUND

Large IT Services Company, which offers customized IT and engineering services expertise to its clients wanted to leverage global offshore infrastructure and network of offices in 31 countries. They provide multi-service delivery in industries such as financial services, manufacturing, consumer services, public services and healthcare. The company has its main campus located in the outskirts of the city and has multiple offices across India.

The company wanted to leverage the mobility/BYOD by providing access to business email and calendars; access to productivity applications and access to online collaboration tools such as Instant messengers and video conferencing apps. The organization desires the ability for employees to access productivity applications from outside the organizations boundary on mobile or personally owned devices, as it does not wish to add to its capital expenditure.

CHALLENGES

- Extending access to business data on personal devices
- Evaluate data requirements of diverse set of business users
- Provide connectivity options to users
- Secure communication via video/ IM applications

BUSINESS BENEFITS

- Utilize non-productive hours, such as time spent in commuting to office
- Enable teams to collaborate across geographies
- Employee empowerment leading to increased productivity

SOLUTION

- Use of citrix to deliver secure access to application
- Application access is granted to authenticated users
- Features such as screenshot, forwarding to personal email accounts, and upload transactional information (text, audio or video) to cloud have been disabled on the user device while the user accesses corporate data
- Enable access to device features such as user cameras and microphones
- Create logs of all sessions including user information, time of connection, duration of sessions, etc.
- Provisioning of secure recordings on a need basics by restricting storage on a mobile device and further through encryption

SECURITY CHALLENGES

- Prevent users from taking screenshots of data or, importing data onto their devices
- Barring use of personal email accounts and restricting access to corporate data from these clients
- Establishing visibility over user activity and gathering actionable intelligence
- Ensure seamless transition of VPN connectivity as users switch from corporate to public networks

Security Considerations

From a mobility perspective the principal guidance is classified under four distinct areas as depicted in the figure below:

Device Security	Data Security	Monitoring	Governance
Device configuration, restoration, or migration of profiles, services, software, policies, and files	Security (e .g ., enforce data-in-transit encryption, data at-rest encryption, authentication)	User activity / Device jailbreak / rooting detection, system performance monitoring	Asset management and security compliance audits (e .g ., routine/real-time scan of functions against enterprise policies)
Device features (e.g., timeout lock/ enterprise lock); use of camera, GPS, NFC etc	Segregation of data	Peripheral status monitoring (e .g ., camera, NFC, Bluetooth)	Enterprise dashboard visibility, alerting, logging
Mobile Device Management (e.g., selective wipe/ comprehensive wipe)	Restricted content transfer across domains/ Legal and regulatory considerations	Quarantine malware/ applications	Help desk/self-service administration, troubleshooting

Device Security

Beginning with the on-boarding of user owned devices; organizations need to develop the ability to manage the lifecycle of each device. It may be required to revoke access from devices in violation of enterprise policies or upon employee termination, or in case the device is lost or stolen. Further, the ability to wipe data from devices and removal of applications are critical factors in ensuring security.

i. **Device configuration, restoration, or migration of profiles, services, software, policies, and files**
   - Configure devices as per organizations use case and policy
   - Formulate methodology for enrolment process for devices by installing customized software, installing device management applications and installing digital certificates to authenticate devices to the network etc.
   - Establish system for detection of jail broken devices and to help in identification of rooted devices

ii. **Device features (e.g. timeout lock / enterprise lock/ use of camera, GPS, NFC)**
   - Introduce security functionality such as setting up minimum acceptable length of passwords with desired complexity, specifying device idle timeout and device lock parameters
   - Compliance checking of devices for installation of security patches and anti-virus upgrades, disabling unwanted services on the device such as access to cloud storage or camera, inbuilt recorders etc.

iii. **Mobile Device Management (e.g. selective wipe / comprehensive wipe)**
   - Develop the capability to recover/ delete data on device which have been stolen or lost

Data Security

The threat to data originates from multiple sources, such as the device being stolen or lost, employees downloading freeware or spurious applications, causing malware, worms or virus's to infest the device. Further the increasing use of social networking applications, places the data on mobile devices at risk of accidental disclosure.

i. **Ensuring Security of data on device**
   - Enforce encryption for data at rest and data in transit;
   - Use appropriate authentication mechanisms to control access to corporate data
   - Control transfer of data from mobile device, such as transfer to removable storage, upload to social networks, upload to cloud storage etc.
   - Evaluate endpoint security solutions such as anti-malware, antivirus etc.

ii. **Segregation of data** – corporate data on mobile devices may be stored in a separate secure container

iii. **Restricted content transfer across domains/ Legal and regulatory considerations**
   - Use appropriate solutions to ensure compliance with measures mandated by regulations and local laws specific to the industry vertical. Certain organizations operating in IT/ITeS and BFSI sectors need to comply with such as RBI , security compliance under PCI-DSS or IT Act 2000 & its Amendments 2008 amongst others
   - Organizations response towards discovery of illegal or pirated content on user owned devices
   - Legal liability arising out of license management, distribution of proprietary information or copyrighted information

Monitoring

Establish processes for monitoring and maintain log of all activities performed by the user

i. **User activity / Device jailbreak / rooting detection, system performance monitoring**
   - Deploy capabilities to guard against day zero threats to the network by ensuring continuous monitoring of the network for unusual events or trends
   - Establish baseline of normal network behavior and identify parameters to flag anomalous behavior
   - Monitor and identify infected devices and disable available services to protect corporate data on such devices
   - Gather and maintain intelligence from all devices connected to the network, to build a view of the context, content and location co-relation

ii. **Peripheral status monitoring (e.g. camera, NFC, Bluetooth)**
   - Monitor user activity such as use of functionality like camera, scanner, NFC etc. to develop on-device statistics and log information for analysis

iii. **Quarantine malware / applications**
   - Prevent the introduction of malware, viruses, Trojans and other malicious code into the corporate network via the use of personal devices
   - Quarantine or block specific features such as chat, messaging, video, and audio based on business case and enterprise policy
   - Prevent use of applications or services which are pirated or cause copyright violations from being used to perform work related tasks, on devices owned by the user

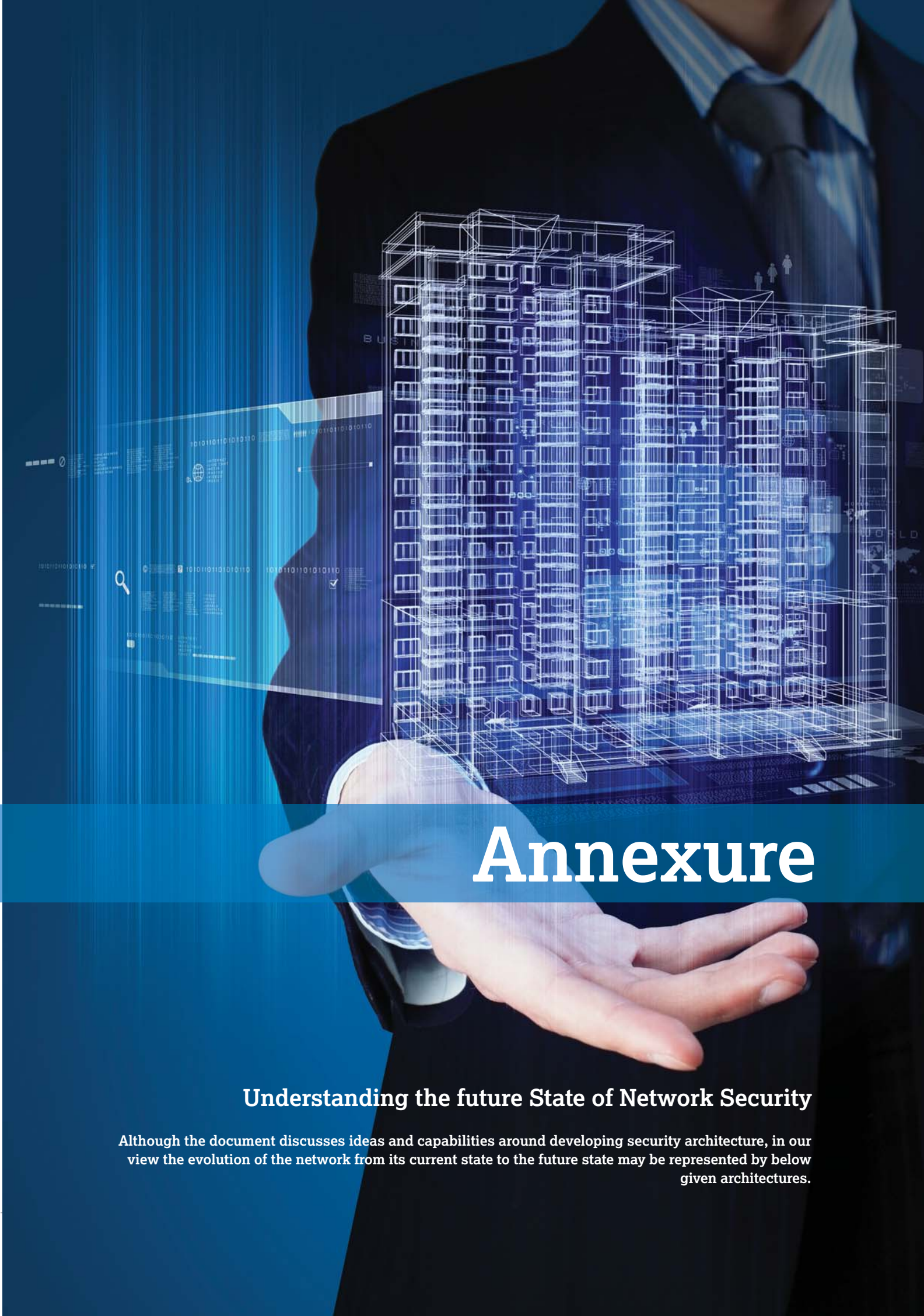
Governance

Establish mechanisms to analyze user activity to create an enterprise wide visibility dashboard to identify instances misuse or policy non-compliance

i. **Asset management and security compliance audits (e.g ., routine / real-time scan of functions against enterprise policies)** - All logs created from monitoring user activity and device scanning may be used to build actionable intelligence for ensuring device security posture is aligned with the organizations policies

ii. **Enterprise dashboard visibility, alerting, logging**
   - Capabilities may be deployed to ensure that unapproved devices are not granted access to the network and all attempts to connect to the network from unapproved devices are tracked and monitored
   - Develop mechanism to ensure real time alerts are issued to track malicious activity
   - Incorporate measures to enable remote tracking and device locking, during instances of employee termination or deliberate absence
   - Use of tools and applications for forensic analysis of device, in case required, to analyze the introduction of vulnerabilities into the device

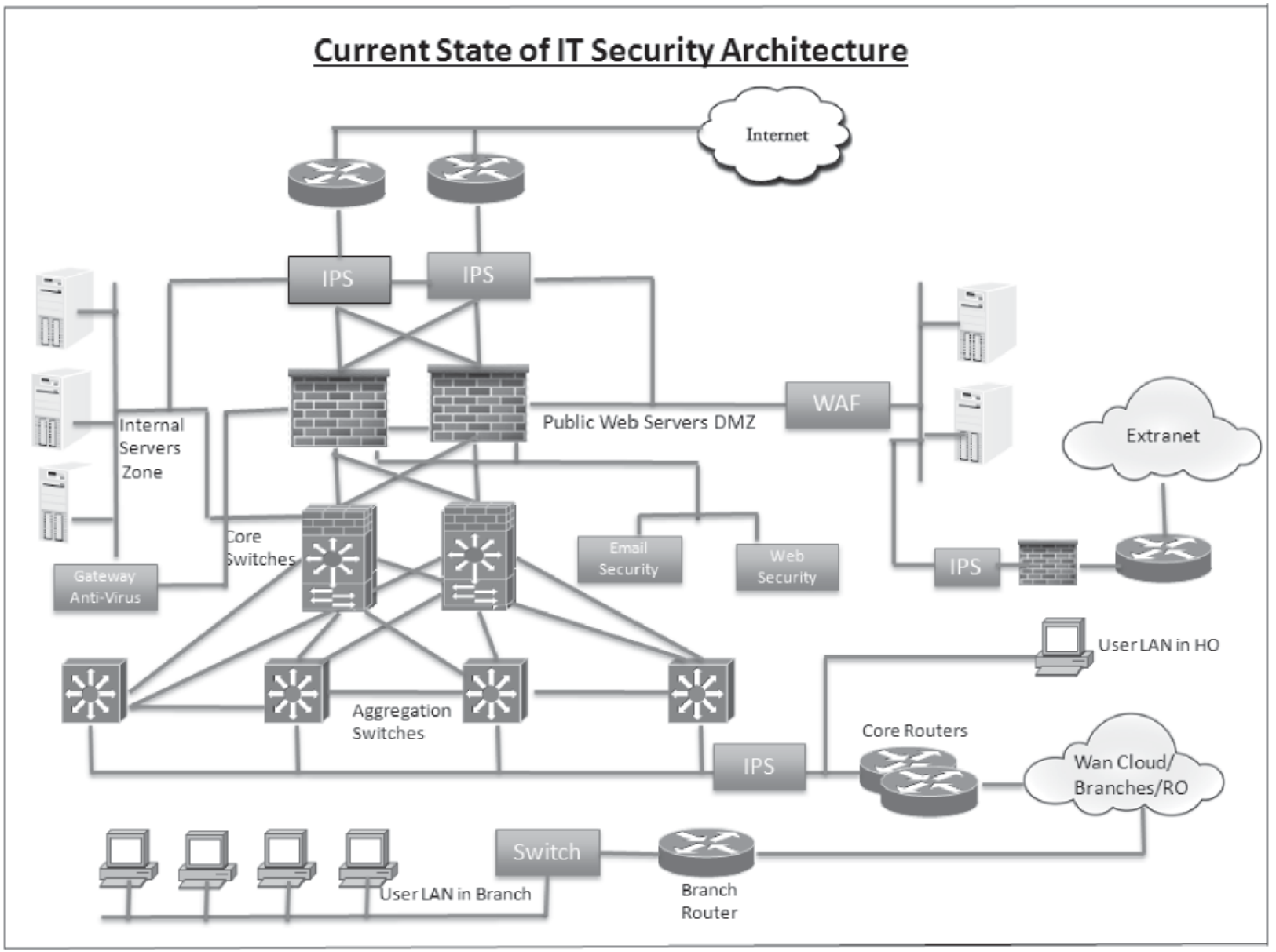
iii. **Help desk / self-service administration, troubleshooting**
   - Consolidate FAQ's into a self-help portal to guide users
   - Simplify device administration by introducing self-service options for users

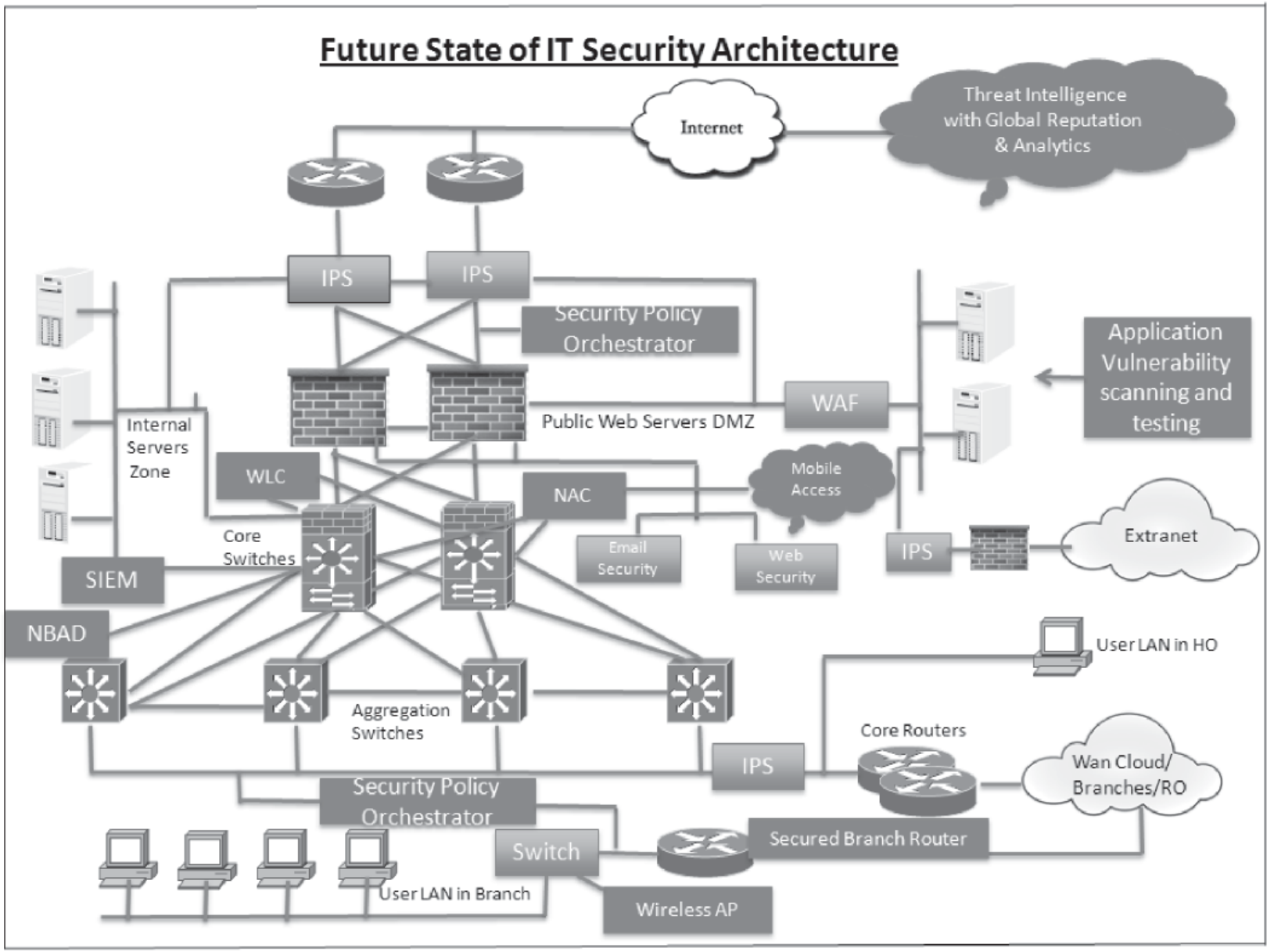


Annexure

Understanding the future State of Network Security

Although the document discusses ideas and capabilities around developing security architecture, in our view the evolution of the network from its current state to the future state may be represented by below given architectures.


Current State of IT Security Architecture
Internet
IPS
IPS
Internal Servers Zone
Public Web Servers DMZ
WAF
Extranet
Core Switches
Gateway Anti-Virus
Email Security
Web Security
IPS
User LAN in HO
Aggregation Switches
Core Routers
IPS
Wan Cloud/ Branches/RO
Switch
User LAN in Branch
Branch Router


Future State of IT Security Architecture
Internet
Threat Intelligence with Global Reputation & Analytics
IPS
IPS
Security Policy Orchestrator
Application Vulnerability scanning and testing
WAF
Public Web Servers DMZ
Internal Servers Zone
WLC
NAC
Mobile Access
Core Switches
SIEM
Email Security
Web Security
IPS
Extranet
NBAD
User LAN in HO
Aggregation Switches
Core Routers
IPS
Wan Cloud/ Branches/RO
Security Policy Orchestrator
Switch
Secured Branch Router
User LAN in Branch
Wireless AP

Acknowledgment

DSCI is grateful to the industry for its continuous support in DSCI Initiatives. The DSCI Reference Architecture Series is a new initiative, where industry collaborates by sharing adoption trends, challenges and ideas for building robust security architecture. The current contribution focuses on emerging trends with respect to Virtualization, Cloud Computing and Mobility/BYOD and is produced as part of DSCI-Cisco Security Thought Leadership Program.

Industry Support

Arun Anand	Vice President & CISO, NIIT Technologies Limited
Atul Khatavkar	VP & CISO, AGC Networks
Harvinder Singh	AVP - Technology Solutions Group, DLF Pramerica Life Insurance
Kalyanaraman Seshadri	DGM, IT Services, HCL
Krishna Bhat	General Manager, Information Security and Privacy, Robert Bosch Engineering and Business Solutions Ltd
Nanda Lal Kundu	Assistant General Manager, CISO, Bank of Baroda
Narayanan K S	Head - Information Risk Management ING Vysya Bank
Parag Deodhar	Chief Risk Officer, Vice President - Process Excellence & Program Management, Bharti AXA General Insurance Co Ltd
P D Mallya	Vice President & Head, Information Security Group, Infosys
Ramesh Kauta	CISO, GE India
Sunil Soni	Assistant General Manager - CISO, Punjab National Bank
Sunil Varkey	CISO, Wipro
Vijay Devanath	GM - Infra & Security, CISO, CRIS

Cisco Team

Mahesh Gupta	Vice-President, Borderless Networks - India & SAARC
Diwakar Dayal	Head - Security Business, India & SAARC
Srikanta Prasad	Principal Consultant
Sushil Menon	Product Sales Engineer
Sanjay Kharade	SE Manager

DSCI Team

Vinayak Godse	Director - Data Protection
Vikram Asnani	Principal Consultant
Aseem Mukhi	Consultant
Mayank Lau	Consultant

DATA SECURITY COUNCIL OF INDIA

A NASSCOM® Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in