White Paper

Secure Network Access for Personal Mobile Devices

What You Will Learn

People around the globe are enamored with their smartphones and tablet computers, and they feel strongly that they should be allowed to use these devices at work. By combining an architecture-based technical implementation with carefully considered business policies, organizations can create a safe and appropriate environment that blends personal and business resources. This paper discusses:

- The growing importance of mobile devices in an efficient, productive workspace
- The technical and business challenges of integrating personal mobile devices into the enterprise network with a high degree of security
- Business strategies for a mobile and bring-your-own-device" (BYOD) environment
- Point versus architectural network options and related products
- The Cisco® BYOD Smart Solution

Embracing the Potential of Mobile Devices

It's difficult to go anywhere today without seeing people using their personal mobile devices. The mobility wave is huge: Globally, business mobile traffic will grow 6.8-fold from 2015 to 2020 and there will be 12 billion mobile-connected devices by 2020 (Cisco VNI Mobile Forecast).

Users and organizations have become increasingly captivated by the possibilities of mobile network access and the growing number of applications available to them. Thus, it's no surprise that mobile device use has extended into the workplace. With devices ranging from corporate-supplied tablets to personal smartphones, employees are connected in more ways, more often, and from more locations than ever before. And with that diversity of use, the lines are blurring between work devices and personal ones, and between business and personal data. Many mobile users may believe that because work time often blends with personal time, company-issued devices should be available for personal use. That belief has contributed to a new definition of the traditional workspace that transcends desktop computers and laptops.

Today's workspace includes many resources that help make employees productive and efficient. Employees expect those resources to provide consistent and highly secure access to intellectual property, stored documents, and internal websites with sufficient bandwidth, storage, and processing power to accomplish tasks quickly and effectively. Applications, communications, and data must travel with employees wherever they work.

Many IT organizations implement this workspace concept in a phased approach. The first phase begins with simply onboarding the mobile devices and helping mobile users get to the resources they are authorized to access in a secure fashion. In the second phase, the IT staff promotes the use of mobile applications to empower employees and customers. The final phase is focused on optimizing the mobile experience. Mobile users may have access to self-service IT or be able to use various functions depending on where they are and what they are doing.

The IT deployment model for mobile applications may be a traditional on-premises model, software as a service, or a hybrid of the two. The trend is accelerating to cloud-based applications for mobility: cloud applications will account for 91 percent of total mobile data traffic by 2020, compared to 82 percent at the end of 2015 (Cisco VNI Mobile Forecast).

Providing an environment that allows employees to connect to corporate resources and to work productively at home, at work, or while traveling can attract a quality workforce, increase productivity, and improve job satisfaction - all critical factors for competitive success. But embracing the any-device phenomenon raises important questions about privacy and the security of sensitive information. As employees demand more freedom and flexibility with regard to mobile device use at work, and as consumer devices provide an increasingly cost-effective and attractive way to keep employees engaged and productive, IT professionals must remain vigilant about maintaining an appropriate experience while protecting the network and corporate intellectual property. Many organizations continue to struggle to introduce personal mobile devices into the workplace with a high degree of security and to embrace mobility with confidence: 43 percent organizations surveyed cited employees using their own devices, software, or cloud applications to do business as an internal security challenge (Cisco 2016 Annual Security Report).

In another emerging trend, organizations now offer mobile access to their partners or customers to better serve them. Enterprises are also increasingly providing contractors with access. This development requires role-based differentiated access. For example, a visitor to a hospital requires only standard Internet access to applications like Facebook. A contractor who is responsible for hospital inventory may require access to certain servers that host the inventory supplies applications.

Clearly, mobile Internet access has become integral to the lives of the world's next generation of workers and customers. Creating and implementing a strategy for managing mobile devices in the workplace will be critical to business success.

Security Challenges of Mobile Device Access

Providing network access to mobile devices is nothing new to today's IT administrators. Many products and policies exist to protect sensitive data and the network infrastructure through which it is accessed. But those efforts are not always successful. As noted in the Cisco 2016 Annual Security Report, 50 percent of organizations surveyed believe they are at a high risk for a security breach by the use of mobility.

One major concern is the issue of stolen, lost, or rogue devices. Content security is also another critical concern: Is there appropriate application access, and is the data protected whether it is local or in the cloud? According to the Ponemon Institute in the 2015 State of the Endpoint Report: User-Centric Risk, 75% of companies say their mobile devices were targeted by malware in the last 12 months. Malware attacks are more sophisticated than the basic phishing attacks of 20 years ago. As such, security remains imperative for mobility initiatives.

A world where employees have free rein to use whatever device they wish increases the IT challenge by blurring the line between devices and data that are owned and controlled by a business and those that are owned and controlled by its employees. The ownership of data becomes an especially nebulous and important issue, with far-reaching implications. Should businesses have access to private communications exchanged on a personal device that is also used for work? Do workplace policies that prohibit specific types of content on corporate devices cover a personal device that an employee brings to work?

As corporations begin to embrace an "any device, anywhere" strategy, IT administrators need to address personal mobile devices in the context of a threat landscape characterized by highly sophisticated and sometimes targeted

attacks. They need to know who is on the network, where that individual is, and whether the appropriate resources are being accessed. Obtaining and acting on this information will require multiple departments to collaborate in defining the procedures that make up an appropriate and successful mobile device strategy. Is the team that manages the inventory of PCs allowed to manage the equivalent consumer devices, or not? Questions of this sort must be addressed.

Giving employees the right to use mobile devices in a world without the traditional boundaries that have guarded sensitive data requires a new and far more pervasive approach to security. Establishing the appropriate mobile device strategy begins with business requirements.

Mobility Strategy Starts with Business Strategy

Creating a safe and productive environment begins with understanding the goals of your particular organization with respect to mobile devices. Some businesses have minor security concerns and actively encourage the use of any type of mobile device. In some other businesses, the vast majority of data must be protected with the highest levels of security. Most organizations set up their network access in one of these four categories:

- **Limited:** Typically selected by organizations that require a tight control of information, such as government offices, trading floor operators, and healthcare establishments. The only devices allowed on these networks are supplied by the business. No policy for personal mobile device access is required because these devices never have network access.
- **Basic:** Ideal for organizations that want to offer basic network services and easy access to almost all users. Universities, for example, were very early adopters of BYOD policies because they want students and faculty to access the network and its resources as easily as possible. Public institutions such as libraries also fall into this category. The vast majority of the resources available on these networks are there to be accessed, not protected. The small amount of data that requires protection, such as grades and salary information, can be easily placed on a secure VLAN and protected from unauthorized mobile device access.
- **Enhanced:** This scenario is technically more advanced than the first two, and it requires more differentiated device and user access and a wide range of security policies. Healthcare establishments are good candidates for this category; consider an example where doctors are able to access highly secure patient records with tablets while visitors have guest access to the Internet only. A virtual desktop infrastructure (VDI) is useful for this purpose because it excels at simplifying management and providing a controlled experience for users by making individual device characteristics transparent to the network.
- **Next-generation:** Organizations in this category are creating environments that encourage mobile device use and generate benefits from that use. In this scenario, for example, a retail business could take advantage of a mobile device application to provide customers with a more enjoyable and informative shopping experience. Other businesses can also benefit from this level of mobile device acceptance.

Network Architectures for Mobility

After an organization decides which mobility policy makes sense for it, it can build an infrastructure that supports that policy. One of the first things to consider is whether the business policy with regard to mobile devices is best served through a point-solution approach or through an overall architecture.

Point Solutions

Many vendors advocate the point approach. Wireless solutions, for example, are an important aspect of integrating mobile devices into a network. Security requires a governance model for the mobile endpoints. The networked devices must also be managed. Mobile device management (MDM) vendors offer a variety of co-managed

inventory, asset, and security products. Virtualization vendors offer a different approach, based on the concept that it can be difficult to truly control information on an endpoint. Virtualization solutions keep all data and applications in the data center and provide VPN access for the device.

In reconciling point-product solutions with the business side of a mobile device strategy, it is important to look at the overall goals that the organization is trying to achieve with increased mobility and a BYOD environment. Certainly, security is important. And, management of the devices is important. But transcending the importance of a single-point solution requires the confidence to embrace the any-device phenomenon at an appropriate level, with the flexibility to evolve that strategy, and with a network architecture that can easily adapt to changes in the strategy.

Architectural Approach

Regardless of the level of access that a business elects to offer mobile device users, the network itself is the first point of intersection where IT administrators can actually see and differentiate what a device is, who owns it, and what it should be allowed to do. With that visibility, the entire lifecycle management of that device becomes viable and auditable.

An architectural solution can encompass all the capabilities of point products in a potentially more efficient integrated fashion that provides network-level visibility and control. The expanded visibility and control can be used to support business-level policies that support specific organizational goals.

The building blocks of an integrated network architecture that supports a mobile workforce are access policy, security, and management. The network connects every element of mobility and the BYOD environment. The access policy defines what the organization is trying to accomplish by empowering their users with mobile device access. The security element controls fundamental data security and provides risk mitigation. Given the extent of today's threat landscape, the architectural approach delivers unmatched visibility and continuous advanced threat protection across the entire attack continuum - before, during, and after an attack - while minimizing complexity. The management component encompasses how devices are managed and how that management relates to network security, policy, and day-to-day operations.

The Cisco BYOD Smart Solution

The Cisco BYOD Smart Solution is a comprehensive offering that helps organizations to support a BYOD network at a business-appropriate level. It provides end-to-end BYOD lifecycle management with highly secure data access and a highly productive end-user and IT experience that accommodates a broad set of work styles and application needs. The solution protects data with a unified policy, delivers an uncompromised experience with powerful collaboration tools, and simplifies operations with proactive management. As part of the Cisco Mobile Workspace strategy, every component of the Cisco BYOD Smart Solution is fully compatible with Cisco network infrastructure products.

The Cisco Mobile Workspace comprises integrated offerings that combine market-leading Cisco and partner products and technologies in business-enabling configurations. All Cisco Mobility Workspace solutions are fully tested, documented, and supported by Cisco Professional and Technical Services or services from Cisco partners. They are to be deployed concurrently on a common technology framework, providing cumulative business and IT benefits.

The Cisco BYOD Smart Solution includes the following components:

- **Workspace management** provides a simple single-pane management interface for any workspace experience.
- **Secure mobility** protects devices, data, and applications from malicious activity and unintentionally harmful end-user actions in a continuous manner.
- **Policy management infrastructure** delivers unified and consistent policy definition and enforcement across wired, wireless, and remote networks.
- **Core infrastructure** provides next-generation wired and wireless networks that support reliable access to critical resources.
- **Collaboration** allows for cooperative work scenarios with next-generation tools.
- **Cisco Validated Designs and Cisco Services** speed the deployment of workspace and business services and reduce the risks of an evolving infrastructure.

Securing the BYOD Environment

Cisco is uniquely positioned to meet the fundamental need for comprehensive BYOD security. The security components of the Cisco BYOD Smart Solution are:

- Policy-governed unified access infrastructure
- Efficient and transparent security
- Simplified management

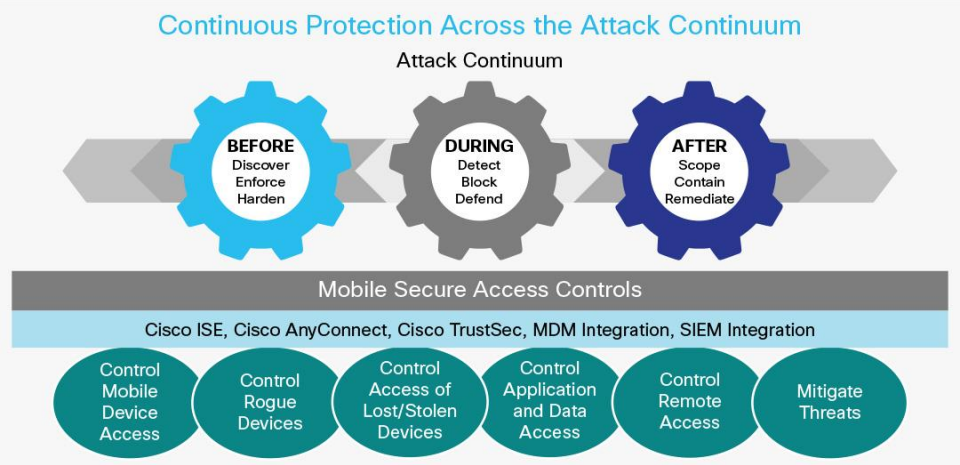
Policy-Governed Unified Access Infrastructure

A policy-governed unified access infrastructure helps ensure highly secure access to data, applications, and systems with high-performance connectivity for every device. Cisco is the only vendor to offer a single source of policy across the entire organization for wired, wireless, and VPN networks, dramatically strengthening security and simplifying network management. Cisco products that support BYOD policy management include:

- **Cisco Identity Services Engine:** The Cisco Identity Services Engine is a unified policy-based service enablement platform that helps ensure the corporate and regulatory compliance of network-connected devices. It gathers real-time contextual information from networks, users, and devices and makes proactive governance decisions by enforcing policy across the network infrastructure. Policy decisions are based on who is trying to access the network, what type of access is requested, where the user is connecting from, when the user is trying to connect, and what device is used. The ISE minimizes IT disruption with zero-touch onboarding that allows a user to easily self-register a device. Its device-agnostic approach accommodates any personal or IT device type. Cisco ISE also integrates with a broad set of MDM and mobile application management (MAM) partners for mobile device security and with security information and event management (SIEM) partners for faster and more accurate threat defense.
- **Cisco AnyConnect® Secure Mobility Client:** Cisco AnyConnect Secure Mobility Client uses enhanced remote-access technology to create a highly secure network environment for mobile users across a broad set of mobile devices. As mobile workers roam to different locations, an always-on intelligent VPN enables the Secure Mobility Client to automatically select the most optimal network access point and adapt its tunneling protocol to the most efficient method.
- **Cisco TrustSec® technology:** Network-embedded Cisco TrustSec technology provides identity-enabled network segmentation and network access enforcement using plain-language policies that map to business requirements. It lowers the total cost of ownership (TCO) by providing scalable and easy-to-change network segmentation, makes use of the existing network infrastructure, and simplifies security management by eliminating manual configurations and complexity.
- **Cisco Intelligent Network:** The Cisco Intelligent Network portfolio of wired products includes Cisco Catalyst® and Cisco Nexus® switches and the Cisco Integrated Services Routers (ISRs). These products provide cost-effective high availability, performance, and security. The wireless infrastructure consists of wireless access points that deliver wired network performance and reliability to wireless devices.

This access layer is a critical line of defense across the entire threat continuum.

Figure 1



Before

Cisco ISE is the brains behind discovering and stopping any inappropriate mobile access. ISE determines the appropriate access based on real-time contextual information from MDM solutions (for example: Is the device registered? Does it have PIN lock? Disk encryption?). ISE enforces the centrally created mobile access policy across the network. ISE also finds mobile devices that may not be registered with MDM vendors. AnyConnect® provides highly secure remote access and redirects any web traffic to Cisco's web security cloud services protect the network from a top source of threats. Making sure that the right person and the right device get to the right IT assets starts the process of protecting applications and data - as well as setting a level of trust.

During

Unfortunately, in today's threat landscape, malware can get through a network even if we minimize the threat vector. With SIEM partners, ISE also works to detect malware and defend the network during an attack. The powers of both bring together the networkwide security events with relevant identity and device context from ISE. This additional identity insight does not require the security professional to translate or cross-reference IP addresses. It facilitates a quicker and more accurate remediation of the mobile threat.

After

If a threat does enter the network, one needs to determine the potential damage and then contain and remediate it. Here is where the embedded Cisco TrustSec technology steps in. This unique tagging technology can enforce the centralized access policy from ISE and contain a threat in a particular network segment. This capability means that the network enforces the policy. We do not need yet another dedicated enforcement device (a point-in-time appliance). Security is woven into the network to increase efficiency and efficacy.

More Efficient and Transparent Security

As a leading provider of networks and mobile device infrastructures, Cisco is uniquely positioned to guide the future of mobile security. Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive portfolios of advanced threat protection solutions and services that are integrated, pervasive, continuous, and open. Cisco provides comprehensive security for mobile devices by combining products such as firewalls, web and email security software, and intrusion prevention systems. The result is intelligent security enforcement from mobile endpoints to the data center and cloud. Network security is transparent to the end user and efficient for the IT department.

Intelligent Cybersecurity

The Cisco intelligent cybersecurity approach addresses the biggest mobile security challenges, covers the entire attack continuum (before, during, and after an attack), and reduces security gaps and complexity. This approach is designed to support the high-level policy creation and enforcement that a BYOD and mobility environment demands while helping to deliver content safely to any device at any location without hampering the user experience. It is based on several core imperatives:

- **Unmatched visibility** to global intelligence with the right context to facilitate informed decisions and immediate action.
- **Consistent control** to enforce policies across the entire network and to accelerate threat detection and response.
- **Advanced threat protection** to detect, understand, and stop advanced malware and advanced persistent threats across the entire attack continuum.
- **Reduced complexity** to provide a platform-based approach that spans the infrastructure, the security appliances, and the cloud with a built-in security services orchestration layer.

Cisco offers a context-aware, network-centric approach to security that supports consistent enforcement throughout the organization, aligns security policies with business needs, provides integrated global intelligence and continuous protection, and greatly simplifies service and content delivery. Organizations can give their employees a flexible endpoint-device choice and various access methods while providing always-on, persistent security for local, VPN, and cloud-based services. In addition to protecting the network at the access layer, Cisco's end-to-end approach offers a robust security portfolio to further close the network's vulnerability to threats.

Network Security

The Cisco portfolio of network security solutions includes proven next-generation firewalls with firewall, intrusion prevention, and advanced threat protection technologies:

- The **Cisco ASA 5500 Series** offers next-generation firewall capabilities to provide highly secure, high-performance connectivity and protects critical assets for maximum productivity. It scales to meet the needs of branch offices to data centers, protecting physical and virtual environments. Available in standalone appliances, in virtual form factors, and as a module for the Cisco Catalyst 6500 Series Switches, Cisco ASA solutions provide comprehensive, highly effective intrusion prevention, high-performance VPN and remote access, and optional antivirus, antispam, antiphishing, URL blocking and filtering, and content control.
- **Cisco FirePOWER IPS** protects the network from common threats such as directed attacks, worms, botnets, and SQL injection attacks for demanding enterprises. Cisco IPS solutions also include appliances; hardware modules for firewalls, switches, and routers; and Cisco IOS® Software-based solutions.
- **Cisco Advanced Malware Protection** is the industry's broadest portfolio of integrated Advanced Malware Protection (AMP) solutions. You get continuous visibility and control to defeat malware across the extended network and the full attack continuum - before, during, and after an attack. AMP is available as an integrated capability spanning FirePOWER network security appliances, endpoint protection for PCs, and Cisco Web and Email Security. For mobile and virtual systems, AMP offers flexible deployment options and extensive coverage to close ever-expanding attack vectors.
- **Cisco Umbrella Roaming** is a cloud-delivered security service that is incorporated into the Cisco Firepower NGFW through a Cisco AnyConnect® client. By providing protection at the DNS layer, Umbrella

Roaming allows you to block threats before they reach your laptops. Plus, security is enforced everywhere with no additional agents required. Umbrella Roaming provides the simplest way to protect users anywhere they go, even when the VPN is turned off.

Content Security

The Cisco Content Security portfolio encompasses web security and email security.

- **Cisco Web Security** addresses the latest web security risks by combining innovative technologies, including acceptable-use policy controls, reputation filtering, malware filtering, data security, and application visibility and control in an on-premises solution. As a cloud-delivered service, Cisco Web Security requires no hardware or up-front capital costs for maintenance and provides exceptional real-time web threat protection. Many Cisco security products offer redirects to the web security services for additional protection.
- **Cisco Email Encryption** technology allows you to safely connect, communicate, and collaborate through email, using their existing applications. It satisfies compliance requirements, combines universal accessibility (send and receive on any email platform) with ease of use (no client software), and is proven in mission-critical deployments of up to 30 million recipients. The simple, two-step implementation gets you up and running in minutes, optimizing IT staff time.

Cisco Desktop Virtualization

Cisco Desktop virtualization delivers the next generation virtual workspace which includes all the applications, content, communication and collaboration services workers need to do their jobs well. It helps IT provide an exceptionally flexible and highly secure converged infrastructure for an uncompromised user experience. To help ensure more protection, access to data center resources with user segmentation and context-aware policy enforcement is provided at the virtual machine level, so data is not stored in the more vulnerable user devices.

Simplified Management

Providing BYOD and mobility access with a high degree of security requires comprehensive yet easy-to-use management. IT administrators need extensive visibility into mobile device activity to accelerate troubleshooting and to free up time for strategic operations. The Cisco BYOD management platform and MDM partner solutions give IT administrators high-productivity BYOD control across the enterprise.

- **Cisco Prime™ solutions:** The comprehensive Cisco Prime management platform delivers converged user access and identity management with complete visibility into endpoint connectivity, regardless of device, network, or location. This extensive visibility speeds troubleshooting for network problems related to client devices, which is a common customer pain point. With Cisco Prime technology, IT administrators can also monitor endpoint security policy through integration with Cisco ISE. Compliance visibility includes real-time contextual information from the network, users, and devices across the entire wired and wireless infrastructure.
- **MDM solutions:** To protect data on mobile devices and help ensure compliance, Cisco is partnering with the MDM vendors AirWatch, Citrix, Good Technology, IBM, MobileIron, and SAP. MDM vendor partnerships provide IT administrators with endpoint visibility, the ability to enable user- and device-appropriate applications, and policy-based control over endpoint access to support company-defined compliance requirements. Cisco works closely with MDM vendors to merge inventory and security control products with Cisco network onboarding and access control. MDM tools alone, for example, can recognize a device such as an iPad and provide connectivity, but they cannot determine when the device affects the managed

environment. Working with MDM partners, Cisco can provide a dashboard on which an IT administrator can see which assets are actually under MDM, which are not, and which are under MDM but are not compliant. Joining forces with MDM partners creates a comprehensive, industry-leading solution.

Benefit from the Mobile Device Phenomenon

For some government offices and financial institutions, allowing employees to access the business network with a personal device may never be appropriate. That in itself is an important mobile device policy. But for most businesses, a suitable level of mobile device use is vital to supporting the efficient mobile workspace that competitive success demands. Integrating mobile device technology into the workspace can provide:

- A more collaborative and productive workforce powered by familiar applications and services available on the devices they choose
- A platform for continuing, cost-effective business innovation
- An IT model for meeting new business demands with lower risk, improved ROI, and investment protection

The Cisco BYOD Smart Solution provides the highly secure access and policy-based management needed to make personal mobile devices an integral part of today's workspace. The Cisco BYOD Smart Solution, along with the Cisco VXI Smart Solution, power the Mobile Workspace. With Cisco policy-based, highly secure, and easily manageable solutions, organizations can integrate personal devices into the workspace and safely take advantage of the mobile device trends that are shaping the competitive landscape to enhance collaboration, productivity, and business success.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-716658-01 06/14