Secure Network Access for Personal Mobile Devices

What You Will Learn

People around the globe are enamored with smartphones and tablet computers, and 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 to an efficient, productive workspace
- The technical and business challenges of securely integrating personal devices into the enterprise network
- Business strategies for a "bring your own device" (BYOD) environment
- Point versus architectural network options and related products
- The Cisco® BYOD Smart Solution

Embracing Mobile Devices

It's difficult to go anywhere today without seeing people using their personal mobile devices. According to the 2011 *Cisco Connected World Technology Report*,[1] 66 percent of students and 58 percent of employees cite a mobile device such as a laptop, smartphone, or tablet as the most important technology in their lives. And one of every three college students and young employees believes that the Internet access those devices provide is as important as air, water, food, and shelter.

With users increasingly captivated by the possibilities of mobile network access and the growing number of available applications, it's no surprise that mobile device use has extended into the workplace. 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 line between work devices and personal devices, and business and personal data, is blurring.

The 2011 *Cisco Connected World Technology Report* states that 66 percent of employees expect to be able to use personal as well as corporate devices while in the workplace. Mainly influenced by students from China (94 percent), Spain (88 percent), and Brazil (86 percent), the report also found that most college students believe that because work time often blends with personal time, company-issued devices should be available for personal use.

Clearly, many people feel that the ability to connect to the Internet at a time and place and with the mobile device of their choosing is extremely important. And that belief has contributed to a new definition of the traditional workspace that transcends desktop computers and laptops.

---

[1] *The Cisco Connected World Technology Report, September 2011.*

Today's workspace concept includes the many resources that help make employees productive and efficient. Employees expect those resources to provide access to intellectual property, stored documents, and internal websites with sufficient bandwidth, storage, and processing power to accomplish tasks quickly and effectively. Cisco refers to this collection of capabilities as the Unified Workspace.

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 in competitive success. According to the *Connected World Technology Report*, approximately half of surveyed employees worked between two and three extra hours per day when they were provided access to corporate networks, applications, and information outside of the office, while a quarter of surveyed employees worked an additional four hours or more.

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 consumer devices provide an increasingly cost-effective and attractive way to keep employees engaged and productive, IT must remain vigilant about ensuring an appropriate experience and protecting the network and corporate intellectual property. According to a 2012 Forrester study of more than 325 global senior IT executives, security was the top concern for BYOD initiatives.[2]

Many organizations are now struggling to securely introduce personal mobile devices into the workplace. A 2012 Economist Intelligence Unit research program sponsored by Cisco found that half of respondents cited corporate security and risk concerns as the biggest obstacle to implementing BYOD.[3]

With mobile Internet access integral to the lives of the world's next generation of workers, 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 via 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. According to the *Cisco Connected World Technology Report*, 7 of 10 employees admitted to knowingly breaking IT policies on a regular basis, and 3 of 5 believe they are not responsible for protecting corporate information and devices.

A world where employees have free reign to use whatever device they wish increases the IT challenge by blurring the line between business-owned-and-controlled and employee-owned-and-controlled devices and data. 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, the location of that individual, and whether they are accessing the appropriate resources. Obtaining and acting on this information will require multiple departments to collaborate in defining the processes and procedures that comprise an appropriate and successful mobile device strategy.

---

[2] Next Generation Workspace Will Evolve Around Mobility and Virtualization; A Forrester Consulting Paper commissioned by Cisco, June 2012.
[3] Data Access in a Mobile Universe: An Economist Intelligence Unit research program sponsored by Cisco, July 11, 2012.

Does the team who owns inventory management of PCs own the equivalent on consumer devices, or not? These sorts of questions must be addressed.

Allowing employees to securely 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.

BYOD Strategy Starts with Business Strategy

The process of creating a safe and productive BYOD 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 fall into the following four categories:

- **Limited:** Typically selected by organizations that require 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 personal mobile device access policy 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 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 to be 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 and 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 would be able to securely access patient records with tablets while visitors would have guest access to the Internet only. Virtual Desktop Integration (VDI) is useful for this purpose as it excels at simplifying management and providing a controlled experience for users by making individual device characteristics transparent to the network.

- **Next-generation:** Organizations under 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. Businesses can also benefit from this level of mobile device acceptance.

Network Architectures for BYOD

Once an organization decides which BYOD policy makes sense for them, they can build an infrastructure that supports it. 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 approach.

Point Solutions

Many vendors advocate the point approach. Wireless solutions, for example, are an important aspect of integrating mobile devices into the network. Once a device is configured into the network, security becomes important. Security requires a governance model for the mobile endpoints. The secure, networked devices must also be managed. Mobile device management 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 virtual private network (VPN) access to 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 BYOD. Certainly, security is important. Certainly, management 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 mobile device strategy changes.

Architecture 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 the device is, who owns it, and what it should be allowed to do. With that visibility, the entire lifecycle of coping with that device becomes viable and auditable.

An architectural solution can encompass all the capabilities of point products in an 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 BYOD are access policy, security, and management. The network connects every element of BYOD. 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. 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 embraces the Cisco Unified Workspace strategy and allows organizations to support BYOD at a business-appropriate level. It provides end-to-end BYOD lifecycle management with secure data access, and a highly productive end-user and IT experience that addresses a broad set of work styles and application needs. The solution secures data with unified policy, delivers an uncompromised experience with powerful collaboration tools, and simplifies operations with proactive management. As part of the Cisco Unified Workspace strategy, every component of the Cisco BYOD Smart Solution is fully compatible with Cisco network infrastructure products.

The Cisco Unified Workspace includes integrated offerings that combine market-leading Cisco and partner products and technologies in business-enabling configurations. All Cisco Unified Workspace solutions are fully tested, documented, and supported by Cisco Professional and Technical Services or services from Cisco partners. They are designed 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** is 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.
- **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 network resources.
- **Collaboration** allows for cooperative work scenarios with next-generation tools.
- **Cisco Validated Design and Services** speeds the deployment of workspace and business services and reduces 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:

- A policy-governed unified access infrastructure
- Efficient and seamless security
- Simplified management

Policy-Governed Unified Access Infrastructure

A policy-governed unified access infrastructure ensures 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 increasing security and simplifying network management. Cisco products that support BYOD policy management include:

- **Cisco Identity Services Engine:** 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 Identity Services Engine minimizes IT disruption with zero-touch onboarding that allows a user to easily self-register their device. Its device-agnostic approach accommodates any personal or IT device type.
- **Cisco AnyConnect® Secure Mobility Client:** Cisco AnyConnect Secure Mobility Client uses enhanced remote access technology to create a seamless, secure network environment for mobile users across a broad set of mobile devices. The seamless environment makes the VPN experience simpler and more secure for users. 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®:** Cisco TrustSec helps organizations secure their networks and services through identity-based access control. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. Cisco TrustSec can be combined with personalized, professional service offerings to simplify solution deployment and management. The core Cisco TrustSec functional areas are identity-aware user and device access; guest user access and lifecycle management; non-user device discovery; data integrity and confidentiality; monitoring, management, troubleshooting; and professional services.

- **Cisco Intelligent Network Infrastructure:** The Cisco Intelligent Network Infrastructure portfolio of wired products includes Cisco Catalyst® and Cisco Nexus® switches, and Cisco Integrated Services Routers (ISRs). These products provide cost-effective high availability, performance, and security. The wireless infrastructure consists of wireless access points that provide wired network performance and reliability to wireless devices.

Efficient and Seamless Security

As a leading provider of networks and mobile device infrastructure, Cisco is uniquely positioned to guide the future of BYOD security. Cisco provides comprehensive security for mobile devices by combining a context-aware, network-centric, integrated security architecture with security products such as firewalls, web and email security software, and intrusion prevention systems. The result is intelligent security enforcement from endpoints to the data center and cloud. Network security is transparent to the end user and efficient for the IT department.

- **Cisco SecureX framework:** The Cisco SecureX framework is designed to support the high-level policy creation and enforcement that BYOD demands. It 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 greatly simplifies service and content delivery. Integral to SecureX are Cisco Professional and Technical Services that use Cisco intellectual capital and best practices to help plan, build, and manage Cisco security technology solutions that support an organization's business goals. Cisco SecureX helps deliver content safely to any device at any location without hampering the user experience. Organizations can provide flexible endpoint device choice and access methods, while providing always-on, persistent security for local, VPN, and cloud-based services.

- **Cisco Secure Intelligence Operations (SIO):** Cisco SIO is the command center for enterprise threat analysis and mitigation, with more than 500 engineers, researchers, and technicians in 11 different locations. SIO uses Cisco's large network footprint to collect a huge amount of network behavior data, and to transform that wealth of information into proactive threat mitigation.

- **Cisco ASA 5500 Series:** As the proven firewall for more than 15 years, the Cisco ASA 5500 Series provides highly secure, high-performance connectivity and protects critical assets for maximum productivity. It scales to meet a wide range of needs, from branch offices to enterprise data centers. Available in standalone appliances and as a module for the Cisco Catalyst 6500 Series Switch, 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 ASA CX Context-Aware Security:** Cisco ASA CX Context-Aware Security is a modular security service that extends the ASA platform to provide precision visibility and control. The service uses the Cisco SecureX framework to gain end-to-end network intelligence from the local network using the Cisco AnyConnect Secure Mobility Client and Cisco TrustSec solutions. Gaining near-real-time global threat information from Cisco SIO, Cisco ASA CX Context-Aware Security goes beyond the capabilities of next-generation firewalls in its delivery of network intelligence and granular control.

- **Cisco Web Security:** The Cisco IronPort® S-Series Web Security Appliance addresses 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. Cisco ScanSafe Cloud Web Security services deliver software as a service (SaaS), which requires no hardware or up-front capital costs for maintenance and provides exceptional real-time web threat protection.

- **Cisco Email Security:** Cisco Business Email Encryption technology allows customers 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 customers up and running in minutes, optimizing IT staff time.

- **Cisco Intrusion Prevention Systems:** Cisco Intrusion Prevention System (IPS) solutions include appliances; hardware modules for firewalls, switches, and routers; and Cisco IOS® Software-based solutions. Cisco IPS solutions protect the network from common threats such as directed attacks, worms, botnets, and SQL injection attacks.

- **Cisco Virtualization Experience Infrastructure (VXI):** Cisco VXI delivers the next-generation virtual workspace by unifying virtual desktops, voice, and video. It helps IT provide an exceptionally flexible and secure converged infrastructure for an uncompromised user experience. To help ensure more protection, secure access to data center resources with user segmentation and context-aware policy enforcement are provided at the virtual machine level, so data is not stored in the more vulnerable user devices.

Simplified Management

Providing secure BYOD access requires comprehensive, easy-to-use management. IT administrators need extensive visibility into mobile device activity to accelerate troubleshooting and free time for strategic operations. The Cisco BYOD management platform and mobile device management (MDM) partner solutions give IT administrators high-productivity BYOD control across the enterprise.

- **Cisco Prime™:** Cisco Prime is a comprehensive management platform that 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. Cisco Prime also monitors endpoint security policy through integration with the Cisco Identity Services Engine to deliver compliance visibility, which 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 ensure compliance, Cisco is partnering with mobile device management (MDM) vendors AirWatch, Good Technology, MobileIron, and Zenprise. 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 cannot determine when the device impacts the managed environment. Working with MDM partners lets Cisco provide a solution in which an IT administrator can use a Cisco dashboard to 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. Securely integrating mobile device technology into the workspace can provide:

- A more collaborative and productive workforce powered by familiar applications and services available on their choice of device
- 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 secure access and policy-based management needed to make personal mobile devices an integral part of today's mobile workspace. The Cisco BYOD Smart Solution, the Cisco VXI Smart Solution, and the Cisco Remote Expert Smart Solution power the Unified Workspace, which is part of the Cisco "Work Your Way" vision for the enterprise. Work Your Way empowers Cisco customers to unify their resources and people through an intelligent network platform to drive profitable growth and increase productivity.

With Cisco policy-based, secure, 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.