White Paper

# Readiness Assessments: Vital to Secure Mobility

## What You Will Learn

Mobile devices have been proven to increase employee productivity and job satisfaction, but can also pose significant threats from unauthorized or malicious users. A security assessment that examines the policy, security, and management capabilities of your network in the context of mobile devices can help accelerate your transition to a secure mobile environment. This paper discusses:

- The benefits and risks of mobility and "bring your own device" (BYOD) policies
- Questions that can help determine your readiness for BYOD
- Cisco mobility solutions

## Securing Your Network for 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. Increasingly, we want mobility our way and on our terms - anytime and anywhere.

With that understanding, it's no surprise that employees want to use their personal mobile devices at work and wherever they go. And granting that wish has proven to be a cost-effective and attractive way to keep workers engaged and productive. According to the Cisco Connected World Technology Report, approximately half of surveyed employees worked between two and three extra hours per day, and a quarter worked an additional four hours or more, when they were provided access to corporate networks, applications, and information outside of the office.

While the benefits of supporting personal mobile devices at work are clear, many organizations are struggling with the basics of securely introducing these devices into their networks. IT professionals are concerned that the rapid adoption of mobile devices in the enterprise has significantly increased the chance for attack. Mobile OS platforms present new security vulnerabilities to exploit. Fake mobile applications can insert malware. And mobile devices offer more doorways into the network for advanced persistent threats (APTs).

According to a 2012 Forrester study of more than 325 global senior IT executives, security was the top concern for BYOD initiatives.[2] That concern is well-founded: Ponemon Institute estimates that the average cost of a data breach can range anywhere from $1 million to $58 million. The impact can also include damaged corporate reputation or brand, leading to lost customers and market share.

[1] *The Cisco Connected World Technology Report, September 2012.*
[2] Next-Generation Workspace Will Evolve Around Mobility and Virtualization; A Forrester Consulting Paper commissioned by Cisco, June 2012.

But securing a network for BYOD and mobile access is not easy. According to an Economist Intelligence Unit report, there is no such thing as a definitive mobile device security policy. Organizations with revenue of up to $500 million are most likely to have only informal policies, and more than 15 percent of companies with revenues of less than $1 billion say their mobile device policies are inadequate.

Regardless of the adequacy of security policies and preparations, and whether or not those policies sanction mobile device use, IT professionals are legitimately concerned that users will access the network with their personal devices. Understanding the related threat landscape and providing controlled access is vital to ongoing secure network and business operations.

## Is Your Network Safe?

Providing a safe environment for personal mobile device access begins with determining the current level of network security. That is best accomplished by analyzing your mobile device policies, security resources, and management capabilities. Cisco offers solutions that can help strengthen your network security and turn BYOD from a liability into an asset.

### Policy

A policy-governed, unified access infrastructure can help provide personal mobile device users with secure, high-performance access to data, applications, and systems. Consider these questions to determine how strong your network policies are when it comes to mobile devices:

- Can you ensure that users access only appropriate resources throughout the network?
  - Yes
  - No
  - Don’t know
- Can you provide non-employees (guests) with limited access to the network?
  - Yes
  - No
  - Don’t know
- Do you have a strategy to protect corporate-owned data on personal devices?
  - Yes
  - No
  - Don’t know
- Do you allow users to download applications to increase their productivity?
  - Yes
  - No
- Do you want to support the safe use of collaborative tools on personal and IT-provided devices?
  - Yes
  - No
  - Don’t know

If your answers indicate that you lack comprehensive knowledge of how mobile devices are being used to access your network, it is vital that you gain visibility and control of who is trying to access the network, what type of access is requested, where users are connecting from, when they are trying to connect, and what devices are being used. Without this knowledge, you risk unauthorized network access and potential security breaches that can result in data leakage, the viewing of sensitive information by unauthorized personnel, and even a worst-case scenario in which a hacker causes loss of business by tampering with your website.

The Cisco® BYOD Smart Solution offers policy-based service enablement that creates seamless mobile access for users while controlling access to intellectual property. Cisco solutions for access control and enforcement 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.
- **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.
- **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.

### Security

A secure BYOD environment can increase productivity and employee satisfaction. Protecting your network from inappropriate mobile device access by employees, guests, and unauthorized users requires end-to-end, automated security enforcement. Your security solution should provide safe, transparent delivery of any content to any device at any location, in alignment with corporate security policies. Consider these questions to determine the strength of your security resources with regard to mobile devices:

- Do you have endpoint protection on all the devices on your network?
  - Yes
  - No
  - Don’t know
- Do you have and enforce device configuration policies?
  - Yes
  - No
- Can you quickly revoke access granted to any device and possibly remotely delete some or all of the data (and applications) on the device?
  - Yes
  - No
  - Don’t know

- Do you control access for personal devices on the network?
  - Yes
  - No
  - Don’t know
- How do you allow remote access to any device?
  - SSL VPN
  - IPSec VPN
  - SSL and IPSec VPN
  - Remote access from any device is not allowed
  - Don’t know
- Is your network ready to support the performance, management, and security requirements of collaborative applications on mobile devices?
  - Yes
  - No
  - Don’t know

If your answers indicate a lack of comprehensive protection from unauthorized or threatening mobile device access, your network runs the risk of threats, such as web-based malware that is secretly embedded in a user’s browser. Implementing a comprehensive security architecture with flexible endpoint device choice and access methods, along with providing persistent security for devices, can help prevent these attacks.

The Cisco BYOD Smart Solution offers a context-aware, network-centric approach to security that enables consistent enforcement throughout the organization, aligns security policies with business needs, and simplifies the delivery of services and content. Supporting business goals such as an optimized and managed experience that goes beyond BYOD is core to this approach. The result is end-to-end, automated security enforcement that is seamless to end users and supports efficient IT operations. Cisco security products that support BYOD include:

- **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.
- **Cisco ASA 5500 Series:** Cisco ASA 5500 Series firewalls provide highly secure, high-performance connectivity and protects critical assets for maximum productivity. 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, and global threat information from Cisco Security Intelligence Operations (SIO).

- **Cisco Web Security:** The Cisco IronPort® S-Series Web Security Appliance combines 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 lets you safely connect, communicate, and collaborate through email, using your 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.
- **Cisco Intrusion Prevention Systems:** Cisco Intrusion Prevention Systems (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.

### Management

Management capabilities that work closely with security products are critical to maintaining network performance and employee access to information. Comprehensive, easy-to-use management tools can also provide visibility into mobile device activity, accelerating troubleshooting and freeing time for strategic operations. Consider these questions to assess whether your current management offerings provide the capabilities you need for a secure, high-performing BYOD solution:

- Do you have visibility into all the devices on the network?
  - Yes
  - Somewhat
  - No
  - Don’t know
- Can you troubleshoot a wide variety of mobile devices quickly?
  - Yes
  - No
  - Don’t know
- Can you monitor and control mobile device use across your wired and wireless infrastructure?
  - Yes
  - No
  - Don’t know
- Can you quickly enable and disable applications on mobile devices?
  - Yes
  - No
  - Don’t know
- Can you securely and automatically onboard a new mobile device?
  - Yes
  - No

If your answers indicate that you would benefit from management that more specifically addresses BYOD issues, you might wish to consider products that provide high-productivity BYOD control across the enterprise. The Cisco BYOD Smart Solution provides a comprehensive management platform and works with a variety of mobile device management vendors to provide these capabilities. The Cisco BYOD management offering includes:

- **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. Cisco Prime also monitors endpoint security policy through integration with the Cisco Identity Services Engine to deliver compliance visibility across the entire wired and wireless infrastructure.
- **Mobile Device Management (MDM) Solutions:** To protect data on mobile devices and ensure compliance, Cisco is partnering with 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.

## Are You Ready for BYOD?

Protecting your network while you reap the rewards of BYOD requires careful preparation, and the questions in this paper are just a starting point. For a more comprehensive approach, take advantage of a Cisco assessment to fully examine the policy, security, and management issues related to a BYOD environment. This assessment can help you map out potential security risks and identify concerns about the implications of opening your network to mobile devices. Once you understand your needs, you can implement BYOD solutions that provide secure information access to mobile users and safeguard your network infrastructure.

## Get Started Today

For more information about a Cisco BYOD assessment and integrated Cisco BYOD solutions, please visit http://www.cisco.com/go/yourway or contact your Cisco sales representative.

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 C11-716659-00 09/12