White Paper

Readiness Assessments: Vital for Secure Mobility

What You Will Learn

Mobile devices have proved to increase employee productivity and job satisfaction, but they can also pose significant threats when used by 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 highly 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 a BYOD environment
- Cisco mobility solutions

Securing Your Network for Mobile Devices

According to the 2014 Cisco Mobility Research, more than **75 percent of organizations support corporate-issued mobile devices**, and slightly less than 50 percent support BYOD policies. A remote mobile employee is viewed as a competitive advantage for up to 70 percent of the organizations. The main reason organizations support mobility, whether it's for their employees or their customers, is to increase productivity. Mobility can transform an organization's efficiencies and engagement.

Although the benefits of supporting personal or corporate mobile devices at work are clear, many organizations are struggling with the basics of introducing these devices into their networks with a sufficient level of security. IT professionals are concerned that the rapid adoption of mobile devices in the enterprise has significantly increased the chance for attack. Mobile operating systems 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).

In some cases mobile initiatives are placed on hold if security measures are not resolved. The security concern is well-founded: The Ponemon Institute estimates that the average cost of a data breach can be up to $3.5M. The impact can also include damage to the corporate reputation or brand, leading to lost customers and market share.

But protecting a network for BYOD and mobile access is not easy. Fifty percent of the organizations surveyed by Cisco have no mobile strategy, and most have no mobile security strategy. 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 revenue of less than $1 billion say their mobile device policies are inadequate. Recent research from Data Dimension's Mobile Security noted that only 27 percent of the organizations surveyed had a clear mobile policy.

Regardless of the adequacy of security policies and preparations, and whether 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 network and business operations.

Is Your Network Safe?

Providing a safe environment for personal and corporate 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 mobility and the BYOD trend from a liability into an asset.

Policy

A policy-governed, unified access infrastructure can help provide both personal and corporate mobile device users with highly 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:

- Do you have definitive mobile access policy? And can you enforce it?
  - Yes
  - No
  - Don’t know
- Can you ensure that mobile users access only appropriate resources throughout the network?
  - Yes
  - No
  - Don’t know
- Can you provide nonemployees (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
  - Don’t know
- 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 a 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 a loss of business by tampering with your website.

The Cisco® BYOD Smart Solution offers policy-based service enablement that creates mobile access for users while controlling access to intellectual property. Cisco solutions for access control and enforcement 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.
- **Cisco AnyConnect® Secure Mobility Client:** Cisco AnyConnect Secure Mobility Client uses enhanced remote-access technology to create a transparent, highly secure network environment for mobile users across a broad set of mobile devices.
- **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 existing network infrastructure, and simplifies security management by eliminating manual configurations and complexity.

Security

A highly secure BYOD and mobile 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 the 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 enforce device-configuration policies?
  - Yes
  - No
  - Don’t know
- Do you have visibility and control of your mobile users’ traffic after they enter the network to enforce acceptable usage and behavior?
  - Yes
  - No
  - Partly
  - Don’t Know

- Can you quickly revoke the 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 any mobile devices (personal or corporate) 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 is not allowed from any device
  - Don’t know
- Do you have protection against Internet threats (the most prevalent threat vector and a critical pathway for mobile devices)?
  - Yes
  - No
  - Don’t Know
- Do you have control during an attack and remediation after it?
  - Yes
  - No
  - Don’t Know
- Is your mobile security pervasive throughout the network and your systems?
  - Yes
  - No
  - 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 and continuous security architecture with flexible endpoint-device choices and access methods can help prevent these attacks.

Cisco offers a context-aware, network-centric approach to security that supports 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 policies is core to this approach. Cisco delivers intelligent cybersecurity for the real world, providing one of the most comprehensive advanced threat protection portfolios of solutions and services that are integrated, pervasive, continuous, and open. The result is end-to-end automated security enforcement that is transparent to end users and supports efficient IT operations. Cisco security products that support mobility and a BYOD environment include:

- **Cisco ASA 5500 Series** firewalls provide highly secure, high-performance connectivity and protect 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 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. Customers 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 Web Security** 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 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 Desktop Virtualization offers additional protection with user access control at the virtual machine level and data is not vulnerable since it is not stored on the mobile device.

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 highly secure, high-performing BYOD solution:

- Do you have visibility into all the devices on the network?
  - Yes
  - Some
  - 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, wireless, and VPN infrastructure?
  - Yes
  - No
  - Don’t know
- Can you quickly enable and disable applications on mobile devices?
  - Yes
  - No
  - Don’t know
- Can you automatically onboard a new mobile device with a high degree of security?
  - Yes
  - No
  - Don’t know

If your answers indicate that you would benefit from management that more specifically addresses mobility and 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™ 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. With Cisco Prime technology, IT administrators can also monitor endpoint security policy through integration with the Cisco ISE to deliver compliance visibility across the entire wired and wireless infrastructure.
- **Mobile device management (MDM) solutions:** To protect data on mobile devices and help ensure compliance, Cisco is partnering with the MDM vendors AirWatch, Citrix, IBM, Good Technology, 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.

Are You Ready for a Mobility and BYOD Network?

Protecting your network while you reap the rewards of mobility and BYOD policies 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 mobile and 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 mobility and BYOD solutions that provide highly secure 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 C11-716659-01 06/14