Cisco Secure BYOD Solution

What Is New?

Q. What is new from security to take organizations beyond BYOD?

A. Cisco is announcing a solution that goes beyond BYOD in enabling you to securely deliver bring-your-own-device (BYOD) computing. The Cisco solution delivers unified security policy across the entire organization and an optimized and managed experience for many types of users with diverse device, security, and business requirements. Cisco is the only provider of a truly experience-focused solution with context-aware set up (on-boarding) and secures access to resources.

The Cisco solution provides the industry's most precise device awareness capabilities, delivering enhanced identity-based security across the entire organization. Innovations in the Cisco Identity Services Engine (ISE) include:

- User self-service setup
- Mobile device management integration for service enablement and more comprehensive policy
- Integrated network-based device sensing and active endpoint-based scanning

Q. What are the benefits to these enhancements? Why should I care?

A. These enhancements offer these benefits:

- Enhanced Cisco ISE: Cisco ISE enables IT to offer mobile business freedom with policy based on when, where, and how users access the network.
- Enhancements improve the user network experience by allowing users to easily self-provision.
- The new device sensor capabilities (integrated on Cisco Catalyst® 3000 and 4000 Series Switches and wireless controllers) offer the industry's most scalable and comprehensive view across the network.
- Real-time endpoint scanning based on policy provides accurate and flexible identification of all devices on the network and current and relevant insight at the network edge.

These automated features result in a better user experience and better security. Cisco is the only vendor to offer a single source of policy across the entire organization for wired, wireless and VPN networks, dramatically increasing organization wide security and simplified management.

- New mobile device management (MDM) partnerships: To protect data on mobile devices and help ensure compliance, Cisco is partnering with multiple MDM vendors AirWatch, Good Technology, MobileIron, and Zenprise. This partnership offers:
  - Greater visibility into the endpoint for IT.
  - Enablement of appropriate applications services based on the user and device.
  - Control over endpoint access based on company-defined compliance policies: for instance, requiring pin lock or disallowing jail-broken devices or implementing remote data wipe on lost or stolen mobile devices.

Cisco uniquely uses the comprehensive context from the MDM solution so that IT has better visibility into and policy controls over BYOD endpoints. Cisco is the only leading vendor to make use of an evolving ecosystem of MDM partners. MDM integration will be available in Q4CY12. As this date approaches, more details will be disclosed.

Q. Why is the Cisco solution better than any other in securing user-owned (any) devices on both wired and wireless infrastructure?

A. The Cisco solution starts with the role of the network. Given the Internet's evolution and the role of the network as a platform for providing comprehensive services such as voice, video, and collaboration tools and for protecting people, businesses, and information, Cisco is uniquely positioned to guide the future of security as a leading provider of networks and mobile infrastructure. Cisco enables organizations to adopt these new market transformations while protecting their business assets, critical services, and employees with the Cisco SecureX Architecture™.

The Cisco SecureX Architecture is a context-aware, network-centric, integrated approach to security that enables:

- Consistent security policy enforcement throughout the organization
- Greater alignment of security policies with business needs
- Integrated global intelligence
- Simplified delivery

The result is intelligent security enforcement from endpoints to the data center and cloud that is transparent to the end user and more efficient for the IT department.

For BYOD, Cisco SecureX gives organizations the capability to provide:

- Flexible endpoint device choice
- Use of all access methods (wired, wireless, and VPN)
- Always-on, persistent security for devices (traditional PCs and mobile devices)
- Cloud-based web security for Internet, intranet, and cloud-based services
- Integration with a unified policy and control system throughout the network

Cisco is the only vendor to offer a single source of policy across the entire organization for wired, wireless, and VPN networks, dramatically increasing organization wide security and simplifying management.

Q. Why is MDM important and what is the value of integration?

A. MDM serves a need similar to patch management for PCs (pushes applications, establishes compliance baselines, etc.). MDM does not differentiate users and devices on the network or apply access controls beyond basic Microsoft Exchange control capabilities. The integration of MDM and Cisco ISE provides comprehensive and flexible network wide policy-based controls over BYOD endpoints. MDM is another source of policy for Cisco ISE to use to increase security and compliance. Discussion of future features after the initial integration is ongoing, and more information will be provided as part of the regular Cisco ISE roadmap.

Q. What are the advantages of the Cisco solution?

A. Cisco offers these advantages:

- Cisco is the only provider of unified policy across wired, wireless, and VPN services integrated into the network with a single management view, helping ensure unique operation efficiency.
- Cisco offers the most comprehensive BYOD solution with diversity of device discovery, profiling precision, and flexible endpoint access control. Cisco is the only vendor to offer network-based sensors and real-time endpoint scanning for new device categories, helping ensure the capability to address a range of BYOD policies.
- Cisco is the only vendor to extend the value of MDM context to the network through a partner strategy. Given the evolving nature of the MDM market, this approach allows Cisco to adapt rapidly as IT explores different BYOD options.

Q. When will the Cisco ISE features announced as part of this launch be available for customers?

A. The BYOD features Cisco announced on March 20, 2012, will be included in future releases later in 2012. These features include user self-service setup and MDM integration.

Q. Who are some of the customers' references to date?

A. Some recent customer references are Diebold, (the ATM manufacturer) Sentara Healthcare and Bowdoin College.

Cisco Secure BYOD Components

Q. Are the products highlighted in the announcement the only products of the Cisco BYOD solution?

A. The Cisco Secure BYOD solution includes other security products. The solution has four main building blocks:

- Unified infrastructure
- Policy enforcement
- Security
- Management

Because enterprise customers are at different stages of BYOD implementation and thus have different policies and priorities, Cisco offers a building-block solution. This solution gives enterprise customers the flexibility to prioritize immediate needs now and the capability to scale later with additional functions.

The unified infrastructure block addresses network access requirements and includes wired and wireless infrastructure products such as:

- Cisco Catalyst switches
- Cisco Nexus® switches
- Cisco Wireless LAN Controllers
- Cisco wireless access points

The device sensors assist in device classification by gathering raw endpoint data from network devices and sending it to Cisco ISE. Cisco ISE then applies the appropriate policies.

The policy enforcement block is central to the Cisco strategy to secure beyond BYOD and addresses the way that enterprise customers implement policy enforcement requirements. Cisco ISE is the main product for this building block and enforces policy based on:

- User authentication
- Device profile
- Device posture
- User location
- Access time and intervals

Cisco ISE is a next-generation context-based identity and access control platform that enables IT professionals to enforce compliance, enhance infrastructure security, and streamline service operations. Cisco ISE enforces security policy on all devices that attempt to gain access to the network.

The security block addresses secure remote access and threat defense. It includes the following products:

- Cisco AnyConnect™ Secure Mobility Client
- Cisco Adaptive Security Appliance (ASA) firewall
- Cisco Web Security Appliance (WSA)
- Cisco ScanSafe Cloud Web Security

Cisco AnyConnect Secure Mobility Client provides the mobile workforce with secure, persistent connectivity and persistent security and policy enforcement.

Remote and mobile users have their web traffic protected whether or not they connect to a VPN server. Without VPN connectivity, all web traffic flows directly to the Cisco ScanSafe data center for real-time scanning to detect inappropriate or malicious content. All communication between an endpoint and the Cisco ScanSafe data center is encrypted to help ensure that no data snooping occurs over public networks.

With VPN connectivity, remote and mobile users use the Cisco AnyConnect VPN Client to establish VPN sessions with the Cisco Adaptive Security Appliance (ASA). The Cisco ASA sends web traffic to the Cisco WSA along with information identifying the user by IP address and user name. The Cisco WSA scans the traffic, enforces acceptable use policies, and protects the user from security threats. The Cisco ASA returns all traffic deemed safe and acceptable to the user.

The management block addresses the management challenge of the BYOD implementation. It covers network management, policy management, and device management. To support this management, the following products and solutions are used:

- Cisco Prime™ Network Control System (NCS): Cisco Prime NCS is a network management tool with a robust GUI that provides network administrators with a centralized solution for policy provisioning, network optimization, troubleshooting, security monitoring, and wired LAN systems management. Cisco ISE is integrated into Cisco Prime NCS to provide monitoring of endpoint security policy. Network administrators gain visibility into compliance based on real-time contextual information from the network, users, and devices across the entire wired and wireless infrastructure.

- Mobile device management: MDM solutions are an important element of a BYOD implementation, and Cisco is partnering with the leading vendors in this area. MDM enables customers to place under management the mobile devices that are accessing their network. They provide onboarding and offboarding capabilities, deliver device and application security, enable full and selective remote wipe capabilities, and provide other features.

Cisco SecureX Architecture is the foundation of the Cisco's security solutions for beyond BYOD.

For More Information

Q. Where can I get more information?

A. For additional information, see SecureX Architecture. http://www.cisco.com/en/US/netsol/ns1167/index.html

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 C67-703415-00 03/12