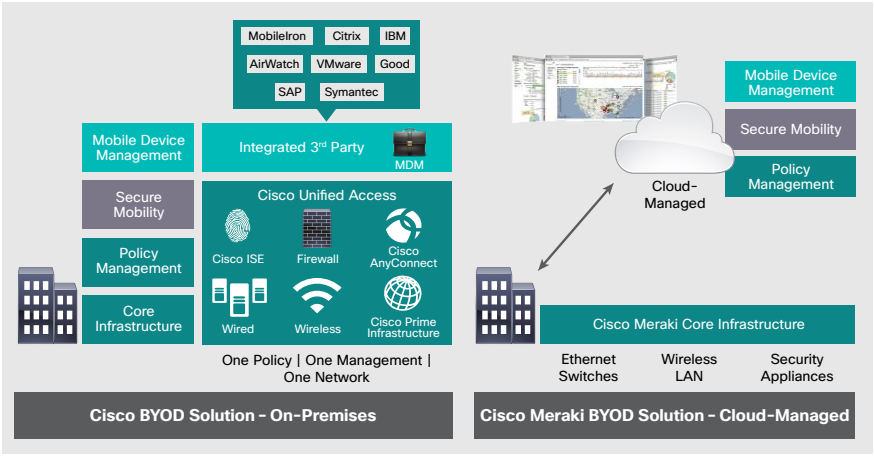
At-A-Glance

Solutions for Secure Mobile Devices



Benefits

For Employees

- **Work the way** you want, using any device on any network to improve work-life balance and increase productivity.

For the Business

- **Adopt agile new business models** to increase productivity, attract and retain talent, and reduce costs.

For IT

- **Simplify operations** by consolidating them in a Cisco "One Policy, One Management, One Network" environment. Use tested end-to-end solutions that let you focus on strategic initiatives instead of mobile infrastructure support.
- **Reduce risk** through highly secure data, application, and systems protections with automated policy enforcement. Take advantage of automatic device registration and integrated management tools, validated designs, end-to-end support, and professional services.

Cisco BYOD Solutions

Workers and organizations alike are embracing the mobile workplace. According to the Cisco® 2014 Mobility Landscape Survey, more than 70 percent of organizations provide corporate-issued tablets and smartphones, while 47 percent offer a bring-your-own-device (BYOD) capability. In both cases, IT must enable the use of mobile devices for improved productivity without compromising security, network performance, and operational efficiency.

Cisco provides both on-premises and cloud-managed solutions that help simplify the highly secure deployment and management of mobile devices in the enterprise.

Mobile Device Challenges

Enterprise mobility presents a myriad of challenges to IT. Network access must scale to accommodate the proliferation of devices and wide breadth of applications used. Access and device policies must be defined and enforced for all authorized devices. Onboarding authorized endpoints should be simple for end users and not resource intensive. With the increasing complexity of this expanded mobile network, IT professionals have their hands full in providing great mobile business experiences for their end users while mitigating security and privacy risks such as malware and the loss of intellectual property.

Cisco Meraki BYOD Solution: Cloud Managed

Built-in BYOD support provided by Cisco Meraki® technology makes it easy to support user-owned and company-issued endpoints – all managed from the cloud. The Cisco Meraki BYOD Solution provides device-based security policies, built-in network access control (NAC), and built-in MDM. This cloud-managed solution helps secure network access and applies device-specific policies from the cloud.

Solution highlights include:

- **Manage tablets, PCs, and Macs:** The Cisco Meraki Systems Manager provides over-the-air centralized management, diagnostics, and monitoring for mobile devices, showing useful metrics and letting administrators lock and erase devices.
- **Enhance wireless performance:** Integrated technology, such as cloud-based automatic RF optimization, Layer 7 application traffic shaping, per-user bandwidth limits, and live monitoring and troubleshooting tools, lets you see and control all the mobile devices on your network.
- **Automatically apply policies by device type:** Device-specific policies can be applied automatically to restrict, quarantine, or throttle devices. Cisco Meraki client fingerprinting technology immediately recognizes iOS, Android, Windows, and Mac devices and lets you apply more restrictive policies.
- **Analyze mobile traffic:** See how many mobile clients have connected, measure their used bandwidth, and see their percentage of total traffic. Network summary reports are automatically delivered to your inbox on a monthly schedule.

Cisco BYOD Solution: On-Premises

The Cisco BYOD Solution is designed to simplify and scale mobile device access by combining best-in-class technology, a validated design, modular building blocks, professional services, and end-to-end support.

The on-premises solution is modular, so you can start with what you need today and add modules as your business needs change, providing investment protection. It has the flexibility to address a diverse set of use cases with multiple deployment options.

Solution highlights include the following:

- **Reliable, scalable core infrastructure:** Based on the Cisco Unified Access™ platform, the solution delivers scalable access to all devices and optimizes the user experiences with gigabit wireless, advanced RF optimization and interference detection, and application identification and classification. Cisco Prime™ Infrastructure management software accelerates troubleshooting by providing a single view into the network.
- **Dynamic policy control with context:** Using the Cisco Identity Services Engine (ISE), the solution delivers unified, consistent, highly secure access control across wired, wireless, and VPN networks. Cisco ISE simplifies business policy management by allowing administrators to easily customize dynamic access controls based on a myriad of contextual data, such as identity, time, device, role, and location – all sensed from the network.
- **Highly secure mobility:** Away from the office, the Cisco AnyConnect® Secure Mobility Solution and Cisco Adaptive Security Appliances (ASA) enable employees to access applications and data over 3G and 4G networks, Wi-Fi, and wired networks with a high degree of security.
- **Streamlined user and device onboarding:** With superior device profiling, Cisco ISE simplifies access by easily onboarding mobile devices the first time they connect, preventing costly IT support calls. Cisco ISE also integrates with a variety of partner mobile device management (MDM) solutions to establish device-compliance policies such as storage encryption or personal identification number (PIN)-lock requirements. Such integrated solutions can also track the device location, remotely wipe devices, and disable features such as cameras and audio recorders.

Next Steps

For more information, please visit http://www.cisco.com/go/byod and http://meraki.cisco.com/solutions/byod.

C45-728052-02 10/14