The Cisco BYOD Smart Solution

SECURITY, FLEXIBILITY, AND PERFORMANCE FOR ANY WORKSPACE

Rising User and Device Demands

Today, organizations have all kinds of devices on their networks. To manage the proliferation of personal devices, Bring Your Own Device (BYOD) policies have moved to the forefront for IT professionals. Users want seamless access to corporate resources no matter which device they use or where that device is connecting from. In addition, numerous types of devices don't have users connected to them – for example, printers. With so many network-connected devices in the enterprise, IT organizations must redefine their roles – and overall network security (Table 1).

As the lines between personal and professional lives continue to blur, security is no longer a question just of how to keep people out; it is also a question of how to let them in. Moreover, new business requirements, such as the need to use collaborative applications, are driving the demand for greater flexibility and more choice, even as users demand the same levels of network performance and security. IT professionals must balance security and enablement so that users can collaborate with confidence.

Table 1. What's Your BYOD Policy?

Policy	Limit	Basic	Enhanced	Advanced
Enforcement	Corporate-only devices	Broad range of device types but access to the Internet only	Multiple device types and access methods	Multiple devices with new services
Example	Financial services company restricts access to confidential financial data	Educational institution allows basic services to everyone (e.g., email)	Healthcare organization offers differentiated services based on role (e.g., email and select corporate data)	Mobile sales enterprise offers videos and collaboration sessions

Providing Optimal Security in a BYOD Environment

Cisco is leading the way in helping companies embrace the BYOD phenomenon. Cisco® solutions empower IT to go beyond simply connecting user-owned devices and securely scale the experience of many users with multiple devices, anytime, anywhere.

The Cisco BYOD Smart Solution delivers unified security policy across the entire organization, as well as an optimized and managed experience for users with diverse device, security, and business requirements. Cisco is the only provider of a truly experience-centric solution that also delivers context-aware onboarding and secure access to resources. It transforms the workspace, resulting in a productive user and IT experience without sacrificing security, visibility, or control.

Core components of a highly secure BYOD solution include:

- 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.

- The Cisco Identity Services Engine is a unified, policy-based service enablement platform that helps ensure the corporate and regulatory compliance of devices connected to your network. It uniquely gathers real-time contextual information from the network, from users, and from devices and makes proactive governance decisions by enforcing policy across the network infrastructure. The policy decision is 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 how (with what device). The Identity Services Engine includes guest posture, device profiling, network access, and mobile device management, and offers simple device registration and onboarding for the end user.
- The Cisco AnyConnect® Secure Mobility Client makes the VPN experience simpler and more secure with enhanced remote access technology. This software includes 802.1X authentication and provides an always-on VPN experience across the industry's broadest array of laptop and smartphone-based mobile devices, including iOS®, Android®, BlackBerry, and Microsoft Windows Mobile® platforms.

- The Cisco Intelligent Network infrastructure includes a complete portfolio of wired, wireless, and VPN access points. Security is uniquely embedded into selected network infrastructure to provide greater visibility and enforcement.
- The Cisco wired infrastructure includes the Cisco Catalyst® and Cisco Nexus® access switch portfolios, which provide cost-effective high availability, performance, and security to your end users.
- Cisco network infrastructure products also include Cisco Integrated Services Routers, which offer unparalleled total cost of ownership savings and network agility through the intelligent integration of security, wireless, unified communications, and application services.
- The Cisco wireless infrastructure simplifies your working environment by combining the mobility of wireless with the performance of wired networks. The new Cisco Aironet® 3600 Series Access Point offers the industry's first 4X4:3 access point, delivering up to 30 percent faster performance than competing solutions, along with exceptional reliability.
- With Cisco solutions, the network acts as a platform to offer services such as video and to protect people and organizations. Cisco's network leadership and expertise sets Cisco apart from other providers in its ability to provide highly secure BYOD environments.
- Once an organization determines its BYOD policy, Cisco network products and the Cisco Identity Services Engine allow you to provision and deliver cross-domain application and network services more securely and reliably in all network environments.

Policy-governed unified access infrastructure creates a highly intelligent network that enables easy business transformations with superior protection.

Efficient and Seamless Security

The Cisco SecureX architecture is a context-aware, network-centric approach to security that enables consistent security enforcement throughout the organization, greater alignment of security policies with business needs, integrated global intelligence, and greatly simplified 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 the end user and more efficient for the IT organization.

Cisco helps to ensure safe delivery of any content to any device at any location without hampering the user experience. Cisco SecureX Architectureenables organizations to provide flexible endpoint device choice and access methods, while providing always-on, persistent security for devices. This includes cloud-based web security for devices browsing the Internet or accessing cloud-based services, automatic VPN connections using common protocols such as Secure Sockets Layer (SSL) and IP Security (IPSec), and integration with network role-based access.

The Cisco Difference

- Unique approach that uses the network and global threat intelligence
- Single source of policy for the entire organization: wired, wireless, or remote networks; physical or virtual devices
- Broadest mobile device OS support through Cisco AnyConnect VPN software, including iOS, Android, and Windows Mobile
- Deepest, broadest, and most accurate device knowledge with the only network- and endpoint-based awareness, ensuring scalability
- Scalable and flexible next-generation enforcement mechanism using existing identity-aware infrastructure
- A modular approach that spans the spectrum of use cases with the freedom to add functionality as needed, fully leveraging the existing infrastructure
- Simple end-user onboarding and device registration to ensure end-user and IT productivity
- Secured and encrypted wireless data from the device to the controller, delivering more protection and compliance
- Highest-performance, highest-quality wireless infrastructure: up to 30 percent faster compared with the competition, delivering the best user experience
- Optimized experience for virtual and native desktop infrastructure
- Unified management across wired and wireless and policy
- Industry's first standards for supporting 802.11r fast roaming and 802.11u cellular and Wi-Fi roaming

Policy and Enforcement

Cisco solutions for access control policy and enforcement include Cisco TrustSec® and the Cisco Identity Services Engine.

- The Cisco TrustSec solution provides intelligent and scalable access control that mitigates security risks across the entire network through comprehensive visibility, exceptional control, and effective management. It uniquely builds upon the existing identity-aware infrastructure while helping to ensure complete data confidentiality between network devices.
- The Cisco Identity Services Engine is the industry's only single policy platform for secure access that integrates posture, profiling, and guest services and helps the network make better context-aware access control decisions. The Cisco Identity Services Engine helps IT administrators accommodate an ever-growing array of consumer IT devices while enforcing compliance, enhancing infrastructure security, and streamlining service operations.

Remote Access with Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility Client uses enhanced remote-access technology to make the VPN experience simpler and more secure. This software includes 802.1X authentication and provides an always-on VPN experience across the industry's broadest array of laptop and smartphone-based mobile devices.

Threat Protection

Cisco provides threat protection through the Cisco ASA 5500 Series, Cisco ASA CX Context-Aware Security, and Cisco web security solutions.

- 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 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 the Cisco TrustSec solutions. Also gaining near-real-time global threat information from Cisco Security Intelligence Operations (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 Intrusion Prevention Systems (IPS) solutions provide protection against common threats such as directed attacks, worms, botnets and SQL injection attacks. It helps organizations meet regulatory compliance requirements. Backed by Cisco SIO with intelligence coming from over 700,000 network devices sending current threat information which is analyzed and pushed out worldwide as reputation data and outbreak filters. Cisco IPS include appliances; hardware modules for firewalls, switches, and routers; and Cisco IOS software solutions.
- For web security, Cisco offers several options. 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.

Data Protection

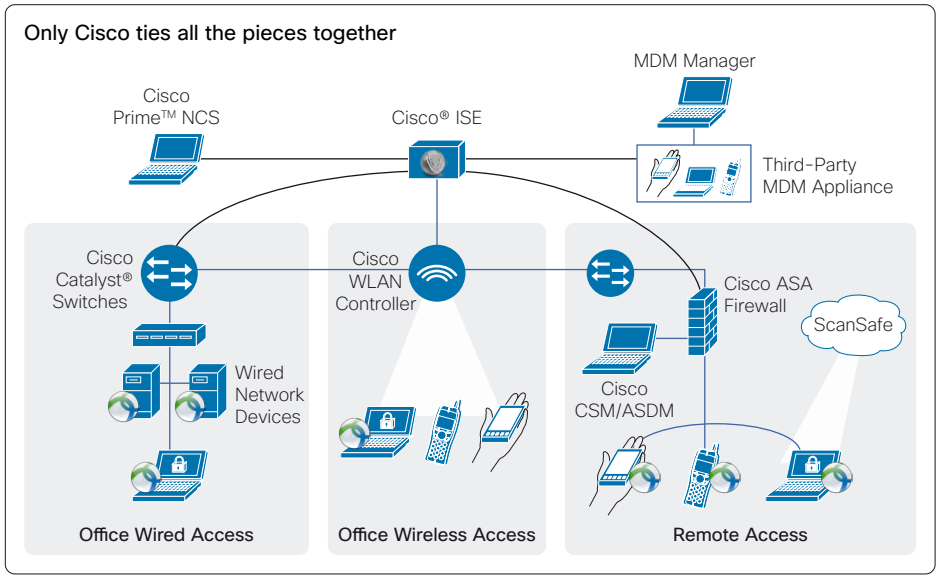
Cisco Virtualization Experience Infrastructure (VXI) delivers the next-generation virtual workspace by unifying virtual desktops, voice, and video. It helps IT provide an exceptionally flexible and secure converged infrastructure for an uncompromised user experience. To help ensure more protection, data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

Simplified Management: Extensive Visibility Accelerates Troubleshooting

Cisco Prime™ Network Control System (NCS) 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 challenge. Cisco Prime NCS also monitors endpoint security policy through integration with Cisco Identity Services Engine to deliver compliance visibility. The visibility includes real-time contextual information from the network, users, and devices across the entire wired and wireless infrastructure.

Figure 1 shows the products included in Cisco's highly secure, end-to-end BYOD solution framework.

Figure 1. Cisco BYOD Solution Framework



Why Cisco?

Cisco is the leader in secure networks and holds a proven track record in network security innovation. The Cisco SecureX architecture uniquely brings together three key elements: a network that provides contextual information and consistently enforces security policies; global threat intelligence; and one of the broadest security portfolios in the industry.

For More Information

http://www.cisco.com/en/US/products/hw/vpndevc/index.html

C45-692412-02 09/12