



Cisco Any Device: Planning a Productive, Secure, and Competitive Future

What You Will Learn

As the traditional corporate network perimeter continues to dissolve and the enterprise becomes more of a borderless environment, smartphones, tablets, other endpoint devices, and web applications are irreversibly changing the way people work and play online. Cisco has embraced the “Any Device” vision, which allows for greater employee choice in devices while maintaining a common, predictable user experience that maintains or enhances global organizational competitiveness, productivity, and security.

Enterprises and large organizations must decide whether to allow or deny certain users, devices, and locations access to company networks, data, and services. Based on real Cisco experiences and results, this white paper discusses the steps and business decisions that information and security officers, enterprise information technology, and information security architects should consider as they begin the journey to Any Device.

Introduction

Every day, 80,000 workers at a global enterprise turn on a range of Windows devices, 17,000 log on to Macintosh computers, 7,000 use Linux machines, and 35,000 check their calendars and email on their Blackberries, iPhones, and Androids¹. The company is Cisco Systems, Inc. Our 70,000+ employees and 30,000+ global contractors, consultants, and business partners decidedly want more choice in the devices they use to work—and where they use those devices to access corporate networks, systems, applications, data, and online services. Although a vast majority of Cisco workers use both a computer and a smartphone to access company IT services, more than 20 percent use more than two devices—and the diversity of those devices is growing exponentially.

As mentioned previously, Cisco has embarked on a long-term vision called Any Device. The goal is to allow greater choice in devices while maintaining a common, predictable user experience that maintains or enhances global organizational competitiveness and security.

The primary business reasons behind the Any Device vision include:

- **Productivity:** Cisco enables tech-savvy employees to use their smartphones, tablets, or laptops of choice to do company work, when and where they want, improving job satisfaction and productivity. **The estimated increase in job-related productivity is 30 minutes per day.**²
- **Evolving workforce:** Members of today’s new technology-savvy generation who are entering the workforce are used to having control of their work tools and environment, and they want to **choose how they can be most productive.**
- **Innovation:** Allowing workers to use new, next-generation devices as soon as they are released may result in further productivity gains. These **early adopters often signal larger marketplace shifts**, which can positively influence Cisco IT adoption and Cisco product strategy.

1. Cisco internal metrics, as of Q2CY11

2. Cisco internal metrics, as of April 2011

- **Acquisition integration:** Cisco's many corporate acquisitions join the fold with their own pools of nonstandard devices. Any Device helps to integrate new divisions quickly and minimize associated security risks. **The estimated cut in acquisition integration time is 17 weeks.**
- **Capital costs:** Cisco employs tens of thousands of contractors and consultants in locations around the world. It is financially unsustainable to provide laptops and smartphones that Cisco owns to this expanding workforce. By migrating contractors and consultants to Cisco® Virtualization Experience Client (VXC) devices, Cisco realizes an **estimated 25-percent annual savings per user**, based upon our existing desktop total cost of ownership.

Other organizations have their own distinct reasons, such as data security, increased mobility, and collaborative work environments, for the necessity of shared access to real-time data. As the choice and number of endpoint devices increase, enterprises must consider what assets they will—or will not—allow to access their applications and data, both within their network and outside it. Then, they need to determine how to plan, track, account for, and enforce those policies.

This paper discusses the risks, rewards, and changes to business, IT, and security policies, the solutions Cisco is currently implementing, and other considerations that Cisco has encountered thus far along its Any Device journey.

Stages of the Cisco Any Device Journey

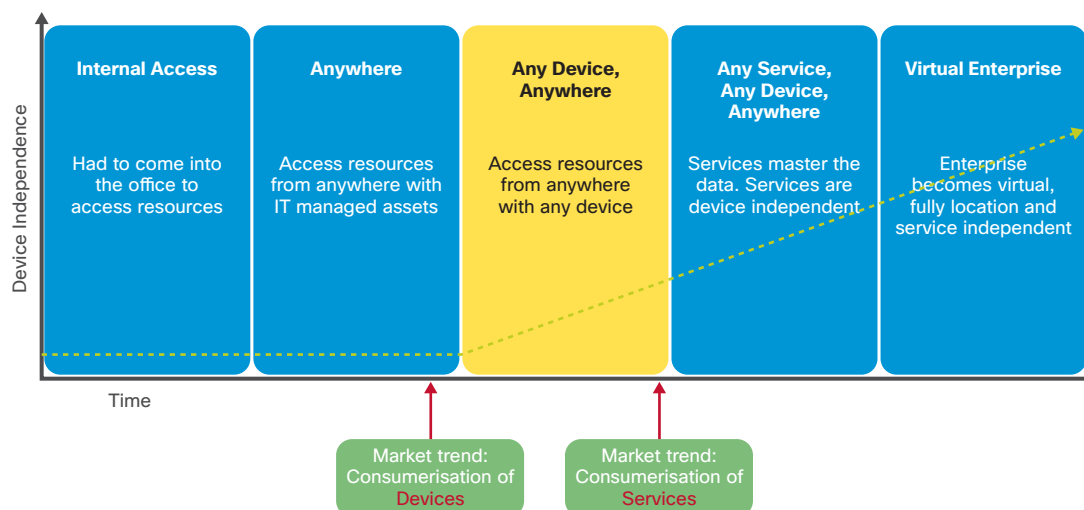
Stage 1: Internal Access

The past 15 years have brought a significant change in the way users access the Cisco network. As the last millennium came to a close, all IT devices resided within corporate locations and employees had to be physically in an office for **internal access** to IT resources, as shown in stage 1 of Figure 1.

Stage 2: Anywhere

Over time, laptops and VPNs gave workers mobility, and an increasingly globalized workforce made more flexible work patterns necessary. Stage 2 depicts how work environments and regular office hours no longer restricted productivity, as a more mobile workforce accessed corporate IT resources from **anywhere**, such as a customer site, home, café, or hotel. This dissolution of location borders enables users to access resources from anywhere with IT-managed assets.

Figure 1. The Stages of Workforce Access Along the Any Device Journey



Stage 3: Any Device, Anywhere

In recent years, the commoditization of smartphones, tablets, and laptops—in addition to outstanding new features, upgrades to functions, more efficient form factors, and shortened device lifecycles—has resulted in employees wanting to use their own devices to do everything from accessing the company email and intranet to using corporate business applications. These factors all came into play in a relatively short timeframe that challenged corporate IT support. Employees who joined Cisco through an acquisition already had been using and wanted to continue to use their own devices for work. Thousands of Cisco extranet partners also required access to certain applications, and providing Cisco IT-managed endpoints was a solution with high capital and operating costs.

Cisco IT recognized the need to embrace the instantaneous use of these next-generation technologies to enable productivity, rather than using the typically historic approach of limiting and managing the deployment of new technologies as they enter the workplace. Further, this rapid adoption of new client technologies has led to the advent and implementation of other enterprise approaches, tools, and technologies that have created communities of users and allowed a transformational change in how IT provides support and end users are able to use the knowledge of peers to solve common problems.

Cisco IT's role within these communities is not to own, but to be part of and contribute as another peer. For example, the introduction of Apple products within Cisco was led initially by users who brought these devices into the environment as their preferred tools and platforms on which to conduct business. An estimated 3,000 Mac users were within Cisco before IT officially made these tools available to the greater population. Independent of IT, Mac users initiated a new effort to provide the required setup, use, and maintenance assistance through email aliases, wikis, intranet, and video content. When Cisco IT began offering the Mac as an option as part of its PC-Refresh policy, IT adopted and supported the self-support model without disrupting or changing the Mac community. IT has embraced this foundation and used it to develop more self-supporting services.

Together, these factors signaled the need for a new corporate device strategy that answered the fundamental yet imperative question: *As device borders dissolve, how can we enable people to access corporate resources from **any device**, and from **anywhere**?*

Not every worker requires the same level or type of access into the corporate infrastructure. Some need only mail and calendaring services on their smartphones, whereas others may require greater levels of access. For example, Cisco sales professionals can access ordering tools from their smartphones, increasing their ability to close a sale. Cisco extranet partners can use their own workstations to access a virtual desktop environment, allowing Cisco to maintain greater control over our corporate assets.

Stage 4: Any Service, Any Device, Anywhere

Cisco currently allows users to access corporate resources housed on-premises. In the future, the consumerization of services—applications, storage space, and computing power—will offer greater flexibility and cost advantages compared to in-house IT services. Some devices and scenarios already require access to external cloud services for corporate transactions (refer to Figure 2). Although this emerging application and service borderless trend is beyond the scope of this paper, the Cisco Any Device strategy is a sound foundation upon which future **Any Service, Any Device, Anywhere** architectures and eventually the Virtual Enterprise can be built.

Stage 5: Virtual Enterprise

The **Virtual Enterprise** is a logical evolution from stage 4, where an enterprise becomes increasingly location- and service-independent, the enterprise has a mature identity model that allows for granular access control and external collaboration, and the full extent of security controls and capabilities is being applied to the enterprise data. The Virtual Enterprise will be addressed as we progress further toward this future state.

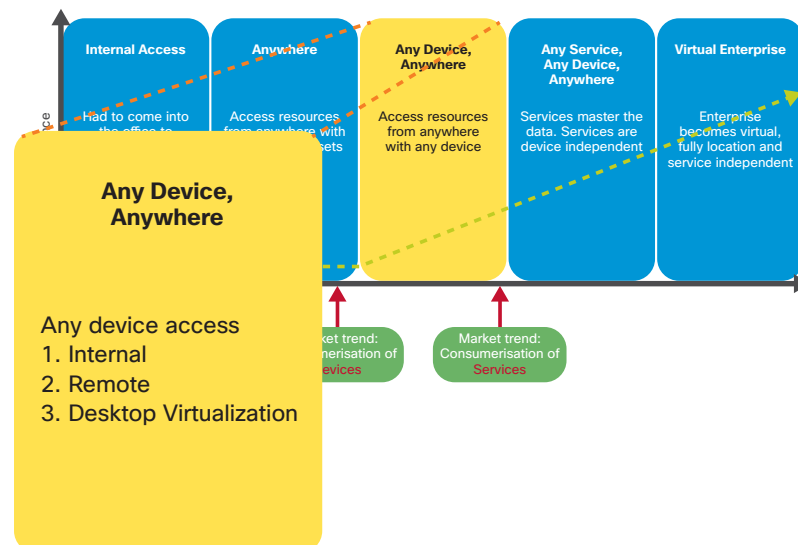
Access on Any Device from Anywhere

This section explores the steps Cisco is taking to come to a more mature Any Device architecture, including how Any Device has challenged traditional security norms, and the solutions Cisco has deployed in our network.

In implementing various Any Device solutions, Cisco focused on three scenarios:

- Remote access
- Internal access
- Desktop Virtualization access

Figure 2. Three Ways to Access the Corporate Network Using Any Device



Remote Access from Any Device

Step 1: Proxy-Based Access from Any Device

The massive adoption of mobile smartphones over the past 5 years increased pressure on Cisco IT to allow access to corporate resources from devices such as Palm, Windows Mobile, Nokia, iPhone, Android, and others. Although offering this access had productivity benefits for Cisco, there were also significant risks (refer to sidebar: “[Potential Any Device Risks](#)”). Cisco opted for a pragmatic approach by delivering a controlled set of services—email and calendar—to mobile devices through proxy-based access. Users can choose their device, while Cisco enforces security policies that maximize data security and confidentiality. For example, users must configure and enter a four-digit PIN to access their email or calendar. Ten failed attempts locks the service, and the connection times out after 10 minutes of inactivity. And if a smartphone is lost or stolen, the worker simply calls the Cisco Helpdesk representative, who can issue a wipe command to the device.

Although this approach may not be foolproof, choosing not to offer this solution would have introduced even greater risks to the organization. As mobile devices continually accessed the corporate network through a wireless LAN (WLAN)—in addition to those who chose access capabilities beyond corporate control, such as Yahoo IM and Gmail—Cisco had virtually no control over our security posture prior to the rollout of this service. By enabling mobile mail access, Cisco provided users with an attractive access package, incorporating simple, but effective, access control. Cisco has currently protected about 35,000 handheld devices³ through this mobile mail access. As Cisco offers new access to other corporate resources through smartphones, the security requirements will increase accordingly.

3. Cisco internal metrics as of May 2011

Step 2: Full Remote Access from Any Device

After Cisco IT implemented the mobile mail services for handheld devices, it addressed upgrading and expanding remote access for all portable devices. Traditionally, remote workers with IT-provisioned laptops accessed the Cisco corporate network using VPNs. However, demand was increasing from workers who wanted to use a variety of Mac, Windows, and Linux PCs, whether IT provisioned them or not. Further, the growing popularity of tablet PCs meant users of these devices also wanted remote access. These requests posed a significant challenge to the Cisco security paradigm of IT-controlled assets.

As a result, Cisco introduced the concept of a “trusted device.” A trusted device can be any type of device, but it must adhere to a certain security baseline to obtain full remote access to the corporate network. Cisco defines a trusted device using the following architectural principles:

- **Device security posture assurance:** Cisco must be able to identify unique devices when they enter the corporate network and link them to a specific user, as well as control the security posture of devices used to connect to corporate services. This capability is a critical one for Cisco incident-management teams.
- **User authentication and authorization:** Cisco requires corporate users to be authenticated. Authentication identifies users while preventing unauthorized access to user credentials. In addition, Cisco prevents the authentication of terminated workers and denies them access to corporate assets and data.
- **Secure data storage:** Activities used for corporate services (for example, reading email, accessing documents, or collaborating using the Cisco Quad™ enterprise collaboration platform) must secure any data stored locally on the device. Users should be able to access and store data on the device without the risk of leaving corporate data behind, a situation that could lead to unauthorized access.

With so many users selecting their own mobile devices and attaching them to the corporate network, the network becomes vulnerable to security holes, putting IT and data assets at risk. Cisco AnyConnect™ Secure Mobility—with its VPN client, web security, and adaptive security appliances—answers this concern by providing an intelligent, transparent, and “always-on” connectivity experience with context-aware, comprehensive, and preemptive security policy enforcement, and secure mobility across today’s managed and unmanaged mobile devices (Figure 3).

Trusted Device Policy

Architectural principles should be translated into technical specifications to guide organizations toward implementable solutions. Trusted devices should comply with the following policy enforcement and asset-management requirements:

Policy Enforcement

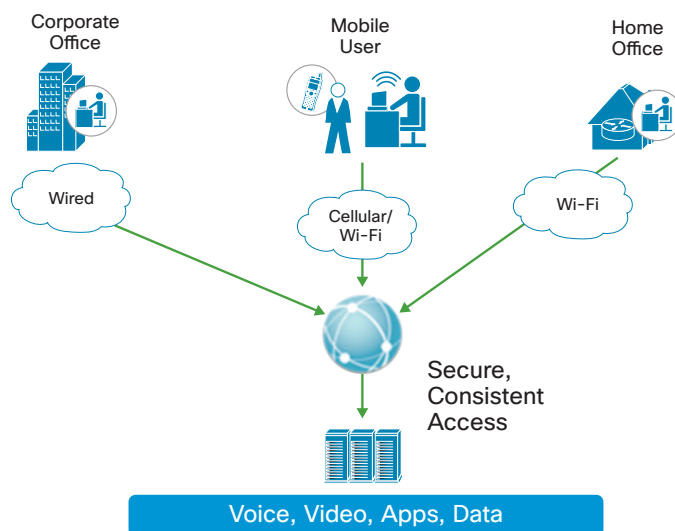
Devices that access corporate services should validate the implementation of the following security controls before connection. Unauthorized removal of these controls should disable access to enterprise resources:

- Local access controls that enforce strong passwords (complexity), 10-minute inactivity timeout, and a lockout after 10 unsuccessful login attempts
- Data encryption that includes device and removable media encryption
- Remote wipe and lock capabilities if an employee is terminated or a device is lost or stolen
- Inventory tracking capability to check the presence of specific security software, patch updates, and corporate applications

Asset Management

Devices that access corporate services should adhere to the following controls:

- Uniquely identifiable where identification is not trivially spoofed
- Explicitly and individually authorized for corporate access, and registered and traceable to a specific user
- Capable of blocking corporate access
- Capable of producing forensic log data (for example, security software logs, user authentication and authorization, and configuration changes) if required for possible investigation

Figure 3. Cisco AnyConnect Secure Mobility

The Cisco AnyConnect Secure Sockets Layer (SSL) VPN client addresses many of the security challenges associated with giving Cisco employees the flexibility to use devices not under IT control or management. Cisco IT allows only registered devices to connect to the network. To make sure a device attempting to establish an SSL VPN session is registered, the Cisco AnyConnect application checks the certificate of the device against its serial number. Requiring device registration also associates the device with a person, aiding security investigations and helping ensure user accountability.

Cisco IT uses Cisco ASA 5500 Series Adaptive Security Appliances to check devices for compliance against corporate security standards. For example, Cisco users cannot establish a VPN connection until they have configured a screen-lock password. The Cisco AnyConnect appliance also helps prevent nonemployees from connecting to the Cisco network using lost devices. If an employee informs Cisco IT of a lost device, Cisco IT can immediately terminate any active VPN sessions and prevent further VPN connections from that device. Cisco IT can also easily terminate accounts of employees who leave the company.⁴ Security on iPhone, Nokia, and Android mobile devices is even tighter because their certificates are distributed by a Mobile Device Management solution. This solution allows more detailed enforcement of security policies, inventory management, and remote wiping of devices if a device is lost or employment is terminated.

Cisco is currently in the process of integrating the Cisco AnyConnect client with the Cisco ScanSafe solution for cloud-based web security and the Cisco IronPort™ Web Security Appliance (WSA) for on-premises web security. These complementary solutions protect users from web-based malware, whether or not they are connected through an active SSL VPN connection. The Cisco ScanSafe solution blocks malware infections, keeping devices—and the corporate network—safe, even if users browse malicious URLs when neither on the network nor connected through a VPN.

Potential Any Device Risks

Organizations should plan to address the following potential Any Device risks:

- Loss of control over corporate data stored on the device, including regulatory or customer data
- Loss of control over device posture:
 - Less control in overall device security potentially increases the risk of exploitation and creates an attack vector to Cisco infrastructure and services
 - Devices may not conform to policy and operational models, potentially damaging business relationships or affecting legal or regulatory requirements
- Less visibility into the devices connected to the network, that is, where they are and who owns and operates them, leads to challenges for security, licensing, regulatory and legal assurance, and audit

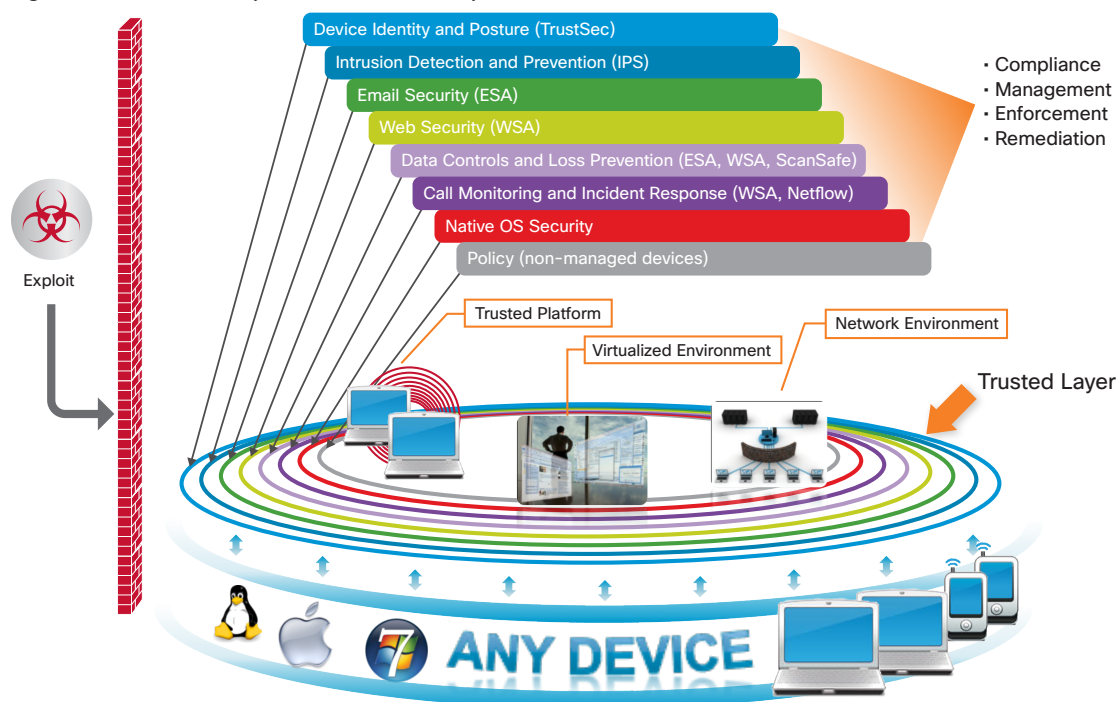
4. Visit www.cisco.com/web/about/ciscoitwork/downloads/ciscoitwork/pdf/Cisco_IT_Case_Study_AnyConnect_Deployment.pdf

Internal Access from Cisco Any Device

Step 1: Focus on Network-Based Malware Controls

A corporate-owned device is an important tool in maintaining corporate data security and integrity. Cisco does an outstanding job of protecting our managed-hosting environments by installing and managing multiple layers of defence on our corporate-owned and deployed computers—including antispam, antispyware, managed antivirus, host-based intrusion prevention, and patch management. However, as Cisco shifts away from managed hosting environments and corporate-owned devices, those same controls must move away from the endpoint and be built into the managed network. Cisco currently uses such tools as the Cisco IronPort Web Security Appliance (WSA), the Cisco IronPort Email Security Appliance (ESA), and Cisco Intrusion Prevention Systems (IPSS) in addition to third-party-developed protection for NetFlow, zero-day malware protection, and event management tools, among others, to protect our network (refer to Figure 4).

Figure 4. Network Security Controls in a Cisco Any Device Environment



A security proxy such as the Cisco IronPort WSA at the Internet edge significantly reduces incoming threats from wired and wireless networks. While satisfying the network security requirements of the Cisco Any Device strategy, the Cisco IronPort WSA deployment also protects the business. In its initial deployment in Cisco Internet gateways in the Eastern United States, the WSA blocked more than 3,000,000 malicious transactions⁵ over a period of 45 days⁶.

The Cisco IronPort ESA is an email gateway with industry-leading threat prevention for spam, viruses, malware, and targeted attacks. It incorporates outbound controls with data-loss prevention, acceptable-use policy enforcement, and message-based encryption. Shifting email security into the network not only protects a variety of devices, it also improves productivity. For example, in one month, the Cisco Ironport ESA blocked 280 million⁷ email messages to Cisco.com addresses—88 percent of the total attempted messages.

5. Including malware downloads, browser hijacking software, unwanted advertisement software, botnet check-ins, and Trojan (backdoor) connections

6. April 14 until May 31, 2011

7. Data from Q1CY11

Cisco also relies on the detection capabilities of Cisco IPS for intelligence monitoring and alerting across our networks. Cisco IT and security can quickly operationalize any intelligence on threats, allowing us to identify and respond without dependency on the endpoint. Because Cisco IPS is available in dedicated appliances or integrated into Cisco firewall, switch, and router platforms, it is deployed in every Cisco location around the world. This coverage allows the Cisco Computer Security Incident Response Team (CSIRT) to act quickly on any incidents that arise across the entire network. As Cisco IT shifts from leased and managed devices to user-provided devices, the ability to closely inspect the network layer becomes paramount. With diminishing visibility into devices, investment should be made in technologies that provide comprehensive, real-time situational awareness of threats at the network layer.

Step 2: Strengthen Device Access Control

In the past, the Cisco CSIRT relied heavily on IT systems—such as inventory, asset management, and host management systems—to link devices involved in incidents to users. If a device had been compromised, the Cisco CSIRT could look it up in hardware and software inventory systems, tie it to a particular user, and communicate with that user to remediate the problem. This solution is not possible in an Any Device world. The Cisco CSIRT has significantly retooled IT systems for the Any Device strategy, for example, linking Dynamic Host Configuration Protocol (DHCP) records and MAC addresses with application login and not device login information to help determine user identity.

In the near future, the Cisco TrustSec® architecture—which provides policy-based access control, identity-aware networking, and data integrity and confidentiality services—will help to solve this problem. Through the 802.1x protocol, the Cisco TrustSec network login identifies users and associates them with their devices. It also enables Cisco to provide differentiated access in a dynamic network environment and enforces compliance for an expanding array of consumer and network-capable devices. For example, Cisco TrustSec technology can take advantage of the trusted device security baseline. When devices are regarded as trusted, they are granted full access to corporate resources on the internal network. Moreover, the Cisco Identity Services Engines (ISE) platform—Cisco's consolidated identity and access-control solution—provides the next-generation architecture for identity and policy management.

Desktop Virtualization Access from Any Device

Mobility and new devices accelerated the Cisco Any Device strategy, and a third factor quickly emerged: How to integrate acquisitions and manage offshore and offsite outsource relationships.

During the past several years, Cisco has acquired numerous companies, whose integration caused challenges for Cisco IT and security organizations. Every acquired company had its own devices and security policies and standards, which were often quite different from those used at Cisco. The Cisco Information Security team was responsible for ensuring that endpoint devices met Cisco policy and standards. There were only two feasible solutions, each with its own set of challenges. The first was to replace acquisition devices with Cisco IT-provisioned and -supported devices, and train workers on their use. This process would result in a costly and lengthy transition that affected productivity for weeks or months. The second option was to keep existing devices in place, but risk lowering the security posture of the entire enterprise. Another solution had to be found.

Corporate policies were also strained by the shift to outsourcing. Fifteen years ago, outsourcing was limited to simple tasks. Today, it occurs in most parts of the organization and can touch many business processes. The current Cisco contingent workforce is greater than 45,000, with 17,000 performing daily activities from 350 third-party locations. Cisco also maintains outsourced partner relationships with more than 200 different third-party companies.

To date, most of the on- and offsite contingent workforce has been provisioned with Cisco IT-supported devices that comply with Cisco policy. For offshore and offsite outsourcing, Cisco IT maintains an extranet infrastructure that supports all third-party network connections. Cisco IT manages 70 percent of all extranet connections end to end, including devices, WAN connectivity, and the remote network at the

third-party location. However, because Cisco outsourcing has increased in volume and complexity, this model no longer meets the time-to-capability and TCO business expectations.

Desktop virtualization, together with the network security capabilities described earlier in this paper, will help overcome these challenges while providing significant benefits (refer to the sidebar “Benefits and Challenges of Desktop Virtualization”). Cisco projects that desktop virtualization will result in a potentially greater than 20-percent cost savings and a 40- to 60-percent increase in time-to-capability for acquisitions and offshore and offsite outsourcing locations. This centralized, fully scalable, location-independent service will also improve data security and device compliancy. Cisco already has begun a desktop virtualization pilot with 2,000 users in the United States, and other global locations will follow later in 2011.

Cisco Lessons Learned

Devising and implementing an Any Device strategy is a significant change for any organization, and such a transformation will be accepted more smoothly and more successfully with a consistent governance structure. Along this enterprisewide Any Device journey, Cisco IT and security professionals have learned many lessons:

- The Any Device journey requires a cross-domain effort from desktop, security, network infrastructure, and communications departments.
- Organizations should recruit a single executive sponsor who assumes responsibility for organizing the cross-functional team, educating executives, and reporting on results and metrics.
- Do not underestimate the amount of effort required to segment your user population and conduct user analysis. This analysis should determine which users are entitled to what services, and should be the first action when starting your Any Device journey.

Organizations make significant investments to comply with applicable regulations for data security, integrity, privacy, and audit. In 2010, Cisco updated its Code of Business Conduct to include usage guidelines for personally owned devices, and the Information Security department is rewriting many of its security policies to become more data-centric. In some instances, however, these investments may contradict the Any Device vision. For example, Cisco employs onsite doctors and nurse practitioners to provide healthcare services to employees. Touch-screen tablets are a valuable tool for these practitioners to take from patient to patient in a healthcare setting, and also to use

Benefits and Challenges of Desktop Virtualization

Desktop virtualization is a computing model that centralizes programs, applications, services, and data. Although the user experience is much the same as a typical computer experience, the data, operating system, and applications do not fully reside on the end user’s device. This computing model—also called Virtual Desktop Infrastructure (VDI)—has many potential advantages:

- Consistent experience: Users enjoy the same interface across all VDI-enabled devices.
- Increase in productivity: Users can access data and applications from any VDI-enabled device, no matter where they are. Often access to applications is faster because the VDI environment is in the data center.
- Lower risk of malware: IT can ensure that applications are kept up-to-date, patches are consistently hardened, and users install the patches.
- Lower risk of data and intellectual property loss: Data is centralized, backed up, and available, even if the device fails or is lost or stolen.
- Faster time to market: Important users, such as acquisitions and partners with their own devices, can be integrated into the corporate environment more quickly.
- Application compatibility: Desktop virtualization can act as a compatibility bridge to run corporate applications in a known operating environment.
- Easier to support: Provisioning a virtual desktop is quicker relative to issuing a new PC, and virtualization lends itself well to a centralized IT support model.

Desktop virtualization may not be a solution for all applications or user communities.

Notable challenges include:

- Unsuitable for certain applications: Today there are challenges with high-bandwidth applications, such as computer-aided design, video, and unified communications.
- Unsuitable for certain devices: The desktop virtualization user experience is not tailored to certain devices, such as smartphones or tablets with small screens.
- Limited platforms: Most desktop virtualization solutions focus primarily on Windows devices.
- High-latency environments: VDI struggles in high-latency network environments.

in conjunction with Cisco TelePresence® conferencing to diagnose and treat patients remotely. However, these tablets are exposed to Health Insurance Portability and Accountability Act (HIPAA) data. Cisco does not allow our healthcare workers to use their personal tablets in this setting, and ensures proper security and data management protocols are followed with only corporate-owned devices.

First Steps Along Your Own Any Device Journey

As Cisco ventured out on the Any Device journey, we identified 13 critical business areas that are affected by this new paradigm. Table 1 spotlights these focus areas and provides a list of questions that have helped Cisco—and can help you as you begin your own journey—to recognize and veer around potential problems and determine how best to approach these considerations as you go. Consider these questions and be meticulously honest in your responses as you set forth on your own journey.

Table 1. Questions to Ask for the Any Device Journey

Business Area	Business Questions to Answer
Business continuity planning and disaster recovery	<ul style="list-style-type: none"> Should noncorporate devices be granted access or restricted from business continuity planning? Should there be an ability to remotely wipe any end device accessing the network if it is lost or stolen?
Host management (patching)	<ul style="list-style-type: none"> Will noncorporate devices be permitted to join existing corporate host-management streams?
Client configuration management and device security validation	<ul style="list-style-type: none"> How will device compliance to security protocols be validated and kept up-to-date?
Remote-access strategies	<ul style="list-style-type: none"> Who should be entitled to what services and platforms on which devices? Should a contingent worker be given the same entitlement to end devices, applications, and data?
Software licensing	<ul style="list-style-type: none"> Should policy change to permit installation of corporate-licensed software on noncorporate devices? Do existing software agreements account for users accessing the same software application through multiple devices?
Encryption requirements	<ul style="list-style-type: none"> Should noncorporate devices comply with existing disk-encryption requirements?
Authentication and authorization	<ul style="list-style-type: none"> Will noncorporate devices be expected or permitted to join existing Microsoft Active Directory models?
Regulatory compliance management	<ul style="list-style-type: none"> What will organizational policy be on the use of noncorporate devices in high-compliance or high-risk scenarios?
Incident management and investigations	<ul style="list-style-type: none"> How will corporate IT security and privacy manage incidents and investigations with non-corporate-owned devices?
Application interoperability	<ul style="list-style-type: none"> How will the organization handle application interoperability testing with noncorporate devices?
Asset management	<ul style="list-style-type: none"> Does the organization need to change how it identifies the devices it owns to also identify what it does not own?
Support	<ul style="list-style-type: none"> What will the organization's policies be for providing support to non-corporate-owned devices?

The Road Ahead

The Any Device journey at Cisco is an ongoing and long-term investment in the future. Over the next several years, Cisco will continue our plan to move important data and applications off of devices and into the network or cloud, strengthen network security, and integrate identity and policy controls on devices as they interact with the network. The next steps of this plan will help address Any Device challenges in the following business areas:

Application Interoperability

Although about 60 percent of the devices currently connecting to the Cisco network are Windows desktops, this percentage is shrinking as the popularity of other devices grows. Moving forward, Cisco will have less control over the type or versions of software installed on devices, increasing the likelihood of interoperability problems occurring between applications, browsers, versions, and runtime environments. The prevalence of web applications has simplified the problem, but not solved it. As the variety of desktops, smartphones, and tablets continues to grow, so does the number of browser environments. Cisco executives have championed a “browser standard” initiative for internal web applications, based upon World Wide Web Consortium (W3C) standards. Industry web development standards facilitate application interoperability in an ecosystem that includes different browsers, operating systems, and end devices.

Cisco is also relying on desktop virtualization to present a compatible operating environment on any operating system. A desktop virtualization pilot, currently numbering in the thousands of users, is planned to be made available to 18,000 workers by July 2012.

Software Licensing

Like most enterprises, Cisco uses asset-management systems to track software licensing. Cisco must address many policy questions regarding Any Device software licensing scenarios, such as:

- Will users be allowed to install corporate software on their own devices?
- Will existing contracts with software vendors allow corporate software on non-corporate-owned devices?
- Will Cisco need to track non-corporate-owned devices, and if so, how?

Cisco is investigating the use of information gathered by Cisco TrustSec technology, such as user identity and MAC address, to implement an asset-management system that tracks all devices, and detailed reporting mechanisms that account for noncorporate hardware and software assets.

Business Continuity Plan and Disaster Recovery

Cisco has workers with company-owned assets working at other companies' locations, and also has many contingent workers working in Cisco offices around the world. Who is responsible for ensuring that data remains secure and intact? Cisco backs up its Windows PCs centrally, but many of our partners do not want their intellectual property backed up to a third-party system. If users are not included in corporate business-continuity services, what other provisions are in place for these users to return to work quickly if an outage occurs? One possible solution is desktop virtualization, which can disassociate sensitive data from devices.

Cisco has begun to manage our user interactions through the network. The company is moving confidently toward a future where fewer applications and data reside on the desktop, using a combination of desktop virtualization and Software as a Service (SaaS) or cloud computing. Some corporate applications or locations will transition to more of a transaction-based approach, where users, actions, and data can be managed, tracked, and backed up consistently. This evolution will lead Cisco IT to an effective and secure “Any Service, Any Device, Anywhere” future state and eventually to the virtual enterprise.

For More Information

Cisco is making significant strides toward implementing an Any Service, Any Device, Anywhere environment for our organization, and we will continue to share our experiences and lessons learned to help you circumvent the problems that may appear during the process. The knowledge and methodology Cisco has used to transform our business and IT environments toward Any Device and beyond can be applied to other organizations large and small.

Speak with your Cisco representative to learn how to position your business, IT, and security infrastructure strategically to prepare for a move to Any Device architectures.

For information about Cisco solutions that enable Any Device, refer to:

- [Cisco AnyConnect Secure Mobility Client](#)
- [Virtualization Strategies](#)
- [Cisco TrustSec technology](#)
- [Cisco IronPort Email Security Appliances](#)
- [Cisco IronPort Web Security Appliances](#)



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C11-681837-00 08/11