Global Knowledge®

Expert Reference Series of White Papers

Understanding Cisco Security Solutions: Are You Ready for a New Era of Risk?

Understanding Cisco Security Solutions: Are You Ready for a New Era of Risk?

Rich Hummel, CCNA, CCNAW, CCSI

Introduction

We've all seen the news pieces where the FBI or the Department of Homeland Security talk about security, and how anyone who sees something suspicious should report it to the local authorities. The Department of Homeland Security has been promoting the security awareness campaign, If You See Something, Say Something™.

After the 9/11 attacks and subsequent terrorist incidents, it became clear that the public needed to increase its level of awareness and proactive response to suspicious activity. In essence, every citizen is being asked to be an extension of the security apparatus. The logic being that the more sets of eyes that are looking for suspicious activities, the increased likelihood of stopping an attack before it occurs.

It's no different in the world of information security. Security is no longer the purview of those individuals who have been specifically trained to install, configure, and monitor firewalls, intrusion detection, and prevention systems and advanced malware protection. Everyone in the IT shop (e.g., collaboration, mobility, storage) needs to have a working knowledge of security threats and the tools available to help mitigate those attacks.

Attacks on private networks have increased in persistence and sophistication. The days of the lone hacker sitting in a basement trying to break into the Pentagon's database for fun are over. Today, there are teams of individuals, both state and privately sponsored, whose sole purpose is to break into corporate or government networks and either steal sensitive data, or deploy malware that will bring those networks to their knees. That malware can be planted into a system and lay dormant for weeks, months, or even years before becoming active.

These facts have changed the security landscape from one of simply detecting threats and preventing network access. Today we have an attack continuum, where protection is required not only before, but during and after, an attack. During the attack, the goal is to limit the impact of the attack. After the attack, data from the intrusion is analyzed and used to prevent future attacks. This continuous feedback loop requires additional resources over the traditional model, and not only resources specializing in security.

Even employees who are not part of the IT staff need to understand their role in protecting sensitive information. Maintaining even the most rudimentary security practices (securing laptops, etc.) can go a long way to preventing security breaches. While convincing sales people, clerical staff, and engineers that they play a pivotal role in securing company data may be a challenge, without it there are significant holes in the company's security profile.

In other words, security is everyone's business.

In this paper we are going to look at security awareness in organizations, types of security threats, security in Cisco training, and Cisco security solutions.

Security Awareness in the Enterprise

Enterprise Management Associates (EMA) conducted a survey of more than six hundred people (non-IT and non-security staff) entitled *Security Awareness Training: It's Not Just for Compliance* that revealed more than fifty-six percent of corporate employees had not received security or policy awareness training from their organizations.

This is a problem because without training, people will do the same things at work that they do at home, only the consequences of their actions can be much more damaging. Clicking on a link in an email can release malware that can infect hundreds of machines in seconds, or open up a path for data theft. These individuals don't even know they're doing anything wrong until someone points it out to them.

Companies need to educate all employees about security threats that they can utilize not only in the workplace, but at home as well. This will allow employees to establish solid security habits that become the rule rather than the exception.

The same EMA study showed that employees have some very bad habits when it comes to security:

- Thirty percent leave mobile devices unattended in their vehicles.
- Thirty-three percent use the same password for both work and personal devices.
- Thirty-five percent have clicked on a link contained in an unsolicited email.
- Fifty-eight percent store sensitive information on their mobile devices.
- Fifty-nine percent have admitted storing work information in the cloud.

The lack of security awareness is obvious. Some basic training that makes all employees aware of their responsibilities towards security can prevent future breaches.

When we consider security in a discussion like this, we tend to think of firewalls, intrusion detection systems, or advanced malware protection. However, these activities are the responsibility of the IT organization, or more specifically, the security specialist(s) in that organization.

Herein lies the problem. In this model, security is always someone else's job. Security awareness is limited to those few IT professionals, and if asked, the vast majority of people in any organization do not consider themselves part of the security infrastructure. If we then consider the fact that the majority of security breaches worldwide are caused by employees who are unaware of their poor security practices, the necessity of a paradigm shift in the way we think of IT security becomes obvious.

Security Awareness and Challenges for Organizations Public and Private

Let's take a look at some different types of organizations other than enterprise and some obvious, or better yet, not so obvious security challenges. Our goal should be to create a level of security awareness in all aspects of our lives so they become second nature, whether at home or on the job.

Families

For families and parents, online safety of children and family members is of paramount importance. In terms of our financial security, it's critical to protect information that could impact our personal finances. By protecting our computers, we protect precious family assets such as photos, as well as videos and music.

We also need content protection on Internet browsers for our children, as well as monitoring their social interactions to ensure their safety. This consideration is no different than in our professional lives. If we understand the need for security awareness in our private lives, it will become a more natural consideration in our professional lives.

Schools

For faculty, staff, and students, the Internet has provided huge learning opportunities as well as risks. Students, teachers, and administrators need to understand how to protect themselves, and must understand the link between the online and "real" world. This may seem strange to some, the need for teaching students the difference between their online world and the real world.

But in today's immersive online content, it is important to constantly define that difference for our children. Learning how to protect computers and engage in appropriate online behavior will reduce vulnerabilities and create a safer online environment.

Small / Medium-Size Businesses (SMBs)

Small and medium-sized businesses face critical challenges due to limited resources and information, as well as competing priorities. The speed at which technology is evolving makes it difficult to stay current with security since SMBs tend to have more limited IT budgets.

However, better security awareness and planning can help these businesses protect their intellectual property and trade secrets, and reduce loss of productivity due to downtime.

State and Local Governments

Local, state, and central governments maintain an enormous amount of personal data and records on their citizens, as well as confidential government information, making them frequent targets.

Yet many government entities are challenged with insufficiently secured infrastructure, lack of awareness, and competing funding and resource priorities. Better security helps government bodies provide reliable services to the public, maintain citizen-to-government communications, and protect sensitive information.

Recently, I was at a conference of IT managers for county and local governments in the state of Texas. During a session focused on data security, it was shocking the consensus agreement that because few applications outside of email were used, there was little need for network security. The misunderstanding of potential attacks through email was astounding.

Security Risks

It's important to recognize the different types of risks that exist in the online world. When online, keep this in mind: *Stop. Think. Connect. Stop* for a moment. *Think* about how you will take care of your information and personal data before acting. *Connect* responsibly.

- **Advanced Persistent Threat (APT):** A concentrated attack by allied hackers focused on a single target. It infects a system and lays dormant and leaves few traces when done. These attacks are generally after the intellectual property of technology companies.

- **Distributed Denial of Service (DDoS):** Typically an attack on an Internet domain. Huge amounts of data flood a system until it is brought to its knees. Legitimate site requests are lost, or the site becomes too slow to function properly. This may not necessarily involve a loss of data, but the cost to its victims is substantial.

- **Cross Platform Malware (CPM):** Malware used to be the concern of those running Windows operating systems. That has changed with the emergence of malware targeting Java, Linux, and OSX.

- **Metamorphic and Polymorphic Malware:** Malware that has the ability to change code as it works its way through a system. Each version of the code makes permanent changes to its code, but each succeeding version functions the same way as the original. The longer it resides on a system, the more difficult it becomes to detect and remediate.

- **Phishing** – It is what it sounds like: A perpetrator is out there looking to catch a fish. You'll receive an email that looks like it's from your bank, or some other trusted party, asking you to visit the party's website to update your personal information. The email will include a link to what you think is its website. It will look exactly like the merchant's website. But if you take the time to look at the URL, it will have nothing to do with the website you thought you were visiting. Once you've entered your personal information, the hook is set and the perpetrator reels you in.

- **Insider and Privilege Misuses / Miscellaneous Errors:** We combine the two here because they are related, the difference being on intent. Misuse of privileges can be by an employee or business partner who is granted privileges and uses those privileges for malicious intent. Errors are can be posting of private information on a public website, or sending information to the wrong recipients.

- **Spyware:** The two important things to know about spyware programs are 1) they can download themselves onto your computer without your permission when you visit an unsafe website and 2) they can take control of your computer. Keep your computer up to date—especially your operating system, web browsers, and antivirus/antispyware protection.

- **Poor Password Management:** Choose strong passwords that are not easy to guess. Avoid your address, pet's name, or a child's name. Think of creating a password by using the first letter of each word of a favorite saying. Substituting capital letters and/or numbers for some of those letters will strengthen the passwords even further. Make sure to change your passwords regularly.

- **Social Media:** Although social media can be a fun experience and helps keep you connected, it can also create an opportunity for information leakage or even compromise personal identity and safety. Be smart with your identity on social media sites. Make sure to review and user privacy settings. Keep all tagged photos private. Do not share information that can help people steal your personal information.

Cisco Certifications and Security

When it comes to certification classes, Cisco does include some security awareness in its basic switch /route classes Interconnecting Cisco Network Devices Parts 1 and 2 (ICND1 and ICND2). Included are basic rudimentary techniques to help secure your network. If we accept our earlier conclusion that the source of many security breaches are employees being unaware that they have poor security breaches, then these techniques are a foundation on which to build an IT staff where all members assume some security responsibility.

Part of the basic networking training (ICND1 and ICND2) is the capability of implementing basic security practices on Cisco devices. The following are some key points to remember about securing devices:

- **Secure Location**: Be sure to locate your routers and switches in a secure location—a locked room where limited access is permitted. Physical security is often overlooked, even though it is the most basic of security techniques. Biometrics and card access should be required for hardware managing the most sensitive data.
- **Disable Ports**: In high-security environments, unused ports should be disabled so that unauthorized systems cannot connect to the network.
- **Configure Port Security**: To better manage enabled ports, port security should be configured to limit which MAC addresses have access to those ports.
- **Set Passwords**: Be sure to configure passwords on the console port, auxiliary port, and the vty ports. Also configure the enable secret for access to priv exec mode.
- **Login Command**: Do not forget the login command after setting the password on the port. The login command tells the Cisco device that anyone connecting must log in and forces the prompt for a password.
- **Login Local Command**: If you are looking to create usernames and passwords for login, then use the *login local* command to tell the Cisco device you wish to authenticate persons by the usernames and passwords configured on the device.
- **Encrypt Passwords**: Be sure to encrypt all passwords in the configuration with the *service password-encryption* command!
- **Banners**: Be sure to configure banners that do not have the word *welcome* in the message or any other inviting phrases. You want to make sure that the banners indicate that unauthorized access is prohibited.
- **Secure Communication**: If you are looking to remotely manage the device, look to using Secure Shell (SSH) instead of telnet, as the communication is encrypted.

Curriculum-specific to firewalls, Intrusion Prevention and Detection Systems (IPS/IDS) and Advanced Malware Protection (AMP) are reserved for security certifications.

As of January 2014, Cisco has reworked its network security certifications, offering a new Cybersecurity Specialist badge and updating its Cisco Certified Network Professional (CCNP) Security Certification to provide new training and a wider view of network security.

The CCNP certification maps to the job role of the Cisco Network Security Engineer responsible for security in routers, switches, networking devices, and appliances. CCNP-equipped engineers choose, deploy, support, and troubleshoot firewalls, VPNs, and IDS/IPS solutions for their networking environments.

Cisco has introduced four new courses and related exams, including Implementing Cisco Edge Network Security Solutions; Implementing Cisco Threat Control Solutions; Implementing Cisco Secure Access Solutions; and Implementing Cisco Secure Mobility Solutions.

The new Cybersecurity Specialist Certification is aimed at providing network security analysts with the latest threat-detection and mitigation skills, leveraging advanced security solutions from Cisco and other providers. The new training course and related exam for the cybersecurity specialist—focusing on event monitoring, security-event alarm, traffic analysis, and incident response—is Securing Cisco Networks with Threat Detection and Analysis.

In addition, Cisco also has unwrapped four new security training courses for network security professionals to stay abreast of the vendor's products, including: Implementing Advanced Cisco Adaptive Security Appliance (ASA) Security; Implementing Cisco Bring Your Own Device Solutions; Implementing Core Cisco ASA Security; and Implementing & Configuring Cisco Identity Services Engine for Wireless Engineers.

Cisco Security Solutions

Until now, solutions have focused on policy and application control and have been unable to address advanced and zero-day attacks. ASA's FirePOWER Services enhancement overcomes that limitation through context-aware visibility into users, devices and apps, and analytics for detection, tracking, and remediation of attacks.

Prior to the Sourcefire acquisition, Cisco's ASA CX was the firewall of choice. In September 2014, Cisco announced it was integrating Sourcefire's FirePOWER services with its ASA hardware. Suddenly, ASA CX was legacy software. Cisco will continue to support it as their customers migrate to FirePOWER. Cisco will continue to invest in CX, but the long-term solution is FirePOWER.

When implementing FirePOWER services, they can be added to existing ASA 5500-X and ASA 5585-X deployments or included with new deployments of those firewalls. Cisco SMARTnet Technical Services provides access to support tools and expertise. Managed Services provides full-time threat monitoring and management. Finally, the Sourcefire Incident Response team assists customers in diagnosing, identifying, and remediating risks using FirePOWER technology. The contextual awareness that AMP provides also feeds into Cisco's big data analysis tools.

These services can be managed with the Cisco FireSIGHT Management Center. Visibility is gained into users, mobile devices, client-side apps, virtual machine (VM)-to-VM communications, vulnerabilities, threats, and URLs. Also, activity within the network and across next-generation firewall (NGFW) deployments is controlled from this point.

Cisco FireSIGHT Management Center provides comprehensive, actionable indications of compromise (IoCs) that relate detailed network and endpoint event information. It gives further visibility into malware attacks.

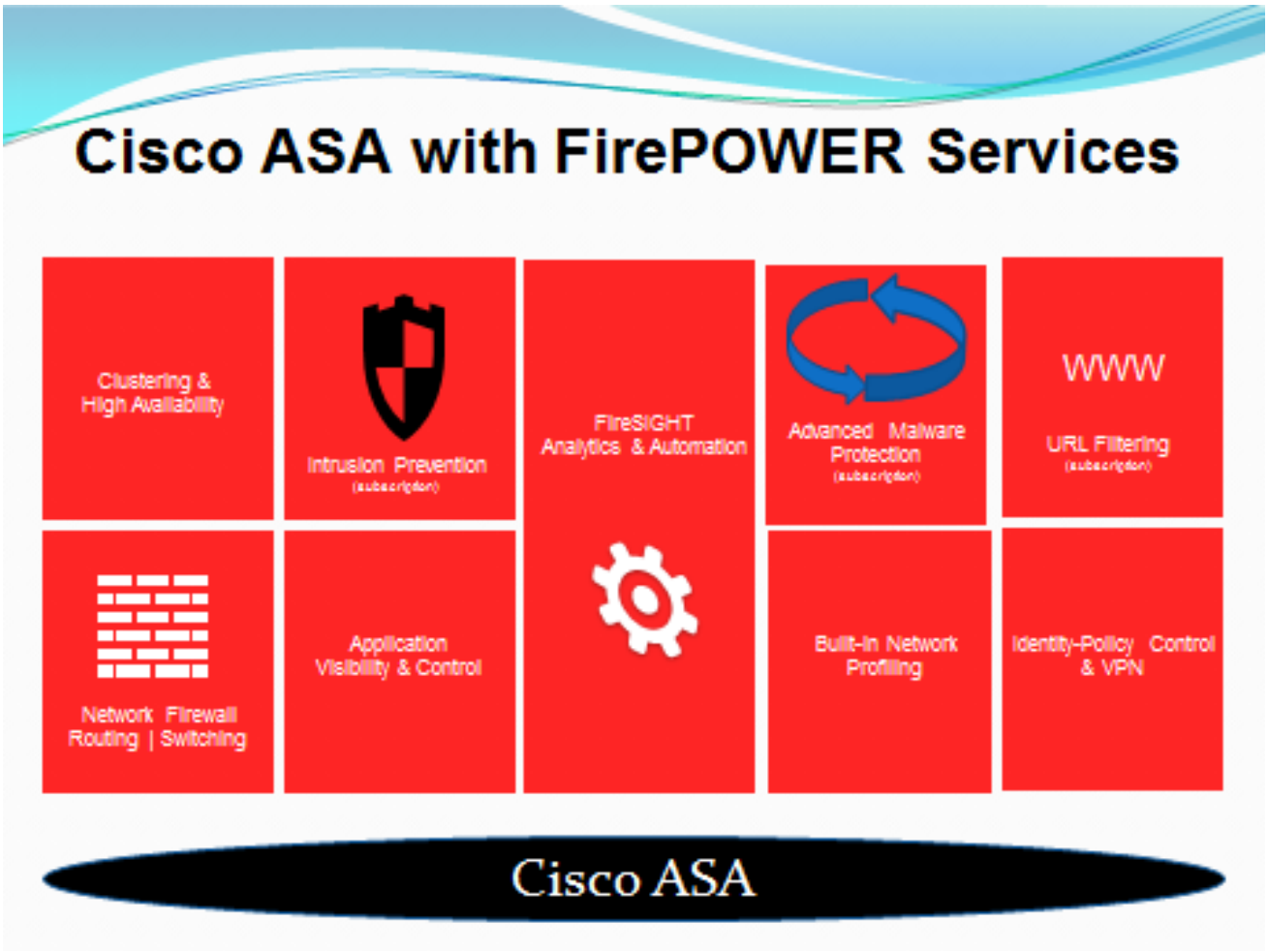

Figure 1. Cisco ASA with FirePOWER Advanced Services

Security and Other Cisco Solutions

Cisco has developed solutions that provide security to their solution portfolio that are not what we traditionally think of as security products (firewall, IDS/IPS). These solutions are used across the entire Cisco solution portfolio from mobility to data center to collaboration.

Cisco TrustSec®

Cisco TrustSec is an intelligent access control solution. With minimal effort Cisco TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, as well as exceptional control over what and where they can go. Cisco TrustSec uses software-defined segmentation to reduce the risk of malware propagation, simplify security operations, and assist in meeting compliance goals. Traffic classification is based on endpoint identity, not IP address. A unique, single-policy platform that uses your existing infrastructure helps ensure highly effective management. Although it is able to support any network, Cisco TrustSec works best on a Cisco infrastructure, using infrastructure-embedded features such as device sensors for visibility, security group access for access enforcement, and MAC Security (MACsec) encryption for data integrity.

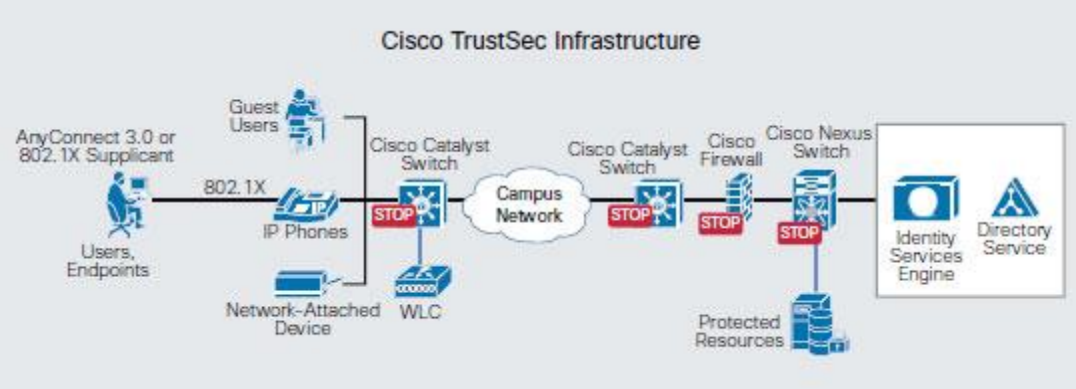

Figure 2. Cisco TrustSec Architecture

Application Centric Infrastructure (ACI)

Cisco has introduced a range of new information security products and upgrades as part of the launch of its ACI framework, which is designed to make security policies easier to enforce across both physical and virtual environments.

For starters, Cisco announced an ACI Application Policy Infrastructure Controller (APIC), designed to enforce access and security policies across the network fabric. ACI Security Solutions supports next-generation Cisco ASA physical and virtual firewall technologies by stitching them directly into the ACI network fabric, and can be managed using the ACI Policy Infrastructure Controller management tool.

In addition, Cisco updated its ASA 5585-X Series Next-Generation Security Appliance, which can be scaled up to handle 640 Gbps, work with Nexus 9000 data center switches, and also provide automatic load balancing, to be compatible with ACI. It's also released a virtual version of its popular ASA firewall, dubbed the Cisco ASA Virtual Firewall (ASAv), which will likewise work with the ACI fabric.

Security for Mobility: Cisco AnyConnect

When researching security options that are available from Cisco, a word that is hard to miss is AnyConnect. Cisco has developed the AnyConnect Secure Mobility Client as a "next generation" Virtual Private Network (VPN) client. AnyConnect is not limited to providing VPN access; it has a number of other capabilities that enable an enterprise to truly secure the endpoint.

Here we'll take a look at the different functions provided by the AnyConnect Secure Mobility Client and how it can be used to secure an endpoint.

AnyConnect Secure Mobility Client Capabilities

To clear up any confusion, there is an AnyConnect VPN client that exists, which provides only endpoint VPN access. The AnyConnect Secure Mobility Client extends these capabilities with a number of available modules; many of these modules were formally wrapped into other packages. See the available modules listed in Table 1.

AnyConnect Module	Capabilities
Network Access Manager (Formally Cisco Secure Services Client)	Provides the detection and choice of an optional Layer 2 Access Network and provides device authentication for access.
Posture Assessment	Allows AnyConnect to determine the operating system, antivirus, anti-spyware, and firewall software that is installed on the client, before a remote access connection is made. The Host Scan Application is the one used to obtain this information.
Telemetry	Can be used to send information about the origin of malicious content detected by the antivirus software. The IronPort Web Security Appliance (WSA) is sent this information and can better secure the network by modifying URL filtering rules based on the information.
Web Security	Routes HTTP traffic to the ScanSafe Web Security Scanning Proxy Server for content analysis, malware detection, and acceptable use policy review.
Diagnostic and Reporting Tool (DART)	Captures a snapshot of system logs and other diagnostic information of the client, which can be used when troubleshooting a problem with Cisco's Technical Assistance Center (TAC).
Start Before Login (SBL)	Can be used to start AnyConnect before a user is able to log in, which can force a user to connect to the enterprise infrastructure over a VPN connection before logging in.
Customer Experience Feedback	Can be used to provide Cisco with client information that is used to give insight into the user experience.

Table 1. AnyConnect Modules

It is important to note that two different product lines deploy AnyConnect: the Adaptive Security Appliance (ASA) and supporting IOS devices (e.g., the Integrated Services Routers [ISR]). Support for all the features shown in Table 1 requires a connection through a Cisco ASA. IOS devices are limited and support only the SSL VPN (WebVPN) feature.

Bring Your Own Device Security (BYOD)

Cisco offers two flavors of BYOD security: on premises and cloud managed. The Cisco Meraki BYOD cloud-managed solution integrates all hardware and software technologies into an "out-of-the-box" solution that is easy to deploy and use. The on-premises-managed Cisco BYOD Solution combines Cisco and partner technologies to provide fully featured network and device policy management, plus enforcement capabilities.

Cisco Meraki

Allows you to automatically apply security policies by user and device type, which helps to secure LAN resources and protect against viruses. Customizes authentication, firewall and traffic-shaping rules, and bandwidth restrictions based on users' identities. Implements device-specific policies to automatically restrict, quarantine, or throttle user-owned and untrusted devices. Provides Internet-only access to untrusted devices, isolating your network from viruses and blocking access to internal resources. Automatically scans PCs to ensure that they're running antivirus software, blocking vulnerable devices from accessing the network.

Provision and manage devices: Allows self-service setup for new users and ensure that they're managed when they log on to the network. Centrally manages network settings such as wireless connectivity, security settings, and VPN configurations across all devices. Preconfigures exchange server and credentials with Enterprise Active Sync. Locates and tracks laptops and mobile devices, both on and off your network. Secures data by locking devices, setting passcode complexity requirements, and establishing a maximum number of failed attempts. Remotely locks or erases devices that have gone missing, and even selectively wipes confidential data from users' devices.

The solution supports the growing number of client devices on your network with Cisco Meraki wireless access points and manages them all with the built-in mobile device management (MDM) toolset. Cisco Meraki System Manager provides BYOD support for user-owned and company-issued mobile devices.

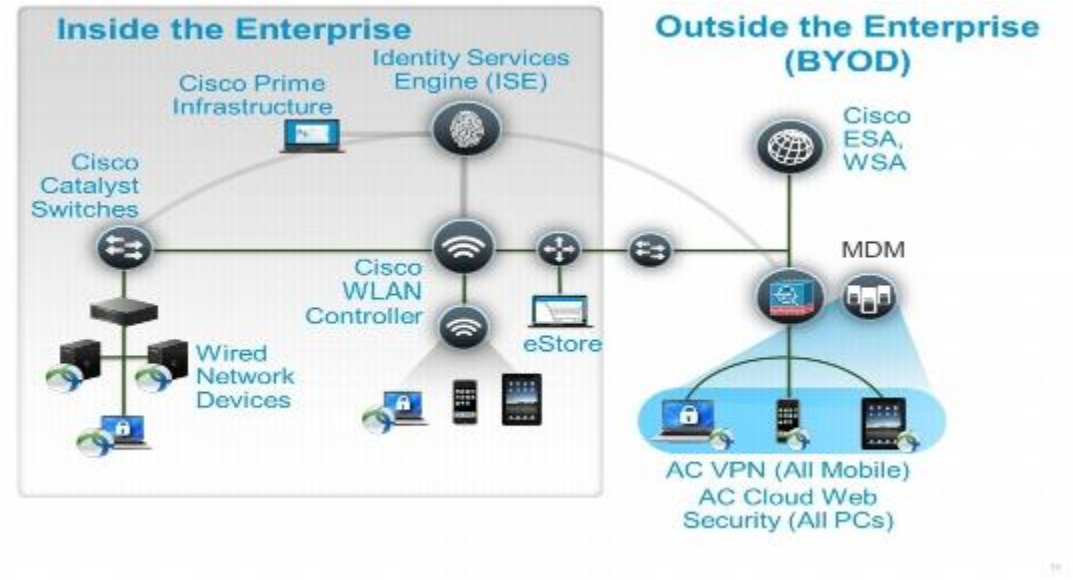

Figure 3. Cisco IT Security Architecture for BYOD and Wired and Wireless Access

On-Premises Solution

Provides secure access with a unified policy: A single policy secures data, applications, and systems across your entire organization. It provides guest, posture, device profiling, on- and off-premises network access, and MDM from leading partners such as MobileIron, Citrix, IBM, and AirWatch. Innovations in the Cisco Identity Services Engine (ISE) include new zero-touch on-boarding and central policy integration via open application programming interfaces (APIs) with MDM solutions.

In fact, you can now set an MDM wipe policy or network access policy based on MDM posture. Cisco ISE is the only solution to provide both network-based and endpoint-based scanning. Data security in the network (on and off premises) is provided to help ensure that your intellectual property is protected.

Conclusion

As the landscape has become more complex, the responsibility for securing organizational data has spread beyond the traditional IT professional. While there are more diverse security solutions, there are more diverse and sophisticated security threats. This has resulted in the need to provide security awareness and training to everyone in the organization. This includes the family organization. Creating an atmosphere of security awareness in one's personal life creates positive security habits in one's professional life.

Cisco has continued to evolve its security solutions and training. The acquisition of Sourcefire, along with their legacy security solutions, has secured Cisco's position as a leader in enterprise security solutions, and this has resulted in the development of cutting-edge security certifications.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Cybersecurity Training

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Rich Hummel has a bachelor's degree in electrical engineering from New Jersey Institute of Technology, and a master's degree in technology management. He has worked extensively with wireless, video, and cloud technologies.