WHITE PAPER

INTEGRATING WIRELESS AND WIRED SECURITY

As mobility becomes commonplace, strategies for wireless and wired security must be woven together.

Executive Summary

Over the past few years, managing client endpoints has been like living on an active fault line — with constant shifts in technology, management and security strategies.

The explosive growth of advanced and highly portable devices, combined with the expansion of wireless local area networks (WLANs) and cell phone networks, has catapulted mobile computing forward. The result? IT departments find themselves supporting the use of notebook computers, tablets, smartphones and other endpoints for enterprise purposes both within their organizations' facilities as well as at remote locations.

Security has struggled to keep pace with the ever-evolving nature of mobile technology. This is especially true in the case of bring-your-own-device (BYOD) programs that permit employees to use their own mobile devices for both business and personal use. This blending of environments causes unprecedented challenges for many organizations. How does an organization provide users with the freedom of choice that they increasingly demand while ensuring that sensitive information remains protected?

TWEET THIS!

Table of Contents

The solution revolves around tight integration of wireless and wired security practices. Mobile devices must be secured so that they provide as much protection for information as traditional client endpoints, such as desktops. Ensuring that all endpoints receive the same basic level of scrutiny, regardless of where they are or what network they are on, goes a long way toward safeguarding an organization's sensitive information.

The Need for Integrated Security

Security used to be a much simpler endeavor not that long ago (think years, not decades). Before the advent of mobility, most client endpoints were static desktops. For the most part, they resided within an organization's own facilities and used wired connections to attach to trusted internal networks.

In this premobile time, there may have been some notebooks used for remote access, and perhaps even some employees authorized to use their personal systems at home for limited remote access. But these endpoints accessed the organization's networks via dial-in modem connections, which limited their exposure to attack. The security controls for these systems were largely network-based: firewalls, intrusion detection systems, antivirus servers and the like.

The advent of WLANs marked the next phase in the evolution of client endpoints. Instead of being forced to use slow dial-up lines, notebooks could use Wi-Fi connections to access the Internet and reach an organization's remote-access servers. Using WLANs greatly increased throughput and gave people much more flexibility in where they could work, but this also put their computers and information at much greater risk of exposure. Additional security controls, such as virtual private networks (VPNs), were used to protect communications from Internet-based threats.

Today, the world has entered a new phase in client endpoints: the mobility revolution. Ever smaller devices provide increasing capabilities. For example, today's smartphones have far more computing power and speed than desktop computers did just a few years ago. And these mobile devices are no longer limited to WLAN access; now they use both cell phone networks and WLANs.

Plus, they can use a variety of wireless personal area network (WPAN) technologies (Bluetooth, near field communications and others) to link directly to other computing devices. Instead of having to protect one network interface and connection, organizations' IT and security teams must protect multiple network interfaces simultaneously, in ever more dynamic environments.

Given the increasing popularity of BYOD endpoints, organizations continue to have reduced control over the clients using their resources. Although the security industry now produces technologies specifically intended to protect BYOD environments, such as enterprise mobile device management (MDM), most of these solutions are still maturing and are more easily circumvented on BYOD endpoints than on organization-issued devices.

Organizations must increasingly rely on network-based security controls to protect and monitor the security of the organization's information. But because mobile devices are frequently used on outside networks, IT departments also must rely on host-based protection to provide an additional layer of defense.

The best solution for protecting today's client endpoints — and tomorrow's — is a holistic, unified security strategy that brings together wired, wireless and endpoint security. That approach can ensure that all endpoints receive adequate protection, no matter what internal or external network they are on and no matter what environment they are in.

The benefits of a holistic strategy include consistent security controls for every endpoint, financial savings through the use of BYOD endpoints, improved security protection and reduced risk.

The Myth of BYOD

Lately it seems that the bring-your-own-device movement is getting a lot of attention.

Organizations are grappling with the issue of whether or not to permit BYOD. It's often thought of as a daunting technical task to protect sensitive information stored on or accessed by BYOD endpoints.

But the truth is that for the most part, BYOD is nothing new. Many organizations, if not most, have been permitting employees to telework from their personally owned endpoints for many years, providing at minimum the ability to access corporate e-mail from home computers. So what's changed?

- **The rise of mobility:** People use a much wider variety of devices, with variable security.
- **Access to corporate resources:** Mobile solutions now provide the potential to tap most enterprise data, from the benign to the highly sensitive.
- **Awareness of risks:** Organizations now know the vulnerabilities that unsecured mobile devices pose.

In short, BYOD has become considerably riskier than it used to be, even as employees increasingly demand to use their own devices as opposed to those issued by the organization.

The Path to an Integrated Strategy

The exact composition of an integrated security strategy will vary between organizations, but each strategy will typically share the following major elements: hardening the network infrastructure, hardening the endpoints, protecting endpoints and networks from threats, and maintaining security.

1. Harden the network infrastructure.

Organizations must harden their networks to eliminate as many vulnerabilities as possible. Hardening a network also involves restricting access. These actions reduce the chances of a successful compromise.

What follows are three effective approaches that apply at a high level to both wired and wireless networks. The details differ based on network type. Just because organizations are integrating wired and wireless network security doesn't mean that security needs are identical.

Action Item: Implement separate segments for groups of client endpoints. It reduces risk to have different classes of endpoints on different network segments. Having segmented networks also makes it much easier to apply distinct policies to each class of endpoints. For example, an IT department could set network-based security controls on BYOD networks to compensate for the lack of host-based security controls.

Ideally, every client segment should be configured to access servers and other designated systems only, not endpoints on other client segments. This will reduce the spread of malware and other attacks that target endpoints on a local subnet.

A segmented approach has another benefit: It easily allows BYOD endpoints to be treated as less trusted than organization-issued endpoints. An organization can give BYOD clients access to a few low-risk internal resources only, such as e-mail and calendaring.

An organization can also decide to limit authorized configurations, such as prohibiting wired BYOD access. In fact, some organizations are eliminating wired connections altogether for client endpoints — even organization-issued devices.

Action Item: Only allow authorized client endpoints to use the network. Another possible method for network infrastructure hardening is to require some sort of device authentication. This could be performed using network access control (NAC) for organization-issued endpoints and using enterprise MDM for both organization-issued and BYOD mobile devices. Note: Some enterprise MDM solutions can manage notebooks as well as the smartphones, tablets and other mobile devices more traditionally associated with MDM.

At a minimum, an organization should confirm that each endpoint has the appropriate client software installed (a NAC agent or an MDM agent, for example). It is also important to keep an accurate and comprehensive inventory of all client endpoints authorized to use the network so that other endpoints can be blocked from being able to use the organization's networks. There also needs to be some sort of incident response capability triggered whenever a rogue endpoint tries to connect to the organization's network.

Action Item: Protect networks from eavesdropping. Eavesdropping is inherently different for wired and wireless networks. Most wired networks have little risk of eavesdropping because they are fully switched. Organizations concerned about eavesdropping should migrate to fully switched environments for their client endpoints if they haven't already done so.

For WLANs, network communications must be encrypted to prevent their contents from being intercepted. There are known vulnerabilities in the Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) schemes, so it's recommended that networks be configured to use stronger protocols such as WPA2, which does not suffer from the vulnerabilities inherent in WEP and WPA networks.

2. Harden endpoints.

Organizations need to reinforce all endpoints to the greatest extent possible. Obviously, whether the endpoints are organization-controlled or BYOD will affect the degree to which the IT team can control this effort.

NAC solutions (discussed in detail in the *Network Access Control Software* section) can be quite effective at checking the security posture of both organization-controlled and BYOD endpoints before allowing the devices to access the organization's resources. NAC can be used to enforce minimum policy requirements for endpoint hardening. What follows are three effective approaches to hardening endpoints.

Action item: Standardize endpoint security configuration settings. Security configuration settings define the controls of a device's operating system and applications; for example, providing an option to require or not to require user authentication before granting access to the operating system (OS).

It's generally recommended that organizations standardize and automate security configurations for endpoints, particularly client endpoints, because doing so can effectively mitigate risk and is far more efficient than manually implementing settings. Standardizing endpoint settings improves consistency, strengthens overall security, and allows automation of setting implementation and monitoring.

Here are examples of recommended security practices to implement through standardized security configurations:

- Disable all unneeded services, applications and protocols. This reduces the so-called "attack surface" of the endpoint — the number of ways an endpoint can be compromised.
- Implement the principle of least privilege. Each user, application and logical entity on an endpoint then can access only the functions and the information necessary to support approved use of the endpoint. For example, an application that provides a flashlight function should not need access to the address book.
- Require users to authenticate before accessing the endpoint's OS and applications containing sensitive data. This protects each endpoint and the organization's information from access by unauthorized users.

Action Item: Patch and upgrade endpoint operating systems and applications. Keeping software fully up to date also helps eliminate vulnerabilities. This requires both patching software (installing the latest updates to eliminate known vulnerabilities in the software) and upgrading software (installing newer versions to replace old ones).

Vendors frequently discontinue support of older versions of software, which means that patches will not resolve new vulnerabilities found in the software. The only way to get rid of vulnerabilities, in many cases, is to switch to a newer version of the software still supported by the vendor.

There are many mechanisms available for patching endpoints. Many apps include built-in features to check for, download and install updates. There are also enterprise patch management technologies that organizations can install on desktop and notebook endpoints, and MDM technologies with patching capabilities that they can install on mobile devices.

At this time, no single product can handle all the patching responsibilities for all the OSs and apps on your endpoints; hybrid solutions must be used instead. If an organization supports enterprise mobile device usage, it should already have the necessary technologies up and running. Ensuring patching should therefore require little additional effort.

Organizations also need to carefully consider how well large patches (and full upgrades, when applicable) can be installed over external networks. This can be particularly problematic for mobile devices that use metered networks, such as those of cell phone carriers.

A single application update could be hundreds of megabytes, or even multiple gigabytes. Downloading just one such update over a metered network could use all available bandwidth for a given month or result in substantial overage charges. Updating such devices generally necessitates either connecting them to an unmetered network (a WLAN, for instance) or connecting them to a notebook or other endpoint that is already connected to an unmetered network, with the network-connected endpoint acquiring the updates on behalf of the mobile device.

Organizations should plan for these situations and also educate users on the importance of keeping the OSs, software and apps on their mobile devices current.

Action Item: Use host-based firewalls. Endpoints no longer necessarily reside behind network firewalls and other network-based security controls. They are increasingly connected directly to public networks, such as open WLANs. Host-based firewalls can prevent unauthorized connection attempts to the endpoint from other hosts.

Host-based firewalls have been widely available for desktops and notebooks for many years. But they have relatively limited availability for smartphones, tablets and other mobile devices because people have relied on network-based firewalls from cell phone carriers to shield them from malicious activity. As organizations migrate mobile devices to WLANs, however, these network-based firewalls no longer protect them, so host-based firewalls are needed to compensate.

Hardening Users?

It's easy to focus on hardening networks and endpoints and to forget all about hardening another vital component of security: users.

All the security technologies in the world can't safeguard an organization's information if its users don't follow sound security practices. It's important to provide security and awareness training for all endpoint users. In particular, it's important to emphasize issues that technical controls can't address, such as physically protecting mobile devices.

3. Protect endpoints and networks from threats.

Eliminating vulnerabilities isn't sufficient to totally protect endpoints and networks because it's impossible to eliminate every last vulnerability. What's more, many threats succeed by tricking users through a technique known as social engineering. Therefore, organizations must protect their endpoints and networks from threats in several ways, including the following action items.

Action Item: Detect and block malicious activity. Antivirus, antispam, and intrusion detection and prevention software are all useful at spotting and rejecting malware. And though there are host-based and network- or server-based versions of these tools, most are not widely available for smartphones and tablets. For those endpoints, it is particularly important that network- and server-based controls be used to provide protection by monitoring the endpoints' network communications.

This works fine when users connect to the organization's enterprise but not for the use of external resources. One option is to use a VPN tunnel to direct all communications for the endpoints through the organization's network infrastructure.

Although this may be the only protection that this network traffic receives — making it invaluable — its raises some serious concerns: the slowing of network activity, the privacy implications of monitoring personal activity and the bandwidth requirements for carrying all the traffic. Ideally, such controls should be on the endpoint, so it's wise to encourage security product vendors to make versions of their controls available for smartphones and tablets.

Exfiltration of sensitive data is another growing concern for organizations. Data may be exfiltrated by malicious insiders (such as disgruntled employees), by employees who make innocent mistakes or by a successful cyberthief. The primary security control for discovering data exfiltration is data loss prevention (DLP) software (see *Data Loss Prevention* section).

Action Item: Protect network communications from eavesdropping and manipulation. Although this white paper has touched on the need for encrypting wireless network communications, organizations also must protect the confidentiality and integrity of all communications passing over untrustworthy networks. Otherwise, information may be intercepted and accessed or manipulated.

Even if a wireless network provides strong protection for its communications, it can only protect them on the wireless network itself — not the wired network to which the wireless network connects. Therefore, the IT team needs to use encryption to protect sensitive information sent over any untrusted networks.

One option is to protect traffic at the network level, typically through establishing VPNs. Many mobile device carriers support private VPN services that protect an organization's mobile device communications.

A downside of such VPN solutions is that they may direct all traffic for the organization's mobile devices through its networks. This may not be a problem for organization-issued endpoints, but it may be a major issue for BYOD endpoints, whose owners may have privacy and performance concerns about having all of their personal computing activities routed through the organization's networks and monitoring technologies. There may also be problems with bandwidth and other aspects of supporting increased traffic flow.

In addition to VPNs, IT departments can protect communications at the application level. An example of this is when a web-based app uses the Secure Sockets Layer or Transport Layer Security protocol to protect HTTP communications (better known as HTTPS). HTTPS can be used to protect web traffic. If an organization transmits most or all sensitive information through webmail or other web-based apps, HTTPS offers a way to achieve confidentiality and integrity for sensitive information without the overhead of a VPN.

Action Item: Reconfigure endpoints to block emerging threats. Suppose that a not-yet-patchable server vulnerability is discovered in a service that only a handful of the organization's staff members use, for non-mission-critical purposes. What if remotely exploiting the vulnerability can give a hacker full administrator-level access? The IT department should be able, either through domain policy management or through third-party security automation technologies, to rapidly disable this service on all endpoints until a patch becomes available and is installed.

Test It, Then Test It Again

So the IT team has eliminated vulnerabilities in an organization's networks, endpoints and users, and protected its networks, endpoints and users from threats. What's next?

The team should perform a security assessment to determine the effectiveness of those security controls. Two possible options include penetration testing and vulnerability assessments.

Never assume that because a security control has been implemented, it's working the way it was intended to work. The infrastructure changes and evolves; so too must its security controls.

4. Maintain security.

When focusing on security maintenance, a key ingredient is configuration management. From time to time, the configuration of endpoints will need to be updated.

The most obvious example (as explained earlier) is the installation of patches and upgrades. Another example is the adjustment of security configuration settings to reflect changes in policy, threats and vulnerabilities. Additionally, software patches and upgrades may offer new or altered security configuration settings; these need to be set properly.

Another important component of security maintenance is performing periodic assessments of endpoint and network security. As vulnerabilities and threats change over time, and the effectiveness of security controls waxes and wanes, so does the level of risk to be mitigated in endpoints and networks. It is important to periodically reassess risks to determine if changes to security controls are needed, including the addition of new controls.

A relatively recent trend known as continuous monitoring can reduce (but not eliminate) the need to perform periodic assessments on endpoints. Continuous monitoring, which essentially performs vulnerability assessments all the time, is made possible through automated security technologies. Tools such as patch and vulnerability management software can quickly check an endpoint and identify missing patches, unsecure configuration settings and other security-related problems.

It is easy to see why continuous monitoring plays an increasingly critical role in maintaining endpoint security. Vulnerabilities are being exploited all the time, so it's no longer sufficient to audit the security of an endpoint every year, or even every month. It's imperative to remediate weaknesses as quickly as possible, and continuous monitoring can discover them very quickly.

A final security maintenance component is incident response. Every organization needs to be prepared for security incidents involving their endpoints, such as malware infections and lost or stolen devices. Incident response efforts should strive to protect the organization's sensitive information from disclosure by detecting and containing incidents quickly, by removing compromises from endpoints and by remediating the vulnerabilities that the incident exploited.

Data Loss Prevention Software

Data loss prevention software has emerged as a valuable security control for protecting an organization's sensitive information, particularly when it is stored on or accessed from end-user devices. Here is a closer look at DLP software.

How DLP Software Works

There are many techniques for identifying sensitive information. They tend to fall into three groups:

Pattern matching: These techniques examine information for patterns, such as a string of data that matches the pattern XXX-XX-XXXX (where X is a digit, 0–9) and that likely represents a Social Security number. Other types of patterns to check for include keywords (such as "SSN").

Fingerprinting: These methods generate cryptographic hashes on chunks of known sensitive information. They then look for repeated instances of the hashes, as if a piece of sensitive information were copied from one file to another.

Statistical analysis: The most sophisticated techniques involve statistical modeling. Existing documents containing sensitive information are analyzed to determine their statistical qualities, and then new documents are checked for similar qualities, indicating duplicate documents or information duplicated from one document to another.

Each of these types of techniques has strengths and weaknesses. Pattern matching techniques, while effective for novel sources of information, can be easily tricked by simple character substitution and other means. For example, a person might remove the hyphens from within a Social Security number, turning it into an innocuous nine-digit string.

Patterns are most effective at finding accidental exfiltration of information, such as someone e-mailing a file to the wrong person. They have limited effectiveness against people who are aware of the types of patterns that DLP software filters out. Fingerprinting techniques can be quite effective for finding chunks of information copied from one location to another, but simple obfuscation of information can circumvent these detection techniques.

Consider the Social Security number example: Assume that the "fingerprint" is the cryptographic hash of a unique SSN. What if a person were to retype the SSN, omitting the hyphens? Or insert a different character in place of the hyphens? Or type the SSN in reverse?

The statistical analysis techniques may be the most effective method at finding novel documents. But as statistical-based intrusion detection systems have shown, any system based on creating a baseline and identifying anomalies from that baseline can be fooled by "slow and low" attacks that (over time) go unnoticed because they subtly change what a network analysis considers normal behavior for a system.

Another aspect of the techniques to consider is false positives — alerts falsely indicating that an attack has occurred. Because pattern matching is the least sophisticated category of techniques, it is also the most prone to false positives. Fingerprinting techniques tend not to be susceptible to false positives because of the unique nature of cryptographic hashes.

Statistical analysis techniques are somewhat susceptible to false positives, depending on how they are tuned. False positives can be a major problem if a DLP system is preventing users from getting their work done in a timely manner.

When these techniques are used, what are they examining? Generally there are three sources of sensitive information that DLP solutions can monitor.

The first is storage, ranging from enterprise file servers and databases to system hard drives. The second source is network communications. And the third source is the actions performed by users on endpoint systems themselves. These three sources are better known as "at rest," "in motion" and "in use," respectively.

Monitoring data at rest and in motion is pretty straightforward; monitoring data in use is much more complicated. Examples of the types of user behaviors a DLP solution might review include writing sensitive data to a local hard drive or removable media; pasting sensitive data from one document to another; printing sensitive data; performing a screen capture of sensitive data; and transferring sensitive data to another location (such as e-mailing a sensitive file or posting a document with sensitive data to a website).

Encryption and DLP

Monitoring data in use is often necessary because of the use of encryption to protect stored and transmitted information. Obviously, if information is strongly encrypted, the pattern matching, fingerprinting and statistical analysis techniques aren't going to work on that data.

The one place where the information is available unencrypted is at the endpoint, where the user is manipulating it — viewing it, copying it, printing it and the like. Monitoring data in use is also necessary for those cases in which data isn't being stored or transmitted, such as printing.

Blocking Data Exfiltration

It's certainly valuable to monitor sensitive data and to detect improper use, but it's more valuable to be able to prevent that improper use. With blocking, a DLP solution — by itself or in collaboration with other security controls — prevents an improper action. For example, it can prohibit sensitive data from being pasted into a new document.

Although blocking is worthwhile in preventing security breaches, it can lead to false positives that disrupt legitimate tasks within an organization. Because of this, it's wise to run new DLP solutions in monitoring mode only (with blocking disabled) so the IT security team can see if particular uses within an organization spur false positives. With that information, the DLP monitor can be tweaked appropriately to avoid disrupting work. Once false positives have been reduced to a minimum, the organization can enable the blocking mode.

User Education about DLP

A final component of a successful DLP solution is user education. Users need to be taught how they are allowed to work with sensitive information. And, just as important, they need instruction on what not to do, such as e-mailing sensitive files unencrypted over public networks. No DLP solution is infallible, so user education is an important supplement.

Network Access Control Software

As the name implies, NAC software controls endpoint access to an organization's wired and wireless networks. NAC applications work by automatically examining specified characteristics of an endpoint attempting to connect to an organization's networks and ensuring that those characteristics meet the organization's policy requirements. If they do, a network allows the device access; if not, it doesn't. These gateway scans protect an organization's networks and sensitive information from exposure to improperly secured endpoints, while typically performing necessary checks in a matter of seconds.

NAC solutions can be set to review a variety of characteristics, such as whether:

- security patches for the operating system and applications are current;
- security configuration settings for the OS and apps comply with the organization's policy requirements;
- antivirus software is installed, enabled and up to date;
- the endpoint system has undergone an antivirus scan recently;
- a host-based firewall is installed, enabled, up to date and configured to block inappropriate traffic;
- the endpoint is organization-issued or BYOD.

In addition to validating the security posture of endpoints, NAC solutions can also be set to check user credentials and then to authenticate users before granting their endpoints access to the organization's networks. NAC tools also typically keep detailed logs of their activities to authenticate users and authorize network access.

How NAC Software Works

When an endpoint attempts to access a NAC-patrolled network, that system only gains access to the NAC solution itself initially. The endpoint can access the full network only after it passes all NAC checks. If it fails to do so, the system will likely be given access to a quarantined network, such as a separate virtual local area network (VLAN). That way, untrusted systems can be kept separate from trusted ones that have cleared their NAC reviews.

This approach allows for remediation — for patches to be installed and missing security controls to be put in place on banned endpoints, for example. After remediation, an endpoint receives a follow-up NAC review.

Some NAC solutions can grant network access in a more granular fashion. For example, an endpoint that meets a basic level of requirements can have access to specified low-risk resources (such as corporate e-mail), while an endpoint that meets a higher level of approval gains access to moderate-risk resources.

NAC solutions that authenticate users can also use role-based access control to limit which resources particular users and their endpoints can access, based on the role profiles of the users and the security level of their endpoints. For example, a user who is authorized to access medical records might only be allowed access to e-mail from an endpoint that meets a basic level of requirements, but would be allowed to access medical records from endpoints with higher levels of assurance.

There are also NAC solutions that support guest management practices, which essentially treat a failed user authentication attempt as a failed endpoint check. This allows endpoints with authentication issues to have their problems fixed via the network before granting full network access.

NAC Architectures

There are two types of NAC solutions: agent-based and agentless. Agent-based solutions require installing an agent on each endpoint system, but they also typically provide superior checking capabilities. Agentless solutions are not as robust, but they are able to do remote scanning of endpoints to identify relevant characteristics, allowing their use with personal devices.

An organization likely will find that a combination of agent-based and agentless technologies proves most effective in collectively managing all endpoints that attempt to use the organization's networks.

NAC Responsibilities

Despite their utility, organizations should be cautious about ceding too much security responsibility to NAC solutions. These tools can be invaluable at finding common problems, such as a user who accidently attempts to work from a weakly secured or unauthorized endpoint. Even so, NAC solutions can't stop malware and other malicious foils from tricking users, and they can also inadvertently produce inaccurate results.

NAC should be one of many security controls deployed to protect an organization's information.

TWEET THIS!

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified

PEOPLE WHO GET IT™