



Security for Government

A multilayered strategy combats new threats and can reduce costs and enhance productivity

Table of Contents

- 2 Enhancing Productivity
- 2 Assessing Security Risk
- 4 Improving Network Threat Defense
- 4 Assuring Physical Security
- 5 Taking Advantage of Data Loss Prevention
- 7 Securing Remote Access
- 8 Achieving Endpoint Security

Executive Summary

There are many threats and scenarios that keep IT security teams up at night. Consider this statement regarding the shifting nature of threats: “There is no perimeter. The perimeter is every Internet connection and session out there.”

That statement, from a government security chief discussing cybersecurity trends, rings true for CIOs and chief information security officers everywhere — from the smallest rural county agency to the largest state or federal department. Threats are evolving and security strategies need to evolve with them.

Several trends are driving organizations to revise their strategies for securing their IT infrastructures.

First is the sheer number and variety of threats — increasingly sophisticated, targeted and financially motivated.

A second issue is the simultaneous rise in the use of mobile and wireless technologies, coupled with the increasing intelligence of endpoint devices — notebooks, smartphones, netbooks, e-readers to name a few — capable of running enterprise applications.

Third, the growing interconnectedness of organizations creates more points of vulnerability, broadening the scope of even minor security breaches.

A fourth issue is the growing number of virtualized environments, which require specialized approaches for securing the hypervisor that negotiates transactions between the physical server and its resident virtual machines.

Simply hardening the edge of the network is no longer sufficient. Today, agencies need to overlay a defense-in-depth strategy that stretches end to end and approaches data management in the context of risk — emphasizing vulnerabilities rather than threats.

Enhancing Productivity

It's hard enough keeping staff productive without malware slowing down networks and individual users' systems. Social networking, instant messaging, file sharing and multimedia viewing can wreak havoc for the IT security team.

Although these new tools often boost productivity, they also can be major sources of the very malware that the IT team works so long and so hard to keep out of the network. For example, Facebook has been the source of several forms of attack — from “clickjacking” schemes to take over users' systems to a self-described “hilarious video” link that tricks users into giving up login credentials.

Many organizations have begun adopting and are increasingly reliant on social media tools to enhance collaboration among staff or with the public, customers, suppliers and constituents. This elevates the need for trusted systems. After all, trust is the basis on which social media operates.

More threatening are known vulnerabilities in web applications and the browsers used to access them, which experts say are fast becoming an avenue of choice for hackers using SQL injection and cross-site scripting. Exploitation of vulnerabilities in commonly used programs, such as Adobe Reader and QuickTime, is also on the rise.

Although the discovery of new operating system vulnerabilities has slowed somewhat, the existing holes are being hit more than ever, according to the SANS Institute, an information security research and education organization.

Clearly, this adoption of social media tools and other web applications to enhance productivity comes with a new host of security threats. Organizations need to be willing to make an adequate investment in security to make the most of these

productivity gains. Yet, the budgetary case that IT departments must make to fund security initiatives can be hard to quantify.

What organizations need today is a systematic approach to their defense-in-depth plans. Security strategies should align with operations and mission goals — not merely comply with them. What does that mean?

Security professionals have to assess and prioritize vulnerabilities, determining which ones pose the greatest threat, and then assign a risk value. This requires the collaboration of the IT team, security staff, and the program and project managers (in essence, the operations owners).

The objective is to tailor risk profiles that offer options on how best to deploy new technologies, such as desktop virtualization, social media, cloud computing, mobile apps and telepresence. Security strategies should not block new tools. Instead, they should identify multiple adoption tactics and detail protection initiatives that must take place simultaneously.

As agencies develop, buy and deploy new services and applications, the security team must be involved at the outset. Always design security into systems, using programming best practices, establishing controls based on knowledge (such as the Consensus Audit Guidelines) and adhering to operations process architectures that make security a condition of rollout.

Assessing Security Risk

Fundamental to providing end-to-end security is an understanding of risk. Within an organization, differences can exist among IT, financial and program or mission officials over what constitutes an acceptable spending level for security. The threats themselves constantly change, often requiring renewed investment in tools and training.

The result? The IT staff must justify security spending based on an assessment of risk. It's generally easier to identify the organization's potential risks than it is to quantify them.

Risks can be broadly categorized by what an organization stands to lose should certain data be exposed, certain devices lost or certain systems breached. That list includes money, privileged information, reputation — even the viability of the organization itself.

Mapping the risks back to specific elements within an agency's IT ecosystem provides a mechanism for laying out investment opportunities for mitigating those risks.

For example, if the loss of personally identifiable information (PII) threatens confidence in the agency, then access controls and data encryption are called for, in addition to the hardening of public-facing websites against malware insertion. Some of these investments would protect against other threats, so the outlay can be amortized over multiple risk categories.

The Three Basic Risks

A well-thought-out network defense strategy mitigates several loss vectors, such as:

- **DATA LOSS**, by identifying and managing sensitive or proprietary data and taking steps to ensure unauthorized access or transmission is not allowed;
- **FINANCIAL LOSS**, by taking adequate steps to avoid data breaches that can lead to monetary fines, extensive legal fees and costs associated with victim notification;
- **REPUTATION LOSS**, by defending against attacks that disrupt network traffic and prevent staff, the public, constituents and partners from getting through (and eventually leading to weakened confidence in the organization).

That's why many organizations have difficulty calculating an exact value for a risk mitigation investment. Exposure factor, annual rate of occurrence and single loss expectancy can all be factored into so-called annual loss expectancy. Because the information used to calculate these figures can vary widely, agencies need to be alert to the possibility of false confidence based solely on these calculations.

Given that it's not always possible to put a definitive quantitative value on risk, the trend now is dynamic risk assessment, which takes into account changing circumstances, coupled with a focus on specific vulnerabilities in an organization's systems. This approach assumes it is impossible to eliminate every threat but quite possible to systematically approach vulnerabilities and reduce them.

Another vulnerability-based avenue for risk mitigation begins at system or application conception. The premise: By the end of development, at the point of testing or deployment, it's too late to conduct a security risk assessment. Vulnerabilities identified at this stage should have been identified and designed out earlier.

Industry and government have collaborated to create resources for developing reduced-risk systems. One such resource is the Common Weakness Enumerations Top 25, a compilation of programming practices likely to introduce cyberweaknesses.

IT shops should use the list when crafting service-level agreements for new programs. With current software, the IT team can compare existing components in apps against the list to shine a light on where vulnerabilities might lurk.

Another resource, the annually updated Consensus Audit Guidelines (CAG), provides a list of the most important security controls that organizations should adopt based on known attacks and weaknesses. Initially aimed at federal government agencies, the CAG list offers all organizations pointers on how to prioritize cybersecurity investments to address the most likely threats.

Compliance with standards or regulations in an organization's particular industry or field also makes sense when conducting risk assessments. Groups such as the Information Systems Audit and Control Association (ISACA) provide extensive guidelines for building risk assessment frameworks. Keep in mind that security regulations typically provide only a minimum level of security and should not be considered best practices.

Focusing on Data Risk

One of the difficulties of assessing security risk is that threats are dynamic. It can be hard to proactively plan for future security threats when your planning is based on knowledge of previous vulnerabilities that have been exploited. Predicting where the next attack will come from is obviously not easy to do.

Three Controls Every Agency Should Institute

The Consensus Audit Guidelines (CAG), developed by a consortium of governmental, academic and IT industry security practitioners, consist of 20 of the most important controls that organizations should have in place to secure their systems. Here are the top three:

- 1. MAINTAIN A COMPLETE INVENTORY OF DEVICES ON YOUR NETWORK.** This requires active monitoring with an asset discovery tool. Information should include the device type, where it resides, its IP address and who is responsible for it. Notebooks are obvious candidates for an inventory, as are mobile phones and smartphones. But don't overlook networked printers, storage (including USB and other removable devices) and Voice over IP (VoIP) phones — any gear that communicates over the network. Be sure to encrypt this asset information.
- 2. INVENTORY YOUR SOFTWARE.** Why? Because computer attackers will scan it, seeking vulnerable versions to exploit through botnets, hostile web pages and other cybercrime tactics. Establishing a control effort starts with setting an approved list of software for each system on the network, then scanning systems using a discovery tool to monitor for variations from the list. In some cases, these tools come bundled with enterprise versions of antivirus and intrusion detection packages.
- 3. ESTABLISH STANDARD, SECURE CONFIGURATIONS FOR ALL OF THE COMPUTERS ON YOUR NETWORK.** Any deviations from the standard image should be approved by the IT department and carefully documented. To maintain the hygiene of trusted machines, run a monitoring program monthly to check that no machine configurations have drifted or been altered.

One approach is to recognize attack vectors that are already sufficiently protected and then look elsewhere for future vulnerabilities. Much of the traditional security focus is oriented around the notion of protecting the network. So attackers are shifting tactics. The focus is now turning to the real prize that they are after today, data itself.

This shift in focus is due, in part, to the growing use of remote access and reliance on wireless devices, which creates new vulnerabilities for data. This is requiring organizations to rethink their security and risk calculations to be more data-centric — and thus shifting the focus of their security budgets as well.

A related threat vector garnering increased attention has been internal threats from staff, both unwitting and deliberate, stemming from both remote access and internal network

access vulnerabilities. This is another area where organizations are increasing their security spending.

Improving Network Threat Defense

Make no mistake that cyberattacks will happen. Symantec's State of Enterprise Security 2010 report found that 75 percent of 2,100 survey respondents (from industry, academia and government organizations worldwide) have experienced an attack within the past year. The average financial impact was \$2 million.

A solid defensive posture acts as the linchpin of enterprise security. The National Security Agency (NSA) advises organizations to adopt both protection and detection as countermeasures. Moving from a reactive to a proactive posture will help fortify an organization's security bench strength.

A defense-in-depth approach avoids reliance solely on a brittle infrastructure — one that's hard on the perimeter but soft and vulnerable once an intruder gains access to the network. The key elements of a defense-in-depth approach include:

- **PHYSICAL SECURITY:** Organizations increasingly find that they must integrate their physical and logical security teams to adequately protect remote users and to take advantage of the latest automated components used within their physical security infrastructures.
- **USER AUTHENTICATION:** Many organizations mandate two-factor authentication; a password coupled with a biometric identifier, for example. Identity management ties authentication credentials to systems policies, balancing the resource needs of individuals in an agency with the need to protect assets from unauthorized use.
- **DATA ENCRYPTION:** Required encryption also has become more common, for data both at rest and in transit. The advancements in encryption software and processor speeds no longer create response latency when encrypting files.
- **IMPROVED EDGE PROTECTION:** With the perimeter now a shifting piece of the infrastructure, routers and switches need the capability to host firewalls, antivirus, intrusion detection systems (IDSs) and analysis tools. Organizations can buy these items as software for existing firewall hardware, or they can move to dedicated unified threat management devices that bundle these tools on appliances.

Antivirus protection addresses only part of the picture and requires frequent patch upgrades because of the constantly changing profiles of virus-based attacks.

An IDS, which often includes antivirus, relies on profiling to identify anomalous behaviors on the network. An IDS logs each such event and reports it to a network management

The Virtualization Dynamic

The growth in virtualization and data center consolidation has created new security requirements for shared physical environments.

Several techniques can mitigate the risks inherent in virtualized environments. First, before virtualizing any systems, the data center team should validate that all applications and operating systems are fully patched.

Additionally, Microsoft advises running virtualized applications on trusted platforms and segmenting virtual machines (VMs) into groups with similarly critical applications. Tools exist that let network administrators analyze traffic among VMs and that provide alerts if malware is found.

Recent research and development also has the potential to harden the hypervisors that oversee VM operations. North Carolina State University researchers, under a grant from the U.S. Army and the National Science Foundation, have developed a tool that restricts any alteration of the hypervisor code and prevents any new code from being added. While this tool is still in the development stage, it shows promise for securing virtualized environments.

console, where it can be combined with other reports to give administrators a snapshot of trends and to alert them of possible breaches.

More robust tools can also stymie an attack by allowing dynamic reconfiguration of firewalls to close ports of entry. In a dire situation, an IDS can even shut down network components to quarantine and halt the spread of infection, creating a way to quickly annex servers and storage devices to protect them from tampering.

Defense in depth also encompasses layered defense, a related concept that takes into account the possibility of intrusion at different layers in the network protocol stack. Recently, the application layer has received attention because hackers increasingly are targeting specific applications in their efforts to snare confidential data.

The idea behind a layered defense strategy is that careful patch management, coupled with agencywide configuration management policies for end-user devices, can ward off fraudulent users by denying them access.

The ability to load a Trojan file or masquerade as a legitimate user becomes much more difficult with each additional layer of security. The aggregated layers also act as a deterrent: Cybercriminals will naturally prey on less-protected infrastructures.

Assuring Physical Security

Cybersecurity often focuses on detecting and preventing network intrusion. But physical intrusion is another piece of

the equation that is gaining increased attention. Many agencies are turning to updated technology solutions, such as motion detectors with door and window alarms or full video surveillance.

Both of these forms of physical intrusion detection have gone digital. Once information is converted into packets, an organization can apply intelligent tools to increase the productivity of security staff and to analyze events in real time.

In the case of video, the advent of affordable, high-resolution color is only part of the story. The real advance is digital, in which image streams are delivered as IP packets over the agency's network. This improvement facilitates the following security upgrades:

- **SEPARATE WIRING IS NO LONGER NEEDED.** Alarm and surveillance data can be converged onto the agency's network, avoiding or eliminating the need for expensive dedicated wiring.
- **MULTIPLE CAMERAS CAN BE VIEWED ON A SINGLE MONITOR.** For example, a Panasonic video server can display six cameras simultaneously but register 256 for sequential viewing. Adding multicast capability means security staff members are not limited to a single physical location for viewing video signals.
- **CAMERAS AND EVENTS ARE PROGRAMMABLE.** A hallway might be a critical path to guard. It's possible to program the channel carrying the appropriate camera view to warn the operator only when there is motion in the hall.
- **VIDEO CAN BE STORED IN DIRECT ACCESS MEMORY.** This does away with a reliance on old-fashioned tape. Security staff reviewing events can search stored imagery by time, or in some cases, by matching with reference images or shapes. For ultra-critical applications, users can integrate their IP video systems with facial recognition programs.

That last point is key. A reliable video storage array ensures that data will be kept safe for a set period of time. Specify a redundant array of independent disks (RAID) storage subsystem for assurance that a single drive failure won't mean the loss of data or that a work shift of surveillance goes unrecorded.

Meanwhile, through a gradual evolution of technology, physical access to facilities and logical access to the IT infrastructure are converging via smart cards and tokens issued to staff, contractors and suppliers.

Combined physical and logical access to the IT infrastructure makes use of peripherals located at doorways, both external and internal, that interact with cards or tokens to grant or deny access based on an individual's identity profile. The same card or token then acts as an authentication component, combined with a password, for access to systems.

Beyond that, access controls use a variety of technologies, including one-time password generators, barcodes, radio-frequency identity (RFID) and magnetic stripes. Often, a single card bears more than one technology.

To ensure a uniform security approach, organizations should choose physical security components with overall architecture in mind. Otherwise, cost and complexity can quickly escalate through installation of incompatible systems.

Taking Advantage of Data Loss Prevention

At its root, end-to-end security emphasizes protecting data — making sure it is kept safe from corruption, misuse and outright theft. Organizations that take a data-centric approach will have the best chance of creating the most effective data loss prevention (DLP) program at a reasonable cost.

Data loss prevention works best when incorporated into a larger data management policy, according to research by the Aberdeen Group, an IT research company. By understanding the value of various types of data, the IT security group can more easily justify investments in data protection.

Initially, the agency must identify its high-value sets of information. Aberdeen categorizes data into the following:

- Revenue generating (licensing fees or tuition, for example)
- Essential to future revenue (plans and intellectual property)
- Essential to operations (administrative or financial information)
- Protected by law (records containing personally identifiable information)

Applying what-if scenarios to data can yield values that agencies can use to measure the return on investment in DLP.

A DLP strategy must also account for data in various states, such as:

- At rest (in servers and storage systems within data centers)
- In use (when downloaded to a fixed-location PC or a mobile device)
- In transit (moving through the network infrastructure)

A comprehensive DLP solution will identify where mission- or operations-sensitive data resides and how it moves through the infrastructure. In that sense, the infrastructure is the route to protecting information, not the object of protection itself.

A strong DLP solution should be able to recognize information in context. For example, personal credit ratings are three-digit numbers between 300 and 850; Social Security numbers have nine digits that do not include some numbers on or before

certain dates; personal telephone numbers in North America have 10 digits, but no area codes ending in 00; and so on.

A solution that scans such numbers would need to have detailed — and perpetually updated — parameters built in to avoid false alarms and flag potentially corrupt information. Moreover, the use or movement of large blocks of consecutive numbers might indicate an anomaly to be flagged.

Data loss prevention solutions — from manufacturers such as McAfee, RSA, Symantec, Trend Micro and Websense — typically allow organizations to customize policy settings that align with mission and operations objectives.

For example, if the agency issues benefits, the issuance of a specified number of consecutively numbered checks to a single payee or the generation of multiple checks in exactly the same amount would be flagged as a possible financial system breach.

Beyond policies, you need the right tools and technologies to embed practices in systems to avoid data loss. First among these is encryption. Encryption can be applied to protect data at rest and in motion. A growing number of agencies specify full-disk encryption of notebook PCs and other portable devices, such as USB drives.

Should these be lost or stolen, they are useful only as pieces of used hardware. There are still additional risks: Someone obtaining a computer in runtime mode would have access to the files. And disk encryption carries the need for good key management so that in an emergency a disk can be decrypted.

Encryption can also be applied to messages and to message attachments, as well as to hard disks at the file level. Again, the effort starts with a solid key management program so that users, partners and suppliers can interact securely.

In all cases, encryption should conform to the more recent Advanced Encryption Standard (AES) with its longer bit-length rather than to the older Data Encryption Standard (DES).

A related technology gaining use for financial transactions, including credit card and other sensitive records, is tokenization. This is a process of replacing segments of sensitive data streams with unique symbols that are reinterpreted at the receiving end.

Some manufacturers of encryption products, such as RSA, also offer tokenization products. Others, such as Symantec, offer a range of deployment options such as on-the-fly, hosted e-mail encryption and external monitoring.

Data loss prevention also extends to the protection of applications, whether web or otherwise, that invoke or house data. This requires deploying access controls based on user profiles and privileges, coupled with tools that analyze incoming traffic for unauthorized or suspicious behavior.

This way, comprehensive, end-to-end protection can be implemented for both insider and outsider threats. Some manufacturers, such as Websense, offer this functionality in a single appliance.

Looked at from another angle, DLP requires both perimeter protections and defenses at the device or client level.

This is a rapidly maturing market: EMC, McAfee, Symantec and others have acquired many point-product startups in the last couple of years. Meanwhile other manufacturers, such as Cisco Systems, have forgone acquisitions in favor of partnering with DLP product makers to resell tools bundled with their appliances.

Because DLP can add complexity to network and applications management, it is wise to start by prioritizing data according to its sensitivity and working to protect the most sensitive information first.

Finally, don't overlook the human factor in deploying DLP. Staff and other users of an agency's systems can be the weakest link in the data custody chain, whether through ill intent or simple carelessness. The IT security team should provide

The Vectors of Data Loss

Until recently, data loss prevention strategies focused primarily on databases and the data center. But there are many vectors by which data can escape:

- **PEER-TO-PEER NETWORKING:** Never allow P2P file-sharing tools on any machines within the agency. Individual users might think that because their primary purpose is the exchange of music, such tools are harmless. Aside from the fact that organizational assets used in potentially illegal ways can expose an agency to liability, P2P programs can be (and have been) used to transfer every type of file.
- **E-MAIL AND WEBMAIL:** Be sure to monitor these closely. Even staff legitimately trying to exchange information through internal e-mail servers or webmail applications can errantly expose that information to possible interception.
- **SOCIAL NETWORKING:** Filter access to social network sites and other types of entertainment sites, which often are distribution points for keyloggers and malware. Sites catering to social network services have become dangerous territory when people connect from their agency's networks because of the potential for malicious downloads.
- **LOOSE HARDWARE:** Notebook PCs, smartphones and removable media — especially USB drives — are all subject to loss or theft. Tools exist that can track down misplaced or stolen mobile devices and remotely wipe their contents.

periodic training to remind users of organizational policies on data handling and computer hygiene best practices.

Awareness, more than technology, will reduce the number of staffers who leave thumb drives exposed on their desks, send unencrypted critical data in attachments or succumb to well-crafted spear phishing e-mail.

Securing Remote Access

Remote access to enterprise information resources has become so common that many organizations have begun reducing office space, preferring to have staff in remote or mobile mode while providing “hotel” office space to staff members that absolutely need to come into the office. A growing number of agencies now also provide remote access based on mirroring the services that users have to systems within the firewall.

Online access to applications from commercial sites has become so widespread that users in many agencies expect it from their networks and are disappointed when it’s not available. Similarly, the automation of and access to information about inventory, purchases and delivery has made interorganizational connections indispensable.

Meanwhile, ubiquitous broadband and Wi-Fi connections — driven by the desire for anytime, anywhere access and the popularity of smartphones as computing endpoints — have created their own set of security requirements.

Remote access is typically delivered via three possible routes:

- **VIRTUAL PRIVATE NETWORKS (VPNs):** By far the preferred means of remote access, VPNs imitate the secure connections available via the proprietary (and typically expensive) value-added networks of earlier years, but use the Internet as the information conduit. VPNs pair hardware and software to create encrypted point-to-point links.

Remote users in fixed locations, such as branch offices, typically rely on VPNs with IP security (IPsec) operating at the network layer of the Open Systems Interconnection (OSI) suite. Mobile users tend to tap Secure Sockets Layer (SSL) VPNs operating at the application layer.

- **ONLINE VERSIONS OF APPLICATIONS:** Many applications (typified by Microsoft Outlook) allow access via web versions that usually require only a password.

- **THIRD-PARTY SERVICES:** Apps available from outside services create a third path into the agency’s network. Hosted applications, as well as services such as Research in Motion’s BlackBerry e-mail forwarding, represent potential security vulnerabilities.

Notwithstanding the need to secure endpoints, the network infrastructure remains the hub from which the agency’s IT and security teams formulate, deploy and monitor security policies.

Most activity traveling to and from endpoints passes through the central infrastructure. Securing remote access, therefore, is fundamental to protecting the organizational infrastructure against denial-of-service attacks, data loss and information tampering.

An effective approach to securing remote access incorporates these four elements:

- **AUTHENTICATION:** Rigorous remote security starts with strong authentication policies. Two-factor authentication combines a password with unique biometric information or a second, one-time-use password generated by an authentication server.

- **ENCRYPTION:** Even after establishing an authentication process, agencies should require strong encryption using AES for data both at rest and in transit between points on the network.

Available tools run the gamut, from applications such as the BitLocker To Go file feature in Microsoft Windows operating systems and apps preloaded on USB drives to stand-alone tools for mobile devices such as McAfee Endpoint Encryption, PGP Whole Disk Encryption and Symantec Endpoint Encryption.

- **SMART FIREWALLS:** Firewalls are evolving into total security packages as manufacturers combine classic firewall functions with high-level features such as multiple VPN tunnels and virtualized firewalls within a single appliance. The Cisco Systems ASA 5540 exemplifies this type of device; other makers include Barracuda Networks, Blue Coat Systems, D-Link, Fortinet, Juniper Networks, McAfee, Netgear, RSA and SonicWall.

- **CONTINUOUS NETWORK MONITORING AND ANALYSIS:** Security experts recommend monitoring all network traffic and analyzing packet activity for behavioral anomalies. Inexpensive storage and increasingly powerful packet analysis tools now make it possible to segregate eight to 12 hours of network traffic and analyze it for malicious behavior.

Many network analyzers can do this automatically — a must given the sheer volume of data. There are stand-alone hardware and software bundles (from Cisco Systems, Fluke Networks and Juniper Networks, for instance), as well as software (from eEye Digital Security, H3C 3Com, OmniPeek and SolarWinds, for instance) that run on existing edge hardware.

A DLP solution should also be an integral part of any remote access security strategy. The agency’s IT shop also needs to button up all web applications in use. Online apps have become ready hosts for malware. This is true not only for social media sites such as Facebook and YouTube, but also for other web applications widely used in enterprise settings.

Control of online apps begins with software design. Emerging consensus on safe coding practices emphasizes white-listing functions — allowing only specifically authorized actions and disallowing anything else. The IT staff needs to ensure that these apps not only rely on a trusted infrastructure but that intrusion detection mechanisms also monitor their use.

Achieving Endpoint Security

Endpoints — the many devices through which the network infrastructure manifests itself to users — include desktop and portable computers, tablet systems and e-readers, smartphones and VoIP units, and output devices such as printers and smart copiers. Users access IT resources via these endpoints, and if the endpoints are unsecured, so do hackers and cyberthieves.

The smart approach calls for seamlessly integrating endpoint security into the agency's security architecture. Otherwise, it becomes impossible to manage multiple add-on technologies as new threats arise.

A few basic principles for securing endpoints apply to users both inside and outside the firewall:

- Security systems for endpoints require approaches that manage likely risks without encumbering users with complexity that impedes productivity. Of equal importance, tools and policies must not drive users to create homegrown workarounds, such as pulling the agency's data onto possibly virus-laden home computers.
- Software updates and security patches should be installed centrally, en masse, not by individual users. This will maintain standard, secure configurations.
- Security should exist within a policy framework that is easy to understand and to enforce. Agencies might need to develop additional policies for subsets of users based on their jobs, data use and access needs.
- Users must understand that they represent the first layer of defense in a defense-in-depth strategy. They must follow password best practices, log out of idle websites and online apps, use security tools and abide by policies that they may find a nuisance, and report any anomalies they spot while using devices on the network.

Beyond these basics, agencies also need to address the special security concerns of remote users:

- Lost or stolen devices should be inaccessible, or useless, to strangers. That implies full-disk encryption for

notebook computers as a basic requirement. Smartphones need to be password-protected and provide remote data-wipe functions.

- In wireless environments, access points must be physically secured and safe from tampering. Location services can create logs that show who has used the network and when — data that can offer clues to suspicious use patterns.
- All wireless devices should incorporate the latest implementation of the Wi-Fi Protected Access 2 (WPA2) standard.
- Rogue wireless access points must be disconnected to make sure they don't elude network access control procedures. Finding and rooting out unprotected rogue APs requires a detection tool and inspection of facilities.
- Because remote users often communicate with organizational IT assets across VPNs, encryption on VPN tools should extend to the keystroke level to confound keylogger programs.

As a practical matter, given the sheer number and variety of attacks, the IT security team should have the network scan every endpoint device weekly, looking for configuration deviations, the status of patches and evidence of malware. Depending on the agency's size, patch management can be automated or conducted manually by network staff.

A Trio of Trends

In any network security scenario, it's important to keep in mind that security services all derive from the network. The network should maintain and recognize all endpoint components, including passwords, encryption, configurations and disk images.

Three trends are emerging as network administrators and information security officers try to deal with the incessant waves of threats and attacks — and the complexity of cybersecurity tools.

One trend calls for moving to network switches and routers with integrated cybercontrols such as scanning and user ID management — essentially, unified threat management. Some organizations are also implementing managed security services.

A third trend is to increase the "signal-to-noise" ratio of threats by assigning them a progressive or logarithmic value depending on the threat type and the potential for damage. Programmed into monitoring tools, a mathematical approach can separate truly alarming threats from the more mundane.