1105 GOVERNMENT Information Group Custom Report

2010 IT Security Buyer's Guide

Security: Challenges and Opportunity Await Agencies

Federal agencies face pressure – from the White House and internal agency managers to users and even the general public – to make security a priority. And they have. But sometimes – conflicting mandates, the Obama administration's pledge to make government more transparent, upticks in mobile users and social networking, changes to FISMA reporting requirements, greater agency collaboration, high profile breaches and improprieties, such as the SEC porn debacle and the shift to cloud computing have complicated that mission.

Some agencies, of course, have accommodated those factors more easily. Others have fallen prey to common missteps, such as investing haphazardly in promising technology to fill gaps, ending up with a hodge-podge of technology that can complicate the work processes and overburden users, increasing the likelihood that they will find ways to disable or work around security mechanisms. The most successful agencies turn the challenges of topnotch security into an opportunity to assess their IT resources, business practices and security needs, then work the results into a solid security strategy.

The Drivers

A number of issues and initiatives have prompted federal agencies to take stock of their resources and scramble to provide additional security measures.

Greater transparency. When Barack Obama took office, he pledged that government would become more transparent. Agencies continue to struggle with how to protect information and ensure privacy but make government's workings more visible to the public. In January, 300 "high-value" data sets on Data.gov marked the first deliveries that agencies made toward the Administration's Open Government Directive. Going forward, they will have to address individual privacy concerns and authentication.

More nimble, responsive government. Another promise from the current administration was that government would become more responsive-to citizens, other facets of government and third party partners and collaborators. The expected result: a nimble government that operates much like a business, treating citizens like valued customers and resolving issues efficiently and expeditiously. At the Digital Government Institute's Government Customer Service Conference, David McClure, Associate Administrator for GSA's Office of Citizen Services and Communications, noted that "We're paying a great deal of attention to citizner engagement customer service." Indeed, GSA estimates that 41 percent of people in this country communicate with government online. But this level of responsiveness requires a smooth flow of information between agencies, citizens and other parties, and support for mobile and social networking technologies, which can make a government organization more vulnerable to breaches.

Mobility. Federal agencies are under mandate to offer teleworking options to their employees. And in 2008, nearly 103,000 employees were teleoworking, many up to three days a week. The benefits of teleworking are well documented – it's a cheaper alternative to providing office space for workers. It offers workers, and therefore agencies, greater flexibility, which in theory should lead to productivity gains and provide support for an agency's Continuity of Operations Plan (COOP). In addition, teleworking is a greener solution, greatly reducing the gas consumption and fluorocarbons for employees who commute by car. And the telework option, as well as the implementation of mobile technology to field agents and other agency personnel, help agencies to become more nimble and responsive per the Obama administration's mandate. Workers can respond and take action no matter where they are. But increased mobility equals increased security concerns – from protecting data on mobile devices to the transmission of information securely across mobile networks.

Changes to FISMA reporting requirements. While FISMA requirements have boosted security, the compliance reporting required is cumbersome, time-consuming and costly, costing about $1,400 per page. Under new guidelines, though, agencies will report on their security efforts and submit updates every month through CyberScope, a Web-based portal that will be overseen by the Department of Homeland Security. The new automated process will eliminate burdensome paperwork but it will allow an agency to present a nearly real-time view of its security status. But agencies must be vigilant and apply the appropriate tools to continuously monitor their IT and security resources.

High profile breaches. attacks and improprieties. Government has increasingly found itself under attack by malevolent forces or compromised by mismanagement and employee foibles. Missing laptops from the Commerce and State departments, the VA and other government organizations underscore a need for better security as do viral attacks and a preponderance of malware. Attacks on networks have become more organized, sophisticated, insidious and widespread. The Deloitte 2010 CSO Cybersecurity Watch Survey found that most organizations aren't aware of the type of attacks that compromise government and enterprise networks. And many, the report said, overestimate the abilities of the security solutions they use to guard against attacks. In the wake of the 2009 attack on Google, allegedly by the Chinese government, then director of national intelligence Denis Blair told the Senate Select Intelligence Committee that government networks lose sensitive data daily as result of similar attacks.

Social networking. The SEC's recent tangle with employees accessing porn sites from work, showed that even government agencies aren't immune to employees using IT resources on "company" time to engage in inappropriate and in some cases illegal activities. The scandal also raised the question of how to secure data and resources with social network gaining prominence. Facebook, YouTube, Twitter, MySpace and serve to create a more responsive, nimble and transparent government. They can be used to promote government initiatives and disseminate information. While some called for more stringent measures and a ban on social networking altogether, more reasonable voices have said that government would be better served to come up with policies and strategies that accommodated social networking but mitigated risk and vulnerability.

Cloud Computing. Government clearly has its head in the clouds. And it's no wonder that the move toward cloud computing has gained steam. With budgets tightening, the ability to share resources, pay only for what is used, and deploy applications and updates easier while minimizing disruptions and facilitating updates has mass appeal. Of course, cloud computing comes with a host of security concerns, which have caused many agencies to delay adoption.

Collaboration. Increasingly, government agencies must work together, exchanging information to do everything from coordinating responses to national disasters and tracking terrorist operations to administering benefits and uncovering securities crimes. At the Government Customer Service Conference, GSA's McClure called on agency IT professional to collaborate and to strive "to integrate information channels" in an effort to better the "citizen experience." But while the easy flow of information among agencies and outside parties facilitates transparency and makes for more responsive government, it opens up a host of security concerns regarding access, identity management and data protection.

Taking Action

Understandably, many agencies are overwhelmed by current demands for improved and comprehensive security, as they scramble to meet mandates and fill gaps in their own security plans. But a number of initiatives, including FISMA reform, are creating opportunities for government groups to move forward with tighter security. As OMB announced FISMA reform, NASA quickly announced its own move to continuous monitoring and online reporting of compliance.

And as the National Defense Authorization Act moved through Congress, where it was approved by the House of Representatives, changes to FISMA and the creation of an Office of Cyberspace in the White House promise to bring security under a more comprehensive umbrella.

"These provisions will establish strong, centralized oversight to protect our nation's critical information infrastructure and update our comprehensive policy for operating in cyberspace," said Rep. James Langevin, D.-R.I., one of the sponsors of the amendment to the Act that includes Office of Cyberspace initiative.

In addition, the second iteration of the Comprehensive National Cybersecurity Initiative (CNCI2) announced this spring has promised to ease the burdens of cost and limited resources that agencies are grappling with. Among its initiatives isprovide a way to manage the federal enterprise network as a single network enterprise with trusted Internet connections; deploy an intrusion detection system of sensors across the Federal enterprise; pursue deployment of intrusion prevention systems across the Federal branch enterprise; and coordinate and redirect research and development (R&D) efforts.

And at a recent Input conference, GSA's McClure hinted that all agencies might eventually be privy to military-grade secured computing. He called for the creation of "a forge.gov" that would offer some services "would be available to federal agencies for free. It would provide no-cost development and code repository support for open-source applications." ❑

The only way to be prepared for anything is to prepare for everything.

Threats are constantly evolving — as is technology. Cloud computing and Web 2.0, for example, offer whole new security concerns. To address your challenges, CDW•G can help you design solutions combining everything from IP video surveillance to secure remote access and data loss prevention systems. We can even help with risk assessment and compliance. We'll ensure you find balance between security and your organization's preferences. Plus, we understand the contract, policy and purchase requirements unique to government. When anything happens, we'll make sure you're ready.

Symantec™ Protection Suite Enterprise Edition

$53.86

Purchase three years of support for the price of two years of support[1]

250+ user license with three-year Essential Support[2]

CDWG 1856441

symantec.

McAfee® Total Protection for Data

$74.80

101-250 user license[3]

CDWG 1389843

McAfee®

CA Threat Manager Total Defense

$45.99

100-249 user license with one-year Enterprise Maintenance[4]

Download free trialware at CDWG.com/ca

CDWG 1654523

ca. Internet Security

More Security. Less Cost. Completely Installed.

CDW•G®

Your preparation begins here. 800.767.4239 | CDWG.com/federal

[1] Buy three years of support for the price of two years of support; pricing valid through 8/31/2010 [2] Essential Support includes 24x7 technical phone support and upgrade insurance; call your CDW•G account manager for details [3] Licensing requires a minimum purchase of 11 licenses; includes one-year Gold Support (24x7 technical support, upgrade protection and virus definition updates) [4] Enterprise Maintenance includes 24x7 technical phone support and upgrade protection. Offer subject to CDW•G's standard terms and conditions of sale, available at CDWG.com. ©2010 CDW Government LLC

FISMA Reform Brings Changes to Agency Security Strategies

Federal agencies breathed a collective sigh of relief when OMB announced that significant changes would be made to FISMA and its tedious reporting guidelines. While many would agree that having to hold to FISMA has helped boost security, most abhor the periodic reporting process, which is time-consuming, costly…and static.

With FISMA reform underway and changes to the reporting structure, government organizations are quickly gearing up to accommodate the bevy of changes to FISMA and to report monthly online – a move that Jerry Davis, deputy chief information officer for IT security at NASA said would give agencies the opportunity to obtain a "near real-time understanding of risk posture, and not the production of paperwork."

He noted that the old system of certification and accreditation was "largely ineffective" and did not "ensure a system's security." Davis said NASA would drop the traditional paper-based reporting structure in favor of the proposed online method.

And an amendment included in the National Defense Authorization Act currently making its way through Congress promises to add top-down support and accountability to FISMA, creating a National Office for Cybersecurity and a Federal Cybersecurity Practice Board that will guide agencies in meeting FISMA reporting requirements.

In addition, the Department of Homeland Security will assume "primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within FISMA," according to a memo from OMB Director Peter Orszag and Cybersecurity Coordinator Howard Schmidt. And OMB will oversee DHS. shall be subject to general OMB oversight."

"The cybersecurity coordinator will have visibility into DHS efforts to ensure federal agency compliance with FISMA and will serve as the principal White House official to coordinate interagency cooperation with DHS cybersecurity efforts."

While "OMB will be responsible for the submission of the annual FISMA report to Congress", among other duties, "the cybersecurity coordinator will have visibility into DHS efforts to ensure federal agency compliance with FISMA and will serve as the principal White House official to coordinate interagency cooperation with DHS cybersecurity efforts," the memo said.

The shift toward online reporting frees agencies from the rigors of periodic reporting and is a more fluid alternative, but it requires continuous reporting, constant vigilance and continuous monitoring. That spells changes for agencies, which must ensure that the mechanisms are in place to facilitate continuous, online reporting, as well as ensure comprehensive security and FISMA compliance.

While it is impossible for agencies to completely eliminate IT risk, they can use FISMA compliance as an opportunity to assess and mitigate risk. And although missions and objectives vary from agency to agency, there are several guidelines that apply to all government organizations. In a white paper, Tripwire underscored seven practical steps that agencies need to take to ensure that they comply with FISMA.

Gain situational awareness. An agency must assess its IT and security resources, as well as its management structure.

Reduce and monitor privileged access. The more access users have to IT resources, the greater the likelihood that security features will be disabled along the way. Limit access to only what is necessary and monitor with vigilance.

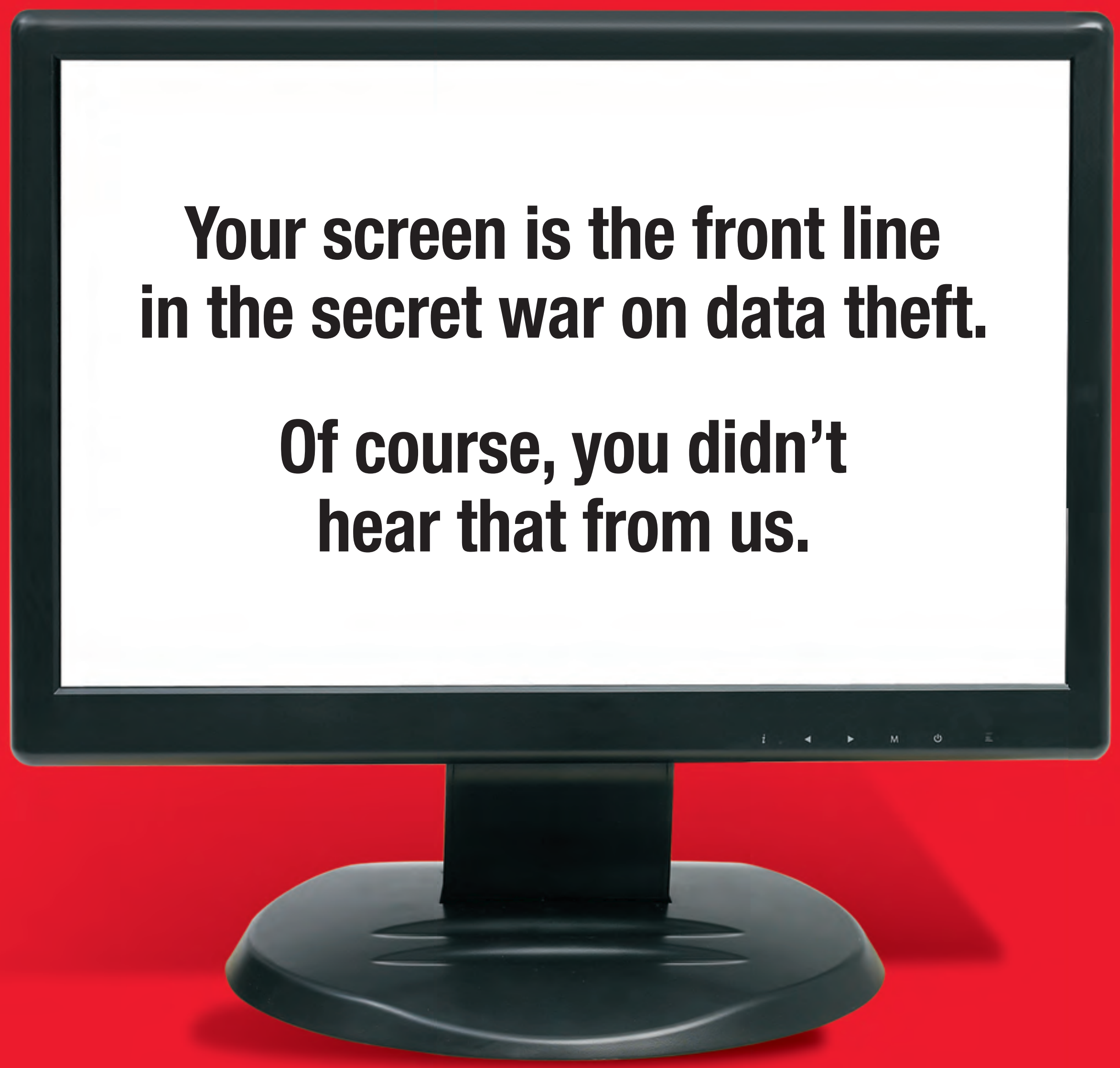
Define and enforce configuration standards. Organizations like the Center for Internet Security, the SANS Institute and the National Institute of Science and Technology (NIST) offer guidelines to help groups define, implement and verify configurations and security settings.

Integrate and help enforce change management processes. All modifications to security and other processes bring change to the work place. Agencies must assess and manage that change.

Create a library of trusted server builds. Trusted and approved server builds can be used to deploy authorized configurations more quickly and reduce the chance of security failures.

Integrate into release management testing and acceptance procedures. Standardization and documentation are key to information security. Release management determines whether components work together.

Ensure that all production activities go through change management. Production actions must be authorized, scheduled and audited by those in charge of change management. ❑


Your screen is the front line
in the secret war on data theft.
Of course, you didn’t
hear that from us.

3M™ Privacy Filters

Defend vulnerable on-screen data from sneak peek attacks with 3M Privacy Filters. Disarmingly simple yet decisively effective, they offer a crisp, clear view of your screen while discouraging wandering eyes from invading your space. What’s more, they can be deployed at a moment’s notice. 3M Privacy Filters—putting peace of mind easily within reach.

3M is your solution for privacy on every screen. For more information on 3M Privacy Computer Filters and 3M Mobile Privacy Film, **visit www.3MPrivacyFilter.com/Government or call 800-553-9215.**

3M

Best Practices Offer Guide to Security

Successful agencies know what works and what doesn't, when it comes to assessing, investing in and deploying security products, applications and services. While every security strategy is different, because agencies have different needs, there are several guidelines that all agencies should follow.

Assess what you have. Agencies can use creating a security game plan as an opportunity to assess its IT resources and determine not only obvious gaps in your security scheme but also in workflow and processes. So many IT infrastructures and security initiatives are built piecemeal that agencies often have a patchwork of solutions that don't work well together. Once an agency understands both what it has and what it's missing, it can fill in the gaps more efficiently.

Invest wisely. While it's tempting to grab onto the latest, greatest technology as a panacea for security woes, tight budgets and an abundance of solution choices call for agencies to be more prudent in their purchasing strategies. A thorough assessment of an agency's security landscape and vulnerabilities can guide a purchasing strategy.

Establish a security policy and enforce it. Agencies should first assess existing policy and determine where the holes or vulnerabilities might be, then fill the gaps. A security policy should be solid but also flexible enough to accommodate changes in work environments and technology. And it should address and include provisions for social networking.

In addition, there should be clear consequences for security violations and an agency must follow through with the stated reprimands and penalties. A strong security policy also needs the proper technology and human resources behind it. Security officers need the most current technology for monitoring and ensuring compliance.

Small things count. Some of the best laid strategies are compromised by the smallest of transgressions, missteps or practices. For instance, users often create easy to remember, therefore easy to hack, passwords and do not change them frequently enough.

Know your vendor. Vendors do more than provide products and services, they serve as agency partners and are privy to sensitive information and processes. Most vendors implement their solid security measures, but an agency should never assume. Ask for a detailed rundown of a vendor's security strategy and initiatives. A recent audit at the VA found that 10-20 percent of its contacts with vendors didn't include information security clauses.

Train, train, train. Qualified IT security professionals are in short supply. The Comprehensive National Cybersecurity Initiative 2 (CNCI2) announced this spring will focus on training and education and the creation of educational tracks and degree programs to turn out security professionals. In addition, a number of measures in that initiative will coordinate and manage "the federal enterprise network as a single network enterprise." By understanding and coordinating security initiatives across agencies, the government can identify the points of vulnerability, recommend where agencies need to take action and stimulate the use of shared resources.

Accommodate change. Many security initiatives bring changes to the work environment and threaten the delicate work culture. Even a small change can be perceived by workers as troublesome and unnecessary – and can threaten to bring business to standstill. For any security strategy to succeed, an agencies need to get workers on board. Complicate the way they work and they're more likely to look for work-arounds and ways to disable security mechanisms, all of which can compromise security.

Take a trial run. A pilot or trial will go a long way in testing a security measure and introducing it to workers. It is an opportunity to work out kinks in the system and create a measure of comfort among the workforce before the full solution is rolled out.

Watch it. Even the best of security plans and measures require constant vigilance. Set up 24/7 monitoring capabilities and act quickly when a vulnerability is exposed.

Assign responsibility. Most agencies have a Chief Information Security Officer. In fact, a survey by the 1105 Government Information Group last year found that 87 percent of the respondents had a CISO or CISO-equivalent in place. But their influence vary from agency to agency. In a (ISC)^2 report, "A View from the Front Line: The State of Cybersecurity from the Federal Chief Information Security Officer's Perspective," 90 percent of the respondents said that they had significant influence on their agency's security strategy. While most CISOs in the (ISC)^2 survey claimed to be satisfied with their jobs and are more influential than ever before, they have a long way to go. According to the study, "76 percent of CISOs report to the agency Chief Information Officer, but none to the Chief Operating Officer, the Chief Financial Officer or the Chief Risk Officer, which CISOs believe limits their overall effectiveness." ❑

The Road to Open Government is Paved with Twitter, Facebook and other Social Networking Sites

Social networking just might help government become more open and accessible to the public. Twitter, Facebook, YouTube, MySpace and other social networking media offer ways for citizens to access government and government to disseminate information and stay connected to its constituency. But as social networking becomes a mainstay for users inside government, it gives rise to a variety of security concerns.

Agencies can't afford to become more vulnerable to security breaches and inappropriate activity but they also can't afford to eliminate such a rich tool for communication and interaction with citizens.

The Obama Administration may have pledged greater transparency and aimed the Open Government Initiative at that goal, but according to an Open Government Research Report conducted by Harris Interactive for RightNow, 57 percent of respondents said they didn't believe that government is putting a serious effort into becoming more open. In fact, most felt that government falls far short of its mission to be more transparent – a whopping 96 percent said that government could improve its interaction with the public. And they identified web sites, mobile devices and social networking sites as the tools government could use to better reach citizens. In fact, a little more than half suggested that agencies build online forums while 71 percent noted that search capabilities on existing websites should be ramped up.

And 34 percent were in favor of government increasing its use of Facebook, Twitter and the like. Social networking sites offer agencies a free way to reach large populations of citizens, promote their services and conduct their business. Those sites help government prepare the public and executive COOP in times of disaster-natural and manmade. They, like mobile technology and agency Web sites, allow citizens to interact with government whenever and wherever they want to. In addition, with proper use, agencies should see an uptick in productivity-they can answer more questions and deal with more issues more quickly than through traditional means.

What's more, onvestigative arms of some agencies like the Justice Department and the IRS use Facebook, MySpace and other sites to help uncover and track and investigate persons of interest, taxpayers and criminals.

The Electronic Frontier Foundation along with the University of California, Berkeley's Samuelson Clinic filed a lawsuit late last year against the Department of Homeland Security, Central Intelligence Agency, Department of Defense, Office of the Director of National Intelligence, Department of Justice, and Department of Treasury in an attempt to uncover just how they use social networking sites to collect information and conduct surveillance.

The EFF recently obtained documents from the IRS and Justice that confirm the agencies are using social networking sites for investigative purposes.

Steps:

Make it a Policy. Include social networking in any security policy, clearly outlining guidelines for using the media at work and in the context of doing business. EFF's investigation found that the IRS has strict rules for social networking use. For instance, agents cannot use deception or set up false accounts on social networking sites in an attempt to collect data on taxpayers.

Suffer the consequences. It's not good enough to simply have a policy. Agencies must make clear the consequences for inappropriate use of social networking sites and enforce them.

Training counts. Agencies should detail how employees can best use tools like Facebook and Twitter to do their jobs. A Justice Department presentation includes instructions on "Obtaining and Using Evidence from Social Networking Sites". In addition agencies must school employees on the parameters for social networking use and warn them to watch what they say or post. A firefighter was recently dismissed after posting a video on Facebook. And employees at a California hospital found themselves pinkslipped after discussing patients on the popular social media site. The IRS includes specific guidelines for social network use as part of its formal training. ❑

Threats, Solutions on the Rise

Security threats may be on the rise but so is the number of security products from which federal agencies have to choose. It seems that products, services and applications change and emerge almost daily to address particular types of threats to government security.

Fending Off Cyberattacks

According to statements in a McAfee white paper by Lee Fisher, McAfee Security Strategist, "We have entered a new phase of malicious activity." As a result "proactive protection is becoming imperative-it is the only way to offer users absolute confidence."

The white paper notes that just a couple of years ago, "McAfee researchers were seeing roughly 300 potentially malicious threats emerging each month, but today the figure has rocketed to 2,000, largely due to the growing number of bots." What's more, attacks are becoming more sophisticated and "designed to specifically slip under the radar of government cyber defenses," McAfee has said. "Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage." Cyberattackers have tapped bots, Trojans and zombies to do their dirty work. And spyware as well denial of service attacks have proliferated.

Recent high profile attacks on the Defense Department's email system and Google point to extremely organized efforts, not just by individuals or criminal organizations, but by governments. According to the Wall Street Journal, in response to the rise in cyber attacks, the U.S. National Security Agency is at work on a system designed to detect cyber-assaults on the electrical grid, nuclear power plants and other infrastructure.

As the nature and sophistication of attacks changes, so do the solutions and strategies that government is adopting. Trusted standard fare like firewalls are no longer the centerpiece for protection against cyber-attacks. Instead, government is investing in things like continuous monitoring solutions that keep an "eye" on the network 24/7. Microsoft, Ncircle, netForensics and others have taken the lead here. In addition, companies like RSA and LogLogic are applying analytics to audit logs.

Keeping Up with Social Networking

Social networking sites are quickly becoming an important tool for government agencies. But use of Facebook, Twitter, YouTube and other social networking media open agencies to greater threats. Some agencies have turned to surveillance software like SpectorSoft or NetVizor, which are housed on the desktop. A variety of products have surfaced to help agencies and the enterprise incorporate social media but mitigate their vulnerability. Socialware, Facetime and Teneros offer SaaS middleware to monitor social media use. And companies like RightNow, Alterian, Scoutlabs, and The Internet Archive are also geared toward monitoring social media activity.

Conitinuous Monitoring

As FISMA reform becomes a reality and agencies are expected to report compliance online, continuous monitoring will become a must-have for government groups.

NIST has clearly stated the need for continuous monitoring, noting that "a continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, technologies and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system."

A variety of solutions are evolving to meet this demand. For instance Splunk offers solutions that can monitor data-streams in real-time and search terabytes of historical data to continuously monitor data coming in ASCII text from any data source. Splunk can monitor changes to files that identify system 'configuration drift' by comparing against a baseline.

The ArcSight ESM Compliance Insight Package for FISMA delivers a comprehensive, continuous monitoring and review solution and proactively identifies and manages incidents.

The RedSeal Network Advisor gathers configurations from network control devices such as firewalls, routers and load balancers and identifies security vulnerabilities in devices.

Safeguarding the Source: Database Security

An Oracle white paper recently quoted Rich Mogull, founder of the Securosis research and analysis firm, as saying, "We need to acknowledge that threats have changed, from noisy to quiet, from the edge of the organization to the center. We also need to understand that attackers' motivations have changed – web site defacement isn't the goal; fraud and data theft are."

Traditionally, government agencies and the enterprise have trained their security efforts on the perimeter of the network, using firewalls, VPNs, and antivirus and antispam software to deflect intruders. But these efforts are just the first steps toward security now that threats are growing in intensity, frequency and sophistication.

In a Forrester Research report, principal analyst

Noel Yuhanna, explains that "despite significant effort to protect enterprise databases, attack rates continue to rise." Today's attacks "are more sophisticated than ever, and many occur without enterprises being aware that an attack is taking place, especially in the case of internal attacks, which are the hardest to detect." Vendors like Oracle offer advanced security measures that offer additional protection by providing encryption and masking, access and authorization controls and auditing and monitoring functions.

What's more, some vendors are teaming up to provide more comprehensive database security. For instance, Praetorian Secure, LLC, recently joined forces with Application Security, Inc. to provide AppSec's database security offerings, which monitor and secure databases in realtime, to government and commercial sectors. ❑