Embracing Mobility, Enhancing Security for Federal Agencies

According to the "2015 Verizon Data Breach Investigations Report" — considered the most comprehensive and authoritative analysis of data breaches — the public sector was the target of cyber-espionage in one of every five attacks in 2014. At the same time, federal government employees increasingly demand access to potentially sensitive files and information across a growing range of portable electronic devices.

CONTENTS

In an environment of increasingly sophisticated breach attempts on the public sector, how can agencies give employees what they need to be productive and ensure all of that data remains secure both at rest and in transit?

This whitepaper outlines the latest solutions federal agencies can deploy to ensure both the freedom and safety of the sensitive information with which they have been entrusted. Topics include:

1. Understanding the challenges and meeting the needs of a mobile workforce
2. How sandboxing can increase security and eliminate threats
3. The impact of mobile technologies on data growth
4. Three key strategies for storage/backup/data restoration
5. Successful migration to a BYOD or CYOD program

Insight PUBLIC SECTOR

According to Federal Times, "Mobile hardware and associated mobile solutions have been some of the fastest growing areas in federal IT over the past few years as agency managers seek to meet the demands of an increasingly mobile workforce and deliver mobile-friendly content to citizens."

The drive toward mobility, however, is accompanied by a number of challenges. At the top of any agency IT manager's list, of course, is the need to maintain security of sensitive information — because as technology has gotten more sophisticated, so too have the cybercriminals who wish to exploit valuable government and private citizen information. The second major issue is the upwardly spiraling quantities of data generated by mobile devices, including the ability to store, manage, back up and restore vital information.

Fortunately, the concept of secure mobility is taking hold among forward-thinking agency IT leaders and teams as they strike a balance between employee access and the protection and management of data. These models and approaches include:

- Enterprise mobility management
- Sandboxing
- Cloud solutions
- Formalized BYOD/CYOD programs

This whitepaper will break down the primary mobility challenges federal IT faces today, along with potential solutions to help your own agency IT department:

- Support the goals of the Digital Government Strategy and Telework Enhancement Act of 2010.
- Improve security practices.
- Increase manageability of mobile-driven data.
- Cut expenses and drive operational efficiencies.

Secure mobility: Maximizing effectiveness, minimizing risk

The dramatic wave of mobile device adoption by society at large makes it one of the biggest targets for cybercriminals. The similar wave of mobile device adoption by government agencies raises the stakes immeasurably when it comes to protecting vital information and maintaining the public's trust. A Mobile Work Exchange report released in June 2014 found that federal agencies had invested $1.6 billion in the mobile workforce since the government's Digital Government Strategy was issued in 2012.

Whether mobile device usage is driven by formal Bring Your Own Device (BYOD) programs or simply by tech-savvy agency employees who find their way around IT and procurement policies, the dramatic growth comes with a measure of security risk.

- **More than 94 million citizens' records, under the care of government agencies, are estimated to have been lost or breached since 2009.**
- Multiply this figure by $194 — the average cost per compromised record for organizations in the United States, according to the Ponemon Institute's annual study — and the numbers become astronomical: **nearly $18.2 billion dollars' worth of damage**.
- In addition, according to the Government Accountability Office's analysis of US-CERT data, the number of reported information security incidents involving Personally Identifiable Information (PII) has more than doubled over the past few years — **jumping from 10.4 million in fiscal year 2009 to 25.6 million in fiscal year 2013**.

More than just hardware

The hardware devices themselves are hardly the only vulnerability point for government agencies. Those adopting mobile devices often encounter new varieties of phishing, malware and social engineering. Add to the equation the greater security demands presented by new compliance mandates, the tightening of security budgets and the reality of badly stretched IT departments, and it's clear new solutions are needed to help secure the increasingly mobile infrastructure of the public sector — including tablets as well as smartphones.

Mobility is also tied to other potential security risks in government agencies. For instance, mobile is often the preferred connectivity approach for popular, cloud-based, file sync-and-share services such as Dropbox, iCloud and Google Drive. In fact, as adoption of cloud computing continues to rise, it is closely linked to widespread mobility usage.

"Cloud-based solutions are particularly useful for a mobile workforce that needs to access easy-to-use applications and real-time information from anywhere, at any time," according to Jeffrey Kaplan, founder and managing partner of THINKstrategies, a leading advisory and consulting firm specialized in cloud computing.

Mobile devices are also an increasingly significant security choke point. In fact, the U.S. Food and Drug Administration issued a safety communication to address cybersecurity threats posed by medical devices and hospital networks, noting that a wide array of threats and practices open up the devices as potential carriers of malware and as intrusion channels to infiltrate and steal protected healthcare information.

11 steps federal agencies should take

There are numerous common-sense steps agency IT organizations and employees should take to safeguard data when using mobile devices. The U.S. Centers for Medicare and Medicaid Services, for example, has identified 11 specific ways for healthcare IT to fortify its defenses against mobile security threats — all of which are equally applicable to other agencies:

1. **Use a password or other user authentication**, and activate screen locking after a set period of device inactivity to prevent access by an unauthorized user.
2. **Enable encryption**, either with built-in encryption capabilities or an installed encryption tool.
3. **Install and activate remote wiping or remote disabling** in the event of a lost or stolen device.
4. **Disable and do not install or use file-sharing applications**, which can enable unauthorized users to access your device without your knowledge.
5. **Install and enable a firewall** to intercept incoming and outgoing connection attempts and to block or permit them based on a set of rules.
6. **Install and enable security software** to protect against malicious applications, viruses, spyware and malware.
7. **Keep your security software up-to-date** to prevent unauthorized access.
8. **Research mobile apps before downloading**, to verify they will perform only functions you approve.
9. **Maintain physical control of your mobile device**.
10. **Use adequate security**, such as encrypted connections, to send or receive information over public Wi-Fi networks.
11. **Delete stored information or sensitive data** before discarding or reusing a mobile device.

For additional ideas on how Insight's formalized BYOD/Choose Your Own Device (CYOD) program assists with the security of your mobile devices, turn to "The way forward: Strategic approaches to employee choice" toward the end of this whitepaper.

The time is now for enterprise mobility management.

While these and other steps are logical starting points for reducing mobile security risks, agency IT professionals need to stay up-to-date on new software tools that can block, identify and remediate security problems when — or ideally, before — they occur. Mobile device management is a must-have within agency IT organizations, and that capability is now being expanded into a comprehensive, organization-wide solution set referred to as enterprise mobility management.

Experts believe such an approach is an essential element in solving problems before they become intractable. THINKstrategies' Kaplan says IT professionals "should also ensure that the right policies and procedures are in place to govern the way applications and information are utilized, provide training to users about common security risks and appropriate best practices, and closely monitor the software and systems to quickly identify any security breaches."

A key requirement for mobile security solutions is the need to keep in mind the tangible benefits of mobile device usage in agencies and to make things easy — better yet, invisible — for end users:

- Slow or otherwise inconvenient tools are an invitation for users to create workarounds and avoid compliance.
- A mobile security software solution should be tailored to the needs of the public sector environment, including specific compliance and workflows.
- It should also provide a number of easy-to-use templates that meet compliance mandates, and adhere to the U.S. Federal Enterprise Architecture (FEA). Using such integrated templates decreases or eliminates the manual activities that would otherwise fall to already stretched IT staffs, while customizing policies in alignment with agency requirements.

Common security challenges

- **Device loss and theft**. Loss or theft of mobile devices is a considerable concern in many industries. Within the public sector, it is paramount.
- **Device vulnerability**. Mobile devices, with increasing adoption, are encountering new varieties of phishing, malware and social engineering, opening them up as intrusion avenues to infiltrate and steal protected information.
- **Cloud usage**. As adoption rises in cloud usage, so do the increasing number of access points for hackers.
- **Inadvertent misuse by insiders**. According to Forrester Research, inadvertent misuse by insiders represents 44% of the occurrences of data breaches within the public sector — making it the largest source of such breaches.

Security breaches have exposed the confidential data of millions of people, putting them at risk for fraudulent activity, including identity theft and other financial crimes. Natural disasters, such as Hurricane Katrina and Superstorm Sandy, have also shown the impact on the availability and potential loss of data. And, of course, state-sponsored and terrorist-initiated attacks are an issue, particularly within the public sector.

Contact Insight's federal government team using the information at the end of this document to discuss Insight's mobility security capabilities with one of our federal government specialists.

Insight
PUBLIC SECTOR

A superior sandbox Solution

- Works quickly to identify previously unknown threats
- Integrates closely with other security layers and solutions
- Efficient, easy-to-install and cost-effective solution
- FortiSandBox identifies 6 million new threats every week
- FortiSandBox has been independently tested and rated as blocking at least 99% of attacks

Contact Insight's federal government team using the information at the end of this document to discuss Insight's sandboxing capabilities with one of our federal government specialists.

Breaking the cyberattack kill chain

Mobile device management is a must-have for government agency IT organizations. In addition, enterprise mobility management offers a comprehensive, enterprisewide solution.

The fact is, data theft is big business. In 2013, more than 2,000 significant breaches exposed 822 million records. In the first half of 2014, more than 500 million records were exposed. And the five largest data breaches of all time happened in the past 18 months.

The strongest security uses a layered approach to disrupt what's known in the IT world as "the attacker's kill chain." But additional protection, from sandboxing, is needed to identify hidden or completely unknown threats.

Sandboxing strengthens security by analyzing suspicious activity in an isolated environment that is identical to the target system. Fortinet's FortiSandbox feeds threat intelligence back to FortiGuard labs to continuously improve other security layers.

A quick look at sandboxing in action

Stage in Attacker's Kill Chain	Blocking the Attack	Sandbox's Role	Fortinet Cyberprotection Statistics
Target identification and reconnaissance	Anti-spam/anti-phishing solutions block email that tricks targets into clicking on malicious links	Hold suspicious emails and analyze files	64,000 spam interceptions per minute
Initiate communications	Web filters block traffic to suspicious websites	Identify suspicious websites from file analysis	27 million website categorization requests per minute
Gain access to target system	Intrusion Prevention System (IPS) blocks malicious attacks launched to gain access to target system	Analyze incoming traffic and identify attacks	680,000 intrusion attempts resisted per minute
Install malicious code on target system	Anti-malware software neutralizes malicious code	Analyze behavior of suspicious and unknown code and identify suspicious or malicious activity	15,000 malware apps neutralized per minute
Steal information	If malicious code gets through, application controls or IP reputation prevent communication with the attack command & control server	Identify attacker's command & control server address via original file analysis	100,000 botnet command & control attempts blocked per minute

Transitioning from chaos to control in data management

Today's data centers have reached a breaking point: exponential growth of worldwide digital data, coupled with declining storage budgets, complex infrastructures and fragmented or nonexistent backup processes. This is every bit as true for public sector agencies as they strive to proceed from chaos to control in backup and recovery.

The statistics on the growth of worldwide digital data are astonishing:

- The amount of digital information is projected to grow from 4.4 zettabytes in 2013 to 44 zettabytes in 2020, according to EMC's Digital Universe study. (Each zettabyte is 1 billion terabytes.)
- The U.S. General Services Administration reports that the federal government operates more than 2,000 data centers, requiring large investments in infrastructure, data storage, and services.
- According to EMC, mobile-connected devices created 17% of all data in 2013, and that number will expand to 27% in 2020.

Data solutions

As data volumes continue to balloon, shoring up and optimizing storage and backup will be key to meeting IT challenges going forward in the public sector. While storage costs have come down, and performance has increased, today's fast-paced organizations are generating enormous volumes of data that need to be managed, stored and protected.

In the public sector, that data comes in a variety of forms, including, but not limited to:

- Citizen, employee, contractor and supplier data
- Tax collection data
- Healthcare data
- Health, scientific and engineering research

Behind the need for storage efficiency are a number of factors:

- **Growing data volumes** — the amount of data continues to grow and, along with it, the demand for more and more bandwidth to back up and restore that data quickly and reliably.
- **Duplicate data** — as data continues to grow, so does the amount of duplicate data that's taking up storage space and burdening backup processes.
- **Multiple solutions** — many agencies rely on multiple solutions for specific systems, making it difficult to manage backup and recovery processes.
- **Shrinking resources** — with the economic recession, storage budgets shrank considerably; although there are signs that spending is on the rise, the trajectory is slow at best.
- **Emerging technologies** — new backup and recovery strategies, particularly around cloud computing, are gaining wider acceptance as a lower-cost alternative to dedicated recovery sites.
- **Increasing regulations** — newer regulations and initiatives require agencies to draw up disaster recovery and other contingency plans.

(Cont.)

3 key solutions

1. Distributed backup architectures
   - No backup hardware
   - Automatic failover
   - Improved resiliency
   - Streamlined processes
2. Federated deduplication
   - Lower storage overhead
   - Fewer WAN bandwidth burdens
   - Higher data reduction ratios
   - Lower costs
   - Faster backup throughput
3. Cloud backup
   - Storage on demand
   - Single interface
   - Shorter backup windows
   - Pay for only what's needed
   - High security

For additional details about Insight's backup and recovery solutions, contact an Insight federal government specialist using the information at the end of this document.

3 solutions for backup and recovery

Insight offers three best-in-class solutions for agencies seeking to manage their rapidly expanding data needs.

1. Distributed backup architecture

Instead of a traditional network architecture based on centralized servers and storage arrays, distributed backup moves the backup process to a decentralized system that allocates backup data across the entire network. In essence, the network itself becomes the backup device.

A distributed backup architecture preserves the scheduling, restoration and synchronization of traditional server-based network backup and can scale by leveraging the free disk space on every computer on the network. It vastly improves enterprise reliability so that if a node or even a data center goes down, the backup and recovery processes remain available.

Distributed backup architectures eliminate the need for capital-intensive backup hardware, making them a powerful and cost-efficient alternative to centralized backup and recovery.

2. Federated deduplication

With federated deduplication, data is saved once using a common deduplication engine, and then moved anywhere across the storage infrastructure — without rehydrating the data or adding the duplicate data back in.

This common deduplication engine increases the efficiency of the storage process and allows data to be moved from location to location over low-bandwidth, affordable links — lowering both the storage overhead and Wide Area Network (WAN) bandwidth burdens. Federated deduplication also increases flexibility, enabling agencies to optimize backup processes, reduce network bandwidth costs and improve backup throughput.

3. Cloud storage and Backup as a Service (BaaS)

For highly efficient enterprise backup needs, cloud storage or remote backup services ensure 100% availability so you can instantly access valuable data. While traditional backup requires you to physically move backup media off-site, cloud backup requires no such intervention. Backup data is automatically stored in a remote location, and the service works continuously to back up files as they are changed.

Cloud storage models shorten backup windows by dynamically adjusting compression rates. To ease security concerns, cloud providers use strong security and encryption — often 128- to 445-bit — for data at rest and in-flight. A single interface greatly reduces management complexity by allowing you to quickly and easily configure backup schedules, select retention periods, view job progress and alerts, and perform restores. Pricing is based on use — as well as age and type of data, volume, number of backup copies and recovery-time objectives — and allows you to scale easily by allocating storage on demand.

With potentially unlimited data retention, ample agility and scalability, and lower capital costs, cloud backup services may be exactly what your enterprise needs to manage storage requirements and protect data.

Balancing mobility with security

In the past few years, two federal initiatives have specifically impacted the need for and usage of mobile devices, and must be considered by agency employees as well as federal IT managers. First, the Office of Management and Budget's Digital Government Strategy is aimed at building a 21st-century government that works better for the American people, including the directive to procure and manage devices, applications and data in smart, secure and affordable ways. Second, the Telework Enhancement Act of 2010 created a framework to increase flexibility and create work-life balance while meeting mission objectives.

Mobile users may access data while in government facilities, as well as at home or in other settings, through a virtual private network. As a result, it's essential to protect roaming users against data theft by maintaining appropriate control of sensitive information on Windows and Mac OS endpoint systems, both on and off the network.

Finally, for mobile users accessing cloud-based services, from Office 365 to more demanding applications, ensure your solution can be deployed both for on-premise infrastructure and cloud environments.

As the use of mobile devices and applications continues to surge, data breaches and other security challenges are likely to occur with more frequency, with the potential for significant economic and operational impact.

Agency IT professionals should collaborate with agency employees to develop a comprehensive mobile security framework. In particular, all parties need to come up with solutions that not only lock out potential cyberthieves, but also ensure users have easy, reliable and secure access to essential data and services through their familiar mobile devices. It's a balance between vigilance, security and compliance with the need for usability, flexibility and support.

The way forward: Strategic approaches to employee choice

Despite the $1.6 billion investment in the mobile workforce since the implementation of the Digital Government Strategy, **just 56% of federal IT managers surveyed felt they were taking "full advantage" of mobility in their agencies**. What were the primary obstacles to their success? Security, funding, culture and procurement issues topped the list.

While great strides have been made to give federal employees the ability to access files and data securely across a growing variety of mobile devices, most agencies still have a long way to go to reach full mobile enablement.

Bring your own device.
At the heart of the agency mobility migration is the decision to embrace a BYOD or CYOD strategy. Though they may seem similar on the surface, one offers significant advantages to federal agencies.

Telecommunications research firm Ovum believes BYOD has a number of pros and cons associated with it , including:

(Cont.)

- **Fits existing employee behavior, demands and requirements**: Ovum research indicates almost 68% of smartphone-owning employees will use that device for work, as will almost 70% of tablet-owning employees. BYOD allows that behavior to continue with organizational support.
- **Desire to cut costs**: BYOD obviously passes the cost of the fast mobile refresh cycle on to employees, but the need to subsidize personal voice and data plans to account for increased work activity can offset or eliminate those savings.
- **Mobility as a long-term strategic investment**: BYOD allows employees to manage the procurement and upkeep of their mobile devices, enabling the IT team to focus on other strategic needs.
- **Heightened risk profile**: It is significantly more difficult to secure devices and data in a mobile ecosystem stocked with a variety of mobile device types, operating systems and methods of acquiring applications. This is the largest drawback for federal agencies and other high-profile industries and organizations.
- **Federal certifications and standards**: For some federal agencies, BYOD simply isn't an option. Within the U.S. Department of Defense (DOD), for example, all eligible mobile device vendors must have "full operational capability" certification on devices that will access DOD systems and data — a certification that only BlackBerry has secured.

Choose your own device.

Instead of offering an unlimited number of device options like BYOD does, CYOD lets employees choose from a number of pre-approved devices to use at work and, often, personally as well.

CYOD strikes a balance between access and standards, allowing more choice than standard agency-issued hardware but more control and security than BYOD. Let's consider CYOD from the same pros and cons:

- **Fits existing employee behavior, demands and requirements**: Based on Ovum's 2013 survey, nearly 60% of employees surveyed would welcome a CYOD strategy, while only 14% were strongly opposed to it. The biggest variable, of course, is the breadth of devices offered.
- **Desire to cut costs**: CYOD often leads to higher procurement costs than BYOD, because the agency is again bearing the burden of device acquisition. On the other hand, device monitoring, maintenance and support costs could potentially be lower, along with data plans negotiated on a much larger scale — a practice endorsed by the White House's Office of Management and Budget.
- **Mobility as a long-term strategic investment**: CYOD acknowledges the importance of employee mobility, and works to balance access and control for the long-term benefit of both agency and employee.
- **Reduced risk profile**: Perhaps the greatest benefit of CYOD — and thus, the reason federal agencies might favor it — is the improved security posture. CYOD ensures sensitive files and data are only accessed through a select number of pre-approved, government owned devices — devices that can be remotely monitored, managed and wiped without concerns about potential usage outside the government's data ecosystem.
- **Federal certifications and standards**: Here again, CYOD is the superior choice for federal agencies. By relying on the agency to create and maintain the list of approved devices, the IT team is able to ensure all devices offered meet all eligible standards and certifications.

CYOD bridges the gap between employee choice and IT's need to manage and secure the agency. With CYOD, you can easily manage the deployment of multiple device options with the right configurations across the entire organization.

Getting the most out of your mobility program

For government IT leaders looking to roll out a CYOD program or transition from a BYOD to a CYOD program, Insight offers two programs designed to help you link your agency's strategic initiatives to the right mobility solutions.

CYOD workshop

We begin with a pre-visit discovery to identify your strategic objectives. Then, during the on-site session, we map your current IT projects — identifying gaps and sequencing issues — and compare your approach with best practices for mobility management from the public and private sectors.

Use this co-developed road map to successfully incorporate CYOD and mobility solutions with services that can help you best execute your mobile strategy.

CYOD portal

Insight.com's CYOD portal extends CYOD purchasing to employees while maintaining IT policy control and purchasing standards. It's a safer, smarter alternative to BYOD solutions.

Customize your CYOD portal with a set of pre-approved mobility solutions, options and configurations that include services such as imaging, asset tagging, activation and more. End users are guided to the standards and options, and then through your custom approval process or straight to checkout.

Contact Insight's federal government team using the information at the end of this document to discuss Insight's mobility management programs with one of our federal government specialists.

Why Insight?

Every mobility management program has its own intricacies regarding security and data requirements. Agencies that rely on Insight for planning and implementation can expect a number of concrete benefits from the engagement:

1. Reduced device and solution procurement costs due to Insight's relationships and sourcing power
2. A wide variety of portable electronic device options to meet employee needs and mobility requirements, from Insight's broad line card of manufacturers and partners
3. A more focused agency IT team by leveraging Insight's scope, scale and federal government-specific resources
4. A smooth transition to a CYOD-based mobile rollout by relying on Insight's CYOD workshops and portal
5. Reduced agency risk and increased compliance through Insight's sandboxing technologies
6. Significant increases in workforce mobility and data security due to:
   - Superior data backup/recovery capabilities that can scale seamlessly at the projected rates of data growth
   - Easier integration with private or hybrid cloud-based architectures
   - Lower agency risk and overhead requirements through mobile device management, monitoring and software/application management systems

Insight PUBLIC SECTOR

[1]Yasin, Rutrell. "Agencies refine mobile approaches." Federal Times. Feb. 25, 2015.
[2] "Mobility Progress Report: Are Federal Agencies Passing the Test?" Mobile Work Exchange. June 2014.
[3]"Data Breaches in the Government Sector." Rapid7. September 2012.
[4]"2011 Cost of Data Breach Study: United States." Ponemon Institute. March 2012.
[5]"Federal Agencies Need to Enhance Responses to Data Breaches." U.S. Government Accountability Office. April 2, 2014.
[6]"Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication." U.S. Food and Drug Administration." June 13, 2013.
[7]"How Can You Protect and Secure Health Information When Using a Mobile Device?" HealthIT.gov. April 2013.
[8]Forrsights Security Survey. Forrester Research. Q2 2013.
[9] "Data Breach Trends During the First Half of 2014." Risk Based Security and the Open Security Foundation. July 2014.
[10]"The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things." EMC and IDC. April 2014.
[11]"The Internet of Things: Data from Embedded Systems Will Account for 10% of the Digital Universe by 2020." EMC and IDC. April 2014.
[12] "Mobility Progress Report: Are Federal Agencies Passing the Test?" Mobile Work Exchange. June 2014.
[13]"Multi-Market BYOD survey." Ovum. 2013.
[14]"Digital Government: Building a 21st Century Platform to Better Serve the American People." The White House. May 2012.