FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

A Data-Centric Approach to Federal Government Security

Federal Agencies – The Ultimate Target of Cyber Criminals

For many adversaries, government agencies are the ultimate target. Agencies possess top-secret information on weapons systems, government contracts, and other sensitive information. They also collect personal data on individuals inside and outside the agencies.

In August 2014, a cyber attack was reported at USIS, a firm that performs background checks for U.S. government employees. The attack compromised data of at least 25,000 workers, including some undercover investigators. The stolen information included Social Security numbers, birth dates, education and criminal history, and names and addresses of relatives and friends tied to the workers.

As seen in Figure 1, over 61,000 security incidents were reported by Federal agencies in 2013, and over 25,000 of those resulted in the loss of Personally Identifiable Information (PII).

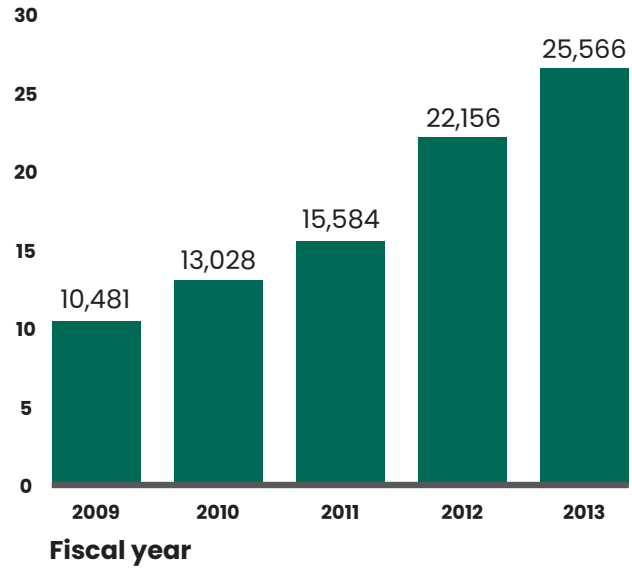
http://www.scmagazine.com/at-least-25k-govt-workers-impacted-by-usis-data-breach/article/367947/

Understanding an Adversary's Strategy

Attackers continue to evolve their techniques to disrupt normal operations and steal confidential intellectual property. They are designing increasingly advanced tactics to infiltrate and maintain a presence on IT systems, waiting for an opportunity to collect and exfiltrate data.

Cyber criminals vary their tactics depending on the defenses of the targeted agency and its supply chain. Some attacks are direct, targeting an agency directly. Other times, they will attempt to undermine defenses at a contractor facility, knowing that the compromised device(s) will eventually provide access to the agency itself.

Number of reported incidents (in thousands)



Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

A sophisticated attack typically includes a number of steps by the attacker, the first five of which must complete successfully to steal data:

Planning The Attack	**The first step includes determining how the attack software will be introduced, the communication methods used while the attack is in progress, and how/where the data will be extracted.**
Attack Software Introduction	**Social engineering is one of the most successful attack vectors because, even today, most people do not understand the risk of opening suspect emails or files or clicking on unverified links. A clever attacker can target users through social engineering attacks such as spear-phishing, where a user is tricked into opening an attachment containing malware.**
Command And Control	**In sophisticated attacks, the malware needs to communicate with the attackers to send discovered information and receive additional software or tools required to continue their attack through lateral movement to other devices.**
Attack Software Expansion or Lateral Movement	**Attackers assume the data they want will reside on multiple machines or be located on adjacent networks and systems.**
Attack Event (Exfiltration)	**For a data-focused attack, this step usually consists of two parts. First, it will copy, obfuscate, and move the target data to an exfiltration point. Often the data will be stored in a password-protected archive or encrypted using proprietary encryption tools. Next, is the exfiltration of the compromised data via remote access tools or the network using FTP, SMTP, or other standard protocols, which help ensure the attacker remain stealth.**
Withdraw	**After a data compromise is complete, the attacker will withdraw and leave attack software in place for future exploitation, or destroy it in an attempt to hide evidence of the attack.**

Multi-stage attacks are sophisticated, using unconventional methods and flexibility to adapt. Defending against these requires equally skillful counter-measures to identify threatening behavior by collecting and correlating attack intelligence. Stopping the attack at any stage is equally effective in preventing data breaches.

Digital Guardian: Data-Centric Security

Fortra™'S Digital Guardian®'s data-centric approach to security is equally effective at protecting against insider threats, outsider threats, or attacks by advanced software. A data-centric approach focuses on three factors; data identification/classification, data monitoring and data protection, to stop the attack at multiple steps.

- **Identify/classify sensitive data continuously**
  – An organization cannot protect data if it does not know where that data is at all times. While many solutions can generate a pointin-time inventory of data through scanning and signatures, this information is largely invalid as soon as new data is created, or existing data is moved or modified. To protect data, an organization must consistently and continuously identify and classify data as it is created or modified.
- **Monitor sensitive data use continuously**
  – Data changes constantly, as business applications, users, customers, and partners interact with it. It moves between internal applications, exists on laptops and mobile devices, or in email to users inside or outside the enterprise. This is particularly important when considering the attacker's goal of stealing data, often

by first copying, obfuscating, and moving the target data to an exfiltration point.

- **Protect sensitive data use contextually** – Protecting data requires more than simply access control or encryption (though both are obviously important). To protect data while allowing full – legitimate – use, requires a contextual understanding of three factors: what actions may be taken with the data; by whom; and, under what circumstances. Privileged users need to configure devices, but prohibited from viewing specific files on those devices.

Automated Data Classification

The key to Digital Guardian's effectiveness is its kernel-based agent, which provides complete visibility to all information and actions on each device. By understanding the sensitivity of each piece of data, organizations achieve greater control without affecting business processes. Digital Guardian supports automated content classification for over 300 file types and 90 languages, including structured and unstructured data types.

Digital Guardian classifies data upon its discovery, access, creation, or revision, and a classification tag is appended securely to its host file or email. Classifications can be permanent or updated with changes to content. Three methods are available for classifying content:

- **Context-based Data Awareness** – Contextual data awareness helps classify data by understanding information about the data file or email message. This includes the application used to create the file, who created/edited the file, the storage location/ repository or the email message sender, recipient, or subject.
- **Content Inspection** – Direct inspection of the data object to identify confidential information allows organizations to apply the appropriate controls based on the content. Automated Data Classification Digital Guardian discovers, classifies, monitors and enforces security policies based on data content in over 300 data formats and 90 single and multi-byte languages, across physical or virtual servers, desktops, laptops, and email platforms.
- **User Classification** – Digital Guardian's User Classification complements automated data classification methods by allowing a user to classify data manually.

Digital Guardian maintains classifications through data "tags" that persist with the data throughout its lifecycle, or until the classification no longer applies due to a change in the data. Tag inheritance allows classifications to follow the data. A derivative ("child") file automatically inherits classification tags from the source ("parent") file.

Persistent and inheritable tagging maintains consistent identification, usage auditing, and policy enforcement among files of common content. This assures sensitive data remains visible to Digital Guardian, and controlled as it moves between files, allowing organizations to monitor, analyze, and manage its entire lifecycle with appropriate policies.

Policy Enforcement on The Endpoint - On and Off the Network

Digital Guardian agents not only classify data, they also enforce usage policies on the endpoint, on or off the network. These agents do this with an understanding of three factors:

- The data being acted on.
- The action being taken.
- The user or application taking the action.

This intelligence allows unimpeded authorized use of data while preventing people or attack software from misusing data. All actions (or attempted actions) are logged in an evidentiary quality audit file for analysis and alerting.

Real Time Threat Detection

When information security violations occur, it is essential to respond immediately. Regulations such as the Federal Information Security Management Act (FISMA), White House Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) PII Requirements, and the National Infrastructure Protection Plan (NIPP) require immediate response to information security breaches regardless of whether they involve classified information.

Digital Guardian provides real-time threat detection: the ability to detect, in real time, patterns indicative of malicious software, system compromise and user behavior, via intelligent correlation rules. These simple to complex rules allow agencies to log, alert, and retain activity in order to develop alert sequencing; a combination and/or sequence of rules indicative of malicious behavior.

Rules can trigger several actions while providing incident response teams with the information they need to address attacks:

- Immediate alerting to the presence of an attack (via prompts).
- Quarantine the machine from the network, without impacting communication to the Digital Guardian Management Console.
- Initiate the collection of forensic artifacts required to support the forensic investigation, such as detailed process information and memory analysis detail.
- Stop the attack in progress by killing a process.

Defending Data from Sophisticated Attacks

A military term that transfers effectively to cyber threat defense is “force multiplier.” In military terms, this is a capability that when added to a combat force, significantly increases the combat potential of that force and thus enhances the probability of a successful mission. In the advanced threat world, that force multiplier is an integrated platform that can detect, correlate, and create actionable intelligence, and then quickly and effectively act on that intelligence with prevention and containment controls.

Digital Guardian – the only data-aware advanced threat solution with visibility from endpoint, server, and network agents – is a force multiplier. It works with other cyber defense products to provide organizations with a coordinated, multilayered defense. Digital Guardian can consume data intelligence feeds from third party sources, as well as provide actionable threat intelligence to SIEM products, enriching the events aggregated from network devices and disparate logs. Digital Guardian also integrates real-time malware alerts from leading network security solutions such as FireEye and PaloAlto Networks to identify and contain zero-day attacks on endpoint systems.

Proven in Enterprise-Wide Deployments

Digital Guardian provides visibility, control and protection across Windows, Linux and MAC host systems, virtual environments, network, mobile and cloud. It is the only solution to address both insider and outsider threats with a single kernel level agent. Some of the world's largest enterprises have deployed Digital Guardian, with large scale deployments in excess of 300,000 agents managed by a single server.

About Digital Guardian

At Digital Guardian, we believe in data protection. We know that within your data are your company's most valuable assets. The sum total of innovations, plans, and potential. We protect your company's sensitive information in a way that minimizes risk without diminishing returns.

For over 10 years, we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats. Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.