VERDASYS

Protecting Against WikiLeaks Events and the Insider Threat

JANUARY 2011

WHITE PAPER

The New Face of the Insider Threat

The current news blitz regarding the massive breach of secret State Department cables to the WikiLeaks website overlooks some important questions about its root causes: Where did the leaked data come from? What are the motivations behind the individual or individuals leaking the data? And, finally, is there any way to prevent sensitive government and company data from showing up on sites like WikiLeaks?

The information supplied to WikiLeaks, and to future "social justice" websites, comes from trusted insiders; privileged users within governments and companies from where the data is stolen. They are co-workers, often with the most critical responsibilities, who have been trusted with access to very sensitive information to accomplish their jobs.

As with many Internet sites information can be sent to WikiLeaks securely and anonymously. And, if the leaker is known, WikiLeaks will go to great lengths to protect the individual's identity. This lack of personal accountability eliminates much of the moral hazard that deters otherwise risk-averse users from exposing sensitive data. With secure sites purpose-built to shelter them, a much wider pool of potential violators can now consider such subversion with little fear of repercussion.

In this new reality it is impossible to know who might compromise sensitive information, and the risk is not limited to the government or military. For instance, would a case manager at a healthcare insurer leak preliminary and unconfirmed research data in hopes of publically pressuring the company to cover an experimental treatment for a terminally ill friend? Or, perhaps a bank executive, disgruntled because of a missed promotion or lost bonus, leaks a "health check" audit from the Federal Reserve — or even potentially embarrassing personal data about a senior manager; the list goes on, with the real risk of affecting any organization whose confidential information is critical to its reputation and business performance.

Insider theft of sensitive data is not new. WikiLeaks is just the latest outlet for the disaffected individual to be amplified in our interconnected world. Founded in 2006 to be a safe haven for whistleblowers, WikiLeaks has published stories on government corruption in Europe and Africa, and exposed the controversial Copenhagen Accords on climate change. It has only recently made global headlines thanks to PFC Bradley Manning's (and perhaps others) alleged theft of US Military and US State Department information. However, unlike historical insider threats, once WikiLeaks publishes data, it is available to the entire free world instantly and without containment.

The new wrinkle WikiLeaks brings is its ability to provide an unprecedented level of public visibility to private information from any source, about any subject, and with the express intent to subvert authority. To some individuals, like alleged data thief PFC Manning, the risk of being caught does not outweigh the reward of making public sensitive and potentially embarrassing information to wield a grudge or promote a "social justice" cause. These activist personalities not only have a global platform from which to share the data they have stolen, they also have the ability to compromise huge amounts of information more quickly and efficiently than ever before. Thanks to cheap storage devices like removable media found almost anywhere; DVD/CD burners standard on every computer; large storage webmail, secure FTP access; and wireless networks, employees with personal agendas will be more likely to jeopardize their careers in order to make a passionate statement.

But the effect of insider data theft goes beyond social justice, and can have a substantial economic impact from board rooms to consumers around the world. Historically, the objective of sensitive data theft

has been to steal for economic gain or espionage; certainly, the betrayal of trust by privileged users has been around as long as there have been secrets. However, because of technological advances in the storage and movement of data, the ease and impact of insider thefts encourages the volume of compromise to rise exponentially. In the last few years, an amazing amount of data has been stolen by insiders at the very largest companies in the world, including documented incidences from Ford, GM, LG, and Motorola to name a few. According to a 2010 study *"A Statistical Analysis of Trade Secret Litigation in Federal Courts,"* by Gorgonzola L.R. (2010), trade secret and IP theft doubled from 1988 to 1995, and doubled again from 1995 to 2004. Trade secret and IP theft is projected to double again by 2017 with 2008 losses reaching one trillion dollars! Who knows what the next target is, or how damaging the exposure? Whatever it may be, the addition of social justice to traditional insider threat motivations means no industry or institution — commercial or government — is immune. From corporate boards to world leaders everywhere, everyone must face the reality that the insider threat is a growing danger that can no longer be overlooked — or they risk suffering its unpredictable consequences.

The Challenge of Preventing Insider Theft

The privileged user is a unique role within an organization. They are given the right to access sensitive applications and information with the express trust to know and abide by all their governing policies. Because of technological limitations, it is a common and accepted risk for privileged users to have access rights to data outside the scope required for their jobs to ensure no legitimate access is denied. But this trust is difficult to verify, and typical IT security controls are unable to monitor activity or enforce policy at the file, application, and user levels simultaneously.

Because of the necessary trust involved, the insider threat is the most difficult data security challenge to solve. Historically, IT security defenses were created to harden the external perimeter of a network to protect from outside threats. Identity and Access Management (IAM) systems were added to authenticate users and control their access to systems and applications, but do not extend to data access control. DLP technology was introduced to prevent data leaks, but at best it is used only to monitor the network and attempt to detect PII data (usually SSN or credit card numbers) from leaving the enterprise improperly. As part of the "defense in depth" security strategy, companies have deployed a variety of point technologies bundled into non-integrated "suites", or as separate tools to encrypt hard drives, email, data, or removable media. However, as traditional IT security assumes users with authorized access pose no risk, these approaches are fundamentally unable to prevent the types of risks demonstrated by the alleged collaboration between PFC Manning and WikiLeaks. The fact is none of these technologies have been effective in preventing insider threat risks.

In particular, the Data Loss Prevention (DLP) approach is often marketed as a solution to the insider threat has proven to be inadequate. Content-aware DLP technology is designed to scan data based on pattern recognition as it traverses perimeter-based infrastructure. Pattern matching can be effective for privacy data such as credit card numbers, but is not designed to handle irregular or imbedded content like images, vector drawings, equations, abstract word groupings, or formulas often found in trade secrets, intellectual property (IP) or classified materials. This limitation in content scanning technology leads to broad definitions for what is sensitive, leading to high "false positive" rates — meaning alerts are sent showing sensitive data was detected, but are confirmed upon further investigation to be part of a legitimate activity. These "block and investigate" steps quickly become unproductive and costly. For commercial adopters of DLP like banks, insurers, and IP-heavy industries, the consistent pain inflicted

by false enforcement has all but prevented the technology's use for policing insider activity without the risk of lost productivity and competitiveness.

The basic design of network-based DLP also makes it easily defeated by even non-technical users. For instance, an oft-used strategy by insiders bent on stealing data exploits the fact DLP typically doesn't detect content obfuscated by the user (e.g. imbedding data as photos in Microsoft Office documents; zipping and encrypting data with free software). But the fatal flaw of DLP is that it simply cannot operate where the insider operates, and where the insider threat almost always occurs — at the point of data use. An insider will burn data onto a CD/DVD, or print a hard copy, or transfer to removable USB media, or employ any method to which content-aware network DLP is blind. Even encryption technology, which is often times used as a stop-gap to enforce file-level access controls, (and can be effective for lost laptops or removable media), cannot prevent the privileged user threat since it provides no further audit or control after an authorized user decrypts the disk or file.

Solving the Insider Threat

So what are effective measures to protect against the theft of sensitive data by privileged users? The answer was first documented in a 1983 study by the DOD called "The Trusted Computer System Evaluation Criteria" (TCSEC) — a.k.a. The Orange Book. The Orange Book was the first to introduce the notion of a "reference monitor" technology as the way to counter insider threats by operating independently between the data and a privileged user. The reference monitor concept was designed to allow full monitoring and control of a user's activities while still understanding the transaction context which determines the risk when data, user, policy, and activity intersect. The reference monitor requires a user's machine to be "instrumented" so as to recognize and intercept risky actions before they can occur. In order for a host system — a laptop, desktop, workstation, classified workstation, or server — to become instrumented it must contain a local reference monitor (software agent) able to confirm the identity of the authorized user; the contextual and content characteristics of the data; the transaction context of the user's actions; *and* whether the policy logic relating all those variables allows the activity to occur. Finally, the reference monitor must combine this complex event metadata into auditable, forensically-accurate event logs while simultaneously applying appropriate controls to mitigate the risk of data compromise — all in real time.

Based upon its description in the TCSEC, a reference monitor technology must have several important characteristics to be successful. It must:

- Operate independently of any application or other security technology
- Be tamper resistant and hardened to prevent it being disabled or spoofed by a knowledgeable privileged user
- Identify data by its context (file type, application source, network source, etc.)
- Analyze data transactions in context (who is the user, what actions are being taken, when does the action take place, what applications are used, etc.)
- Have the ability to interact with the user before the risky transaction is complete
- Initiate a response without necessarily preventing the user from doing their job
- Deter or prevent data compromise while recording all events within an evidentiary sound process

To prevent a privileged user from single-handedly exposing sensitive data to a media outlet like WikiLeaks; a market competitor; or a foreign government, you must instrument the host with secure reference monitor technology:

"Be closer to the data than the insider and yet not be in the way; the only answer is to instrument every data handling instruction at the operating system level, and tie that instrumentation to decision support. In some circumstances, you will want that decision support to be automated and autonomous. In other circumstances, you will want to ring a silent alarm. In yet other circumstances, you will want to allow the insider to proceed after he acknowledges his intent to cross a boundary. In all cases, you will want evidentiary-grade logs."

— **DAN GEER,** CISO, In-Q-Tel

Verdasys Digital Guardian

Verdasys created Digital Guardian to be a commercial implementation of the reference monitor. The solution is designed, architected and implemented specifically to mitigate the risk of the trusted users. Since 2003, Digital Guardian has been proven time and again by our customers to be highly effective at preventing insider threat risks, and will substantially and measurably reduce the likelihood that your company will become a victim of the WikiLeaks paradigm.

Digital Guardian is a proven, multi-tier data security platform which uses host and network based reference monitors to identify, audit, and protect critical data across your extended enterprise. Whether on workstations, laptops, or servers — inside or outside the organization, in physical or virtual environments — Digital Guardian is there to monitor, log, warn, control and, if necessary, block prohibited actions by trusted end users. The Digital Guardian platform delivers policy-driven data discovery, classification, monitoring, control, and transparent encryption for computers, files, devices, network channels (including email, IM and FTP), and applications. Digital Guardian is the only solution on the market that allows companies to:

- Discover and classify sensitive data, and measure how it is used by employees, contractors, partners and outsourcers from enterprise to forensic scales
- Assess the risk associated with the sharing of sensitive data, enabling managers to make informed risk-appropriate business decisions, and create effective data security policies
- Implement automated and rules-based data security, driving accountability down to the user and leading to voluntary compliance and increased risk-awareness
- Alert, block, and record high-risk behavior, ultimately preventing costly and damaging insider threat incidents

Verdasys Digital Guardian was designed specifically to prevent privileged users from compromising sensitive data using the reference monitor concept. Digital Guardian has been proven to deter, detect, and prevent the types of data loss incidents attributed to WikiLeaks.

Digital Guardian and Insider Threat Mitigation

The Digital Guardian platform is uniquely positioned to prevent most insider threats. It begins with Digital Guardian's scalable architecture, designed from the start to deal with the challenges of protecting data from trusted users. Digital Guardian Agents operate in a combined kernel and user mode, allowing them to monitor and control the activities of all users logged into or accessing an instrumented host system. Every activity is recorded and stored as situationally-aware and causal event logs with admissibility and weighted precedence as primary forensic evidence in criminal and civil cases both domestically and internationally. The agent is hardened, tamper-proof, and can be made invisible on the host system, making it a highly effective deterrent against data misuse by privileged users, including system administrators and security managers.

The agent architecture is also capable of understanding the context of data (content, type and title, source) the context of the user (identity, group, role, clearance) and the context of the transaction (type, time, connections open, applications open, location). With this holistic knowledge, the agent applies precise, risk-based logic to initiate the correct mitigating response before a privileged user completes a risky transaction.

The Digital Guardian platform is unique in that it offers multiple automated policy control options enabled autonomously on or offline. Where most DLP solutions are used for passive monitoring and alerting, Digital Guardian is used in enterprise-wide deployments where multiple levels of data security controls are required to actively manage the flow of sensitive data across tens of thousands of laptops, desktops, and servers in globally distributed IT environments. Because Digital Guardian controls are designed to be risk-appropriate, organizations achieve optimal business value by allowing for the maximum amount of collaboration per transaction within a predetermined level of acceptable risk. Control types include:

- **Incident Alerting:** when a user violates a policy or rule, Digital Guardian will deliver alert notification emails to security and line-of-business managers, notifying them in real time that a potential data compromise has occurred detailing the policy and rules violated.

An alert indicating that classified information was being copied to removable media would have warned the security team in real time that PFC Manning was allegedly copying files illegally.

- **Warning and Justification Prompting:** One of the most effective ways to counter the insider threat without interrupting normal operations is to deter the privileged user in the act of compromising data. This control stops short of blocking the activity, and gives the employee a choice to take the action; stop the action; or choose an alternative path to complete the activity in a less risky way if it is a legitimate transaction. Prompts and justifications are exact, persistent, and cost-effective training tools that are applied in real time, and are fully auditable to meet regulatory requirements.

If PFC Manning had been prompted that his alleged actions were improper and were being recorded, he would have likely ceased immediately. His activities would have still been recorded and alerted to security personnel, while at the same time no data would have left the secure facility.

- **Encryption Controls:** Digital Guardian also includes fully integrated policy-based encryption for network file shares, removable media, email, and individual data files. Digital Guardian's patented encryption includes an automated key management and recovery system and 256-AES strong encryption. Digital Guardian encryption controls can be used as both data loss and data access controls based on who the user is, and their rights to the data. [For instance, if an authorized user and a network administrator both accessed the same machine with encrypted files, only the authorized user could decrypt them.] Encryption rules can also be used to ensure audited and secure collaboration among trusted users of similar entitlement across the enterprise, including those in virtual environments and authorized 3rd parties.

Policy-based encryption controls would have allowed PFC Manning to move the data to CD, but would have eliminated the data loss as the content would have been encrypted with no ability to decrypt it outside of the secure facility.

- **Blocking:** Although a control of last resort, Digital Guardian can block a transaction outright. Blocking controls are most often used when the transaction is suspect, or the context of the risk is very high (e.g. user accessing a system remotely, with a sensitive application open, and uploading large amounts of encrypted data to a personal webmail account).

In the alleged case of PFC Manning, a blocking rule could have prevented any data categorized "SECRET" or above from being moved to removable media without authorization. PFC Manning would have simply been blocked from completing any transactions prohibited by his status.

In all cases, the attempt to leak classified information to WikiLeaks would have been prevented, and the perpetrator(s) would have been accurately identified with secured forensic evidence provided by Digital Guardian for admissibility in the Courts Martial. Furthermore, the Security team would have been alerted of the attempted compromise in real time; the suspect(s) would have been apprehended, and no data would have left the secure facility.

Digital Guardian Architecture

Verdasys Digital Guardian is a comprehensive, proven host and network data security solution for tracking and protecting the flow of critical data across your extended enterprise. Digital Guardian consists of a central command servers and a variety of host and network sensors that are deployed across an enterprise. Digital Guardian is fully internationalized and designed for global enterprise deployments.

Digital Guardian Server

The Digital Guardian Server is a web-based application server and console that is the command center for the Digital Guardian Platform. The Digital Guardian Server:

- Manages and monitors all Digital Guardian Agents and network sensors
- Captures, aggregates, and stores all user activities related to sensitive data
- Enables the creation of flexible data classification frameworks and rules
- Manages data security policies and distributes them to all Digital Guardian Agents for enforcement
- Triggers administrative alerts and email notifications when security policies are violated
- Includes an easy-to-use reporting engine for high level, detailed, and custom report creation

The Digital Guardian Server manages all communications; captures, aggregates and stores all user activities related to intellectual property; drives the data classification framework; and manages security policies, distributing them to Digital Guardian Agents for enforcement.

Digital Guardian Agent

The Digital Guardian Agent delivers policy-driven IP discovery, classification, monitoring, and security controls across the extended enterprise. Capable of both context and content data awareness, it also includes integrated removable media, server, file, and email encryption to enforce risk-based usage policies. Agents are hardened, tamperproof, and can be made invisible on the host system. With its root-level visibility to all data activities on the endpoint, Digital Guardian effectively regulates trusted insiders — including system administrators and IT security managers — by providing an auditable and proactive security model independent of infrastructure or user

privilege. Digital Guardian Agents support and are fully capable across Windows, Linux, Citrix and VDI/VM environments.

Digital Guardian Network Sensors

Verdasys offers both host and network sensors. Although not effective against insider threats on the host, network sensors do offer greater defense in depth for compliance use cases. Digital Guardian Network Enterprise Information Protection (EIP) is a two-tiered Deep Session Inspection™ architecture that consists of policy sensors placed around the network to detect and/or prevent data breaches, and a central management center to distribute policies, and collect and organize alerts. Each Network sensor can be delivered as a preconfigured appliance or software. Digital Guardian Network Sensors allows you to gain control of your network with enabling features, such as:

- Control of proxied and direct-to-internet traffic
- Inspection of all network traffic for sensitive content including attachments and compressed files
- Blocking of unauthorized traffic based on content, application, and/or protocol
- Quarantine sensitive or unencrypted e-mails before they leave the network
- Monitor all channels including e-mail, web, webmail, instant messaging, file transfers, telnet, and peer-to-peer
- Monitor external traffic and/or on internal traffic segments to view all network traffic across an organization

Decision Support and Information Assurance

eDiscovery and Forensic Reporting: Digital Guardian includes a fully integrated case management and forensic capability that enables the tracking of data usage by users and groups and allows targeted investigation. All usage logs are in a tamper-proof evidence form (encrypted and digitally signed) and stored for future validation. Drill-down reporting is based on application, file type, network, user action, classification, encryption status, and type of device (desktop, laptop, terminal session). Digital Guardian's tamper-resistant agents record situationally-aware and causal event logs with admissibility and weight precedence as primary forensic evidence in criminal and civil cases, both domestically and internationally.

Audit and Reporting Decision Support Analytics: Digital Guardian deploys with a fully integrated data warehousing and reporting engine that provides high-level, aggregate visibility into data usage across the enterprise with the ability to drill down to forensic levels by user, file, policy, or activity. Digital Guardian reporting includes predefined compliance reports for common regulations like HIPAA and PCI, and an "Easy Query" wizard for the creation of custom reports on the fly. Its powerful analytics provides actionable reporting and real-time decision support on the state of data risk across the entire organization at any scale.

Conclusion: Secure Data Collaboration and Prevent the Insider Threat

WikiLeaks is merely the latest enabler of the populist-driven "Robin Hood" syndrome, but it represents a dangerous new chapter in the asymmetric struggle against the insider threat by combining social activism with the ease, anonymity, and instant global reach of the Internet. The immediate problem facing government agencies and corporate boards is how to prevent trusted employees from leaking sensitive information to WikiLeaks or similar outlets. In these cases, we know privileged insiders are the source of data loss; but we also know that traditional network-based DLP solutions and tactical security point products will continue to fail to detect or prevent rogue users from stealing or exposing unlimited amounts of classified information until it's too late.

To prevent the insider threat and sensitive data loss, organizations must deploy a solution based on the "reference monitor" concept that operates closer to the data than users. The technology must be tamper resistant and hardened; scalable and flexible enough to meet enterprise size and complexity; intervene interactively with the user before a risky transaction can be completed; and securely log and store every user's actions with evidentiary fidelity to support investigation and prosecution.

Digital Guardian goes well beyond the capabilities of DLP to deter, detect, and prevent insider threats. It is the foundation for a strategic data-centric Enterprise Information Protection program that increases the competitiveness and agility of your enterprise by allowing the value of sensitive information to be maximized securely. With Digital Guardian, organizations can implement uniform and meaningful protection for intellectual property, privacy information, and sensitive secrets. It effectively addresses the risks of both insider and outsider threats caused by broken internal processes; lack of end-user training; or the insecure sharing of sensitive data with third parties.

Digital Guardian is the only solution available today that meets all of these needs, and has been proven to scale across global organizations. Since 2003, it has been deployed to protect organizations from the insider threat at Fortune 500 manufacturing, aviation, defense, energy, healthcare, financial services, insurance, and hi-tech companies, and government agencies around the world. If implemented properly, Digital Guardian would most likely have prevented the exposure of classified information to WikiLeaks, and with it the potential for a trusted insider to harm the United States and our global allies for years to come.

With over 200 customers utilizing Digital Guardian across 2 million users, Verdasys brings to bear more than just technology. Our experience working with the world's leading companies in deploying successful EIP programs empowers our services and support teams to help your organization deploy EIP technology, methodology and processes. Verdasys is the preferred partner for companies serious about protecting their sensitive information and mitigating the risk of insider data theft.

ABOUT VERDASYS

Verdasys provides Enterprise Information Protection solutions that are the foundation of our customer's global data security strategy. With greater than 2 million security agents deployed at over 200 of the world's leading organizations, Verdasys is the proven global leader of Enterprise Information Protection solutions for information protection and compliance.

Verdasys headquarters is located in Waltham, MA, with offices in London, Munich, Rome, Madrid, Athens, Tel Aviv, Tokyo, Osaka, Taipei, Singapore and Shanghai.

VERDASYS

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

www.verdasys.com

XXX 01-13-11