



Leading Edge Technology Q4 2011

# Data Protection Strategies in the Age of the iPad®, Malicious Insiders, and PCI

The information explosion gives hackers, thieves, and malicious insiders a target-rich environment that perimeters can't defend. To thread the needle between information protection and legitimate access, CISOs must focus on defending the content of files and communications, not just containers or conduits. Effective protection combines content awareness, policy-based protection, and strong authentication to discover and monitor sensitive information, protect it as it moves across networks, to mobile devices, and in the cloud, and deny illegitimate access without compromising the productivity of legitimate users.

The new Information and Identity Protection solution from Symantec meets all three requirements with integrated, fully-compatible solutions for Data Loss Prevention, Encryption, and strong multifactor User Authentication. The highly automated solution discovers structured and unstructured data and links files to owners and heavy users. It encrypts protected information with a modular, highly scalable solution that remains effective even on lost or stolen devices, or in the cloud—with complete transparency to authorized users.

Symantec Information and Identity Protection addresses the issues raised by use cases involving mobile iPad® users, large-scale disclosures of breached content such as WikiLeaks, and the compliance demands of privacy regulations and standards.

## **Global threats to enterprise information**

The explosion of information in enterprise data stores and online has created a target-rich environment for hackers, thieves, and malicious insiders, and multiplied the risk of errors by well-intentioned employees simply trying to do their jobs. As the risks of data loss and inadvertent disclosure have grown, so have the costs: hacker attacks have compromised technology firms, credit-card processors, and defense contractors, insider exploits have brought down major banks, and the financial, regulatory, and legal impacts are growing by leaps and bounds.

Data theft is no longer just a crime of opportunity by amateur vandals. External hacking and malware attacks now support a covert industry that supplies tools for theft and exchanges for stolen information. Malicious insiders steal information for direct personal gain, to cover up trading errors, or to enhance their careers by offering proprietary intellectual property to prospective employers. Loosely affiliated online organizations disclose confidential information held by companies, governments, and banks based on obscure grievances—and governments report an ominous rise in sophisticated long-term cyber spying by rival states.

Social engineering, inadequate security training, and errors by well-intentioned employees play a role in this new environment. Data thieves scrape information from social networks like Facebook and LinkedIn to target employees with customized "spear-phishing" appeals, then open doors for a breach by implanting key loggers and spyware to capture passwords. Poorly-trained employees place unencrypted copies of confidential data on exposed servers and laptops, creating "data spills"—unmanaged releases of sensitive information to untrusted



Leading Edge Technology Q4 2011

locations, protected at best by passwords the simplest dictionary attack can break.

### **Dissolving security perimeters**

As enterprise data comes under sustained global assault, traditional enterprise perimeters are dissolving. Laptops travel outside defensible perimeters, and have been responsible for major breaches. Portable storage devices are carried across perimeters, making containment a challenge. And consumer-style devices like tablet computers and mobile smart phones compound the problem with platforms that change constantly, making them difficult to secure and manage.

Cloud computing also dissolves enterprise perimeters in a similar way. Data in the cloud is almost perfectly portable: even the people directly responsible for it rarely know its physical location, which may be directly or remotely accessible to unknown actors with powerful technical Resources and plenty of time. Finally, employee mobility is dissolving the “human perimeters” that once kept intellectual property confined within a stable enterprise workforce. Long-term employment and company loyalty were in decline even before the economic downturn churned IT and business staffing. And job stress and financial, political, or career motivations can quickly turn an overworked specialist into an insider threat.

### **The CISO’s dilemma**

Enterprise Chief Information Security Officers (CISOs) can’t respond to rising threats and dissolving boundaries simply by restricting availability of information assets or use of new technologies. As with any business asset, information’s value comes from use, not possession. And new technologies like tablets, smart phones, and cloud computing are popular precisely because—despite the risks—they make individuals and companies more productive. The CISO’s strategic imperative is to balance information protection and legitimate access, focusing on the information itself, wherever it resides or travels. New, information-centric technologies hold the key.

### **Integrated Information and Identity Protection**

Symantec Information and Identity Protection integrates compatible, fully-aligned solutions for Data Loss Prevention, Data Encryption, and strong multifactor Authentication.

#### *Data Loss Prevention*

Symantec™ Data Loss Prevention simplifies the detection and protection of confidential information and intellectual property, whether held in structured formats such as financial records or Social Security numbers, or as unstructured text in files and emails.

The solution works in two stages. The first, *Discovery* phase, locates sensitive information across enterprise networks, storage, and endpoints. Discovery includes technologies that pinpoint the location of *structured* data from “fingerprint matches” with database fields,

Social Security/National Insurance (UK) and credit-card numbers as well as *unstructured* data embedded in the text of patent applications, legal disclosures, and financial records in hundreds of file types including user-defined and custom formats.

The Discovery process is a powerful tool for CISOs to communicate the scale and urgency of the information protection challenge. It identifies the owners of sensitive information, establishes business awareness of and accountability for information protection, and supports



## Leading Edge Technology Q4 2011

A consensus approach that keeps the CISO and IT staff out of an adversarial role with business users. Unstructured or free-form information presents a challenge to Discovery processes, since the software can't rely on defined database locations or invariant patterns for recognition. Too often, the burden of classifying and locating unstructured data falls on IT staff who may not be sensitive to the business value of the information assets under review, face competing demands for their time, and don't own the assets in the first place.

Content owners, the business clients of IT, are in the best position to identify information—structured or unstructured—that requires protection. But their knowledge and judgment are of no value if owners can't be identified and located. Data Insight identifies content owners and heavy users according to the frequency with which they access files and records. Once identified, owners can be recruited to assist with the classification of information as sensitive or not, including an advanced Vector Machine Learning technology for classifying unstructured information.

This approach integrates automated Vector Machine Learning into Symantec Data Loss Prevention to reduce the burden of identifying sensitive information in unstructured data. Content experts or data owners train the software by providing positive examples of proprietary source code, merger-and-acquisition documents, and other intellectual property, as well as negative examples of data the machine should ignore. The machine extracts features that differentiate the positive and negative examples to create a statistical profile that yields a similarity score when compared against an unknown document or message. A companion paper describes this process in detail.<sup>4</sup>

The second stage of data loss prevention is to control information movement. Symantec Data Loss Prevention applies the same technologies—"fingerprint" matching for structured and Vector Machine Learning for unstructured data—to flag or block movement of sensitive information to unsecured storage locations, across the network, or embedded in email and instant messaging. This blocks Unauthorized transmission of information to uncontrolled locations or unauthorized individuals, and maintains a pared-down, well-managed information environment, with no new unauthorized data stores.

### ***Encryption***

Highly secure, efficient encryption meets internal policy and external regulatory requirements to protect sensitive information:

- In all locations, whether inside or outside the corporate firewall
- With optional coverage for any device from servers, fixed network endpoints, thumb drives, smart phones, and across network and email
- Explicitly integrated with Symantec Data Loss Prevention, to identify sensitive information and, based on encryption policies, encrypt it in the same pass

Symantec Encryption solutions protect information on mobile devices and to and from the cloud, to protect email as well as stored information for devices and locations where information is at greater risk. Compared with point solutions or "all-or-none" approaches, Symantec solutions are highly modular, allowing a staged implementation that protects the most critical information first and allows a Rational, budgeted rollout. In addition to encryption, Symantec also offers solutions to disable a lost or stolen laptop using a "poison pill". Used with encryption, this technology ensures that both data and mobile device are unusable by decommissioning it in the field.



Leading Edge Technology Q4 2011

### ***Authentication***

Strong authentication closes the source of many breaches and exploits, but complex processes involving multiple or constantly changing passwords impair productivity, raise IT support burdens, frustrate users, and create incentives for bypassing security controls. Worse, new attack technologies and social-engineering exploits are specifically designed to steal passwords, eroding their protection against unauthorized access.

Cloud-based Symantec User Authentication solutions provide multiple strong authentication deployment options to deliver efficient, economical, multifactor authentication using either hardware or software credentials. Authentication options include—but don't require—hardware one-time-password tokens, smartcards, mobile phones, short messages (SMS) sent to mobile devices, and more—whatever authentication method best matches an organization's policies and infrastructure.

In addition to multifactor authentication, Symantec offers risk-based authentication that evaluate whether a user and the device through which he or she is seeking authentication is known, unmodified, connecting from an acceptable location, and acting as expected. Evaluating these factors, it can grant unchallenged access in the case of low risk, and challenge users evaluated as high-risk to authenticate using an out-of-band process such as a phone call.

By delivering strong authentication through the cloud, using existing devices such as mobile phones, and adding passive device and behaviour profiling, Symantec User Authentication minimizes the costs of dedicated infrastructure, and frees IT resources for other priorities. In addition, it is easily scaled to cover new devices, platforms, and authentication mechanisms—an essential feature in the fast-changing world of consumer-style devices and ever-shifting online threats.

### **Three use cases: iPads, WikiLeaks, and PCI compliance**

Three short use cases demonstrate how an integrated solution like Symantec Information and Identity Protection works in everyday, realworld situations.

#### ***Data protection for iPad users***

Symantec Information and Identity Protection complements the security features of mobile devices like the iPad to address enterprise-level concerns about data protection:

- *Encryption* protects received transmissions and stored data, so sensitive documents that are sent encrypted, stay encrypted
- *Multifactor authentication* uses the device itself to authenticate access to protected network resources, and disables the credential in case of loss or theft
- *Data-loss prevention* can block and flag unauthorized transmission of sensitive materials even when they are encrypted, alerting managers to out-of-policy behaviors even when they pose no immediate threat to information protection

#### ***WikiLeaks***

The WikiLeaks data breach originated from an authorized, properly authenticated insider whose privileges included access to hundreds of thousands of highly sensitive documents. A comprehensive



## Leading Edge Technology Q4 2011

program of information and identity protection has the capability to prevent, stop, or respond to attacks like this one from malicious insiders:

- *Data Insight* links individuals to files, typically to identify their owners. But it can also flag high-volume access, as when an individual—however well-authorized—downloads thousands of confidential documents as in the WikiLeaks case
- *Information prioritization* places high-risk “data spills” at the front of the remediation queue, reducing response time when someone accesses particularly sensitive data and prompting quick review of incidents like WikiLeaks
- *Issue and remediation markers* alerts users that their out-of-policy behavior is being monitored and reported, raising the probability that questionable activity will be aborted before it causes a full-fledged breach

### **PCI compliance**

Payment Card Industry Data Security Standards require that sensitive data be identified and stored in protected locations. Symantec Information and Identity Protection identifies the relevant data—in both structured and unstructured formats—along with their owners, so that:

- *In-depth security audits* can be focused on the highest-priority data, circumventing the cost and delay of blanket audits
- *Business owners* stay aware of the location and security of their data, and maintain accountability for its protection
- *Strong authentication* as required by PCI limits access to critical payment-card processing systems to authorized users, and establishes accountability

### **The Symantec advantage**

Symantec offers all three components of effective Information and Identity Protection—Data Loss Prevention, Encryption, and User Authentication—with technology and market-leading features in every component, and deep integration for efficient management and effective protection. Symantec is the technology and market leader in IT security and information protection, with the scope, scale, and vision to integrate best-of breed technologies into effective, compatible, easy-to-manage solutions. Symantec Information and Identity Protection integrates Data Loss Prevention, PGP® Encryption, and Symantec User Authentication with technologies to deliver seamless coverage and efficient management, scalable to meet business requirements from a single department or office to a global multinational organization.

For further information on any of our content, contact Leading Edge Technology.

**08456 44 79 49**

**[www.leadingedge.uk.net](http://www.leadingedge.uk.net)**