



PROTECTING INFORMATION

According to the McAfee white paper *Data Loss by the Numbers*, of all general data types, the most commonly compromised information includes names and/or addresses, Social Security numbers or equivalents, and credit card numbers.¹



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

In Operation Shady RAT (Remote Administration Tool), McAfee gained access to a malicious command and control server that was used in multiple targeted attacks. More than 70 organizations had been targeted using this system, and the operators were pilfering information for at least six years. The longest exfiltration of sensitive information from a single compromised organization lasted 28 months, and the average lasted almost nine months. In total, upwards of a petabyte of information was stolen.¹

Protecting Valuable Data Assets

Challenges

It's no surprise that malicious insiders and external attackers alike covet sensitive information such as intellectual property, financial records, and personal information. This information has value, and therefore it's a target. Additionally, information is at risk due to careless and negligent employees and other users with elevated levels of trust and access such as partners and consultants. Because information helps drive the business, it must be accessible and usable, lest its value be diminished. Striking a balance, where access is allowed while risk is mitigated, is essential.

Difficulties arise when organizations understand just how much sensitive information they have. Beyond volume, the information rarely resides in a single location; instead, it is spread across structured data stores such as databases and unstructured data stores such as file servers, laptops, smartphones, email messages, removable media such as USB drives, and the like. Generally, this information is accessible from multiple users, across multiple groups, and in multiple geographies. In many cases, the individuals that need access may be business partners or other groups outside of the organization's control.

Most organizations are aware of the results of not adequately protecting their information—with issues ranging from competitive disadvantage brought upon by stolen intellectual property and regulatory penalties to class action lawsuits and costs associated with disclosing breaches. While the implications are clear, executing a solution can be challenging. Common technical issues experienced by organizations trying to build an effective information protection strategy include:

- Discovering where the information is
- Classifying the information
- Enforcing policies to protect how information is handled
- Monitoring real-time access on the network and the endpoint
- Analyzing forensic data related to users interacting with information
- Managing distributed encryption solutions
- Mitigating attacks on databases

In 2006, a laptop belonging to a data analyst was stolen. It contained personal and health data of about 26.5 million active duty troops and veterans.²

Fortunately, these technical issues needn't plague organizations. Today, there are a number of integrated information protection solutions that are purpose-built to address these security risks and streamline the process of enabling information protection controls—and not hinder users with complicated information access mechanisms.

What do Britney Spears, George Clooney, Arnold Schwarzenegger, and Maria Shriver have in common? Each has had their confidential patient data stolen from a healthcare provider and subsequently sold to tabloids for publication.



GEORGE
CLOONEY



BRITNEY
SPEARS



MARIA
SHRIVER



ARNOLD
SCHWARZ-
ENEGER

Solutions

There are several solutions for protecting information that offer the added benefit of reducing costs and complexity. Some are network or endpoint controls, and others are specific to data or overall security management. While many of these solutions can be effective—especially when operating within a Security Connected framework, four technologies are key: data loss prevention (DLP), controls for protecting removable storage and media, encryption, and database activity monitoring (DAM).

Data loss prevention

DLP solutions need to discover and fingerprint sensitive information regardless of format, and, through regular intervals, keep the DLP solution and related controls informed about changes such as new data stores. An effective DLP strategy will combine network- and host-based controls to protect organizations from careless or intentional data loss. Examples include uploading information, sending information outside the organization via IM or email, or even copying information to a removable media device. Operationally, the DLP solution should provide centralized management, which encompasses discovery, policy creation, analytics, and response as well as integration with other controls such as Internet gateways for broad policy enforcement.

Removable storage device and media control

One of the easiest and most common forms of careless and malicious information exfiltration is through the use of removable media devices such as a USB drive, MP3 players, DVDs, and others. Solutions in this category must enforce the types of devices that can and cannot be used as well as the type of information that can be transferred via physical connections or wireless connections such as Bluetooth and infrared. Because USB devices have a small size and large storage capacity, encryption capabilities are essential

when information is mobile. These solutions should provide transparent and automatic encryption of data when approved information is transferred to an approved USB drive. For optimized security management, the DLP solutions and USB drive management should be centralized, as their controls are closely related.

Encryption

Encryption greatly mitigates the usefulness of any lost or stolen data. In addition to USB drive encryption, additional layers of protection can be gained by adding full disk encryption to Macs and PCs. Files and folders, including network files, should utilize encryption, especially if it can be done automatically and transparently as files and folders are shared and moved throughout the organization. By using encryption solutions that are centrally managed with the information protection controls previously outlined, deployments, administration, and policy creation can be more efficient and persistent across the various solutions, resulting in lower TCO.

Database activity monitoring

Just as finding sensitive data can be difficult, so is discovering all of the databases within an organization. Database activity monitoring (DAM) solutions should be able to identify databases and provide database-specific protection—even for unpatched systems. These solutions should leverage a combination of virtual patching, protection from specific, known attacks, as well as the ability to terminate sessions that are seen as violating security policies, as in the case of zero-day attacks. These controls should work across physical databases as well as in virtualized and cloud computing environments. By leveraging the Security Connected framework from McAfee across all information protection controls such as DLP, removable device protection, encryption, and DAM, risks and costs can be mitigated while ROI is improved.

Best Practices Considerations

- Employ a strategy that addresses external attacks as well as careless and malicious insiders
- Implement controls that are specific to data protection and augment them with supporting network and endpoint controls
- Leverage solutions that allow for real-time and forensic analysis
- Enact policies and controls for information protection that address critical data stores, endpoints, and removable media, as well as common information exfiltration points such as email, instant messaging, and web
- Take advantage of encryption—especially on portable devices such as laptops and USB drives—to reduce the risk of sensitive data being recovered from a lost or stolen device
- Protect databases with controls optimized for structured data policy enforcement

Because of the complexity, time, money, and resources required to conduct thorough testing of databases patches, production databases are only patched two to three times per year on average.

Value Drivers

The right solutions for protecting information should provide operational value by helping organizations focus on cost avoidance—not in the insurance sense of the term, but in the sense of real-life data record loss statistics. Right now, the average cost of a data breach is \$214 per data record.³ The right solutions for protecting information should:

- Help limit legal fees, fines, and compliance costs in the event of a data breach
- Provide faster identification of data exfiltration conduits juxtaposed with corporate policies
- Decrease the need for due diligence and exploratory legal fees in the event of a subpoena from third parties (if you handle third-party data)

Related Material from the Security Connected Reference Architecture

Level II

- Protecting the Data Center
- Protecting Information from Insider Threats
- Controlling and Monitoring Change

Level III

- Protecting Intellectual Property
- Protecting Email
- Securing Removable Media
- Enforcing Endpoint Compliance

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.

About the Author



Brian Contos, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books, including *Enemy at the Water Cooler* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies throughout North, Central, and South America, Europe, the Middle East, and Asia. He is an invited speaker at leading industry events like RSA, Interop, SANS, OWASP, and SecTor and is a writer for industry and business press such as *Forbes*, *New York Times*, and *The Times of London*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>

² http://en.wikipedia.org/wiki/Laptop_theft

³ <http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher>

