



PROTECTING INFORMATION FROM INSIDER THREATS



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.

Coca-Cola employees tried to sell Pepsi intellectual property.¹

Defend Yourself Against Insider Threats

Challenges

Insider threats predate the digital era and can be traced back to civilization's earliest documentation. Even one of history's first computers suffered an attack by malicious insiders. In the early 1800s, Joseph-Marie Jacquard of France invented the automatic loom. This device, arguably one of the first mechanical computers ever devised, would, in part, serve as the predecessor to computer punch card. Shortly after it was deployed in factories to automate the creation of textiles and yield faster and superior results than its human counterparts, a group of disgruntled employees (insiders), who, fearing that they were going to be fired, sabotaged the loom.

Insiders have two variables supporting their activities that outsiders don't: trust and legitimate access. This allows malicious insiders to conduct espionage, steal sensitive data, and sabotage assets quickly, easily, and with greater stealth than an external attacker. Careless and negligent insiders pose a similar threat, even if their intentions are not nefarious. Anything that can be done accidentally can be done on purpose; as such, the ramifications can be the same for careless and malicious insiders. Additionally, at the onset of an investigation into insider activity, it is difficult to determine if the act was done with malicious intent.

Another factor that distinguishes insiders from external attackers is that, in most cases, low tech trumps high tech. You needn't be an überhacker to download files you have permission to access to a removable thumb drive and then give that drive to a competitor. Similar activities—such as uploading, emailing, and posting sensitive data, or, in the case of privileged users such as system administrators and database administrators, manipulating sensitive data within a mission-

critical application or database. All of these activities are relatively simple acts that can be carried out without detection by most security controls. This is especially true for organizations that focus primarily on attacks from external entities or simply rely on network-centric controls for security. With an understanding of this situation, attackers ranging from nation-states to organized crime groups to competitors are finding that their return on investment is far better when they attack from the inside. Why hack when you can recruit?

In 2011, the US Department of Homeland Security issued an internal bulletin warning that private utility facilities in the US could be at risk of attacks from disgruntled current and former employees, or even "violent extremists."²

There are very few red flags for insider activity, but there are yellow flags that, when taken collectively, elevate seemingly benign activity to suspicious and perhaps even malicious activity. To achieve this level of visibility, organizations must fundamentally alter their approach to security by combining controls across endpoints, networks, and data. Regardless of whether an attack is sourced from an insider or an outsider, the security controls must work in a connected framework that takes advantage of computer-based correlation to augment human analysis.



In 2011, Ponemon Institute research showed a rise in the frequency of data compromise by malicious company insiders who were looking to make money by selling sensitive data. The research also showed an increase of outsiders and insiders working together to extract sensitive data.³

Solutions

There are a number of scenarios that can spawn from insiders, but information theft is squarely the primary issue. While human analysis is essential to protecting information from insiders, it is impossible to scale if the individuals responsible aren't supported with the right security controls. There is no black box that can be plugged into the network that will mitigate all careless and malicious insider activity. However, there are sets of controls, that when leveraged collectively, can provide strong incident detection, protection, and response capabilities across endpoint, network, and data.

Any organization building a strategy for mitigating both malicious and careless insider activity should be taking advantage of data loss controls that can be installed on the network and desktop. Organizations should leverage solutions that monitor how information is moving around the network and how it is being manipulated on the desktop. Use cases in this area that can be addressed with data loss controls include sending sensitive documents outside the organization, downloading a large amount of data to one's laptop, or copying sensitive material from a document and trying to save it onto a removable thumb drive.

Specific controls for monitoring database activity should be leveraged to protect the most sensitive organizational information, which is commonly stored in a structured format, such as databases. These controls are particularly useful when addressing insiders that are privileged users such as system administrators and database administrators.

With the consumerization of IT and mobility becoming the norm, endpoints, regardless of type, need to be controlled, and accountability needs to be applied. If a user is accessing the network and sensitive information from a local desktop,

remote laptop over a VPN, tablet, smartphone, or virtualized machine, those devices need to be associated with that user and that user's privileges. By enforcing accountability, network access and information access can be better controlled and suspicious activity can be addressed quickly by integrating access controls with intrusion prevention solutions.

The intentionally malicious or careless use of social media is posing a substantial threat to organizations. Solutions should be leveraged that allow users to take advantage of these services while controlling the risk—for example, disallowing the posting of sensitive data such as credit card numbers and government IDs, preventing posting altogether for certain individuals, or even limiting the types of applications and resources available to users within a given social media site. Another important control is the protection of information on a lost or stolen laptop or USB thumb drive. Encryption helps moderate the impact in both of these cases, as do controls designed to deny sensitive information from being stored locally or copied to removable devices.

There are, of course, many types of controls that can be applied to mitigating careless and malicious insider threats. While just a few critical components have been listed here, perhaps the most essential characteristic is not that these controls are deployed, but rather that they are deployed synergistically so that endpoint, network, and data security solutions enrich each other, are centrally managed and monitored, and analysts can quickly review all the pertinent alerts, reports, and events to make empirical decisions more efficiently and effectively.

Best Practices Considerations

- Monitor how users interact with information
- Require accountability regardless of endpoint—laptop, desktop, tablet, or smartphone
- Protect from careless activity such as accidentally sharing, posting, and uploading information as well as lost or stolen laptops and USB thumb drives
- Employ controls across all information states—at rest, in motion, and in use
- Aggregate controls across endpoint, network, and data for holistic visibility
- Centralize security control management for rapid incident identification, analysis, and response

A Ford employee was charged with stealing secret Ford documents and selling them to a competitor.⁴

DuPont suffered a breach when an employee who had worked there for 10 years stole more than \$400 million in research and development information for a competitor.⁵

Value Drivers

Many of the value points from “Protecting Information” apply to this area as well. The core difference is that with the correct technologies, you can know faster (and perhaps sooner) if data loss has occurred and then implement the necessary management and monitoring controls to address the situation. This issue is very important as it relates to areas such as insider trading or divulging of state data to another (foreign) nation state. The core value relative to protecting against insider threats is enabling your environment to protect against the threat while it is happening and to demonstrate proper compliance and controls.

The right solutions for protecting information should provide for operational value by helping to focus on cost avoidance—not in the sense of insurance, but in the sense of real-life data record loss statistics. Right now, the average cost is \$214 per data record.⁶ The right solutions for this component of your reference architecture should:

- Help limit legal fees, fines, and compliance costs in the event of a data leak
- Provide faster identification to removal avenues by addressing data loss prevention as it relates to violations of corporate policies
- Provide for decreased 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

- Controlling and Monitoring Change
- Protecting the Data Center
- Securely Enabling Social Media

Level III

- Protecting Intellectual Property
- Enabling Bring Your Own PC (BYOPC)
- Enforcing Endpoint Compliance
- Protecting Servers

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.foxnews.com/story/0,2933,202439,00.html>

² http://atlasshrugs2000.typepad.com/atlas_shrugs/2011/07/new-terror-report-warns-of-insider-threat-to-utilitiesdhs-bulletin-muslim-extremists-have-obtained-i.html

³ <http://www.ponemon.org/data-security>

⁴ <http://consumerist.com/2010/11/ex-ford-employee-admits-stealing-secrets-worth-50-million.html>

⁵ <http://www.informationweek.com/news/197006474>

⁶ <http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher>

