Advantages of Managed Security Services versus In-house Security Information Management (SIM)
Introduction

Proactively managing information security is a critical component to mitigating the risks to your information assets and to your business. Trade secrets, financial information, and employee and customer data are just some of the private information stored inside an organization’s network. Maintaining the confidentiality, integrity and availability of these assets should be of the utmost importance to every organization.

Leveraging Dell SecureWorks for global Managed Security Services will help manage the risks to your IT assets in an efficient, cost-effective fashion aligned with industry best practices. The major advantages include:

- **Improved visibility into emerging threats.** Dell SecureWorks monitors thousands of customer networks and leverages applied research to ensure that we are always ahead of the latest threats and tactics.

- **Increased efficiency.** No additional operational overhead to invest in SIM and manage an expert team of analysts.

- **Constant vigilance.** A 24x7x365 team of certified Security Analysts with deep event analysis and incident response experience monitor alerts to detect intrusions.

- **Purpose-built technology and architecture.** Built-in redundant architecture delivered through seven integrated Security Operations Centers (SOCs) provides a scalable solution.

- **Focused resources.** Your security team can spend their time on the real threats to your business.

- **Agile processes.** Flexible delivery options to meet the individual security needs of each organization.

Preserving information security is a necessity. Executives must decide the best approach for their organization, weighing the quality of protection, risk tolerance and the associated costs to define their security program.

This article will review the costs and benefits of the two most common approaches to Security Information Management: Managed Security services vs. In-house SIM.

“Technology is moving so rapidly that from a security perspective, it is difficult to keep up. Consider the evolution of cyber crime in just the past decade... today, we confront hacktivists, organized criminal syndicates, hostile foreign nations that seek our state secrets and our trade secrets, and mercenaries willing to hack for the right price...

Just as traditional crime has migrated online, so, too, has espionage. Hostile foreign nations seek our intellectual property and our trade secrets for military and competitive advantage.

State-sponsored hackers are patient and calculating. They have the time, the money, and the resources to burrow in, and to wait. They may come and go, conducting reconnaissance and exfiltrating bits of seemingly innocuous information—information that in the aggregate may be of high value. You may discover one breach, only to find that the real damage has been done at a much higher level.

Unlike state-sponsored intruders, hackers for profit do not seek information for political power—they seek information for sale to the highest bidder. These once-isolated hackers have joined forces to create criminal syndicates. Organized crime in cyber space offers a higher profit with a lower probability of being identified and prosecuted.

Unlike traditional crime families, these hackers may never meet, but they possess specialized skills in high demand. They exploit routine vulnerabilities. They move in quickly, make their money, and disappear. No company is immune, from the Fortune 500 corporation to the neighborhood “mom and pop” business.

We are also worried about trusted insiders who may be lured into selling secrets for monetary gain. Perimeter defense may not matter if the enemy is inside the gates.

The end result of these developments is that we are losing data. We are losing money. We are losing ideas and we are losing innovation. And as citizens, we are increasingly vulnerable to losing our information. Together we must find a way to stop the bleeding...

We must continue to build our collective capabilities to fight the cyber threat...we must share information...we must work together to safeguard our property, our privacy, our ideas, and our innovation.”

---

Robert S. Mueller, III
FBI Director
RSA Cyber Security Conference
San Francisco, CA, March 01, 2012
Comparison of initial and ongoing costs

The Dell SecureWorks Counter Threat Platform (Dell SecureWorks’ backend “SIM” technology) is fully managed and maintained by Dell SecureWorks’ professionals. All components of our Platform are located at our SOCs where they are managed 24x7x365 by our team of experts.

Comparable to any large-scale enterprise software deployment, SIM technologies can take a long time to deliver ROI and bring measurable benefits to the organization. Dell SecureWorks’ services allow you to be a “user” of SIM technology without having to bear the costs of managing a complex and burdensome on-site solution.

The following pages compare the differing cost structures and security scenarios typically encountered by organizations deploying information security processes in-house to those who choose to use Dell SecureWorks as a Managed Security Services Provider (MSSP).

Managing information security in-house

The confidentiality of corporate data is extremely important to any organization. It is therefore understandable that some executives are reluctant to outsource a task that is so integral to the integrity of their business. When all aspects of information security are handled by an internal team, however, the costs are higher and the risks to the business are greater. By managing information security internally, organizations should expect to incur the following costs, at minimum.

Staffing and training

Staffing a true 24x7x365 Security Operations Center requires a minimum of seven full-time employees. While IT departments, network groups or even security teams may have the talent/expertise, they rarely have the “current and well-practiced” skill set that is required to execute real-time or even batched security event analysis. There are millions of events generated every day within an environment, and an analyst must find the one or two true security incidents. To provide the necessary skill sets, analysts must receive periodic training from technical-oriented organizations such as SANS. This training adds thousands of dollars per employee in annual investments.

Of course, nothing can compensate for experience, and finding employees that have this experience can be time-consuming and costly. You must also consider the costs of turnover should personnel critical to the daily operation of the SIM technology depart. SIM technology cannot run itself – if the SIM Manager or other critical staff member leaves, there will be a significant performance lapse even if you have fully trained replacements available.

Having the proper security personnel puts tremendous pressure on IT departments to recruit, train, compensate and retain a 24x7 security staff. The cost of training or enhancing a security professional’s skills for an in-house network can be prohibitive. Tools, such as SIM products, are not easy to understand out of the box and by no means easy to use. Learning how they work takes weeks, if not months, of training depending on the specific SIM technology and your personnel’s background.

Hardware, software and licensing

The bulk of the disclosed up-front SIM costs stem from licensing. The initial licensing costs of most enterprise-class SIM software technologies go well into six figures and annual license fees are typically between 10 and 25 percent. Additionally, with most SIM software solutions, agents must be purchased for all technologies to be monitored with the SIM system. After the initial purchase, the cost of agents must also be considered any time your infrastructure changes.

To be effective, in-house SIM software solutions need dedicated databases and high-end servers for agent systems and management systems. You will need at least one database administrator who knows the underlying database system (Oracle, MySQL, etc.) in and out. In addition to initial hardware capital expenditures, there is often ongoing maintenance of the backend systems which must be kept running optimally for the SIM solution to function properly.
Any company managing SIM in-house should have a mirrored test environment for creating and testing correlation rules. Turning a rule on in production can easily have unexpected, adverse effects such as flooding or slowing the application. A test environment is a must if you intend to effectively manage the in-house SIM system without causing problems throughout the enterprise. This means double the hardware costs at a minimum.

**Implementation**

Deploying SIM software in enterprise environments is a complex and expensive process that can last anywhere from 6 to 18 months depending on the customization required and the amount of resources you can throw at it. Installation is not intuitive and you will need consulting services to successfully deploy an on-site SIM system.

**Management**

Due to their complexity, SIM solutions are nontrivial to manage and maintain. Resources will need to be spent on full-time SIM managers and database administrators in order to keep the SIM technology up and running. Both managers and analysts will need to be familiar with all types of systems in your environment and how they interact, to manage filters and correlation rules. In addition, agents will need to be upgraded when new versions of the underlying monitored devices change and any customization to the agent will need to be repeated in most instances when deploying the upgraded agent.

**Comparison of Dell SecureWorks’ security services**

Development of Dell SecureWorks’ Counter Threat Platform began in 1998 and has been continuously improved during the past 12 years. The experience and expertise gained through the monitoring of thousands of customers networks around the world has driven the enhancement of this purpose-built security technology. The Counter Threat Platform supports our team of SANS GIAC GCIA certified Security Analysts who are solely focused on analyzing security events on a 24x7x365 basis.

We provide real-time enterprise security monitoring and device management, and we lead the industry in customer satisfaction. We have the mature technology, robust processes and experienced security experts needed to effectively detect and respond to both known and emerging threats in real time.

All of our Managed Security Services are provided in an unlimited and unmetered fashion with no hidden or additional costs. Regardless of the number of incidents escalated, calls to the SOCs, events analyzed, etc., the monthly subscription fee will remain constant per monitored/managed device. In order to form a true security partnership, we believe that we cannot place limits on the number of calls to the SOCs, escalated incidents or the time our analysts spend working with each of our customers to secure their critical assets. Nor do we believe in a tiered staffing model where customers are forced to interact with junior-level personnel before speaking with experts. Instead, every call is handled by one of our certified, experienced security professionals. Because of this, we have one standard SLA for each of our Managed Security Services and impose no limits on the level of support we provide for our customers.

The key points on the following pages illustrate the high level of security we provide over and above an in-house solution while lowering the total cost of ownership.
Finding the real security incidents

Dell SecureWorks monitors more than 20 billion events each day and already has in place the people, processes and technology needed to filter the overall haystack of events to the few truly important security events of interest. We are able to accomplish this by continuously tuning our platform to identify new threats when we see them, as well as eliminating non-security events when we identify such activity to be normal business traffic. This enables our solution to scale indefinitely while constantly adapting to new threat environments. This, in particular, is a difficulty we have seen with enterprises which have deployed in-house SIM technologies. Performing this task in-house requires extensive initial and ongoing tuning of the SIM technology simply to cut through the millions of events a typical company sees every day. Failure to manage the technology in a way that does not flood the in-house staff is a problem seen in many failed SIM deployments.

Experience and visibility

We see malicious activity occurring across all of our customers, giving us global visibility into the overall threat landscape as well as threats specific to major industries, including financial services, healthcare, retail and utilities. Our platform leverages the information we gain by applying security findings analyzed from a single customer across our entire customer base. As a result, we can detect and respond to a much greater breadth of attacks with more speed and accuracy than an in-house solution.

Faster response to and resolution of security incidents

The Dell SecureWorks Counter Threat Platform’s filtering system has been constantly tuned and refined during the past 12 years to provide our analysts with only security events of interest and their relevant context. In addition, our experienced analysts know exactly what to do when an event does occur. This allows us to identify and respond to the “needles in the haystack” faster and with more accuracy than is possible with an in-house solution. Once an incident is identified, we work directly with the appropriate customer staff to mitigate the threat and minimize its impact.

Total solution redundancy

All aspects of Dell SecureWorks’ Managed Security Services, from the people to the technology, ensure uninterrupted security monitoring and response. Dell SecureWorks operates seven integrated Security Operations Centers with hundreds of expert Security Analysts. All Dell SecureWorks’ SOCs are staffed 24x7x365 and all Security Analysts are required to hold the SANS GIAC GCIA certification. Additionally, all members of our SOC team are trained cross-functionally in multiple roles to ensure that all critical responsibilities are covered and service is not impacted should anything change in terms of personnel.

Dell SecureWorks’ SOCs operate as a single entity, with the systems mirrored in real time and include integrated video and voice technologies. They each undergo annual SSAE 16 audits and periodic FFIEC
Examinations. All SOCs are equipped with redundant high-speed Internet connections, fiber optic loops and back-up power generators.

In-house solutions expose you to risks associated with infrastructure and staff availability which are not factors with Dell SecureWorks’ services. Should a SIM manager or other critical staff member leave, your organization’s security posture will invariably suffer while provisions are made to re-staff the position. Complete fault tolerance requires building out at least two 24x7x365 SOCs, each with a minimum of seven full-time employees and all corresponding hardware/software necessary to conduct security event analysis. This can be extremely cost-prohibitive.

**Focusing your efforts**

Dell SecureWorks’ solution allows your security team to spend their time focusing on strategic efforts to improve your security, instead of having to spend their time and energy to keep a complex SIM technology up and running, performing event analysis and managing security technology. We find the security incidents that need your attention and help you to work through them so that your team makes the most out of their day-to-day security efforts. Our SOC team strives to be an extension of your own security team, filling in competency gaps and providing unlimited support for any security issue. As a result, your security program is more efficient, runs smoother and provides greater protection for your enterprise.

**Objective security analysis**

Dell SecureWorks’ experts provide objective, in-depth analysis of security activity as a third party who is dedicated to protecting your critical information assets. Their effectiveness is not affected or impacted by any internal influences that can be common in some enterprises, such as political maneuvering or pressure from other groups within the company. As a result, the information provided by our analysts will be consistent and measurable, ensuring that your metrics are accurate and not influenced by factors not related to the security of your organization.

**Flexibility**

Dell SecureWorks’ solution is delivered as a managed service and, because it does not require substantial investments in additional infrastructure, you are not locked into our solution. If your needs change, you have the freedom to pick a solution that is best for your organization. With an in-house solution, your flexibility is compromised by the large capital investment in a solution that may not meet your security needs in the future. With Dell SecureWorks’ solution, you are subscribing to our service, security expertise and threat intelligence visibility – not investing in our technology. Technology solutions can easily become outdated or obsolete in two to three years. Our services ensure that you will always have an agile monitoring solution that protects your assets.

Dell SecureWorks’ Counter Threat Platform can monitor virtually any security technology without the use of agents. The Counter Threat Platform’s filtering system is operationally updated to accommodate new technologies and technology upgrades without additional development, as is
required for agent based technologies. This provides you with the flexibility to utilize the security technologies which best fit your needs.

**Compliance and reporting**

Dell SecureWorks provides unmatched visibility into your organization’s security and compliance posture. The Dell SecureWorks Customer Portal provides access to hundreds of pre-built and easily customizable reports to ensure that stakeholders at all levels can easily understand relevant security information. Granular reports allow IT staff to drill down into specific events and logs, while dashboards, charts and tables allow executives to gain insight into the higher-level security trends. All actions taken against a specific event by both Dell SecureWorks and the customer’s internal security team are tracked to ensure all issues are handled in a timely fashion and that SLAs are being met.

Reporting has also been specifically designed to help customers demonstrate adherence to regulatory requirements and can significantly ease the burden of security compliance reporting for many organizations. Whether your organization is governed by PCI, SOX, HIPAA, FISMA, NERC CIP, FFIEC or GLBA, you can rest assured that the Dell SecureWorks Customer Portal can easily demonstrate compliance to auditors. Dell SecureWorks undergoes annual SSAE 16 certifications and adheres to industry best practices while safeguarding customer information assets.

**About Dell SecureWorks**

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

For more information, visit [http://www.secureworks.com](http://www.secureworks.com)