WHITE PAPER

KEEPING UP WITH CONSUMERS – AND CONGRESS

End users and elected officials are demanding more from companies that handle personal and financial data. To keep up with multiplying regulations and gain market share, more businesses are pooling critical audit and security management processes across the enterprise and using off-site experts to cost-effectively manage their security operations. A big benefit, aside from keeping sensitive data safe, is allowing IT teams to devote more time to helping an organization meet its mission – and margins.

Table of Contents

Alert Logic, Inc.1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.8383 (toll free) | 713.660.7988 (fax) | www.alertlogic.com

Executive Summary

Government has had an increasingly heavy hand in how U.S. businesses protect their networks and the sensitive data within them. The last decade has introduced legislation with major security implications, such as the Health Insurance Portability and Accountability Act (HIPAA), the North American Electric Reliability Council's (NERC) Critical Infrastructure Protection Standards and, more recently, the Payment Card Industry (PCI) Data Security Standard (DSS). With both on- and offline consumers – and elected officials' constituents – almost daily demanding stronger levels of privacy and protection from malicious threats, companies must meet ever-evolving demands or risk having both their reputations and revenue streams destroyed by breaches and the bad publicity that ensues.

More than the fear of bad media exposure, however, is the competitive advantage to be gained by providing customers, business partners and, when required, regulators with proof that it has a solid IT security strategy ... and that it's working. This often means investing in a much higher level of network perimeter protection and continuous monitoring – a level often difficult to reach for companies with limited resources. One way many businesses are keeping up with multiple regulations and winning new business along the way is by bringing together critical audit and security management processes across the enterprise and using off-site experts to cost-effectively manage their security operations.

In doing so, enterprises not only have peace of mind in knowing their assets and systems are constantly monitored, but these software, hardware and outsourcing tools also provide IT, security and audit teams more time to focus on the organization's business needs.

The Need to Know Keeps Growing

Amid a backdrop of ever-evolving threats and security concerns, and driven by increased regulatory and audit scrutiny, the pressure has never been higher for an organization to protect its network and the data flowing through it. With the spotlight now shining brightly on IT and security after years of regulations and embarrassing data breaches, even the highest levels of management now discuss IT controls and audit results. Their expectations and the expectations of customers and shareholders, regarding IT and security controls are rising.

Compounding this problem is the scourge of cybercrime and other malicious activity, be it insiders or external sources, which continues to plague security professionals in all industries as these threats continue to rise in sophistication and frequency.

Proper visibility across the enterprise, as well as the threat and attack activity outside of the perimeter, is critical to ensuring the protection of sensitive information and continuous availability of crucial IT services. This visibility can be gleaned from frequent assessments of the external and internal vulnerabilities present in the IT infrastructure and applications, as well as through the collection and monitoring of log and intrusion data for anomalous activity that could indicate potential compromises.

Increasingly, SMEs and larger companies are turning to more holistic security and compliance solution providers who provide comprehensive and flexible intrusion detection, vulnerability assessment, and log management that meets regulatory requirements. Because demand is growing, so is competition within this space and some vendors are leading markets emphasizing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) over the more traditional Managed Security Service Providers. In addition, they are doing more to secure data within "the cloud" used for Internet-based computing, resource sharing and storage. Vendors such as

Houston-based Alert Logic Inc., which now provides such "cloud covering" in its product suite and IT security monitoring services, are distinguishing themselves in an increasingly crowded market with proprietary software that addresses threats within the cloud.

The Risk Landscape: New Threats – New Laws

In August 2010, U.S. Senators Mark Pryor and Jay Rockefeller introduced a bill called the Data Security and Breach Notification Act, which would cover consumers nationwide and include stealing a person's name, address and phone number in combination with more sensitive data to trigger notification. As with past legislation, it also sets minimum information security standards for IT departments.

The bill requires covered entities to take the following precautions:

- Create a security policy regarding personal information
- Appoint a person responsible for info security
- Identify and assess foreseeable vulnerabilities (reasonable ones), including regular monitoring for breaches
- Prevent and mitigate such vulnerabilities
- Create a process for disposing of person information, electronic as well as paper-based documents

Many companies already do these things as a matter of business or to meet existing security legislation. But the bill is a sign that laws governing how enterprises run their security operations is far from waning.

After-the-fact mitigation for data breaches is costly – often much more so than preventative measures.

Writes lawyer and technology columnist Eric Sinod, referring to the Poneman Institute's annual U.S. Cost of Data Survey: "A recent study relating to data security breaches in the United States shows that total per-incident costs are substantial. The average total per-incident costs in 2009 were $6.75 million, comprised of an average cost of $204 per customer with a jeopardized record. Breaches included within the survey varied from 5,000 records to more than 101,000 records from 15 different industry sectors. The most expensive data breach within the ambit of the study cost almost a whopping $31 million dollars to resolve."

Brand Damage

The loss of customer data be it credit card numbers or patient records, undermines trust in an organization and creates lasting damage to its brand and the goodwill among its customers and business partners. While difficult to measure in hard dollars, this risk can have a lasting effect on an organization's ability to secure funding, reach new customers, or seek preferred treatment with business partners and suppliers.

Fines and Penalties

Because of the increased scrutiny by lawmakers and industry watchdogs, fines imposed for breaches of confidential information such as patient records or credit card information can quickly spell financial disaster for an organization. With fines of up to $1million per day per infraction for utility companies failing to meet the obligations of NERC's Critical Infrastructure Protection requirements, to increased transaction costs for PCI DSS violations, the exposure is just too great to ignore.

Legal Risks

Similarly, failure to meet the obligations of due care can result in unnecessary legal exposure under breach notification laws and potential liability claims. Regardless of the outcome, these legal tussles take valuable time and effort to defend, consuming resources better put to use elsewhere.

Whether it's NERC, PCI or HIPAA, the need to secure an organization's information, and information about its customers is crucial to doing business today. *Proving*, through periodic audits, you are adequately protecting that data is critical to maintaining customer and shareholder trust. Managing the protection of the organization's data requires the support of technology and dedicated expertise to monitor logs, assess security posture, respond to incidents and ensure that the company is actively managing the risks within a business ecosystem.

Mitigating Today's Risks

Vulnerability Assessment

Mandated by PCI DSS and echoed in HIPAA as well as other key pieces of legislation, vulnerability scanning forms the cornerstone of a security and compliance program. By identifying assets not meeting external security requirements or internal policies, a company can prioritize the remediation of those assets or mitigation of the risks through other means and begin to take a proactive stance in meeting its security and regulatory obligations.

Log Management

Having visibility into a network's activity, and the systems attached to it, is a fundamental step in understanding where data is flowing and how it is being accessed. However, the number of products generating relevant logs, the increasing volume of log data, and the explosion in the variety of logs have all increased greatly, which has created the need for some form of log management: a process for securely generating, transmitting, storing, analyzing, and reporting on log data. The mandates for the collection, analysis and storage of this mountain of data are clear and the burden placed upon IT and security practitioners as a result is staggering.

Unfortunately, this information is often ignored or underutilized for many reasons, including:

- The data is too complex and difficult to understand, requiring specialized skills in its interpretation
- The sheer volume of the data collected is overwhelming to the technology and analysts alike
- Providing value from all relevant data means trying to accurately correlate and interpret events over time

By properly leveraging technology it is possible to overcome these hurdles and glean significant amounts of intelligence about your enterprise from log data, and to use this information for proactive security management through alerting and reporting. This log data is also useful when the unthinkable happens, greatly assisting in forensic analysis, supporting internal investigations, and identifying trends and long-term problems.

Intrusion Detection

Intrusion detection solutions (IDS) identify unauthorized, illicit, and anomalous behavior by observing network traffic. This technology has long been haunted by issues surrounding false positives, as well as the sheer number of events that they tend to generate. But IDS solution providers have invested in better ways to improve the "noise ratio" by correlating intrusion events with vulnerability scan data and log streams. The best of breed among vendors now enhance detection results by having expert analyst personnel provide their customers intelligent tuning and refinement of the rules and correlations within the solution. This solid detection and response capability allows an organization to much more effectively prioritize threats while also identifying problems with security policies and acting as a deterrent to individuals willfully violating security policies.

The New Normal: Security as a Service

Companies' IT executives and staff have long known it is impossible to continually monitor networks without technological assistance. In recent years, the rest of the organization's executive suite has come to understand the risk with deploying limited resources to protect the company's assets and reputation. And often the solution has been to install affordable security and compliance solutions that offer intrusion detection, vulnerability assessment, and log management in a service-based, or SaaS delivery model. The SaaS model means you don't have to buy, implement or maintain the expensive and complicated hardware and software usually associated with these solutions.

Cloud-Powered, Managed Solutions for Security & Compliance

Trusted by enterprises, managed hosting providers, and partners worldwide, Alert Logic provides innovative, low-cost, worry-free SaaS offerings to help IT staffs monitor and manage threats and achieve regulatory compliance.

Alert Logic Threat Manager™ satisfies the need for vulnerability assessment and intrusion detection by automatically identifying malicious behavior and network patterns coming from inside or outside of your network. Going beyond just detection, Threat Manager also integrates with leading infrastructure products to block potentially malicious activity, stopping attacks such as failed logins, command execution, Denial of Service, or even reconnaissance attempts. The company's software is distinguished by utilizing a combination of a patented grid-based technology and cutting edge 7-factor threat scenario modeling to accurately identify and prioritize threats in your environment. The end result is more accurate incident identification and prioritization. This "cloud-powered" vulnerability assessment solution provides the flexibility to regularly scan internal and external networks to determine where a company is vulnerable and to provide expert guidance to remediate vulnerable assets.

Certified as a PCI Approved Scanning Vendor (ASV) for the last four years by the PCI Standards Council, Threat Manager's reports serve as proof of compliance to acquiring banks and QSA auditors. Additionally, Threat Manager keeps detailed records of remediation efforts, including notes, files and who was assigned to the remediation cases, giving you insight into how you are meeting your compliance requirements.

Alert Logic Log Manager™ leverages patent-pending cloud architecture to collect, store, report and correlate log data in highly secure and redundant data centers, helping avoid the maintenance and operating costs of on-premise solutions. Log Manager allows a company to meet the regulatory requirements to capture and store log data without having to worry about the ongoing storage and archival costs associated with on-premise solutions.

In addition to the patented management software is an add-on service to Log Manager called ActiveWatch™ that provides 24x7 event log monitoring and review that provides expert analysis and insight on a daily basis. A dedicated team of GIAC security experts analyze logs from a state-of-the-art Security Operations Center and notify you directly if they discover any suspicious activity. If an incident is identified, the analysts escalate a case through Log Manager's integrated incident and case management system. The ActiveWatch™ team then works with you to resolve the incident and get everyone focused back on the business.

In Summary

Organizations are now faced with a multitude of legal, regulatory and industry requirements that have dramatically altered the very IT processes used to ensure the security and integrity of their business and the IT systems they depend upon. Penalties for violations of these various mandates runs the gamut from $1 million per day fines (NERC CIP) to increased transactional costs (PCI DSS), but in the court of public opinion, the impact can be far greater than immediate economic sanctions. The disclosure requirements of many of these mandates mean that the damages incurred have an impact that can be felt for years to come. Through drops in customer confidence, brand equity, and even access to capital markets, economic and organizational disruption becomes the norm, distracting the business from executing its strategic vision and instead reacting to market forces it could have avoided.

This “perfect storm” presented by the sheer prevalence of the above market drivers, are forcing organizations to take a proactive, process-oriented approach to managing the business risks of IT. Implementing and documenting auditable controls, both technical and procedural, to demonstrate “due care” is now essential for already-stretched security and IT teams, who often are already are told to “do more with less” – a mandate that has existed since the dawn of the digital era.

True security professionals must embrace the regulatory and legal landscape as part of the risk equation and seek out new ways to add value to their operations by enabling the business to better manage the risk associated with audits and regulatory or industry requirements as a part of doing business. For many companies, this means turning to managed security providers whose solutions specifically address compliance and allow organizations to effectively monitor existing and emerging threats, particularly those now taking place outside traditional corporate networks and moving into areas where more and more sensitive data is being stored, such as on the Internet. Such “cloud coverage” is important to not only hold off intrusions but also to hold on to an organization’s brand, business partners, costumers and good standing among regulators.

Those who excel at this strategy not only retain existing customers but best stand to gain new ones from competitors who fail to comply with the mandates and paper trails now required from data-driven laws. In this regard, better risk management can position the organization for opportunity, as opposed to attempting to block the activities needed for the business to succeed.

About Alert Logic

Alert Logic's patented solutions are the smartest choice for over-regulated businesses with underfunded IT departments to secure networks and ensure compliance. Its cloud-powered managed solutions combine intrusion protection, vulnerability assessment, log management and 24x7 threat surveillance, and are designed to maximize revenue and profit opportunities for service providers and hosting partners. Enterprises experience a solution that addresses network security and compliance requirements at a low price point, with little dependency on IT resources. Alert Logic is based in Houston, Texas and was founded in 2002. More information about Alert Logic can be found at http://www.alertlogic.com.