

SECURE CONVERGENCE

JOURNAL®

SETTING THE STANDARD FOR NETWORK SECURITY AND BEYOND

Using **LOG DATA** to Manage Operational Risk



OCTOBER 2005 • www.securecj.com

Also inside:

Computer Forensics

Endpoint Security

Email Filters

Product of the Month

Managesoft
Refresh





USING LOG DATA TO MAN

Today's enterprise networks are at risk – threatened by privacy breaches, information leakage, security attacks, policy violations and network downtime. Incidents are increasingly associated with hard dollar losses that go beyond the damage to a company's reputation. About 95 percent of these financial losses are attributable to intentional or unintentional actions by insiders. Security issues – such as worms and viruses, internal or external fraud and policy violations – result in an average of 22 hours of downtime per year. Human error, system failures and natural disasters account for an additional 87 hours per year of downtime, the cost of which can be up to \$6.5 million per hour. More disturbingly, the financial losses from IP theft are rising; already totaling an average of \$1.3 million per company each year.

In addition to security and performance risks, nearly every industry today faces increasingly stringent compliance requirements as new mandates and regulatory laws are enforced. In the finance industry, VISA CISP, FFIEC, GLBA, Sarbanes-Oxley (SOX) and Basel II require strict vigilance of IT departments in banks, brokerages and other financial institutions. Healthcare organizations must answer to HIPAA, as well as VISA CISP and SOX. Retail companies are under the gun as well, and energy providers also have NERC and NISPOM to worry about. In addition, at least 35 states have already proposed bills to notify customers of privacy and security breaches, and we're hearing recommendations for a federal security standard. Companies may suffer fines or criminal charges for failing audits, be subject to investigations, or leveled with lawsuits.

Industry regulation organizations and best practices experts agree on the importance of log data management as a cornerstone of any organization's risk management strategy. Companies can use log data to provide a complete audit trail of user and system activity, while providing critical support to mitigate security and performance incidents. Fortunately, log data is readily available in any

data center, and companies need only find effective ways of collecting, aggregating and archiving it to put it to use.

Managing Risk Proactively

To manage risk intelligently and cost-effectively, companies are looking to log data for answers. Readily available from all network-connected devices, log data can provide a complete, independent record of network activity and user access to applications, servers and devices on a network. Companies can use it to validate policies and perform change control audits in real time. Log data can be used to trigger alerts to unusual or suspicious network behavior and for root-cause analysis to aid in system recovery and damage cleanup. Log data can also provide an audit trail of user logons and access for regulatory compliance and legal purposes.

Log data gives IT insight about who's using which applications and when, who has access to certain servers or applications and who has permission to make changes. It can also be mined for information about accepted and denied connections, as well as what's happening during remote user sessions over VPNs. To sum it up, log data is extremely useful for companies looking to mitigate network risks and resolve issues quickly.

To get the most from log data, an automated, complete solution for log management should be the cornerstone of any organization's IT infrastructure. Unfortunately, that's exactly what many companies lack. This is a problem because there is so much data to manage. In fact, 25 percent of all enterprise data is log data, and that percentage continues to grow. Global 2000 organizations can generate about ten thousand log data messages per second – the equivalent of two terabytes each month. Up to 94 percent of these log messages are seemingly normal, informational, messages. Mining this amount of data is extremely time-consuming and requires a sophisticated and automated solution that covers all aspects of data collection, aggregation and retention.

Roughly 80 percent of Global 2000 companies use

By Dominique Levin

IMAGE OPERATIONAL RISK

homegrown scripts to mine log data. These scripts are ineffective, because they don't capture complete data, and they have difficulty adapting to disparate locations and formats. Additionally they are not standardized or automated, so they require constant maintenance. Most companies lack the headcount to perform these tasks, so they experience slow meantime to repair if there's a network issue.

According to research vice president Paul Proctor of Gartner, Inc, "Homegrown solutions can be effective in organizations with 50 or less audit sources, but they usually collapse in larger installations."

Security Information Event Management (SIEM) solutions are another potential solution, however, like their homegrown counterparts, they can be ineffective and inefficient. Most do not collect 100 percent of all network log data, but focus only on security events and ignore other issues, like misuse or impaired performance. Because they are incomplete, they cannot be used for compliance purposes or to improve availability. Plus, many of these solutions lack back-end infrastructure and, as a result, offer poor throughput and storage efficiency. Moreover, they are expensive to install and maintain.

Best practices for log data management

Fortunately, best practices frameworks like CERT, COBIT and ISO as well as statutes like HIPAA, SOX and GLBA help define what's needed in a log management solution. They recommend that companies audit and monitor system and user activity logs for suspicious behavior, security breaches, unauthorized access and misuse. They also recommend creating a historical repository of events and retaining complete and accurate log data for up to seven years. These recommendations serve as a blueprint for a log management solution that can actually help companies save money and reduce expenses through by putting their log data to good use.

There are four critical areas of concern:

- Authentication & authorization: No individual should

have more rights than he or she needs to execute his or her assigned tasks.

- Configuration and change management: No changes should be made without authorization. A record of what changes are made should be maintained so that the state of a system or application at a previous time can be determined.
- Segregation of duties: One person should not have the right to configure IT systems as well as audit, initiate or approve incompatible activities in those systems. Similarly, development, testing and production environments should be segregated.
- Documentation: All entities must be held accountable. Compliance should be documented and tested on an ongoing basis. The audit trail should allow for testing of the internal IT control framework as well as substantiating regulatory compliance.

Without adequate log management, companies end up wasting an enormous amount of money and resources addressing these areas so they can pass compliance audits. According to a log management survey recently performed by the SANS Institute, over half of Fortune 200 companies spend more than \$250,000 a year managing their logs. Many of the Global 2000 companies spend in excess of \$100,000. Much of this cost can be reduced over time by deploying a log management infrastructure that automates the process of collecting, aggregating, analyzing and archiving log data from multiple network devices, eliminating the need for much of the manual labor currently required to perform log management tasks.

Considerations for effective log management

A thorough log management solution must address security, compliance and availability threats by providing IT with complete, accurate log data files that are readily searchable and accessible. Although it is tempting to focus only on warning messages and alarms, doing so would deny auditors the complete audit trail required for security



policy validation and compliance testing. Also, while a single informational-level message may be of little interest, the number of times an uninteresting message is logged can indicate a performance or availability problem that may affect productivity or eventually cause the network to collapse.

Any log management solution should be completely automated, so that minimal maintenance and administration is required. Automation saves IT departments money and resources. Companies should look for an appliance-based solution that is ready to work out of the box, and discovers network devices and interoperates with numerous platforms to avoid modification to the existing infrastructure. The solution should provide end-to-end log management, from data collection and aggregation, to real-time analysis and long-term archival.

Another important consideration is the extent to which data can be searched and analyzed. To take full advantage of the data, IT should be able to perform ad-hoc searches in real time, receive behavioral alerts automatically, and rapidly generate easy-to-read graphical reports about network activity. Security is also critical; any log management solution must provide central, secure log data archives, which are physically separate from the log data used for real-time analysis. That way, the raw log data is kept intact, while a copy can be used for analysis and searches.

Additional log data protection in the form of scrambling and compression as well as fail-over, fail-back and automatic backup capabilities must be employed to ensure safety and integrity of the log data.

Here's how effective log management can help: A travel firm lost 8 hours of bookings to downtime resulting from a virus attack that went undetected long enough to crash the corporate firewall. It cost the company nearly \$200,000 to perform damage cleanup and the firm estimates it lost nearly \$800,000 worth of online bookings because of its slow meantime to repair after the outage. With adequate log data anomaly detection mechanisms in place – for example, an automatic alert and the ability to pinpoint the

problem – the company could have significantly reduced the cost of damage cleanup while eliminating nearly all of the resulting downtime.

Here's another example: Consider that a technology firm has intellectual property it wants to protect estimated to be worth about 70 percent of the company's value. With an average of 2.5 incidents of theft per year, the company stands to lose \$1.2 million per year. With effective network activity monitoring in place, these incidents could be completely avoided, or at least detected early and stopped. Other examples include reducing the time it takes to answer questions from auditors during a Sarbanes-Oxley audit or the time it takes to troubleshoot network problems by speeding up remediation and providing decision support. Any effective log management solution should enable rapid data searches to facilitate root-cause analysis of any network issue to help IT identify, isolate and fix problems that occur.

Making the most of your data

More than ever, companies need systems in place for monitoring and measuring risk. When managed effectively, log data can aid with segregation of duties and documentation because it provides a complete, independent record of access, activity, and configuration changes for applications, servers, and network devices. Companies looking for an effective solution should turn to best practices frameworks as a guide, and be sure that the solution they choose provides the necessary functionality. In addition, response time and reliability are critical factors to consider, since every second of downtime translates to lost opportunity and wasted resources. The log data is already there; the trick is putting it to good use to mitigate operational and IT risk, reduce costs and ultimately improve network availability and corporate profitability. **SC**

Dominique Levin is the Vice President of Product Management and Business Development for LogLogic. She can be reached at dlevin@loglogic.com.

