

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

July 2008

Beyond Compliance: The Significant Benefits of Log Management

By John Hawley

Each system, application and security device on your network is busily generating millions of records — related to activities such as system configuration, access rights and user activity logs — right now and every minute of every day. These logs provide a wellspring of information to help better secure and manage corporate resources, as well as demonstrate regulatory compliance — if, that is, you can aggregate and decipher all the data they contain.

That's where log management solutions come in. These solutions help organizations cost effectively collect, normalize and archive enterprise-wide, security-related data that can be invaluable for security investigation and compliance reporting. Furthermore, most companies soon discover their additional value: This centralized and normalized view of system, application and network device logs helps their staff quickly troubleshoot and identify the root cause of IT problems.



If you're considering a log management system, start by convening the members of your security, compliance and IT teams. All three departments can benefit from log management, so you should build support to ensure that you pick the right solution for everyone. At this point, you should also identify the use scenarios that will help justify investment in the solution.

Start by identifying the most significant risks to your most critical resources. Next, establish a basic rule (or control) that, if followed, will reduce those risks. Once installed, the log management solution can normalize and archive all activity across all systems related to that control, providing active alerting when it is violated and easy investigation of the activity as needed. By effectively mitigating risk and reducing the cost of demonstrating compliance, the project should quickly gain the support it needs to fund a rollout across more of the enterprise systems.

Often, the most critical use cases relate to detecting inappropriate use of privileged accounts (those accounts with elevated access to systems and applications for performing administrative functions). This is very important because privileged user accounts often have access to sensitive data such as employees' Social Security numbers, credit card numbers and health records, as well as the company's business and financial records. The log management solution complements a strong Identity and Access Management (IAM) program to ensure these access rights are not used inappropriately.

The identity management use cases should also require near-real-time collection of activity logs from the local systems and transfer to the log management solution for secure archive. Remember that privileged user account we were concerned about? That account has the ability to modify logs, covering the tracks that would otherwise quickly identify the inappropriate actions. The various regulations demand these logs be available for 1 to 7 years. Be certain to have a long-term, cost-effective storage plan in place before your new log management solution fills up its native storage capacity.

Finally, identify what actions take place when your control violations have been identified. To comply with regulatory mandates, you must have a consistent and repeatable process for identifying these control violations and then ensuring each is appropriately addressed. When this can be automated, design your log management solution to streamline and efficiently support this process.

The automation of this review process is the next mountain to climb for the log management solutions. Increasingly, companies are realizing that an IT person may not be the best employee to judge whether an event is permissible. Instead, a business manager might be a better person to determine if the violation was a true security breach or a required business activity. For example, an IT person might see that an employee who typically accesses only individual records is suddenly querying 10,000 records at a time. That seems like

A centralized and normalized view of system, application and network device logs helps staff quickly troubleshoot and identify the root cause of IT problems.

suspicious activity, but the security analyst does not know that the employee is analyzing

thousands of records for a new marketing campaign. Sending this alert to his or her manager would explain the action and clear the employee of any malicious intent.

Do you still need more justification for implementing the log management system? That's why you have the IT operations team in on the planning. The log management functionality works equally well with operations data. A normalized, synchronized view of system activities such as configuration changes, system restarts, failed service account login, web page not found or routing node change can quickly provide the historical insight IT operations needs to identify the root cause of a service degradation or failure.

Should your company suffer a data breach from the inside, you'll also want to know exactly who did what and when — and fast. Log management solutions can provide those answers quickly and cost-effectively. And you'll have a complete record of all system activity, time-stamped from multiple systems to provide a time sync across the event stream and the infrastructure.

CA delivers auditing and security event log management solutions that provide real-time data collection, consolidation and analysis of security data across the infrastructure. Both large enterprises and mid-market organizations can benefit from this type of solution, especially those regulated businesses that process credit cards (from public companies to the smallest of hospitals) all of which must adhere to compliance regulations. They all need to be able to quickly respond to questions from auditors, as well as monitor actions for evidence of criminal misuse of data. Log management solutions can streamline this process and enable you to very quickly monitor, investigate and report on activity across the IT infrastructure.

John E. Hawley is Director of Product Management at CA, where he leverages his broad technical and business background to guide product strategy and lead a team that defines and delivers integrated security management solutions. John holds an MBA focused on Product Management and a BS in Information Systems. With over 18 years experience creating, evaluating and deploying IT Management and Security solutions, John has successfully deployed large enterprise network management solutions with the U.S. Federal Government and Ernst & Young. He has creatively led the introduction of new products to telecommunication and security markets on behalf of CA, UUNET and with his own venture-funded software company that he founded and managed.

For the full issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).