Boosting enterprise security with integrated log management

Reduce security risks and improve compliance across diverse IT environments
Introduction

IT organizations of all sizes face tremendous challenges in keeping their computer networks secure and ensuring compliance with the latest security regulations. Most organizations use disparate solutions to collect, analyze, archive and store large volumes of event logs to meet the diverse requirements of internal IT security policies as well as industry standards and government regulations.

A wealth of information exists in the event data generated by the hundreds of network and security devices, servers, operating systems, applications and other endpoints in the typical enterprise IT environment. Unfortunately, this information may not be utilized effectively by existing management solutions. Often, critical incidents are overlooked because the information needed to recognize the significance of the incident is spread across multiple silos of information.

At the same time, many regulatory agencies mandate a formal approach to log and security management. Organizations struggling to maintain the integrity of their computing resources or having difficulty meeting compliance requirements can benefit from a comprehensive log management solution that helps remove the complexities of information security. This white paper explains an integrated approach for reducing potential security risks and facilitating compliance, and introduces how IBM® Security QRadar® Log Manager can help organizations stay a step ahead of the latest security threats.

Understanding the challenges of log management

Today’s organizations have invested in a variety of log management technologies and processes. These tools can vary from “home-grown” scripts, to shareware software, to commercially available solutions, but they are all focused on three fundamental objectives: identifying who is accessing network resources, understanding what data the users can see, and proving that only authorized users are accessing particular types of information.

Unfortunately, many security and network teams are dissatisfied with their current solutions for log management. For one thing, many legacy solutions cannot effectively support the latest devices and applications, including smartphones, tablets and the like. A major challenge for heterogeneous event management is that log formats are complex, are always changing and lack consistency from vendor to vendor. In addition, some solutions only collect data from a subset of networked systems, which results in incomplete visibility.
At the same time, many tools do not scale to support the full volume of real-time network activity, resulting in an incomplete picture of the network and security posture. Moreover, many organizations are frustrated by the lack of correlation and a unified view across the different silos of data, which can result in a sea of “false positives” and information overload. Clearly, the inability to support certain devices or to scale to provide a complete network perspective signals a failure to achieve the fundamental criteria for a compliant log management solution.

**Aligning log management with compliance mandates**

A comprehensive log management approach provides tremendous value to an IT organization. After all, the risks of failing an audit can be serious—from significant financial penalties to potential damage to an organization’s reputation. Many information security regulations and IT security best-practice frameworks recognize this value and specifically dictate some form of log collection and auditing.

However, as organizations define their compliance objectives, many quickly realize that a log management solution alone is not sufficient to meet their requirements. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires surveillance into network and application activity that cannot be achieved strictly through event logs.

Regardless of which regulations an organization must adhere to, it is important to assess the usefulness of a log management solution as part of an overall information security and compliance program. Although the solution can be deployed at the departmental level, organizations can only achieve the full value of integrated log management by deploying the solution across the entire IT environment.

**Measuring the strategic value of log management**

Typically, an organization’s operational practices can fall into the following three categories when it comes to log management:

- **Unmanaged, reactive environment**: No formalized log management solution has been implemented. The organization may leverage some limited tools, but IT staff have to juggle multiple interfaces and often manually correlate incidents with inconsistent data—which can be very time-consuming and costly for the business. The reporting requests of management and auditors go unfulfilled, sometimes with major consequences. Organizations in this category spend much more time fighting fires than strategically planning, and they can fail to detect even obvious security breaches.
• **Localized order:** A log management solution has been implemented, although only at a regional or departmental level. Alternatively, an organization in this category might have implemented a log management solution that provides only a limited set of features, and IT staff are forced to use manual processes and disparate tools to respond to threats across the environment. Or, as mentioned earlier, the solution may provide visibility into network and security events, but it does not provide a deep understanding of applications or user identities. Organizations in this category can gain some value from their solution, but the value is limited.

• **Optimized operations:** A comprehensive log management solution has been implemented across the enterprise, and the entire organization is receiving significant value. IT staff can run flexible searches and advanced analytics across the network and security systems, which can help them to quickly identify—and resolve—potential threats and compliance risks. Managers can receive actionable information to make better network and security decisions, while business leaders can easily get the reports they need to meet mandates for regulatory compliance and risk management.

**Identifying the key requirements for log management**

There are many factors to consider when selecting a log management solution, including:

**What is the breadth of data collection?**

Computing environments are made up of many disparate technologies. These typically include networking products such as switches and routers; security products such as firewalls and intrusion detection and prevention systems; operating systems; and applications including databases, network and systems management tools, and commercial and custom business applications. When evaluating log management solutions, organizations should consider the breadth of data sources supported for event collection, whether the solution can support proprietary applications and new technologies, and how it handles related events from different devices within a multi-vendor environment.

**Does the solution scale to my environment?**

Global organizations can generate billions of events per day, and the right log management solution should be able to support that volume. A scalable log management solution can distribute event collection across multiple systems, while also offering federated monitoring, reporting and administration capabilities within a central console. In addition, the solution should support concurrent querying of enterprise-wide data by several users without affecting performance.

**Is the data secure?**

Many regulatory agencies require event logs to be maintained in an unaltered state, which helps facilitate any future evidentiary use. This means that a log management solution should ensure integrity in the log records from the time they are created to the time they are destroyed. When evaluating solutions, organizations should verify that log archives can be maintained with integrity checks, including hash functions.

**Does the solution provide real-time event correlation?**

To protect data and help ensure compliance, a log management solution should offer a flexible and scalable event correlation engine to turn the flood of events generated across the network into actionable and prioritized information. Many solutions claim to offer correlation, but their capabilities can be so simplistic that they produce hundreds of alerts per day for even a small organization. These alerts, ultimately, get ignored, and the value of such “correlation” goes unrealized for the organization.

**Does the solution meet our audit requirements?**

Organizations that merely collect and archive event logs may not be able to meet the compliance requirements of many regulatory agencies. When evaluating log management solutions, consider whether the solution integrates with or supports detailed alerting, forensics, auditing and compliance reporting capabilities. An effective log management solution can generate detailed reports to support the diverse requirements of many in-house security policies, industry standards and governmental regulations.
Introducing IBM Security QRadar Log Manager
With IBM Security QRadar Log Manager, organizations can automate regulatory compliance activities and reduce security risks across a diverse IT environment.

Address diverse compliance mandates
With more than 2,000 out-of-the-box rules and reports, QRadar Log Manager enables organizations to meet a wide range of auditing and reporting requirements, including the PCI DSS, the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program, and the Gramm-Leach-Bliley Act (GLBA).

Gain visibility and fast access to information
Most organizations generate huge volumes of logs, and analyzing them can pose many challenges. With its customized rules engine, QRadar Log Manager can process each incoming event in real time, assign severity, credibility and relevance attributes, and then trigger an appropriate response via email notification, dashboard posting or by flagging an event for further monitoring. IT staff can run fast, flexible queries on this aggregated log data to quickly identify potential compliance risks and security threats. With pre-defined rules, reports and searches, an organization can quickly analyze log data, generate comprehensive reports and resolve security threats faster.
Rapidly search big data sets
With its instant search capabilities and advanced indexing technology, QRadar Log Manager enables fast, free-text querying of security and network data, including big data sets. This can help organizations simply and quickly detect threats, obtain forensics of big data, and conduct searches more frequently for enhanced security insights.

Use drill-down capabilities for fine-grained control
With a highly intuitive user interface that offers role-based access and a global view into real-time analysis and reporting, QRadar Log Manager provides a straightforward foundation for security and networking teams. Pre-defined dashboards are available by function, and users can create and customize their own dashboards. This means that IT staff can easily monitor specific activities and “drill down” to analyze data and activity trends. As a result, organizations can identify security anomalies and possible compliance risks, and take action before any damage can occur.

Integrate a wide range of devices
QRadar Log Manager can help organizations manage the event logs for a wide variety of network and security devices, including routers and switches, firewalls, virtual private networks, intrusion detection and prevention systems, anti-virus applications, servers, mainframes, endpoints, databases, email and web applications, custom devices and proprietary applications. QRadar Log Manager normalizes the log data into an easy-to-understand, yet flexible taxonomy for easy searching, correlation and reporting across a diverse IT environment.

Easily collect and store log data
QRadar Log Manager can help collect and store massive amounts of data—up to 16 terabytes per appliance. With its federated, distributed architecture, the solution can also scale to collect hundreds of thousands of events per second. QRadar Log Manager supports high levels of data compression, which can eliminate the need for external storage. It also features intelligent data policy management, allowing organizations to make more efficient use of storage by designating which information is to be kept for how long. Less important or sensitive data can be removed sooner; more important data can be retained longer.

Get immediate results with fast deployment
QRadar Log Manager is designed to be easy to deploy so organizations can quickly benefit from log management. Featuring an embedded log repository, integrated log collection, and extensive pre-packaged reports and rules, the solution can begin delivering value within days.

Expanding insights with a security intelligence platform
QRadar Log Manager provides a solid foundation for expanding visibility into security threats with a security intelligence platform. As part of IBM QRadar Security Intelligence Platform, QRadar Log Manager makes it easy to upgrade to layered security information and event management (SIEM) protection through the purchase of an additional license.

QRadar Security Intelligence Platform delivers a highly integrated set of solutions that can help organizations achieve a proactive security and compliance posture—using a single console, a single set of data stores and a single application codebase.

Anchored by powerful SIEM capabilities, QRadar Security Intelligence Platform provides actionable, real-time security intelligence by integrating security and network-monitoring applications into a unified solution. This way, organizations can deploy IT resources based on the analysis of a comprehensive set of data sources.

In addition, QRadar Security Intelligence Platform includes IBM Security QRadar QFlow Collector technology, which provides deep network monitoring and anomaly detection capabilities. As a result, organizations can get more detailed insights about potential threats based on their context. With application-aware network monitoring, IT staff can also help prevent threats by understanding the events that occur at the application layer.
Further, QRadar Security Intelligence Platform extends its security intelligence capabilities into virtual network environments with its IBM Security QRadar VFlow Collector technology. This technology helps organizations detect threats and manage risk in support of data center consolidation and private and public cloud initiatives.

The risk assessment module, IBM Security QRadar Risk Manager, helps organizations monitor vulnerabilities and firewall configurations to reduce risk and improve compliance. Based on contextual knowledge of events and network flow data, QRadar Risk Manager can help identify potential threats against high-value assets, determine possible attack paths and prioritize remediation activities.

Conclusion
Organizations of all sizes are tasked with protecting the information that traverses their network. The right log management solution can help automate IT security management tasks, strengthening defenses against attacks while improving compliance. By leveraging the information in network, security and application event logs, organizations can protect and optimize the use of critical resources. When evaluating log management solutions, organizations should consider how the log data can be used to support important functions across the entire environment, including:

- Does the solution provide effective monitoring and threat notifications to support the day-to-day operation of the network?
- Does the solution help facilitate compliance reporting and auditing, as mandated by internal security policies and regulatory agencies?
- Does the solution meet the security, scalability and workflow needs of your IT organization?

QRadar Security Intelligence Platform integrates the comprehensive log management capabilities of QRadar Log Manager with powerful monitoring, event correlation, threat notification, reporting and auditing technologies to meet the requirements of any IT security management program.

For more information
To learn more about IBM Security QRadar Log Manager, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/software/products/us/en/qradar-log-manager

About IBM Security solutions
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing