Real-Time Security Intelligence for Greater Visibility and Information-Asset Protection
# Table of Contents

Take the Effort Out of Log Management and Gain the Actionable Information You Need to Improve Your Organization’s Security Posture ........ 1
User Activity Monitoring ......................................................... 1
A Flexible, Scalable and Easy-to-Deploy Solution .................................. 3
Reporting for All Audiences .......................................................... 3
Efficient Anomaly Detection ..................................................... 3
How Micro Focus Can Help .......................................................... 5
Conclusion .............................................................................. 6
Take the Effort Out of Log Management and Gain the Actionable Information You Need to Improve Your Organization’s Security Posture

Organizations are doing business in new ways, thanks to new IT infrastructure technologies like virtualization, cloud computing and mobility, which are changing how users interact with information and with each other.

As the enterprise becomes more interconnected and distributed, business agility increases; but information security specialists face new challenges around maintaining effective security and monitoring controls.

To meet compliance requirements, you’ve undoubtedly implemented a tool for collecting and managing logs, but does it provide you with real-time information about—and analysis of—security events? Can you cut through the vast amount of security data that’s generated and gain the visibility you need to enforce continuous policy controls and deal with increasingly sophisticated threats?

It may even be the case that your log management tool no longer meets compliance requirements in full: Compliance mandates are changing, and collecting logs is often not enough. To reduce the risk of audit failure, you must be able to produce reports that both help you review anomalies, and demonstrate to ever-more attentive auditors that you’re doing so.

User Activity Monitoring

According to the 2011 Verizon Data Breach Investigation Report, eighty-six percent of organizations that suffered a breach found out about it from a third party (usually a law enforcement agency). Of these breached organizations, fully seventy percent had evidence in their log files that could have alerted them to the breach, but it went unrecognized. Clearly, although organizations are collecting the right data, they’re struggling to make meaningful sense of it in time—or ever.
When it comes to security reporting and event management, people are often weak links, especially if your processes are predominantly manual. Manually combing through logs to identify security events is time consuming and often fails to deliver the security intelligence you need to take action.

The longer it takes to find a breach, the longer an attacker has to exploit an opening. Even when you find a red flag, can you identify where it’s coming from, or who is compromising your security? And can you do so quickly enough to identify problems that are happening in real time?

In an environment of shrinking or static budgets and teams that are overstretched, your organization needs to work more efficiently to maximize all its resources. The more aspects of security reporting and event management you can automate—monitoring, correlation, and even remediation, for example—the faster you’ll detect and resolve anomalies, and the more time and effort the people on your team can devote to investigating real issues.

Further, if you can link security information and event management with user-activity monitoring capabilities, you’ll be able to tie users to specific actions across your systems. This will make compliance more straightforward. And the more visually you can present the information, the easier it will be for everyone—specialists and non-specialists alike—to understand.

![User-activity monitoring ties users to specific actions across systems.](image)
A Flexible, Scalable and Easy-to-Deploy Solution

Plenty of log management tools are on the market, including a number that are free to download. But if the tool you’re using can do nothing more than manage logs and you want to protect your enterprise, you’ll need to install other tools or software to add further security functionality. Unfortunately, doing this can disrupt the business or cause implementation or integration headaches. If your technology landscape or operating model is changing, a static or inflexible tool may not be able to keep up with your evolving needs. Similarly, it may be unable to cope with new types of potential threats and breaches, or with the challenges of providing privileged-user management and access. Ideally, you’ll implement a single solution that provides both log management and security information and event management (SIEM) capabilities, which deliver real-time intelligence about, and visibility into, your enterprise systems—and make it easier to mitigate security threats, improve operations and enforce policy controls.

 Reporting for All Audiences

Generating appropriate reporting for different parts of the business is vital to ensuring risk and threats are clearly understood, and to meeting audit and compliance requirements. If you’re relying on a simple log management tool, the reporting task can be daunting. Gathering the data, exporting it to an application like Microsoft Excel to make sense of it, then presenting the information visually using an application such as Microsoft PowerPoint is a time-consuming process that’s prone to errors.

With a more sophisticated tool, you can produce reports quickly and easily—within seconds in some cases—using predefined templates that provide rich, graphical formatting. You can include the hierarchy of information that will suit all your audiences, such as top-level summary information for chief risk officers (CROs) and chief security officers (CSOs), with the ability to drill down for details and evidence behind flagged events, and comparative or historical data where relevant.

Not only will you save time and reduce the risk of errors, you’ll also be able to present information in a more accessible and understandable way that satisfies your audiences. Further, by showing the time and cost savings gained through powerful dynamic searching and reporting, you can quickly demonstrate a return on the investment you made in moving beyond manual or tactical log management deployments.

Efficient Anomaly Detection

It’s often difficult to identify events as real or potential issues that require investigation. After all, not every anomaly indicates a potential security threat or breach. For example, if a spike in the number of logins one afternoon disrupts the normal pattern of logins, you may be able to easily explain the anomalous spike
based on known cycles of business operations and related systems. For example, the spike may be the result of partners accessing a sales tracking application, which they do only on the last day of each business quarter.

A one-dimensional view of deviation from a baseline won’t provide the security intelligence to help you identify real problems. You need a tool that will aggregate events and automatically identify inconsistencies in your organization’s environment—without having to build correlation rules that expect you to know exactly what you’re looking for.

The tool you choose should let you analyze anomalies from a virtually unlimited number of perspectives and give you the ability to look at an anomaly based on any combination of attributes and windows of time. This will give you the flexibility and control you need to look for the event patterns and causal relationships that might indicate a deviation and help you determine the exact nature of a threat.

You could, for example, spot the following sequence: An administrator creates a privileged user account that is immediately used to access a particular server and copy information from it onto an external storage device. On logging off, the account is quickly deleted, and the relevant logs are deleted from the file server. With security intelligence like this, you’re better informed: You can see the pattern that points to an anomaly more swiftly and easily, with no need to manually correlate the series of events, and can therefore investigate it more promptly.

Figure 2: A security dashboard puts real-time, actionable intelligence at your fingertips.
Ideally, your tool will provide you with both visual and automated methods for analyzing anomalies. A visual method, like a dashboard, helps you analyze baselines and trends by looking for spikes and valleys in activity and comparing them with the normal-behavior model. If you can view historical as well as real-time data, you’ll be able to build greater security intelligence—whether this means recreating the historical state of the system at the time an individual anomaly occurred, or understanding how your security and compliance posture changes over time.

As effective as visual analysis is, however, its power is strengthened when coupled with a complementary automated anomaly detection capability that provides you with greater depth, breadth and flexibility in detecting deviations.

When the tool detects an event that deviates from normal activity, it instantly generates an alert in real time, prompting a security specialist to deal with it straight away. You might even be able to set up such a tool to automatically start a remediation process that is in line with your internal processes—such as disabling a user account.

How Micro Focus Can Help

Micro Focus® understands the importance and the challenges of gaining the real-time security intelligence that enables organizations to improve their overall security postures and make more informed decisions.

Traditional SIEM solutions that deliver advanced functionality are often very complex. For customers to achieve greater value from SIEM, they need solutions that are simple to use and deploy, rapidly adapt to their ever-changing environments, and deliver true, actionable intelligence—the right information at the right time to the right stakeholders—to help identify and mitigate security threats.

NetIQ® Sentinel™ Enterprise delivers full-featured SIEM functionality that eliminates the complexity other SIEM toolkits introduce and maximizes the IT security team’s ability to align SIEM to organizational needs.

Sentinel Enterprise combines log management with SIEM in a single unified solution. It provides organizations with real-time visibility into the full spectrum of IT activities to mitigate security threats, improve security operations and automatically enforce policy controls across physical, virtual and cloud environments.

It provides an efficient SIEM solution by combining real-time intelligence, anomaly detection and user activity monitoring capabilities to provide an early warning mechanism and a more accurate assessment of IT activities. And because it’s less complex to deploy and use than many traditional SIEM systems, it makes security intelligence accessible to all organizations.
Further, Sentinel Enterprise delivers seamless integration with identity management to tie users to specific activities across all environments. So it’s easier to identify critical risks, significantly speed reaction times, and quickly remediate threats and security breaches before they affect the business.

**Conclusion**

With a simple, yet powerful log management and SIEM solution like Sentinel Enterprise, you'll get the security intelligence you need to meet compliance requirements and better protect your business. You'll be able to make better use of time and resources with automated processes that release security staff from manual tasks and enable them to focus on the things that really matter. You'll also satisfy your internal audiences with graphical reporting that lets them understand your organization's security posture and have confidence in your team's activities.

---

*Figure 3.* Sentinel Enterprise architectural components enable the intelligence and real-time visibility into IT events that organizations need.

Because it’s less complex to deploy and use than many traditional SIEM systems, Sentinel Enterprise makes security intelligence accessible to all organizations.