

Steps to Security Success

A Best-Practice Approach to Security Management Policies

by Ken Baker

You're worried about data breaches or maybe you're working toward PCI-DSS, FISMA or HIPAA compliance, but you're not sure what more you need to do or where to start. You likely have some combination of firewalls, intrusion prevention systems, vulnerability scanners and AV software in place, but these systems generate more information than you can act on, and are completely siloed from each other. You know you need to address your compliance requirements for log collection, but how do you turn all that information from all your different systems' logs into usable information? Also, from that information, you want to be able to easily investigate and quickly respond to suspicious incidents that occur on your network. On top of that, you don't want to spend a lot of time and money on products that don't end up addressing your needs.

In a recent discussion with Brian Singer, Solutions Marketing Manager for Novell Security Management, he outlined a security management model that addresses these concerns with a phased approach comprised of the following three main security management aspects:

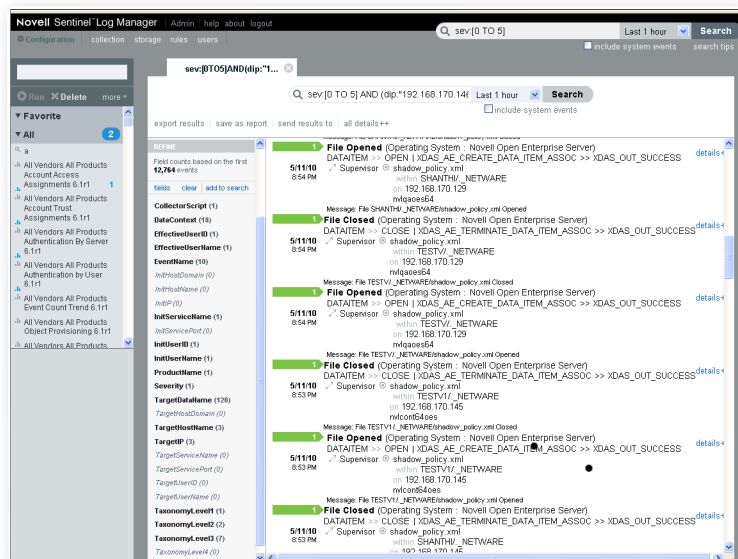
1. **Log Management**
2. **Security Information and Event Management**
3. **Integration of Identity and Access Management**

This phased approach is designed to help you immediately get more value out of your existing investments, and also allows you to grow and add more capabilities as you're ready.

If an organization simply looks at its log data, it can often spot breach warning signs and stop breaches before they ever occur.

> **Start with Log Management**

With any undertaking like this, the first question is where do you start? One way is to get started by determining and prioritizing your high-risk assets and your low-risk assets. Once that's accomplished, you can bring in a log management product to collect information from all those you deem as high risk, which will likely include your firewalls, servers and mission critical applications.



Event search

Figure 1: Novell Sentinel Log Manager helps you spot suspicious activities, changes, or trends, as well as respond to audits or compliance requirements.

The typical log management product collects data from different system logs and then stores that data for a specified period of time to give you a historical account of events that have occurred. With this data you should be able to get reports on what's happening in your environment to help you spot suspicious activities, changes, or trends, as well as to respond to audits or compliance requirements. (See Figure 1.)

According to industry analysts, about 80 percent of the time the steps that hackers take leading up to a data breach are recorded in the target organization's logs prior to the breach. In other words, if an organization simply looks at its log data, it can often spot breach warning signs and stop breaches before they ever occur. This is why log management is a great place to start. It doesn't require complex configuration and provides a fast return on investment.

However, there are some things you need to watch for when choosing a log management product. Cost is always an issue. Some products are simply too expensive and too complex. Some use proprietary data storage solutions that are difficult and costly to deploy and manage. And since you might need to store certain information for short periods of time and other information for longer periods, make sure your log management product supports multiple data retention policies.

For example, PCI-DSS requires the storage of log data for your systems for 90 days online and two years offline. While it's critical to retain this data, you might not want to retain all your data for two years. This means you need a log management product with flexible policy management to handle different types of retention scenarios.

You should also be wary of products that claim to do everything at once. The reality is that it will take time to implement all the features in such products. And if you end up biting off more than you can chew, your project might not ever get off the ground. That's another reason why a phased approach is best. You can implement what you need to demonstrate success at each phase.

Another major evaluation point is that your log management product not only needs to be able to collect log data from all your different systems, but it needs to be able to parse, normalize and

consolidate those different data sets into cohesive reports that are easy to generate, interpret and use. Without this function, making sense of your log data from a collective enterprise perspective will be nearly impossible.

While log management is a great place to start for security management, you need to make sure you don't choose a dead-end product. Taking a phased approach to security management requires that you can build on top of your existing log management product. Beware of products that store data in proprietary formats, can't forward events, lack the ability to integrate or don't have a peer in the area of real-time event monitoring. Your log management choice needs to give you room to grow by providing a path to security information and event management. Novell Sentinel Log Manager (www.novell.com/products/sentinel-log-manager/) provides this path, as well as addresses the other critical evaluation points you need to consider when choosing a log management product.

While log management is a great place to start for security management, you need to make sure you don't choose a dead-end product. Taking a phased approach to security management requires that you can build on top of your existing log management product.

> Add Security Information and Event Management

Once you've deployed your log management product, how do you know when it's time to add the near real-time monitoring and management capabilities provided by a security information and event management (SIEM) product? In his white paper, *The Complete Guide to Log and Event Management* (www.novell.com/docrep/2010/03/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf), Dr. Anton Chuvakin, a recognized security expert in the field of log management and PCI DSS compliance, offers the following three criteria that can serve as a guide to when you're ready to graduate from log management to SIEM:

Response capability: You have the ability to respond to alerts soon after they are generated.

Monitoring capability: You already have or have started to build security monitoring capability through the creation of a security operation center or a team dedicated to ongoing periodic monitoring.

Tuning and customization ability: Your organization is willing to accept the responsibility to tune and customize your SIEM product once it's deployed. This is a necessity since so-called out-of-the-box SIEM deployment rarely succeed or manage to reach their full potential.

In talking about adding SIEM to your log management foundation, Dr. Chuvakin says, "Organizations that graduate too soon will waste time and effort, and won't realize any increased efficiency in their security operation. However, waiting too long also means that the organization will never develop the necessary capabilities to secure themselves."

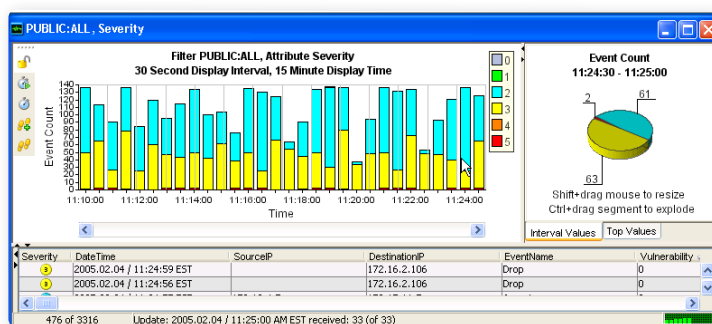
When you're ready to deploy a SIEM product, you want to choose a product that lets you build on and leverage your log management investment. This reinforces the need to also choose a log management product that can integrate or at least forward events to a SIEM product. This integration lets you naturally evolve your capabilities from reviewing periodic reports on log events to looking at those logged events in real time and even receiving immediate alerts on suspicious activity.

One of the features that you want to look for in your SIEM selection is true real-time correlation. Some products might claim to provide real-time correlation, when in reality they're just providing an event stream that shows events as they come in with some rudimentary alerting. True real-time correlation uses correlation rules to look for similarities between individual events that should raise warning flags.

For example, a user logging into one of your systems from an IP address in California probably won't draw your attention. However, if a few minutes later that same user logs in from an IP address originating in Europe you should have cause for concern. But it's unlikely you'll ever notice that event if your SIEM product only streams individual events across a dashboard without spotting the correlation between these seemingly innocuous events. Correlation rules in your SIEM product should be able to determine that such activity is not normal, and then automatically take appropriate action such as blocking the login attempt, notifying you of the activity, or putting that user or IP address on a watch list.

[Novell Sentinel](#) has a correlation engine that lets you create and customize rules that can identify such events and then take the appropriate action to mitigate the situation. This adds intelligence to your security event management by automating the analysis of incoming event streams to find patterns of interest, identify critical threats and complex attack patterns, prioritize events and initiate effective incident management and response.

Novell Sentinel also has a graphical control center interface that provides a real-time, holistic view of security and compliance activities across your IT environment. (See [Figure 2](#).) Novell Sentinel also leverages the same architectural foundation and technologies as Novell Sentinel Log Manager, including its communication bus, log connectors, data log collectors and event management system. Not only does this facilitate communication between all Sentinel Log Manager components and Novell Sentinel, but it provides you an efficient, streamlined solution that can scale to meet your needs.



Control center interface

Figure 2: The graphical control center interface in Novell Sentinel provides a real-time, holistic view of security and compliance activities across your IT environment.

> Integrate Identity and Access Management

Once deployed, your goal should be to continually improve the depth and breadth of your SIEM capabilities. Part of this depth and breadth improvement can come from growing the number of systems in your environment that you proactively monitor and report. Novell Sentinel has data collectors for nearly a hundred different systems from vendors including Apache, Checkpoint, Cisco,

a bit overwhelming. That's okay. If you follow this phased approach to security management, you can start small with the simple-to-deploy, easy-to-use and fast ROI log management provided in Sentinel Log Manager. And as your security management needs and capacity increase, you can easily grow your capabilities and reach with the real-time monitoring of Novell Sentinel, and then if desired you can move up to active user monitoring with Novell Identity Manager integration when you're ready.

While it's important to extend your security management reach through further integration of your SIEM with your various systems, one of the most powerful and important integration points for SIEM is with identity and access management systems.

By taking this phased approach, you can ensure your success every step along the way while making small incremental investments that improve your security and decrease your compliance costs and complexity. To find out more about Novell Security Management solutions visit www.novell.com/solutions/security-management. If you want to see firsthand how easy it is to use and deploy Novell Sentinel Log Manager as your first step toward security management, you can download a free 90-day evaluation version of it at download.novell.com/Download?buildid=woGGwp3Mab4~.

Learn More about Novell Security

- [Novell Sentinel Log Manager](#)
- [Novell Sentinel](#)
- [Guide to Log and Event Management](#)
- [Evaluation of Novell Sentinel Log Manager \(90-Day\)](#)