



Novell® Sentinel™ 6.1

Novell® Sentinel™ 6.1 provides a real-time, holistic view of security and compliance activities across your IT environment. Sentinel replaces labor-intensive manual processes for gathering, responding to and reporting on security and compliance events—enabling you to manage risk more effectively, cut costs and use your existing resources more efficiently.

A More Rigorous Security and Compliance Program

Novell Sentinel makes identifying, managing and reporting on security and compliance events in your environment faster and easier. Through best-of-breed automation, correlation and workflow management, Sentinel can help you reduce the cost of meeting compliance requirements. Sentinel delivers real-time monitoring and remediation for automated security and compliance. With a single view of security and compliance events across the enterprise, Sentinel combines identity management and security events management for real-time results. Sentinel streamlines labor-intensive, error-prone processes and cuts costs through automation, enabling you to deliver a more rigorous security and compliance program.

Software Based on Your Business Requirements

What if your firewall indicates an urgent problem while your IDS indicates that everything is fine? Which is correct? How do you

respond? When you have hundreds or thousands of devices and systems delivering security relevant data 24x7x365, correlation is the key. Novell Sentinel provides more accurate information to help you reduce false positives and focus resources on resolving the problems that really matter. Sentinel also uses in-memory correlation to reduce the load on your database and speed the delivery of critical event data.

Centralized event source configuration and management allow you to manage all of your connected devices right from the Novell Sentinel console to streamline operations and ensure that you always have a complete view of everything you need to monitor. Offline query and analysis functions provide improved forensics capabilities without impacting your need for a continuous real-time view of your environment.

Instead of providing cryptic reports that talk about IP address ranges and port numbers, Novell Sentinel delivers reports that show

Solutions

Identity and Security Management

Products:

Novell Sentinel 6.1



“Novell offers the unique ability to proactively address business needs for a real-time, comprehensive compliance solution that integrates people, systems, and processes.”

Chris Christiansen

*Program Vice President,
Security Products and Services
IDC*



It is a common capability among identity management vendors to detect rogue activity and react accordingly; however, Novell is the only vendor that has the capability to alert security administrators who the rogue administrator is and take action against that perpetrator.

how your security systems comply with and map to your business requirements. Sentinel allows security specialists to apply rules that leverage your unique business requirements, taking away the pain of complex scripting or programming. Because the data that Novell Sentinel collects includes business relevant data, you are now able to get reports that reflect, and are in line with, your business and operational context. With Novell Sentinel, you can now prove you are creating business policies for your users based on company objectives, instead of software parameters.

Using built-in business rules, you can easily:

- *Configure your systems to reflect your organization's policies and best practices*
- *Monitor and track the status of violations and remediation actions*
- *Quickly identify new trends or attacks*
- *Manipulate and interact with real-time graphical information*
- *Drill down into historical details in seconds*

Management across the Enterprise

Managing a distributed, heterogeneous IT security environment is a tall order. Servers, databases, applications, firewalls, routers, switches, identity and access management systems, intrusion detection and prevention systems, and many others produce floods of data that must be correlated and analyzed to get a clear picture of your organization's security and compliance health.

With Novell Sentinel, you get:

- **Integrated, holistic, real-time security management and compliance monitoring across all systems and networks.** *Sentinel correlates and analyzes security and compliance data from all the sources in your environment to help you identify security events in real time and respond to them quickly.*
- **Automatic documenting and reporting of security, systems and access events across the enterprise.** *Sentinel replaces labor-intensive manual processes with automated, continuous monitoring of security and compliance events and IT controls.*
- **Built-in incident management with fully customizable incident-response workflows.** *Automated incident response management enables you to document and formalize the process of tracking, escalating and responding to incidents and policy violations.*
- **The ability to react promptly, resolve incidents efficiently and prove to auditors that your IT controls work as required.** *Sentinel provides a framework that enables business policies and compliance requirements to drive IT policy and action. This allows you to demonstrate and monitor compliance with internal policies and government regulations such as SOX, HIPAA, GLBA and FISMA.*
- **Support for cross-platform and mixed open source and proprietary environments.** *Sentinel is compatible with Windows*, UNIX*, Solaris* and Linux* platforms. It can connect to any device via a wide range of connection methods.*
- **Seamless integration with Novell identity management, access management and security management products.** *Sentinel delivers real-time information and historical identity reporting.*
- **True identity context for enterprise security.** *Sentinel includes out-of-the-box capabilities such as identification, visibility*

and remediation of suspect activities throughout your enterprise.

- **Efficient resource utilization.** Validate that users who are provisioned to resources actually utilize those resources.

Complete Reporting

Industry research indicates that the biggest threat of data breach is from former employees who attempt to access resources after their employment has ended. Wouldn't it be nice to be able to provide internal auditors and system administrators with immediate

notification that a recently deprovisioned user is attempting to access corporate resources?

Novell Sentinel Reports provides a complete solution for visualizing the enterprise security environment, documenting regulatory compliance and efficiently managing operational risk. Sentinel Reports includes a comprehensive set of out-of-the-box reports and dashboards, which you can easily configure to meet your organization's specific requirements—or you can create your own reports using industry standard report builders.



Novell emphasizes integration. The result is a cross-platform, enterprise-wide system that combines identity and access management with security information and event management.

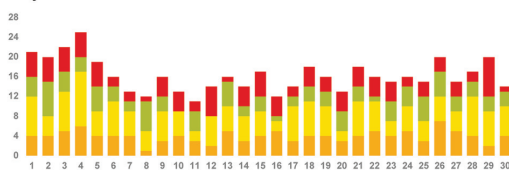
Suspicious Activity Overview: Monthly

All Identities

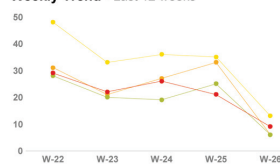
June 01, 2008 to June 30, 2008



Daily Trend



Weekly Trend - Last 12 weeks

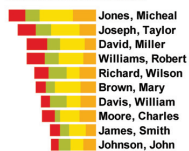


Violations by Department

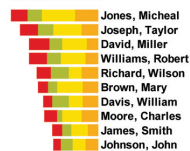


Violations Details - Top 10 Identities

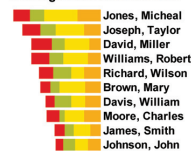
Authentication Failures



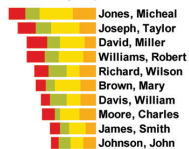
Access Denials



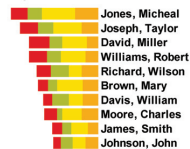
Privilege Escalation Denials



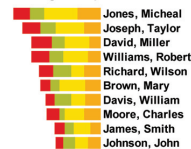
Affected by Exploits



Impersonators



Privilege Recipients



[Learn more](#)

Count on Novell Sentinel to deliver efficient, cost-effective, real-time security event management and compliance monitoring—with one tool to help you monitor potential threats, report and resolve them, and prove your organization is both secure and compliant. For more information, please visit: www.novell.com/products/sentinel/

www.novell.com

With Novell Sentinel Reports you can:

- *Demonstrate that you continuously monitor your critical IT assets and IT controls*
- *Prove that you have a documented, repeatable process in place for resolving security and compliance incidents*
- *Gain the insight you need to effectively monitor, measure and improve your security posture*
- *Discover trends and anomalies you can't detect manually*
- *Track and report all security-related activities—including user activity, incidents and policy violations—on assets affected by SOX, HIPAA, FISMA, PCI and other standards and regulations*

Reduce Costs, Minimize Risk and Maximize Efficiency

It is a common capability among identity management vendors to detect rogue activities and react accordingly; however, Novell is the only vendor that has the capability to alert security administrators who the rogue administrator is and to take action against that perpetrator.

Novell emphasizes integration to deliver a single view of security and compliance activities across the enterprise. The result is a cross-platform, enterprisewide system that combines identity and access management with security information and event management. This solution enables your organization to reduce costs, minimize risk and maximize efficiency while maintaining the highest levels of security and regulatory compliance.



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA