opentext™ | Cybersecurity

Product Flyer

Sentinel

Powerfully simple security management

“Even though we were experiencing up to 35 serious security incidents a day, Sentinel allowed us to achieve early detection and fast resolution, ensuring that these incidents had no impact whatsoever on the running of the Games.”

Vladan Todorovic
Technical & IT Security Manager
for the Youth Olympic Games
Atos Origin

Organizations are transforming their IT infrastructures and the way they use them in significant ways. These transformations have generated an array of difficulties and challenges that can adversely affect an organization’s ability to secure its enterprise.

For example, technologies such as virtualization, cloud computing and mobility have changed the way organizations do business. These technologies have enabled users to behave and interact with information and each other in new and exciting ways. However, the technologies have also created distributed, interconnected enterprises that information-security analysts find increasingly difficult to monitor and secure.

To improve their overall security posture and make more informed decisions, organizations require real-time information about and analysis of security events. They need the ability to cut through the complexities of managing vast amounts of security data, dealing with sophisticated threats and enforcing continuous policy controls. They need a solution that enables them to quickly and accurately determine which of the events in reams of event data constitute critical events and security anomalies.

Product Overview

OpenText™ Sentinel 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 reduces the complexity of traditional security information and event management (SIEM) and lowers the barriers to SIEM adoption, making security intelligence accessible to all organizations. Sentinel also provides organizations with a more efficient SIEM solution by combining real-time intelligence, anomaly detection and user activity monitoring to provide an early-warning mechanism and a more accurate assessment of IT activities.

Sentinel delivers the industry’s only seamless integration with identity management to tie users to specific activities across all environments. As a result, it enables organizations to easily identify critical risks, significantly speed reaction times and quickly remediate threats and security breaches before they impact the business. This identity-centric approach helps organizations easily spot critical risks, speed reaction times, and quickly remediate threats and security breaches before they impact the business.

Capabilities and Features

- **Anomaly Detection**—Identifying events as real or potential issues that require investigation is often difficult. With Sentinel anomaly detection, you can automatically identify inconsistencies in your organization’s environment without building correlation rules that expect you to know exactly what you are looking for. When you implement Sentinel you establish baselines for your organization’s specific environment, enabling you to immediately deliver better intelligence and faster anomalous-activity detection. Comparing trends with a baseline allows you to view historical activity patterns, enabling you to rapidly develop models of typical IT activities—or states of normalcy—that make it easy to spot new, potentially sharmful trends.

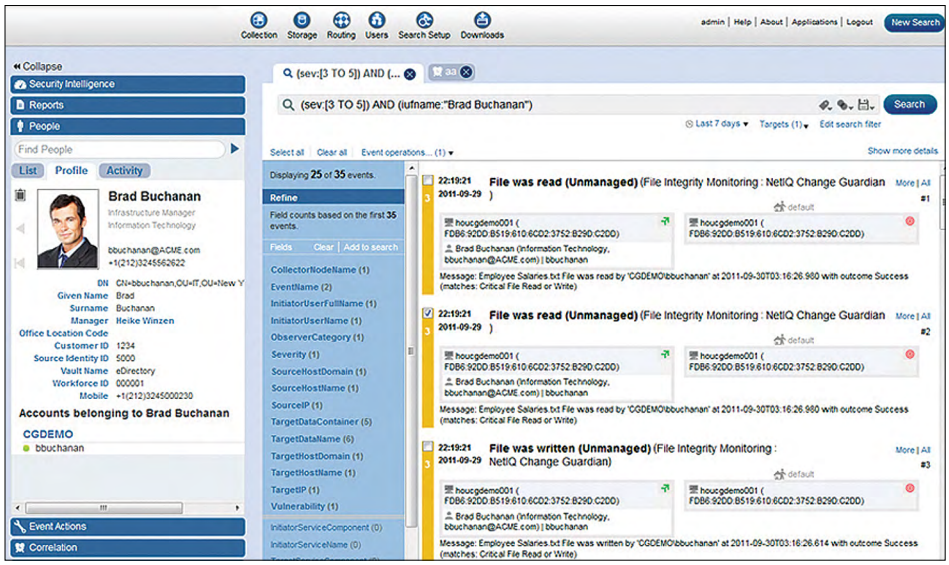

Figure 1. Sentinel delivers industry leading user activity monitoring capabilities by leveraging identity management to tie users to specific actions across systems.

- **"Big Data"-based Scalable Storage**—Often, enterprises are not prepared for growth—and the additional security events that must be captured and analyzed. Sentinel gives you the option of storing event data in a Hadoop Big Data backend. This enables you to scale your usage up very quickly and efficiently. Additionally, you can now combine Sentinel's SIEM data with data from other products that are populating the Big Data backend. Sentinel is certified to work with Cloudera-provided Big Data backend components, ensuring you have the most scalable and dependable event storage solution available.
- **Flexible Deployment Options**—Sentinel is delivered as a soft appliance via an International Organization for Standardization (ISO) image on all major hypervisors, including VMware, HyperV and XEN, and as installable software on SUSE Linux Enterprise Server and Red Hat Enterprise Server. Sentinel deployment and licensing models are extremely flexible, allowing you to deploy SIEM and log management across your organization's enterprise to meet its particular usage needs.
- **High Performance Storage Architecture**—Sentinel employs an efficient, file-based event storage tier optimized for long-term event archiving. The event store provides 10:1 compression, fully supporting fast, indexed searches. And Sentinel gives you the option of synchronizing or moving some or all of your organization's event data to a traditional relational database. Significantly enhanced searching reduces the time it takes to find data and generate reports.

Organizations are transforming their IT infrastructures and the way they use them in significant ways. These transformations have generated an array of difficulties and challenges that can adversely affect an organization's ability to secure its enterprise.

- **Graphical Rule-Builder**—Sentinel allows you to quickly build event-correlation rules directly from the events it collects in your environment—without the need for administrators to do significant training or learn a proprietary scripting language. Additionally, you can test rules before you deploy them to reduce false-positive alerts, improve event correlation and ultimately deliver improved exploit detection. This significantly increases your organization's time to value while decreasing its total cost of ownership.
- **Identity Enrichment**—Through out-of-box integration with NetIQ Identity Manager, Sentinel delivers the industry's only seamless identity management integration that ties users to specific activities across the enterprise. Enriching security data with the unique identity information of users and administrators provides significantly more insight into the who, when and where of users' system access. In addition, by infusing identity into event data, Sentinel intelligently protects against insider threats and delivers a more actionable remediation mechanism.
- **Simplified Filtering, Searching and Reporting**—Sentinel simplifies the collection of IT infrastructure events to automate tedious compliance-audit and reporting functions and significantly reduce the complexity, time and costs of locating and preparing data auditors require. This helps your organization quickly adhere to government regulations and industry mandates.
- **Enhanced and Expanded Packaged Reports**—Sentinel simplifies reporting through its data aggregation and normalization capabilities, prebuilt reports and customizable policies, and fast search capabilities. You can generate reports against real-time search results on the fly with the simple push of a button, allowing you to instantly report on the data you want without the chore of modifying a confining, prebuilt template.

> **“It would have been impossible to keep up with the dramatic increase in network security activity without at least 10,000 personnel. Sentinel gives our centralized monitoring team a comprehensive holistic view of security events so we can immediately act on what is most critical.”**
>
> **Keith Rohwer**
> Director of Research, Development, Testing and Evaluation
> NCDOC

Connect with Us
www.opentext.com

Key Differentiators

Unlike tactical SIEM solutions, which are simple but not designed to deliver real security intelligence, and traditional SIEM solutions, which are powerful but require significant skills and customization and are difficult to adapt to changing environments, Sentinel delivers the highest value in security intelligence, because it delivers both the simplicity and power to help answer the question, “Am I Secure?”

- ”Big Data” backend provides a highly scalable event storage solution that helps ensure compliance and is supported by a proven, high-availability framework.
- Virtual software appliance packaging allows for fast and easy deployment. Unlike hardware-based options, virtual appliances can easily expand to handle growth and additional capacity.
- Identity enrichment provides rich context to security events to provide greater insight for detecting and preventing insider-based threats.
- Simplified administration with graphical rule building interfaces and capacity planning. Administrators can develop correlation rules quickly during implementation and easily maintain and update them as business needs change, providing a lower total cost of ownership.
- Day-one value is possible with security intelligence dashboards that allow monitoring the organization’s security almost immediately after installation.
- Intuitive data searching allows security administrators to easily find the data they need and quickly turn search into a report.

To learn more about Sentinel, click here.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000133-001 | O | 12/23 |