NetIQ Sentinel 7

Powerfully simple security management

Introduction

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 enabled distributed, interconnected enterprises for which information-security analysts find it increasingly difficult to effectively monitor and maintain security.

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

NetIQ® Sentinel™7 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. NetIQ Sentinel 7 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.

NetIQ Sentinel 7 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. With its real-time intelligence, Sentinel empowers organizations to protect against the rise of advanced threats, improve security operations and continuously enforce policies.

SOLUTION:

Security Management

PRODUCT:

NetIQ Sentinel 7

NetIQ®

Capabilities and Features

- **Anomaly Detection** – Identifying events as real or potential issues that require investigation is often difficult. With NetIQ 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 harmful trends. To enhance these capabilities, you can further tune your environment's baselines and corresponding anomalous event detection. NetIQ Sentinel also shows you how your security and compliance posture changes over time.
- **Flexible Deployment Options** – NetIQ 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. NetIQ 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. Sentinel employs a flexible searching and event-forwarding mechanism, allowing the deployment architecture to adapt to your environment, even with a highly distributed deployment.
- **High Performance Storage Architecture** – NetIQ 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 NetIQ 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. The Sentinel storage architecture eliminates the need for third-party database licensing, reducing your organization's total cost of ownership.

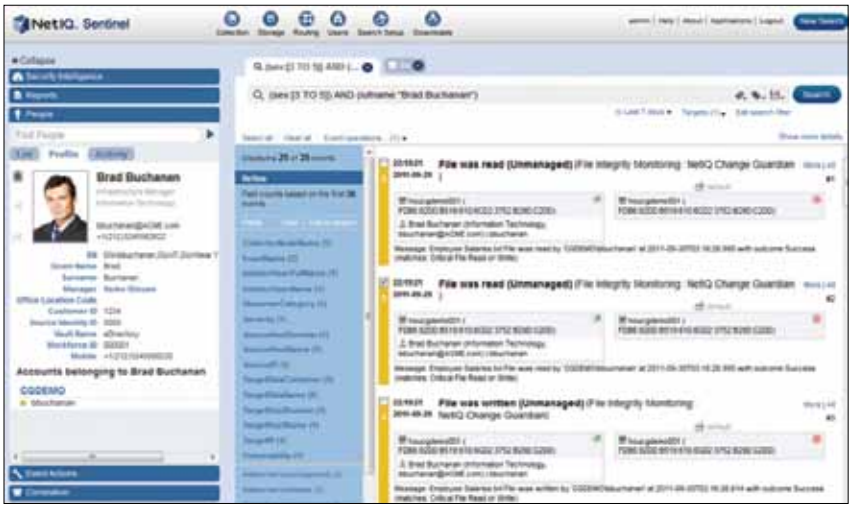

Figure 1: NetIQ Sentinel7 delivers industry-leading user activity monitoring capabilities by leveraging identity management to tie users to specific actions across systems.

Learn more about NetIQ Sentinel Log Manager at www.netiq.com

- **Graphical Rule-Builder** – NetIQ 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, NetIQ 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, NetIQ Sentinel intelligently protects against insider threats and delivers a more actionable remediation mechanism. NetIQ Sentinel also includes identity integration with Microsoft Active Directory and will include integration with other identity management products in the near future.
- **Simplified Filtering, Searching and Reporting** – NetIQ 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** – NetIQ 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.
- Unified Single Solution – NetIQ Sentinel combines log management with SIEM in a single unified solution.

NetIQ®

Key Differentiators

Unlike tactical SIEM solutions, which are simple but not designedto deliver real security intelligence, and traditional SIEM solutions, which are powerful but require significant skills and customization and are difficulttoadapt to changing environments, NetIQ Sentinel 7 delivers the highest value in security intelligence, because it deliversboth the simplicity and power to help answer the question, "Am I Secure?"

- 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 providegreater insight for detectingand 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.

For more information, please visit ***www.netiq.com/sentinel7****.*

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us:

PB595001SENT PS 04/12