WHITE PAPER

NetIQ Sentinel 7

Security Intelligence Made Easy

For security professionals who must answer the question, “How secure are we?” but are overwhelmed with the constant change and complexity of the computing environment and emerging threat profiles, NetIQ® Sentinel™ 7 is a powerfully simple Security Information and Event Management (SIEM) solution built to help protect sensitive information assets and achieve regulatory compliance while cutting through the rapid cycle of change in enterprise IT.

This white paper highlights NetIQ Sentinel 7’s ability to increase your visibility and understanding of potential threats and speed remediation without the need of extensive training or expertise—all while gaining the security intelligence and control you need to secure your enterprise with greater confidence and assurance like never before.

NetIQ

WHITE PAPER

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Table of Contents

Real-Time Security Intelligence, Visibility and Protection 4
New and Other Key Features 4
NetIQ Sentinel Architecture 6
Event Source Management Framework and Collectors 7
Sentinel iSCALE Message Bus 8
NetIQ Sentinel iTRAC Automated Workflows 8
Anomaly Detection Engine 8
How Anomaly Detection Works 8
Analyzing Anomalies 9
Point Anomalies 10
Contextual Anomalies 10
Historical Comparison Anomalies 11
Automatic Anomaly Detectors 11
Acting on Anomalous Events 11
Dealing with Anomalous Continuations 11
Dynamic Web-based Graphical Analysis of Anomalies 11
How Sliding Time Window Analysis Works 12
Correlation Engine and Rule Builder 13
High Performance Storage and Reporting 14
NetIQ Sentinel Log Manager 16
NetIQ Sentinel Link 16
Intelligent Workload Management 16
Real-Time Intelligence, Visibility and Protection 17
About NetIQ 18

Real-Time Security Intelligence, Visibility and Protection

Organizations are significantly transforming their IT infrastructures, and the way they use them. 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 maintain security and monitoring controls.

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.

NetIQ® Sentinel™7 is a security information and event management (SIEM) solution that provides organizations like yours with real-time intelligence about, and visibility into, enterprise systems, enabling them to mitigate security threats, improve operations and enforce policy controls across physical, virtual and cloud environments. Sentinel delivers industry-leading user-activity monitoring capabilities by leveraging identity management to tie users to specific actions across systems. To speed remediation, especially for unknown threats and insider attacks, Sentinel has the ability to quickly detect anomalous activities in both distributed and traditional IT infrastructures. Sentinel provides a superior security foundation to address advanced threats, improve operational efficiency and streamline regulatory compliance processes.

New and Other Key Features

- **Anomaly Detection**—It is often difficult to identify events as real or potential issues that require investigation. With Sentinel anomaly detection, you can automatically identify inconsistencies in your organization's environment without having to build 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. Sentinel also shows you how your security and compliance posture changes over time.
- **Flexible Deployment Options**—NetIQ delivers Sentinel as a soft appliance (via an International Organization for Standardization [ISO] image) on all major hypervisors (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. 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**—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. The Sentinel storage architecture eliminates the need for third-party database licensing, reducing your organization's total cost of ownership.
- **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 significant training, or to learn a proprietary scripting language. Additionally, you can test rules before you deploy them to reduce false-positive alerting, improve event correlation capabilities, and, ultimately, deliver improved exploit detection capabilities. 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 integration with identity management 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. Sentinel also includes identity integration with Microsoft Active Directory and will include integration with other identity management products in the near future.

Figure 1

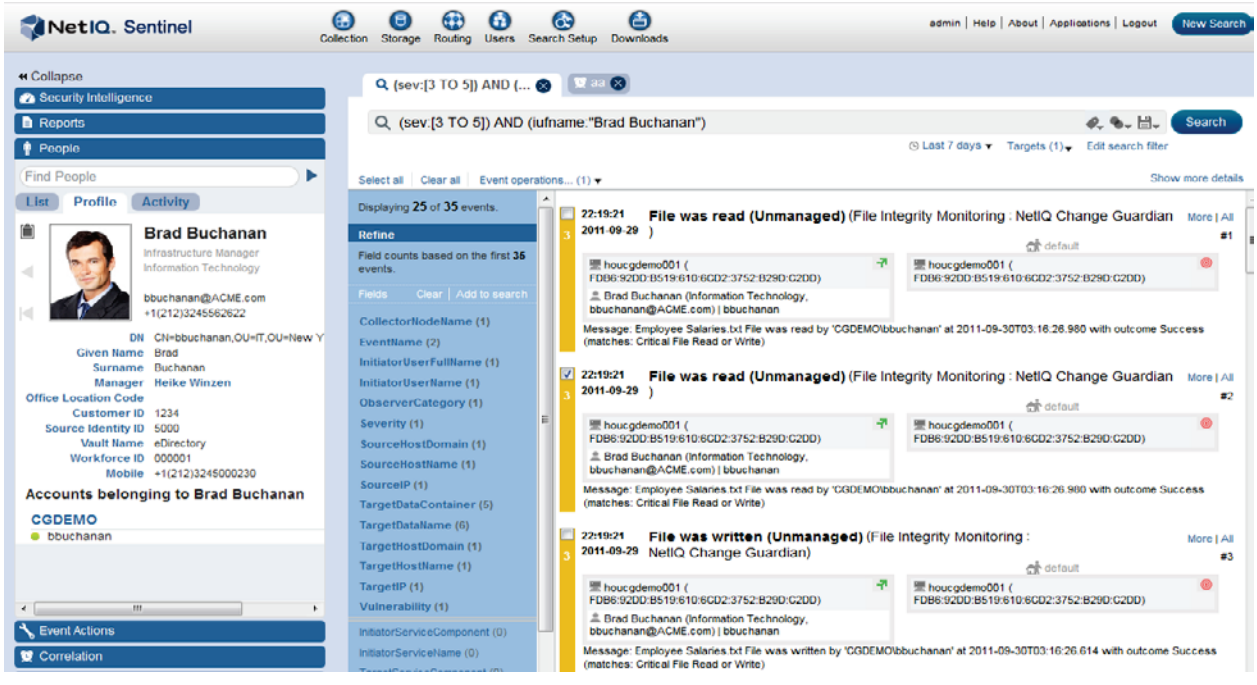

Figure 1: NetIQ Sentinel delivers industry leading user activity monitoring capabilities by leveraging identity management to tie users to specific actions across systems.

- **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, pre-built 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 having to modify a confining, pre-built template.
- **Unified Single Solution**—Sentinel combines log management with SIEM in a single unified solution.

NetIQ Sentinel Architecture

The following key architectural components enable Sentinel to deliver the intelligence and real-time visibility into IT events organizations need:

- Event source management framework
- Collectors and collector managers
- Sentinel iSCALE message bus
- Sentinel iTRAC automated workflows
- Anomaly detection engine
- Dynamic web-based graphical anomalies analyzer
- Correlation engine and rule builder
- High performance storage, search, and reporting components

Figure 2

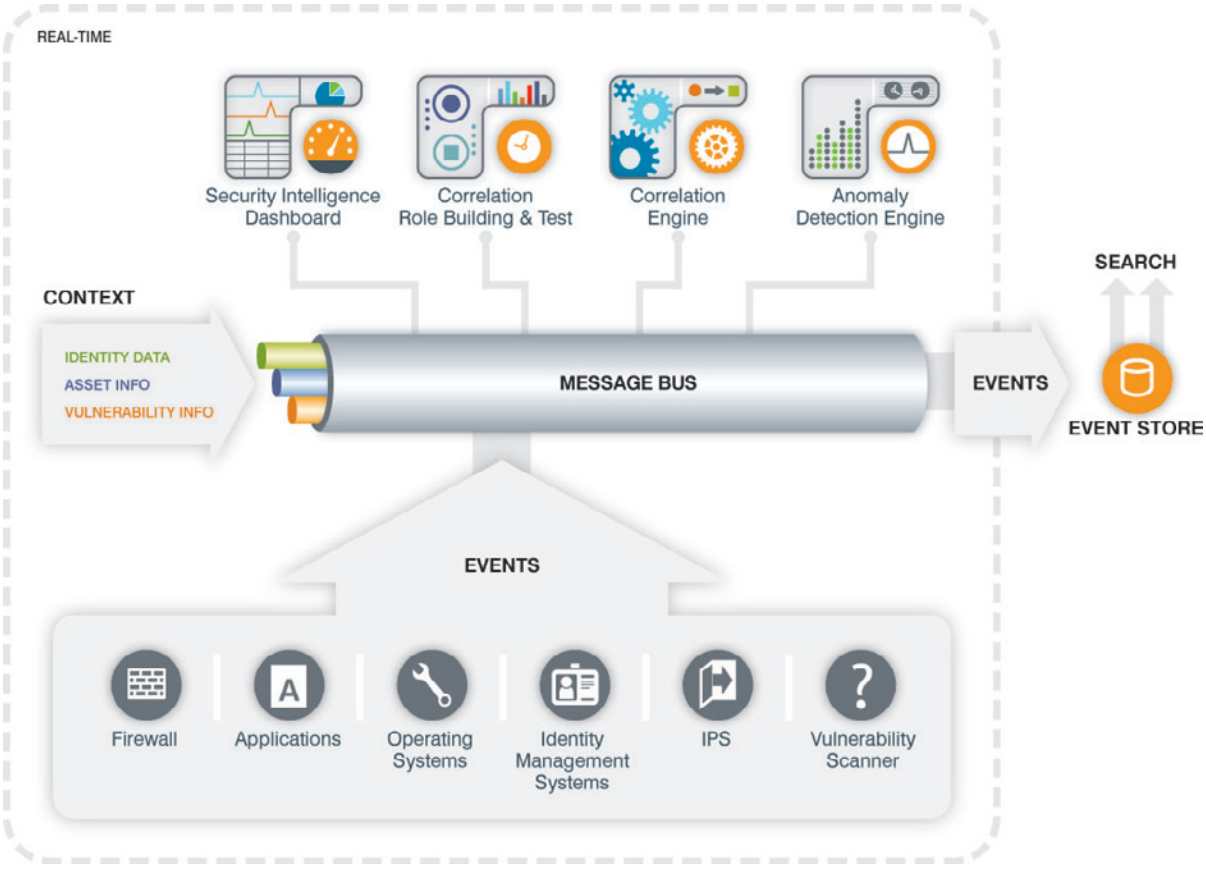

Figure 2: NetIQ Sentinel key architectural components enable Sentinel to deliver the intelligence and real-time visibility into IT events organizations need.

Event Source Management Framework and Collectors

NetIQ Sentinel includes a centralized event source management (ESM) framework that facilitates and streamlines deployment and data source integration. The framework enables data-collector configuration, deployment, management and monitoring for a wide array of systems. Sentinel connectors and collectors work in conjunction to obtain raw log data, parse the data and deliver a rich event stream before it correlates, analyzes and sends event data to storage.

Sentinel collectors and collector managers provide a flexible set of tools that let you monitor virtually any source of security-relevant data, including proprietary and custom devices, referential sources, operating systems and applications. With their built-in intelligence and ability to automate mundane manual processes, collectors can respond to rules and take action in response to specific conditions. They can collect and filter events remotely or locally. Additionally, with the exception of a few systems (such as mainframes), collectors are agentless, which allows them to gather data remotely without requiring that software be installed on the monitored system or device.

NetIQ Sentinel also provides integrators that allow two-way communications with third-party helpdesk or trouble-ticketing systems, as well as with devices that do not produce easily readable logs, such as mainframes.

The collectors in Sentinel automate the event-filtering process, sending the majority of events to storage for later analysis, while sending certain types of events to the anomaly detection engine or correlation engine for immediate analysis. To further identify and classify events, collectors also add to them data such as event taxonomies and business relevance, enhancing your organization's ability to analyze the events' significance.

Sentinel iSCALE Message Bus

An iSCALE message bus enables communications between Sentinel components. This bus enables easy integration with NetIQ Identity Manager and other products capable of message-bus communications.

The Sentinel message bus-based architecture has a highly scalable design, allowing large systems to use Sentinel without a significant performance penalty. The bus owes its high-performing nature to the Sentinel architecture's lack of reliance on a back-end relational database, which would act as bottleneck to performance and cost-effective scalability. Instead, Sentinel uses in-memory processing to capture and filter events promptly, enabling analysis on thousands of events per second in real-time. The bus allows organizations to scale components independently without duplicating their entire systems, and without adding database licenses and costly hardware.

NetIQ Sentinel iTRAC Automated Workflows

NetIQ Sentinel iTRAC is a built-in, automated workflow and event remediation system that establishes workflows to automate the incident identification and resolution processes. Sentinel iTRAC workflows specify a series of actions to take when specific events occur. You can tune these predetermined processes to reflect your organization's best practices, and completion of each activity provides an audit trail for demonstrating regulatory compliance. In addition, iTRAC allows you to automatically delegate tasks to external systems, such as third-party helpdesk solutions and other systems.

Anomaly Detection Engine

Anomaly detection, which is new to Sentinel with version 7, enables you to establish specific baselines respective to your organization's IT environment, allowing Sentinel to deliver better intelligence and faster anomalous-activity detection. You can also create and view historical pattern activities, and you can develop models of typical IT activities that allow you to easily spot new, potentially harmful trends. In addition, you can customize your organization's environmental baselines to see how its security and compliance posture has changed over time and to reduce false-positive alerts and report on anomalous events.

How Anomaly Detection Works

As Sentinel gathers event data, it converts event streams into multidimensional statistical streams. These statistical streams lead to behavior models that allow the engine to examine the combination events' multiple characteristics for abnormal behavior.

For example, some rudimentary baselining solutions rely on one-dimensional statistical models, such as counting how many logins took place during a certain time interval. The multidimensional statistical models the Sentinel anomaly detection engine creates can gather, aggregate, and store a continuous statistical stream that encompasses multiple attributes of login events. From this stream the anomaly engine can compare how many failed logins occurred in relation to the overall number of logins. Then it can go even further by indicating that the majority of these failed attempts occurred on certain database servers or some other device. Multiple levels of classification give your organization's security analysts significant flexibility and control as they look for causal relationships that might contribute to a deviation; they can also help analysts determine the exact nature of a threat.

To analyze multiple characteristics of an anomaly at a given point in time, Sentinel transforms statistical streams into a collection of single-variable time-series streams. These time-series streams are analogous to "buckets of time." Sentinel creates a bucket of time for every event attribute it's interested in counting and analyzing. For example, it might create a bucked of time for failed logins, a bucket of time for attempted logins, a bucket of time for file deletions, and so on, with each bucket of time having a capacity of one minute.

In this example, during a one minute period starting at 8:00a.m., the failed login bucket will count events with failed logins. The attempted logins bucket will count attempted logins. And the file deletions bucket will count events with file deletions. At the end of the minute, these buckets might respectively contain counts of 200, 500 and 15. At 8:01a.m.,Sentinel will create a new series of time buckets to count these event attributes for the next one minute interval. This process will continue, eventually yielding a collection of time buckets that represent how many times these event attributes occurred for every minute of the day.

NetIQ Sentinel can leverage this collection of single-attribute time series (buckets) by feeding different combinations of them into its anomaly detection engine, which allows your organization to analyze anomalies from a virtually unlimited number of perspectives. You can look at an anomaly based on any combination of different attributes, adding or removing attributes from the equation as desired to see how it affects the analysis. And because the collection of time series represents discrete intervals of time throughout the day, you can go back in time and, on demand, examine an anomaly for a five minute slice of time—from 9:00 a.m. to 9:05 a.m., say, or a thirty minute slice of time from 9:15 a.m. to 9:45 a.m., or any slice of time during any part of the day.

This ability, known as dynamic time resolution, allows your organization to analyze anomalous behavior in a virtually unlimited number of scenarios based on different event attributes and windows of time. Sentinel can provide this dynamic time-resolution capability for both near real-time and historical analysis.

Analyzing Anomalies

The Sentinel anomaly detection engine provides two main methods for analyzing anomalies: visual and automated. For visual analysis, Sentinel provides a powerful, intuitive dashboard that allows you to analyze baselines and trends. Using this method, you can watch for spikes or valleys in activity and compare them with the normal behavior model.

Through the Sentinel dashboard, you can use the following techniques to analyze time series:

- Inspect rates of change and deviations from baselines (normal behavior) by comparing activity against multiple baselines.

- Detect anomalous patterns via dynamic time resolution and aggregation of current data and baselines.
- Zoom into contiguous patterns of interest.
- Examine statistical metrics, including historical comparisons of selected baselines for certain time periods.
- Drill down into individual categories of multilevel categorical baselines and statistics.
- Seamlessly transition between real-time and historical data.
- Recreate the historical state of the system during the time of the anomaly, including calculated metrics.
- Examine contextual association between users, assets and other attributes contributing to anomalies.
- Drill down to the events causing anomalies.

As effective as visual analysis is, manually watching for anomalous activity consumes significant time. In addition, your ability to mentally visualize all off the dimensions and attributes that contribute to an anomaly may be limited.

Complementing its visual analysis capabilities, the Sentinel automated anomaly detection method gives you greater depth, breadth and flexibility in detecting deviations from normal activity.

NetIQ Sentinel allows you to set up automated anomaly detectors that watch for specific deviations from normal activity. When they detect an anomaly, the detectors send alerts in real-time. You can then further investigate the anomaly through the dashboard.

You can create automatic anomaly detectors that watch for and analyze the following three main types of anomalies:

- Point anomalies
- Contextual anomalies
- Historical comparison anomalies

Point Anomalies

Point anomalies are simple threshold-based anomalies. For example, you might want Sentinel to inform you if the number of failed logins to your organization's payment card industry (PCI) network exceeded the threshold of 500 failed logins by a certain percentage during any one-hour interval.

Contextual Anomalies

Contextual anomalies refer to activity that might be normal under certain conditions, but anomalous under other conditions. Sentinel contextual anomaly detection allows you to look for anomalies based on the context of these different situations. For example, in an organization that has 1,000 people, 1,000 logins between 8 a.m. and 9 a.m. would likely be considered normal. However, after 9 a.m. the normal number of logins might drop to one hundred or lower. The normal number of logins after 5p.m. and on weekends would probably drop even more significantly.

NetIQ Sentinel allows you to configure its anomaly detection to match the desired contextual thresholds of these different time periods. Solutions that don't offer contextual anomaly detection, as Sentinel does,

force you to choose between setting thresholds too high or too low. If you set thresholds high to accommodate peak times, these solutions won't detect the anomalous behavior that might occur during low periods. If you set the thresholds low so you can catch all potential anomalies, you'll be overwhelmed with false-positive alerts during peak times.

Historical Comparison Anomalies

Also known as *baseline* or *relative* anomalies, historical comparisons allow you to compare behavior between different points in time. For example, you can have Sentinel alert you if logins increase during any 15-minute interval by 30 percent, compared with15-minute intervals during the previous hour. Or you might want to watch for increases in logins on Monday between 9a.m. and 10a.m., compared with the number of logins on the previous Monday between 9a.m. and 10a.m. Historical comparison anomalies give you great flexibility to compare activities between different time intervals on an ongoing basis, further enhancing your organization's ability to detect abnormal activity or behavior.

Automatic Anomaly Detectors

The Sentinel dashboard makes it easy to create a wide range of automatic anomaly detectors. Simply follow the wizard to name your detector, select the type of anomaly you want to detect, and configure the detector's parameters of interest—such as minimum time interval groupings, types of events (login attempts, failed logins, file deletions, and so forth), thresholds, and historical comparison values (days of the week or times, for example). As part of the anomaly detector's definition, you can also specify notification parameters, such as whom the detectors will notify and how soon they should send another notification if the anomaly occurs again.

Acting on Anomalous Events

When it identifies an anomaly, Sentinel generates an anomaly event that it feeds back into the Sentinel event stream. Various components downstream—including the reporting and storage layers, the correlation engine, and the iTRAC workflow (which can send alerts and kick off different remediation processes)—can then act on these events. The correlation engine has the ability to use anomaly events to give it further context for evaluating rules and identifying defined patterns that include certain kinds of anomalous events in conjunction with other types of events that together comprise malicious behavior.

Dealing with Anomalous Continuations

In certain situations, attacks might repeatedly generate significant numbers of anomaly events, which could have the potential to overwhelm you if you are analyzing or investigating the attacks. Sentinel has a built-in continuation and update mechanism to address this problem. With this mechanism, Sentinel has the ability to reduce the number of identical anomaly events the engine emits (within a specified time interval) by recognizing that subsequent occurrences of the initial anomaly event are simply continuations of the event.

Dynamic Web-based Graphical Analysis of Anomalies

With version 7, Sentinel has a completely refreshed, powerful and easy-to-use web interface. The interface's new security-intelligence dashboard plays a major role in enabling you to manage, monitor and analyze activity.

The dashboard presents real-time and historic graphical views of how things change in your organization's environment over time. At the center of the dashboard, a spark line shows the aggregate statistical peaks and valleys of actual activity for a defined automatic anomaly detector, as compared with normal trends and baselines for specific time intervals. On the right side of the main graph, the dashboard lists graphical and numerical comparisons of actual and normal activity for individual, relevant event attributes associated with a defined anomaly detector (such as the number of login attempts, failed logins, or deleted files) for these time intervals.

Additional information and statistics on detected anomalies are listed below the main graph. These items provide access to further details. For example, the information might be an alert for file deletes. When you click this alert, you get details such as IP sources or user IDs that correspond to the file deletes.

How Sliding Time Window Analysis Works

One of the most powerful components of the Sentinel dashboard is its sliding-time-window analysis feature. Powered by the product's time series generation capability, the sliding window allows you to view graphical and statistical analyses of nearly any time slice. The time window could represent activity from 15 minutes ago to the present, for example. By grabbing the time window's left-hand sliding bar, you can dynamically move the window back in time to include several more minutes, hours, days, weeks, or months. Grabbing and moving the right-hand sliding bar changes the time window's end-time from real-time to any ending point in the past that you might want to examine.

As the time window slides backward or forward in time, Sentinel automatically updates the dashboard's display of graphical and numerical analyses to reflect the actual activity associated with the time slice. It also displays the relevant reference model for the slice. This sliding-window-of-time capability makes it very easy to visually re-create the state of activity across multiple dimensions of your organization's environment at any specific point in time for virtually any time interval, and to then compare this activity against the environment's model of normal behavior. Not only is this extremely powerful for real-time analysis, but also for forensic analysis.

Figure 3

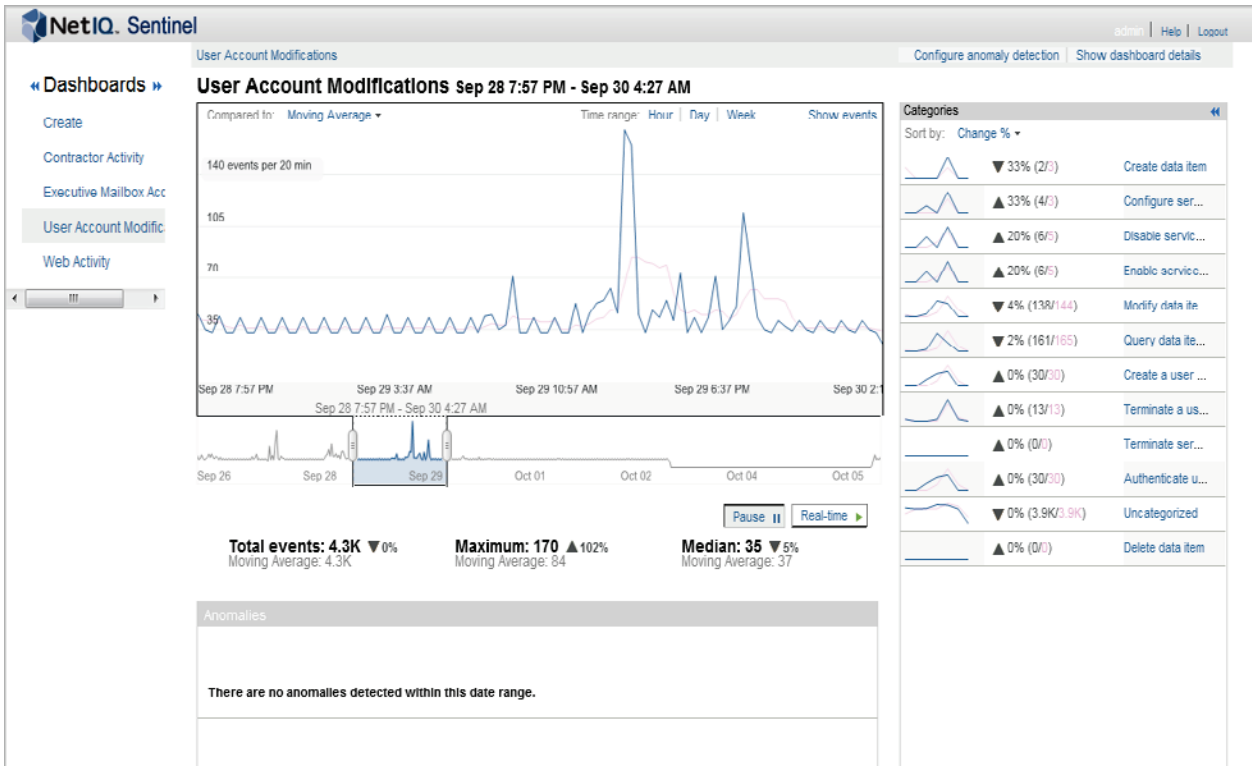

Figure 3: NetIQ Sentinel security dashboards put real-time, actionable intelligence at your fingertips.

Correlation Engine and Rule Builder

Complementing the new anomaly detection engine, the Sentinel correlation engine enables you to define policies or rules to detect known malicious behavior. The rules represent descriptions of how known attacks manifest themselves in an event stream. As the correlation engine receives events from the Sentinel message bus, it evaluates the events against the attack criteria defined in its rules. This allows the correlation engine to identify attacks in real time.

The rules also specify appropriate actions for remediating attacks. When the correlation engine determines what actions need to occur as a result of a specific event, it sends the information back through the message bus to iTRAC, which leverages its workflows to automatically kick off notification and remediation processes. Automated event correlation allows you to spend less time analyzing log files and more time responding to incidents. It reduces the potential for analysis errors that could allow a security or compliance incident to go undetected.

The Sentinel correlation engine allows for different constructs of complex rules, such as nested, sequenced, and cause-and-effect rules. This enables more robust analyses of the event stream and provides the ability to easily create new rules based on your organization's needs.

The graphical rule builder is also a powerful new feature in version 7 of Sentinel. You don't need to understand the Rule LG scripting language or the Sentinel internal event taxonomy to build event correlation rules. You can quickly build them by using drag-and-drop operations to move events that Sentinel has already collected in your organization's environment. The graphical rule builder exposes to

even casual users the raw power of the correlation engine. The rule builder also simplifies the overall rule-definition process.

Additionally, the rule builder lets you easily test rules before deploying them, thus reducing false-positives, improving event correlation capabilities and ultimately delivering improved exploit detection capabilities. With the graphical rule builder, you can quickly target critical threats to speed remediation time and minimize business impact.

Figure 4

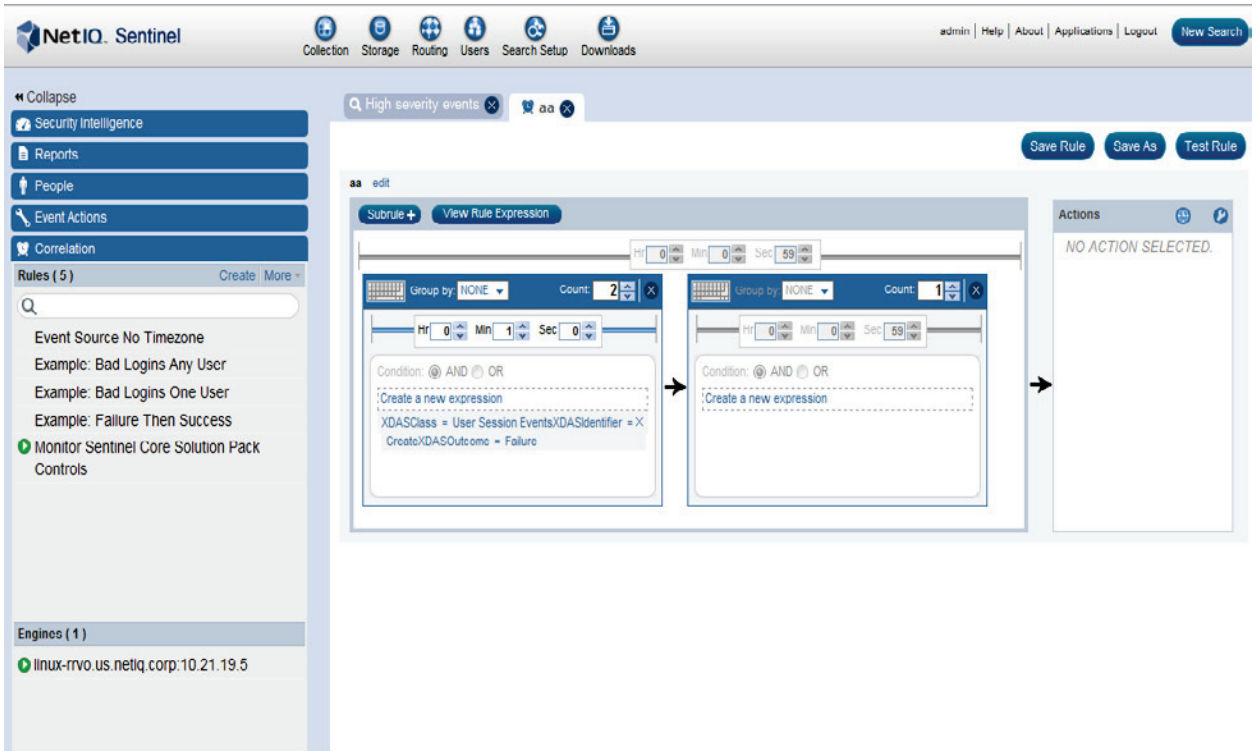

Figure 4: NetIQ Sentinel uses easy drag-and-drop operations for correlation rule building.

High Performance Storage and Reporting

With version 7, Sentinel debuts a new two-tier storage design that provides the best of both log management and SIEM functionality. The front tier of its storage design is optimized for the long-term archiving of events. It uses an efficient, file-based event store that provides 10:1 compression, fully supports indexed searches, and speeds most reporting tasks. If you want, you can also synchronize this file-based storage with temporary second tier storage that gives your organization the flexibility to store some or all events in a traditional relational database.

The new file-based storage tier leverages the NetIQ® Sentinel™ Log Manager data store design. It gives you the flexibility to use your organization's existing hardware and storage investments—including off-the-shelf online data storage, storage area networks (SAN) and network attached storage (NAS)—to deliver high-event-rate storage connectivity for archive capacity expansion. As a result, your organization can reduce the cost of Sentinel log-data storage by opting to store this data on its own hardware.

The Sentinel file-based storage tier's 10:1 data compression maximizes storage capacity and provides data signatures on collected data logs to ensure their integrity. Sentinel stores both raw data and enhanced event data in its file-based storage. The format of the raw data varies based on its associated connector and event source, but typically, it contains information about the raw data message, the raw data record ID, the time the raw data was received, the raw data's event source, the collector, the collector manager node ID, an SHA-256 hash of the raw data and more. Raw data is stored in a way that ensures all logs are intact and unmodified. Storing the data in an untouched format helps organizations meet forensic-related regulatory requirements. Again, raw data is compressed to minimize storage space.

To enhance its collected data's usefulness, Sentinel links rich formatting to raw data, transforming it into an informative event structure. These event structures consist of taxonomy, normalization and business-relevance metadata that make it easy to better understand and leverage the collected information. As it does raw data, Sentinel compresses and stores event structures in its front tier file-based storage.

To facilitate searching and reporting on collected data, Sentinel generates event index tags for all stored events. It then stores these tags as event indices in its file-based storage. The index tags (or indices) act as pointers to data, so searches can easily retrieve events with fields that match the search criteria. To ensure that searches execute as quickly as possible, Sentinel does not compress event indices.

Sentinel also provides customizable long-term data retention policies that enable you to determine how long collected data will remain in local storage before Sentinel automatically migrates it to archived storage. These policies also allow you to determine how long Sentinel holds archived data in storage before deleting the data.

While file-based storage facilitates fast event-data searches and report generation, your organization can also use second-tier temporary relational-database storage to create more complex and sophisticated reports. Sentinel synchronizes required data between its file-based storage and database storage as the needs of scheduled reports dictate. When report generation completes and the database-held data is no longer needed, Sentinel automatically scrubs the data from the database to minimize its data footprint. With database storage, your organization has the option to use an embedded database in Sentinel or synchronize with its own external relational database, such as Oracle or MS-SQL.

This two-tier storage system aligns with a recently released Gartner report that states, "SIEM vendors need to extend their architectures to better support the disparate requirements of the real-time data collection/monitoring and historical analysis use cases. Their real-time collection infrastructures may need to be augmented with a second data store that is heavily indexed and optimized for ad hoc query activity, and the long-term storage of historical event, context and state data." (Mark Nicolette, Joseph Feiman, Gartner Inc. "SIEM Enables Enterprise Security Intelligence")

In essence, the new Sentinel storage architecture combines in a single solution the best of Sentinel Log Manager and previous versions of Sentinel to deliver:

- Significantly faster search capabilities
- Dramatically improved reporting performance
- Simpler report creation
- Reduced storage consumption and costs

The architecture also delivers the reporting advantages of relational databases while maintaining file-based performance and a relatively small data footprint. In addition, Sentinel doesn't require an external database or data warehouse and includes an easy-to-use, advanced query builder for visualizing the

enterprise security environment, documenting regulatory compliance and efficiently managing operational risks.

NetIQ Sentinel includes a number of predefined report templates and the ability to quickly build queries that report on event activity within the context of established business rules, regulatory requirements and industry standards. It helps provide a holistic view of network events and your enterprise's overall security and compliance health.

NetIQ Sentinel Log Manager

NetIQ Sentinel merges SIEM and log management capabilities into a single solution. However, organizations that do not require a full SIEM product can take advantage of NetIQ Sentinel Log Manager. Like Sentinel, Sentinel Log Manager delivers the ability to intelligently collect, aggregate, store, analyze, and manage data logs from all of your organization's systems and applications. It leverages the proven Sentinel data integration framework with its broad set of data collectors for databases, operating systems, directories, firewalls, intrusion detection and prevention systems, antivirus applications, mainframes, web and application servers, and more.

NetIQ Sentinel Log Manager also provides data indexing and one-click reporting to greatly simplify report generation for audit and compliance efforts. Its ability to mount archived data stores enables organizations to seamlessly query and report on both online and archived data, further simplifying and expediting compliance efforts. With Sentinel integration, Sentinel Log Manager gives organizations a flexible and easy-to-use log management solution that provides a clear path to complete, real-time security information and event management.

NetIQ Sentinel Link

Collecting and correlating event logs with critical security information in distributed environments can be a tremendous challenge. Sentinel Link provides an innovative way to forward log event data to Sentinel for advanced, real-time correlation and integration with identity management solutions.

The Sentinel Link feature is designed to forward logs from a distributed instance of Sentinel Log Manager to either Sentinel for real-time monitoring, or to another deployment of Sentinel Log Manager for centralized log archiving and storage.

It is the bridge between log collection and security event correlation. Instead of using Syslog, FTP or an equally unreliable proprietary protocol, Sentinel Link sends all communications using web services over HTTPS. This allows your sensitive log data to be transferred across the wire in a secure, reliable, firewall-friendly way. If the receiver is down or unreachable because of network issues, Sentinel Log Manager prevents data loss by caching the logs until it can make a connection. Sentinel Link includes configuration options to limit the data rate for low bandwidth environments, or to schedule log transfers at a specific time of day or day of the week to take advantage of off-peak hours.

Intelligent Workload Management

Intelligent workload management enables IT organizations to manage and optimize computing resources in a policy-driven, secure and compliant manner across physical, virtual and cloud environments to deliver business services for end customers. NetIQ takes a differentiated approach to intelligent workload

management, called WorkloadIQ™, that integrates identity and systems management capabilities into an application workload, thereby increasing the workload's security and portability across physical, virtual and cloud environments. Sentinel is a pillar of WorkloadIQ, providing real-time event monitoring of IT workloads and faster reaction times to secure IT assets across physical, virtual and cloud environments.

Real-Time Intelligence, Visibility and Protection

NetIQ 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 SIEM and lowers the barriers to SIEM adoption, making security intelligence accessible to all organizations. Additionally, it provides organizations with a more 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.

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

About NetIQ

NetIQ is an enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and IT operations complexities. Our portfolio of scalable, automated management solutions for Security & Compliance, Identity & Access, and Performance & Availability and our practical, focused approach to solving ITchallenges help customers realize greater strategic value, demonstrable business improvement and cost savings over alternative approaches.

For more information, visit www.netiq.com.

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: 713.548.1700
N. America Toll Free: 1.888.323.6768
info@netiq.com
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.