Overview Guide

Sentinel 7.0.1

April 2012

Legal Notice

For more information, please contact NetIQ at:

1233 West Loop South, Houston, Texas 77027
U.S.A.
www.netiq.com

Contents

About This Guide

The guide introduces you to Sentinel, a WorkloadIQ product.

Audience

This guide is intended for information security professionals.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *NetIQ Sentinel 7.0.1 Overview Guide*, visit the Sentinel 7.0 documentation Web site.

Additional Documentation

Sentinel technical documentation is broken down into several different volumes. They are:

- Sentinel Quick Start Guide (http://www.novell.com/documentation/sentinel70/s701_quickstart/data/s701_quickstart.html)
- Sentinel Installation Guide (http://www.novell.com/documentation/sentinel70/s701_install/data/bookinfo.html)
- Sentinel Administration Guide (http://www.novell.com/documentation/sentinel70/s701_admin/data/bookinfo.html)
- Sentinel User Guide (http://www.novell.com/documentation/sentinel70/s701_user/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  The Sentinel SDK site provides information about building your own plug-ins.

Contacting Novell and NetIQ

Sentinel is now a NetIQ product, but Novell still handles many support functions.

- Novell Web site (http://www.novell.com)
- NetIQ Web site (http://www.netiq.com)
- Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Self Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)

- Patch download site (http://download.novell.com/index.jsp)
- Sentinel Community Support Forums (http://forums.novell.com/netiq/netiq-product-discussion-forums/sentinel/)
- Sentinel TIDs (http://support.novell.com/products/sentinel)
- Sentinel Plug-in Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Notification Email List:** Sign up through the Sentinel Plug-in Web site

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide: NetIQ Office Locations (http://www.netiq.com/about_netiq/officelocations.asp)

United States and Canada: 888-323-6768

Email: info@netiq.com

Web site: www.netiq.com

1 Sentinel Product Overview

Sentinel is a security information and event management (SIEM) solution as well as a compliance monitoring solution. Sentinel automatically monitors the most complex IT environments and provides the security required to protect your IT environment.

1.1 Why Security is Important

Security must become a top concern for companies in today’s world to reduce costs and insure customer loyalty. Each leaked record costs an average of $200. It would take only one breach and a couple of hundred thousand lost records to have a significant effect on a business.

When and if your company is attacked, you may incur the following expenses:

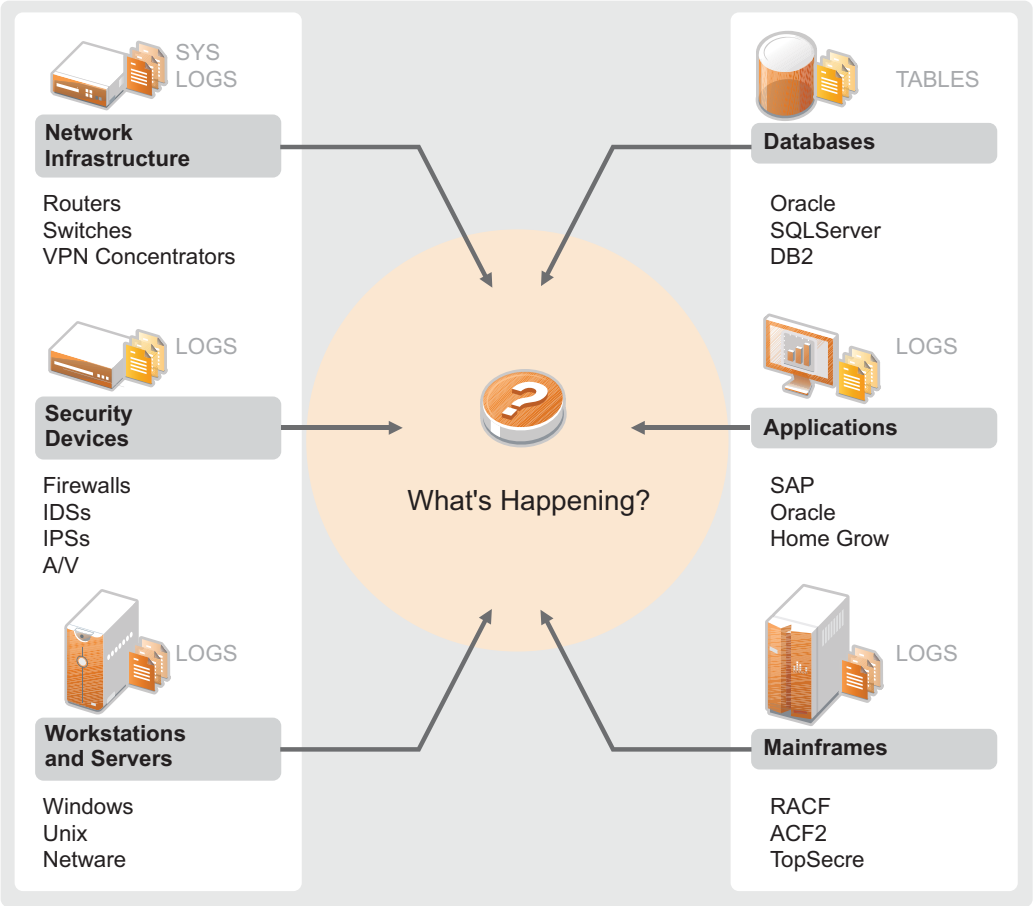
- Legal costs
- Investigation and forensic costs
- Increased Audits
- Fines and penalties
- Hidden cost of lost credibility with customers
- Customers due to the loss of credibility

This demonstrates the importance of securing your IT environment. In today’s world the lines between insiders and outsiders is blurring due to the use of the internet and the growing use of Cloud technology.

1.2 Challenges of Securing the IT Environment

Securing your IT environment is a challenge due to the complexity of your environment. There are many different applications, databases, mainframes, workstations, and servers that all have logs of events occurring. Plus you have the security devices and network infrastructure devices that all contain logs of what is happening in your IT environment.

Figure 1-1 *What Happens in Your Environment*



The challenges arise because:

- There are many devices in your IT environment
- The logs are in different formats
- The logs are stored in silos
- The amount of information generated in the logs
- You can't determine who did what without manually analyzing all of the logs

In order to make the information useful, you must be able to:

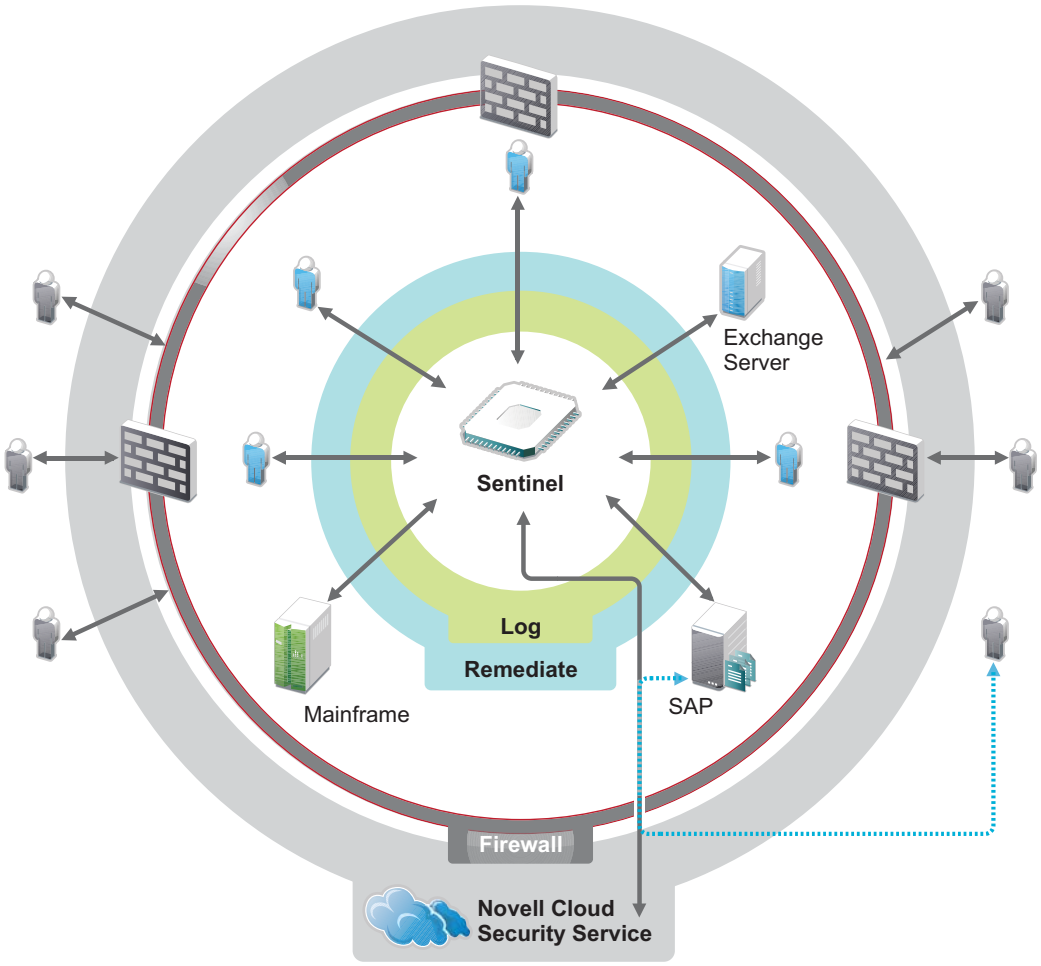
- Collect the data
- Consolidate the data
- Normalize disparate data into events that can be easily compared
- Map events to standard regulations
- Analyze the data
- Compare events across multiple systems to determine if there are security issues
- Send notifications when the data is outside of the norms
- Take action on notifications to comply with business policies
- Generate reports to prove compliance

After you understand the challenges of securing your IT environment, you need to determine how to secure the enterprise for and from the users without treating them like criminals, or burdening them to the point where it is impossible to be productive. Sentinel provides the solution.

1.3 The Solution Sentinel Provides

Sentinel acts as the central nervous system to the enterprise security. It pulls in data from across your entire infrastructure—applications, databases, servers, storage, and security devices. It analyzes and correlates the data, and makes the data actionable, either automatically or manually.

Figure 1-2 *The Solution Sentinel Provides*



The result is that you know what important things are happening in your IT environment at any given point, and you have the ability to tie the actions taken on resources to the people taking those actions. This allows you to determine user behavior and effectively monitor control. No matter if that person is an insider or not, you can tie together all the actions they take so that truly risky activities become clear before they do damage.

Sentinel does this in a cost-effective way by:

- Providing a single solution to address IT controls across multiple regulations

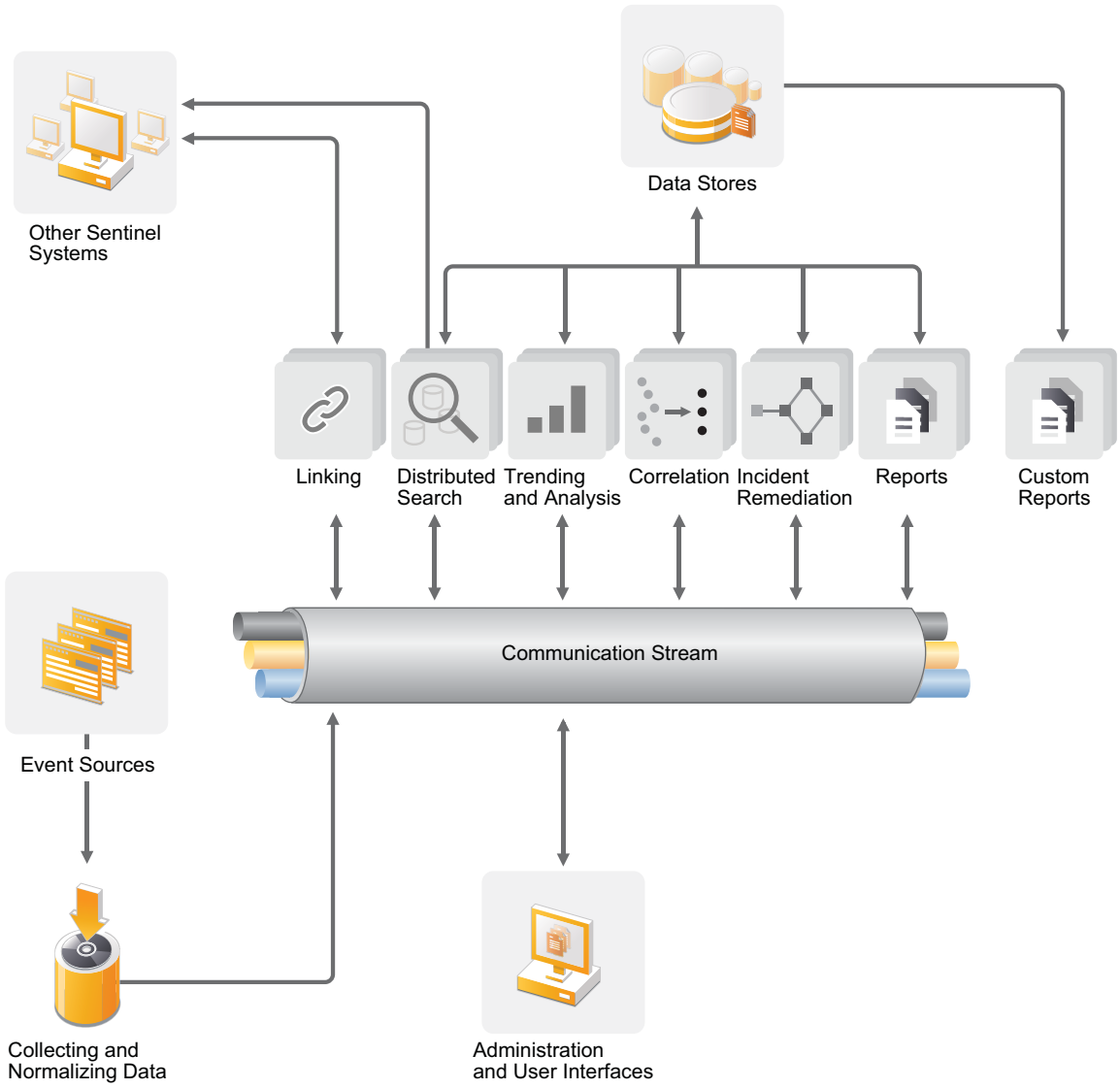
- Closing the knowledge gap between what should happen and what is actually happening in your networked environment
- Demonstrating to auditors and regulators that your organization documents, monitors, and reports on security controls
- Providing out-of-the-box compliance monitoring and reporting programs
- Gaining the visibility and control required to continually assess the success of your organization's compliance and security programs

Sentinel automates log collection, analysis, and the reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel provides automated monitoring of security events, compliance events, and IT controls allowing you to take immediate action if there is a security breach or non-compliant event occurring. Sentinel also allows you to easily gather summary information about your environment so you can communicate your overall security posture to key stakeholders.

2 How Sentinel Works

Sentinel continuously manages security information and events throughout your IT environment to provide a complete monitoring solution. The following figure depicts how Sentinel works.

Figure 2-1 *How Sentinel Works*



Sentinel works by:

- Gathering logs, events, and security information from all of the different event sources in your IT environment.

- Normalizing the collected logs, events, and security information into a common format.
- Adding the normalized information to a message bus that can move thousands of message packets per second.
- Communicating with all of the Sentinel components through the message bus for scalability.

At this point the different Sentinel components access the message bus and Sentinel does the following:

- Stores events in a file-based data store with flexible, customizable data retention policies.
- Provides the ability to hierarchically link multiple Sentinel systems, including Sentinel Log Manager, Sentinel, and Sentinel Rapid Deployment.
- Allows you to search for events not only on your local Sentinel server, but also on other Sentinel servers distributed across the globe.
- Performs a statistical analysis that allows you define a baseline and then compares it to what is occurring to determine if there are unseen problems.
- Correlates a set of similar or comparable events in a given period to determine a pattern.
- Organizes events into incidents for efficient response management and tracking.
- Reports capabilities based on real time and historical events.

The following sections describe the components of Sentinel in detail.

2.1 Event Sources

Sentinel gathers security information and events from many different sources in your IT environment. These sources are called event sources. The event sources can be many different items on your network.

The following graphics depict some of the different event sources Sentinel can gather information from:

Security Perimeter: Devices and software used to create a security parameter for your environment.

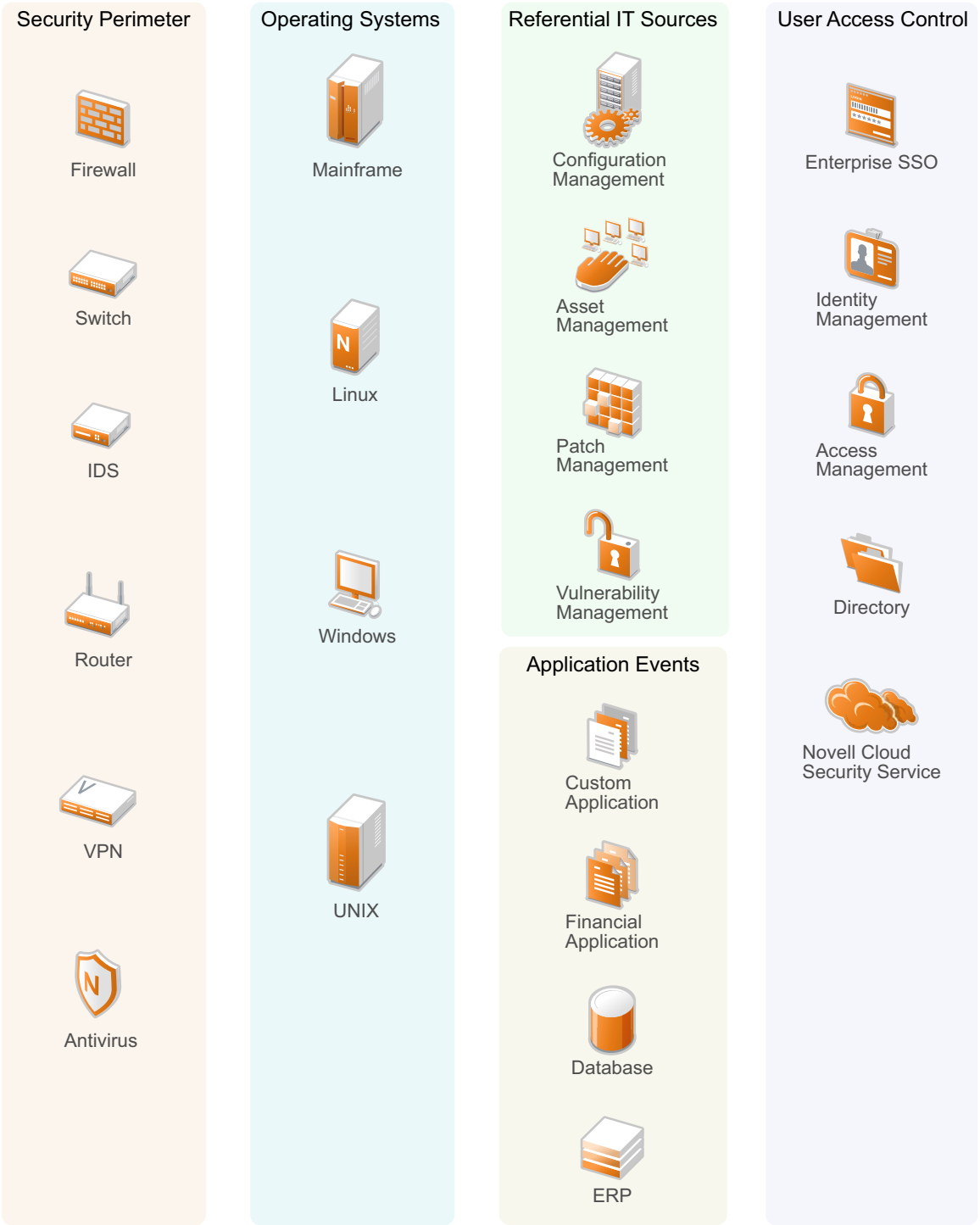
Operating Systems: Events from the different operating systems running in the network.

Referential IT Sources: The software used to maintain and track assets, patches, configuration, and vulnerability.

Application Events: Events generated from the applications installed in the network.

User Access Control: Events generated from applications or devices that allow users access to company resources.

Figure 2-2 *Event Sources*



2.2 Sentinel Event

Sentinel receives information from devices, normalizes this information into a structure called an event, categorizes the event, and then sends the event for processing. By adding category information (taxonomy) to events, events are easier to compare across systems that report events differently. For example, authentication failures. Events are processed by the real time display, correlation engine, dashboards, and the backend server.

An event comprises more than 200 fields. Event fields are of different types and of different purposes. There are some predefined fields such as severity, criticality, destination IP and destination port. There are two sets of configurable fields: Reserved fields are for Sentinel internal use to allow future expansion and Customer fields are for customer extensions.

Fields can be repurposed by renaming them. The source for a field can either be external, which means that it is set explicitly by the device or the corresponding Collector, or referential. The value of a referential field is computed as a function of one or more other fields using the mapping service. For example, a field can be defined to be the building code for the building containing the asset mentioned as the destination IP of an event. For example, a field can be computed by the mapping service using a customer defined map using the destination IP from the event.

- Section 2.2.1, “Mapping Service,” on page 14
- Section 2.2.2, “Streaming Maps,” on page 14
- Section 2.2.3, “Exploit Detection (Mapping Service),” on page 15

2.2.1 Mapping Service

The Mapping Service allows a sophisticated mechanism to propagate business relevance data throughout the system. This data can enrich events with referential information that will provide context that enables analysts to make better decisions, write more useful reports, and write well-thought out correlation rules.

You can enrich your event data by using maps to add additional information such as host and identity details to the incoming events from your source devices. This additional information can be used for advanced correlation and reporting. The system supports several built-in maps as well as custom user-defined maps

Maps that are defined in Sentinel are stored in two ways:

- Built-in maps are stored in the database, updated using APIs in Collector code, and automatically exported to the Mapping service.
- Custom maps are stored as CSV files and can be updated on the file system or via the Map Data Configuration UI, then loaded by the Mapping service.

In both cases, the CSV files are kept on the central Sentinel server but changes to the maps are distributed to each Collector Manager and applied locally. This distributed processing ensures that mapping activity does not overload the main server.

2.2.2 Streaming Maps

The Map Service employs a dynamic update model and streams the maps from one point to another, avoiding the buildup of large static maps in dynamic memory. The value of this streaming capability is particularly relevant in a mission-critical real-time system such as Sentinel where there needs to be a steady, predictive and agile movement of data independent of any transient load on the system.

2.2.3 Exploit Detection (Mapping Service)

Sentinel provides the ability to cross-reference event data signatures with Vulnerability Scanner data. Users are notified automatically and immediately when an attack is attempting to exploit a vulnerable system. This is accomplished through:

- Advisor Feed
- Intrusion detection
- Vulnerability scanning
- Firewalls

Advisor provides a cross-reference between event data signatures and vulnerability scanner data. Advisor feed contains information about vulnerabilities and threats as well as a normalization of event signatures and vulnerability plug-ins. For more information on Advisor, see "Configuring Advisor" in the *NetIQ Sentinel 7.0.1 Administration Guide*.

2.3 Connectors

The Connectors provide connections from the event sources to the Sentinel system. Using industry-standard protocols to get events, such as syslog, JDBC to read from database tables, WMI to read from Windows Event Logs, and so on, Connectors provide:

- Transportation of raw event data from the events sources to the Collector.
- Connection specific filtering.
- Connection error handling.

2.4 Collectors

The Collectors normalize and collect the information from the Connectors. Collectors are written in Javascript and define the logic for:

- Receiving raw data from the Connectors.
- Parsing and normalizing the data.
- Applying repeatable logic to the data.
- Translating device-specific data into Sentinel specific data.
- Formatting the events.
- Passing the normalized, parsed, and formatted data to the Collector Manager.

2.5 Collector Manager

The Collector Manager manages data collection, monitors system status messages, and performs event filtering as needed. The main functions of the Collector Manager include:

- Transforming events.
- Adding business relevance to events through the mapping service.
- Performing global filtering on events.

- Routing events.
- Determining real-time, vulnerability, asset, or non-real-time data.
- Sending health message to the Sentinel server.

2.6 Communication Bus

The communication bus architecture is built using a standards-based, Service-Oriented Architecture (SOA) that combines the advantages of in-memory processing and distributed computing. The communication bus is named iSCALE and it is a specialized message bus capable of handling high data volumes.

- Section 2.6.1, “Message Bus,” on page 16
- Section 2.6.2, “Channels,” on page 17

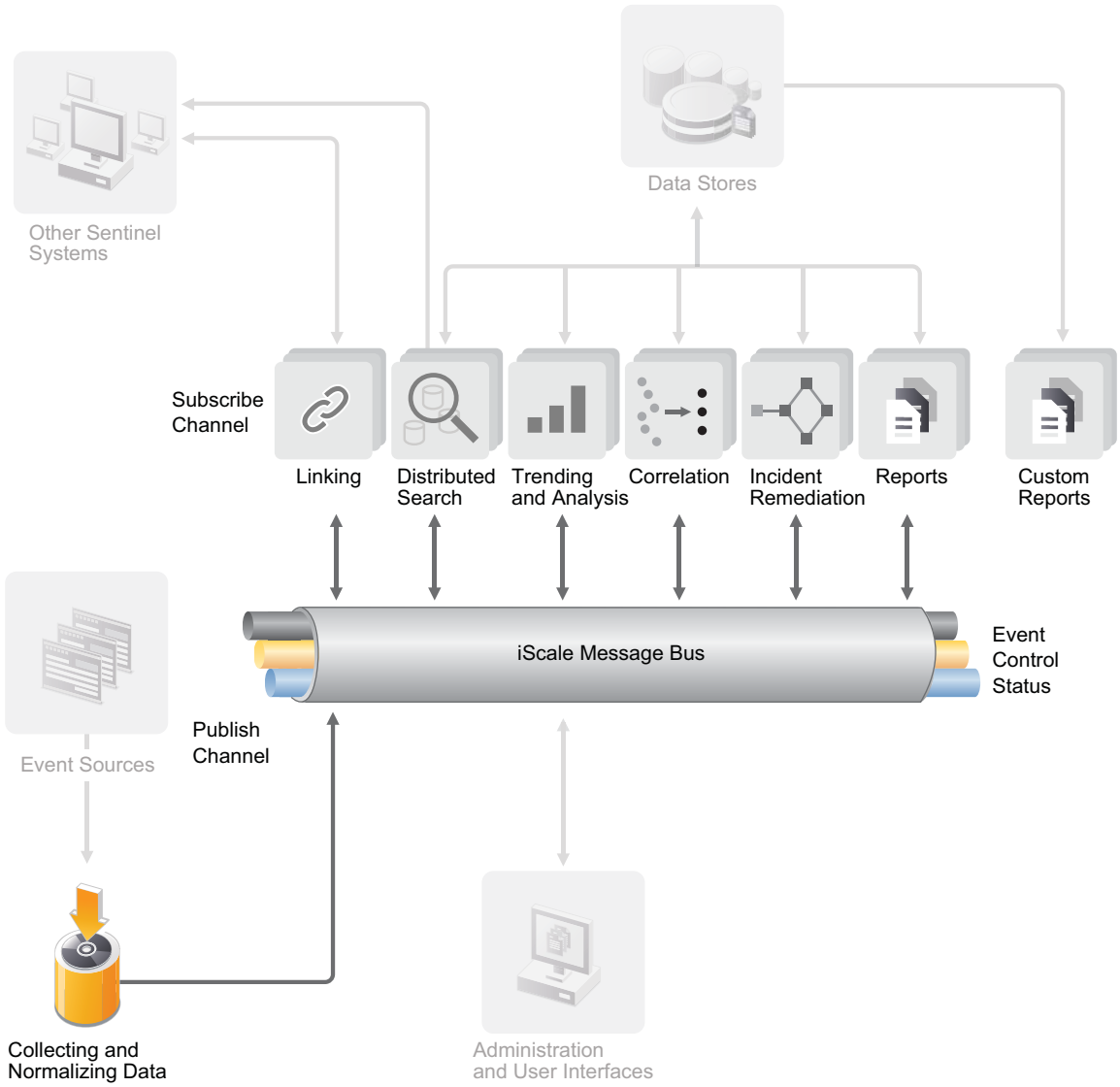
2.6.1 Message Bus

The iSCALE Message Bus allows for independent scaling of individual components while also allowing for standards-based integration with external applications. The key to scalability is that unlike other distributed software, no two peer components communicate with each other directly. All components communicate through the message bus, which is capable of moving thousands of message packets per second.

Leveraging the message bus’ unique features, the high-throughput communication channel can maximize and sustain a high data throughput rate across the independent components of the system. Events are compressed and encrypted on the wire for secure and efficient delivery from the edge of the network or collection points to the hub of the system, where real-time analyses are performed.

The iSCALE message bus employs a variety of queuing services that improve the reliability of the communication beyond the security and performance aspects of the platform. Using a variety of transient and durable queues, the system offers unparalleled reliability and fault tolerance. For instance, important messages in transit are saved (by being queued) in case of a failure in the communication path. The queued message is delivered to the destination after the system recovers from the failure state.

Figure 2-3 *iSCALE Message Bus*



2.6.2 Channels

The iSCALE platform employs a data-driven or event-driven model that allows independent scaling of components for the entire system based on the workload. This provides a flexible deployment model because each customer's environment varies: one site can have a large number of devices with low event volumes; another site can have fewer devices with very high event volumes. The event densities (that is, the event aggregation and event multiplexing pattern on the wire from the collection points) are different in these cases and the message bus allows for consistent scaling of disparate workloads.

iSCALE takes advantage of an independent, multi-channel environment, which virtually eliminates contention and promotes parallel processing of events. These channels and sub-channels work not only for event data transport but also offer fine-grain process control for scaling and load balancing the system under varying load conditions. Using independent service channels such as control channels and status channels, in addition to the main event channel, allows sophisticated and cost-effective scaling of event-driven architecture.

2.7 Sentinel Data Storage

Sentinel provides multiple options to store the data collected. By default, Sentinel receives two separate but similar data streams from the Collector Managers: the event data and the raw data. This data is stored in the local file system of the Sentinel server.

You can configure Sentinel to store the data in a networked storage location. You can also configure Sentinel to store the event data in an external database using data synchronization policies. For more information, see "Configuring Data Storage" in the *NetIQ Sentinel 7.0.1 Administration Guide*.

2.8 Filters

Filters in Sentinel allow you to customize the event search and prevent data overload. This feature provides a Filter Builder that helps you build search queries ranging from easy to complex. You can save a search query as a filter and reuse it as required, so you can perform a search by selecting the filter rather than specifying the query manually every time.

You can reuse filters while using or configuring Sentinel features, such as:

- Creating Security Intelligence dashboards.

  For more information, see "Creating a Dashboard" in the *NetIQ Sentinel 7.0.1 User Guide*.
- Viewing real-time events in Active Views.

  For more information, see "Viewing Events" in the *NetIQ Sentinel 7.0.1 User Guide*.
- Configuring a Data Retention policy.

  For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel 7.0.1 Administration Guide*.
- Configuring Data Synchronization.

  For more information, see "Configuring Data Synchronization" in the *NetIQ Sentinel 7.0.1 Administration Guide*.
- Testing a Correlation rule.

  For more information, see "Correlating Event Data" in the *NetIQ Sentinel 7.0.1 User Guide*.

Sentinel provides a list of filters by default. You can also create your own filters. For more information, see "Configuring Filters" in the *NetIQ Sentinel 7.0.1 User Guide*.

2.9 Correlation

A single event may seem trivial, but in combination with other events, it might warn you of a potential problem. Sentinel helps you correlate such events by using the rules you create and deploy in the Correlation engine, and take appropriate action to mitigate any problems.

Correlation adds intelligence to security event management by automating analysis of the incoming event stream to find patterns of interest. Correlation allows you to define rules that identify critical threats and complex attack patterns so that you can prioritize events and initiate effective incident management and response. For more information, see "Correlating Event Data" in the *NetIQ Sentinel 7.0.1 User Guide*.

2.10 Security Intelligence

The correlation capability in Sentinel provides the ability to look for known patterns of activity, whether it be for security, compliance, or other reasons. The Security Intelligence capability looks for activity that is out of the ordinary, which may be malicious, but does not match any known pattern.

The Security Intelligence feature in Sentinel focuses on statistical analysis of time series data to enable analysts to identify and analyze deviations (anomalies) either by an automated statistical engine or by visual representation of the statistical data for manual interpretation. For more information, see "Analyzing Trends in Data" in the *NetIQ Sentinel 7.0.1 User Guide*.

2.11 iTrac

iTRAC workflows are designed to provide a simple, flexible solution for automating and tracking an enterprise's incident response processes. iTRAC leverages Sentinel's internal incident system to track security or system problems from identification (through correlation rules or manual identification) through resolution.

Workflows can be built using manual and automated steps. Advanced features such as branching, time-based escalation, and local variables are supported. Integration with external scripts and plug-ins allows for flexible interaction with third-party systems. Comprehensive reporting allows administrators to understand and fine-tune the incident response processes. For more information, see "Configuring iTRAC Workflows" in the *NetIQ Sentinel 7.0.1 User Guide*.

2.12 Reports

Sentinel provides the ability to run reports on the data gathered. Sentinel is prepackaged with a variety of customizable reports, some of which are general and some of which are device-specific (For example, SUSE Linux). Some of the reports are flexible to allow users to specify the columns to be displayed in the results.

Users can run, schedule, and e-mail PDF reports. They can also run any report as a search and then interact with the results as they would any search, such as refining the search or performing an action on the results. You can also run reports on Sentinel servers which are distributed across different geographic locations. For more information, see "Reporting" in the *NetIQ Sentinel 7.0.1 User Guide*.

2.13 Event Analysis

Sentinel provides a powerful set of tools to help you easily find and analyze critical event data. The system is tuned and optimized for maximal efficiency in any particular type of analysis, and methods to easily transition from one type of analysis to another are provided for seamless transitions.

Investigating events in Sentinel often starts with the near real-time Active Views. Although more advanced tools are available, Active Views display filtered event streams along with summary charts that can be used for simple, rough analysis of event trends, event data, and identification of specific events. Over time, you build up tuned filters for specific classes of data, such as output from correlation. You can use Active Views as a dashboard showing an overall operational and security posture.

You can then use the interactive search to perform more detailed analysis of events. This allows you to quickly and easily search for and find data related to a specific query, such as activity by a specific user or on a particular system. By clicking on the event data or using the left-hand refinement pane, you can quickly zero in on specific events of interest.

When analyzing hundreds of events, the reporting capabilities of Sentinel provide custom control over event layout and can display larger volumes of data. Sentinel makes this transition easier by allowing you to transfer the interactive searches built up in the Search interface into a reporting template, which instantly creates a report that displays the same data but in a format better suited for a larger number of events.

Sentinel includes many templates for this purpose. Some templates are tuned to display particular types of information, such as authentication data or user creation, and some are general-purpose templates that allow you to customize groups and columns on the report interactively.

Over time, you will develop commonly-used filters and reports that make your workflows easier. Sentinel fully supports storing this information and distributing it with people in your organization. For more information, see the *NetIQ Sentinel 7.0.1 User Guide*.