opentext™ | Cybersecurity

Product Flyer

ArcSight Sentinel for Log Management

ArcSight Sentinel for Log Management is a ready-to-run software appliance that combines the SUSE Linux Enterprise Server 11 operating system and Sentinel for Log Management software with an update service. When deployed as a virtual appliance using VMware or Xen, the automated OpenText update service ensures that the operating system and software are up to date, without any hassles.

ArcSight Sentinel for Log Management at a Glance
Simplifies compliance, improves security posture and provides a strong compliance and security foundation

ArcSight Sentinel for Log Management provides data indexing and one-click reporting to greatly simplify report generation for audit and compliance efforts. It can also mount archive data stores so you can seamlessly query and report on both local and archived data, further simplifying and expediting compliance efforts.

Simple and Cost-Efficient Log Management Deployment

ArcSight Sentinel for Log Management by OpenText is an all-inclusive software appliance that enables organizations to improve IT enterprise security and simplify regulatory compliance in a cost-effective and easy way. ArcSight Sentinel for Log Management cuts through deployment and management cost and complexity, and it requires no expensive proprietary hardware or major infrastructure changes. With the log management software, the embedded operating system and the automatic update service all delivered in one product, you can immediately leverage powerful out-of-the-box functionality within minutes of installation, which enables you to automatically detect most data sources with minimal configuration. This innovative solution allows you to leverage your existing investments and deploy the product on almost any hardware to significantly reduce cost and technology complexity.

ArcSight Sentinel for Log Management delivers an intelligent, scalable and cost-effective software appliance log management solution to proactively manage risk. It does this by providing visibility into your IT infrastructure through its advanced and flexible data collection and reporting capabilities. In addition, it simplifies the task of regulatory compliance by providing the forensic evidence you need to meet compliance mandates and regulations while delivering investigative response and proactive security management capabilities. Built on the powerful and reliable OpenText™ security information and event management (SIEM) solution, ArcSight Sentinel by OpenText, ArcSight Sentinel for Log Management gives you a quick return on your investment by allowing you to deploy an all-in-one software appliance log management solution.

Secure and Flexible Data Collection

ArcSight Sentinel for Log Management provides out-of-the-box support for syslog as well as native log collection from other protocols.

In addition to User Datagram Protocol (UDP), it supports syslog over the more secure and reliable Transmission Control Protocol (TCP) and Transport Layer Support (TLS) protocol, which include authentication and custom certificate support. ArcSight Sentinel for Log Management automatically detects different event source types, such as PIX, Linux and Solaris, and it has a universal syslog collector for unrecognized syslog events.

ArcSight Sentinel for Log Management leverages the proven ArcSight Sentinel data collection framework, which offers a 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. These interpretive collectors parse, normalize, filter and enrich log data to facilitate the analysis,

visualization and reporting of events for your security and compliance efforts. In addition to the solution's out-of-the-box collectors, you can customize or create your own to address your organization's unique needs.

Flexible and Optimized Data Storage

Proprietary storage solutions significantly increase overall costs while also creating dependence on the vendor's reporting and search tools. ArcSight Sentinel for Log Management eliminates expensive proprietary storage solutions by storing its collected log data on standard storage systems and providing data signatures to ensure log integrity. To minimize storage requirements, the solution automatically compresses data at a 10:1 ratio. ArcSight Sentinel for Log Management easily connects to a storage area network (SAN) or network attached storage (NAS) to facilitate and expand archive storage capacity and allow you the flexibility to use your existing IT investments.

Flexible Search and Storage

Distributed search capabilities allow you to deploy the solution at remote locations and search all event data from a single console. This feature gives you event information at your fingertips and allows you to easily access it to prepare for audits or simplify compliance with government regulations. As collected log data ages, most organizations migrate it into an archive for long-term storage. Unfortunately, if you ever need to query or report on that archived data, most log management solutions require you to first migrate it back to short-term storage. ArcSight Sentinel for Log Management can mount archive data stores so it can query and report on both local and archived data, which greatly simplifies and accelerates your compliance and forensic analysis efforts.

ArcSight Sentinel for Log Management is an all-inclusive software appliance that enables organizations to improve IT enterprise security and simplify regulatory compliance in a cost-effective and easy way.

Dynamic, One-Click Reporting

ArcSight Sentinel for Log Management greatly simplifies report generation for audit and compliance efforts with its data indexing and one-click reporting approach. ArcSight Sentinel for Log Management makes it easy for you to securely collect and search through local or network event data and choose from a wide variety of built-in reports to quickly meet compliance requirements for Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX) and many other regulations and mandates. Intuitive searching and one-click reporting make ArcSight Sentinel for Log Management an ideal tool for any situation where you need transparency and log analysis, whether you're generating a required weekly report or performing a detailed analysis after a specific security event has occurred for forensic purposes.

With one-click reporting in ArcSight Sentinel Log Management, you can receive and interpret data from a wide variety of different data feeds without spending hours on customization. Using its powerful, Lucene-based search engine, you simply enter the criteria that you want to report on and ArcSight Sentinel for Log Management returns the results in a straightforward list that is often sufficient for many basic compliance or audit needs. With a single click, you can automatically format the results into a more formal presentation that displays results with the specific fields and parameters you need for the most common compliance and audit reports. You can also customize or create your own formatting templates.

Intuitive and Easy-to-Use Interface

ArcSight Sentinel for Log Management leverages Web 2.0 technology to deliver an intuitive, simple-to-use and responsive interface that delivers a superior user experience. Through the interface, you can easily view data usage trends and identify potential problems. It also lets you configure data collection, schedule and manage reports, create data retention policies, and configure rules for data filtering and actions—such as e-mail alerts, sending Simple Network Management Protocol (SNMP) traps, writing to a file or even forwarding events to ArcSight Sentinel for real-time processing.

Building Block for Real-Time SIEM

Along with providing a quick and easy way to address many of your compliance and audit concerns, ArcSight Sentinel for Log Management is also a solid building block for a real-time SIEM implementation. Most log management products do not provide integration or an easy path to full SIEM. However, ArcSight Sentinel for Log Management easily integrates with the real-time monitoring capabilities of ArcSight Sentinel, as well as with the OpenText™ Compliance Management Platform and Identity and Access Management solutions from OpenText. ArcSight Sentinel for Log Management provides a clear roadmap to identity-aware security in a way that lets you seamlessly add and integrate new capabilities as your security and compliance needs grow.

Key Features and Differentiators of ArcSight Sentinel for Log Management

- **Simple and cost-effective log management deployment**
  - Delivers an all-in-one software appliance log management solution
  - Runs on VMware, Xen or bare metal
  - Reduces deployment and management costs

To learn more about Sentinel for Log Management, or to start a trial, go here.

Connect with Us
www.opentext.com

- Is a scalable solution available in 500 events per second (EPS), 2500 EPS or 7500 EPS

- **Advanced and flexible log data collection**
  - Leverages ArcSight Sentinel for advanced and flexible log data collection, including out-of-the-box syslog support and native collection from other protocols
  - Automatically detects log sources
  - Supports collection and limited processing of unrecognized log messages
  - Supports data collection with a high EPS rate
- **Distributed search and one-click reporting**
  - Queries and searches archived and local data seamlessly from one central console
  - Converts searches into reusable reports with one-click reporting and prepackaged report formats
  - Enables quick drill-down and refinement of search criteria through hyperlinked search results
  - Provides out-of-the-box reports and ad hoc indexed searching, including ad hoc forensic searches
  - Includes Web 2.0-based search tools that can automatically update results as additional results are found
- **Secure, cost-effective data storage**
  - Compresses data automatically to maximize storage capacity
  - Uses data signatures to ensure log integrity
  - Enables nonproprietary local data storage as well as SAN and NAS connectivity to expand archive capacity
  - Supports customizable retention policies
- **Simple, scalable and powerful administration**
  - Features an intuitive, AJAX-based interface
  - Enables graphical display of data usage trends and any potential problems
  - Enables easy integration with ArcSight Sentinel, and Security and Compliance Management, and Identity and Access Management solutions from OpenText for full SIEM functionalit

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.

761-000073-003 | O | 10/23 |