Hewlett Packard Enterprise

Data sheet

HPE Security ArcSight Logger Software

Unify collection, storage, and analysis of machine data for security intelligence

Benefits

Provides the ability to:

- Capture variety, volume, and velocity of information necessary to detect security breaches
- Setup, upgrade, and maintain with just a few clicks
- Cost-effectively store data with the high compression ratio

Highlights

- Comprehensive data collection
- Flexible deployment architecture
- Secure and reliable
- Ultra-fast investigation and forensics
- Non-stop compliance
- Easy to deploy and manage

Industry-leading data collection solution that can simultaneously address cyber-security, compliance, and IT Operations log management needs as your enterprise grows.

In today's non-stop world, you need to unify machine data across the enterprise for compliance, regulations, security, IT operations, and log analytics.

ArcSight Logger Software is an integral part of ArcSight SIEM solution and is used for collecting, storing, searching, reporting, and managing your security data.

"ArcSight is the best-in-class solution for the market today and is the leader in the market. Most of our customers either are looking to procure HPE ArcSight or are looking for services around the solution in order to help them enhance the way they use the technology today."

–Hernan Barros, Director of Product Management, TELUS Security Solutions

Comprehensive data collection

It collects machine data at ingest rates of terabytes of data per day from any source (including logs, clickstreams, sensors, stream network traffic, security devices, Web servers, custom applications, social media, and cloud services). It enables you to search, monitor, and analyze the data to gain valuable security intelligence across your entire organization.

Flexible deployment architecture

ArcSight Logger Software can be configured as a cluster providing load-balanced collection, with search queries distributed across the platform. It can be installed on a Linux® system or on a VMware® Virtual Machine (VM). ArcSight Logger can leverage an existing NAS, direct-attached storage (DAS), and SAN investment as the primary datastore. Regardless of whether the storage is onboard or off-board, data is efficiently compressed at an average ratio of 10:1, which reduces the storage and maintenance costs.

It utilizes HPE ArcSight Common Event Format (CEF), an extensible, text-based, high-performance format so that data can be easily collected and aggregated for analysis by an enterprise management system, such as ArcSight ESM, User Behavior Analytics, or any third-party application which provide event orchestration, automation, correlation, prioritization, and analysis of the security events.

Secure and reliable data collection

ArcSight Logger Software delivers encrypted, compressed logs, keeping data safe from interception, alteration, and deletion, for both data at rest and in motion. It supports:

- HPE Secure Encryption to help you to meet compliance regulations and privacy challenges by securing your sensitive data at rest. It also supports Transport Layer Security (TLS) and Secure SocketLayer (SSL) encryption protocols for data in motion.
- Federal Information Processing Standard 140-2 (FIPS 140-2).
- Security administration and user/group role definitions. Administrators can set access rights on various report categories, reports, and report options (such as view, publish, and edit) based on user roles.

"HPE ArcSight [Logger] allowed us to have a centralized mode of log management and gave us a comprehensive view of the organization security standpoint. Without HPE ArcSight, there is no way that we could have aggregated so many events and get the visibility that we have."

–IT Professional, Medium Enterprise Financial Services Company

Ultra-fast investigation and forensics

When seconds mean the difference between a successful or thwarted attack, obtaining the right information at the right time is critical. ArcSight Logger Software enables ultra-fast investigation of indexed data via a simple search interface. Interesting search patterns can easily be converted into real-time alerts.

ArcSight Logger Software provides ad hoc searching of billions of events in less than 10 seconds over years of data, which allows you to identify breaches and conduct detailed breach analysis.

Non-stop compliance

ArcSight Logger Software ships with built-in content that can be used for cyber security, compliance, application security, and IT operations monitoring. Additional content packs—specific to regulations such as PCI, ITGOV, and Sarbanes-Oxley (SOX)—are available as add-on options and are mapped to well-known standards, including National Institute of Standards and Technology (NIST) 800–53, ISO-17799, and SANS.

Easy to deploy and manage

Monitoring dashboards on the go is now easy with the mobile app. It connects to your data in real-time to give you a current snapshot of your organization. Use the mobile app to give view-only access to your extended teams, support, or contractors, avoiding unauthorized access.

For large deployments, ArcSight Logger Software can be configured, managed, and monitored through ArcSight Management Center (ArcMC), a centralized management console (sold separately), allowing you to connect to data easily and with just a few clicks. It can be configured, managed, and upgraded easily even in large deployments, allowing you to focus on your use cases and not the tool itself.

"ArcSight Logger has allowed us to achieve compliance with PCI requirements very quickly and helped us monitor our network for anomalies so we can stay on top of emerging threats."

–Security Officer, Fortune 500 Financial Services Company

Why HPE ArcSight?

ArcSight SIEM solution is scalable, high-performance, simple to use, and powerful. It is a comprehensive solution developed for security experts by security professionals. It takes a holistic approach to security intelligence, uniquely unifying Big Data collection, network, user and endpoint monitoring and forensics with advanced security analytics. It provides effective out-of-the-box use cases that include real-time threat detection and response, compliance automation and assurance, and IT operational intelligence.

While many vendors claim to provide a robust SIEM solution, the ArcSight team has the security expertise, experience, and leadership that few vendors can match. ArcSight has been acknowledged as a Magic Quadrant Leader by Gartner for the past 12 years, longer than any existing vendor.

Our industry-leading solution, proven methodologies, and a decade of experience with the largest dataset of its kind make Hewlett Packard Enterprise uniquely qualified to help you achieve security posture and operational excellence.

Learn more at
hpe.com/software/arcsight

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-5108ENN, April 2016