Data sheet

HP ArcSight Logger

Unify enterprise IT data

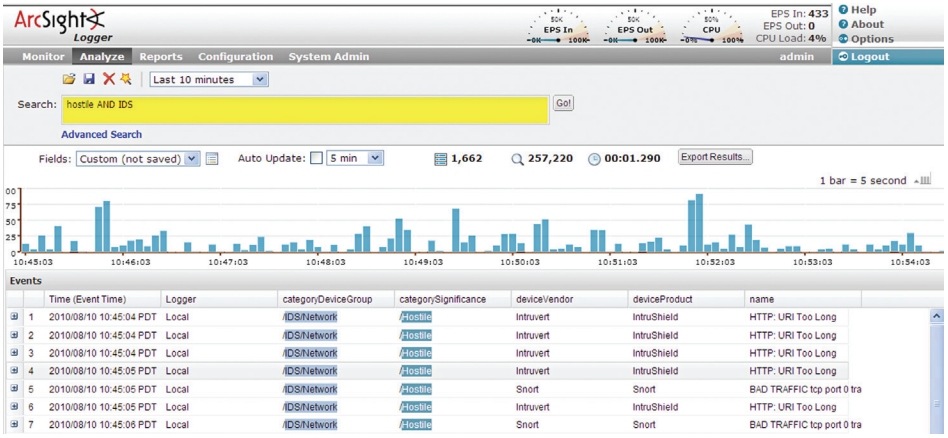
Highlights

- Collect everything: Borderless collection of any data from any device in any format from 300+ log-generating sources
- Analyze anything: High-performance interactive searches, comprehensive drill-down reports, and real-time alerting
- Use anywhere: Uniquely architected solution to meet the needs of diverse teams to use machine data for IT GRC, IT Operations, SIEM solution, and log analytics

HP ArcSight Logger delivers industry-leading, cost-effective log management solution that unifies searching, reporting, alerting, and analysis across any type of enterprise machine data for IT GRC, IT Operations, SIEM, and log analytics.

HP ArcSight Logger is a universal log management solution that unifies searching, reporting, alerting, and analysis across any type of enterprise log data making it unique in its ability to collect, analyze, and store massive amounts of data generated by modern networks. It supports multiple deployments such as an appliance, software, virtual machine, and within the cloud in both Windows® and Linux environment.

Figure 1. With HP ArcSight Logger, users can do a simple device- and vendor-independent search and analysis



The need for a universal log management solution

Logs provide an audit trail that can be analyzed to detect and conduct detailed forensic analyses of cyber attacks, streamline regulatory audits, assist in application development, and improve IT service levels. Previously, log analysis was largely asset centric and adoption of commercial tools was specific to an IT group and its managed assets. These solutions were designed to collect logs from specific sources and were optimized to solve a particular problem. However, these tools are inadequate to tackle the current challenges that IT teams face today.

Today, you face evolving security threats, the growing burden of compliance, and increased pressure to meet demanding service levels. The questions that need to be answered through log analysis are increasingly user centric and can span any and all infrastructure. Traditional log management tools cannot be expanded to analyze logs across the enterprise because they are limited by the type of sources they can collect from; have restricted search/reporting capabilities intended to solve very specific problems; and are not scalable and can breakdown under modern loads.

Stretching first-generation log management tools imposes significant trade-offs between log collection rates, log analysis speed, and log storage efficiency. The next generation, universal log management solution must eliminate the classic trade-off between performance and efficiency, and provide enterprise- and infrastructure-wide visibility into log data. Unlike point solutions, it should be flexible enough so that it can be either used by individual teams or expanded into an enterprise-wide log management solution when needed.

Improve visibility

Comprehensive collection
HP ArcSight Logger can collect data from 300+ log-generating sources using built-in functionality of ArcSight Connectors and support for raw logs from any syslog or file-based log source.

ArcSight Connectors collect, categorize, and normalize log data from more than 300 distinct log-generating sources. Additionally, ArcSight FlexConnector tools extend log collection capabilities to include custom sources and in-house applications.

Data enrichment to simplify analysis
HP ArcSight Logger leverages the ArcSight Common Event Format that does not require familiarity with source-specific log formats—thereby avoiding the need for device- or vendor-specific analysis or knowledge (see figure 1). Moreover, all raw data sent to HP ArcSight Logger is also fully indexed and available for fast searching and reporting via a simple Google™-like search interface. Interesting search patterns can easily be converted into real-time alerts via SMTP, SNMP, or syslog for fast detection and mitigation of security issues.

Unmatched performance
Most log management tools support fast log analysis only by compromising collection rates and storage efficiency, or by requiring more hardware. HP ArcSight Logger is uniquely architected to overcome that trade-off, thus enabling a single instance to capture raw logs at rates of up to 100,000 events per second, compress and store up to 42 TB of log data, and execute searches at millions of events per second.

Enterprise scalability
HP ArcSight Logger is available in a range of performance options such as an appliance, software, virtual machine, and within the cloud. Large organizations with multiple administrative domains or managed security service providers can choose to deploy multiple HP ArcSight Logger products in a distributed, hierarchical, or peer-to-peer manner to extend capacity and performance. Role-based access controls protect both system and event data.

Flexible storage options
HP ArcSight Logger offers multiple storage options. In addition to RAID-enabled onboard storage for appliances, both software and appliance solutions can also leverage an existing NAS, DAS, and SAN investment as the primary data store. Regardless of whether the storage is onboard or off-board, log data is efficiently compressed at an average ratio of 10:1.

Pre-packaged content
HP ArcSight Logger ships with system content that can be used for cyber security, compliance, application development, and IT operations monitoring. Additional content specific to regulations, such as PCI and SOX are available as add-on solution packages, and are mapped to well-known standards, including NIST 800–53, ISO-17799, and SANS.

Getting started

Download, install, and get instant value with HP ArcSight Logger at hp.com/go/hplogger. The downloadable trial version of HP ArcSight Logger provides access to all enterprise features (see figure 2). Using this version, organizations can collect up to 750 MB of log data per day and store up to 50 GB of compressed logs. Users can leverage HP ArcSight Logger user community for additional information or support.

Highlights

- Centralized security management console for HP ArcSight log analytics solution
- Ease of deployment, management, and scalability
- Manage large deployments easily enabling high scalability
- Simplified change management through single console

Audit-quality log data

Several audit-quality controls are built into HP ArcSight Logger to ensure confidentiality, integrity, and availability of data. Integrity checks are enforced in accordance with the NIST 800–92 Log Management standard. ArcSight Connectors offer secure transmission, bandwidth controls, log traffic prioritization, local caching, and other measures to minimize data loss and any impact on business-critical traffic.

Bi-directional integration with HP ArcSight ESM

HP ArcSight Logger integrates bi-directionally with the market-leading enterprise threat and risk management offering, HP ArcSight ESM, and is packaged along with ArcSight ESM into HP ArcSight Express. The integration allows HP ArcSight Logger to forward security events to ArcSight ESM for real time, cross-device correlation. In turn, ArcSight ESM users can search longer-term data on HP ArcSight Logger using a simple click of a mouse without switching user interfaces. ArcSight is unique in offering a tightly integrated platform for both log management and SIEM, leveraging a common collection infrastructure to provide a low TCO and high ROI.

HP ArcSight Management Center

Centralized console

A centralized security management center that unifies management, configuration, and monitoring of HP ArcSight log management solution for large enterprises. The HP ArcSight Management Center allows customers to manage large deployments of HP ArcSight Logger(appliance and software), SmartConnectors, FlexConnectors, and Connector Appliance (ConApp) through a single consolidated view. Management Center enables you to focus on your use cases, feeds, and threats effectively as opposed to managing log management solution.

Table 1. HP ArcSight Logger features for downloadable and enterprise versions

Functionality	HP ArcSight Logger (free version)	HP ArcSight Logger (enterprise version)
Daily limit on log data	750 MB	Unlimited (based on License)
Comprehensive log analysis	•	•
Real-time monitoring and alerting	•	•
Indexing, searching, and reporting	•	•
Contextual drill-down dashboards	•	•
Granular role-based access	•	•
Authentication and authorization	•	•
HP ArcSight standard community support	•	•
Distributed search		•
HP enterprise support		•

HP ArcSight Logger specifications (Software)

Model	Devices	Max log volume	Max search volume
L750MB	10	750 MB/day	500 GB
L5GB	50	5 GB/day	2.5 TB
L30GB	200	30 GB/day	8 TB
L80GB	500	80 GB/day	42 TB
L160GB	Unrestricted	160 GB/day	42 TB
L250GB	Unrestricted	250 GB/day	42 TB

Software Generic Spec	**Supported OS:** Red Hat Enterprise Linux v6.2, 64-bit Oracle Enterprise Linux, v6.1, 64-bit CentOS, v6.2, 64-bit Hyper-V on Windows Server 2008 R2, 64-bit VMware Virtual Image **Recommended Minimum Hardware:** CPU: 1 or 2x Intel® Xeon® Quad Core or equivalent Memory: 4–12 GB Disk space: 4-12 GB **Storage:** Average compression of 10:1 (dependent on data type and data source)

HP ArcSight Logger Specifications (Appliance)

Model	L3500	L7500-SAN	L7500s	L7500x
Devices	200	Unrestricted	500	Unrestricted
Max EPS	2,000	75,000	5,000	100,000
Capacity (compressed)	8TB	50TB	42TB	
Hardware Spec	1x Intel Xeon, E5-2620 2.0GHz, 6-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor		
Memory	32 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM		
Storage	4 x 500 GB (1.5 TB RAID-5)	External – SAN	4 x 3 TB (9 TB - RAID 5)	
Host Bus Adapter	N/A	2 x 2-port 16 GB Emulex HBA	N/A	
Dimensions (DxWxH)	27.5" x 17.1" x 1.7"		29.5" x 17.1" x 1.7"	
Connector Management	Yes		N/A	
Generic Spec	**Management:** Web browser, CLI, Web Services API **Supported OS:** Red Hat Enterprise Linux v6.2, 64-bit **Supported Sources:** Raw Syslog (TCP/UDP), Raw File based logs (FTP, SCP, SFTP) Analysis optimized collection using HP ArcSight SmartConnectors FlexConnector framework for legacy event sources HP ArcSight CEF (Common Event Format), HP ArcSight ESM **Storage:** Average compression of 10:1 (dependent on data type and data source) **Power:** 2 x 460W CS Platinum Power Supply **Ethernet Interfaces:** 4 x 10/100/1000 **Chassis:** 1U			

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Get the support you need

HP ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more about HP ESP Global Services at hp.com/go/arcsight.

Learn more at
hp.com/go/hplogger

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-1065ENW, September 2013, Rev. 3