

SCALABLE LOG COLLECTION

ArcSight Connectors provide audit-quality log collection from all event-generating sources across the enterprise.

HP Enterprise Security Product Brief

Organizations archive and analyze log data for a broad set of reasons ranging from security monitoring to IT operations, and from regulatory compliance to fraud detection. An effective log collection infrastructure layer simplifies and optimizes the aggregation of logs across thousands of devices and hundreds of locations. It serves as the foundation of log management and security information and event management (SIEM) platforms.

Comprehensive and efficient enterprise-wide log collection goes beyond providing a common taxonomy to facilitate analysis. With the rapid growth of the regulatory landscape, organizations need to collect from a much broader set of event sources, including physical devices, network and security devices, hosts, databases and the gamut of commercial and homegrown applications. Breadth and depth of device support in terms of log collection is therefore paramount.

The various devices, hosts and applications that generate logs span hundreds or even thousands of physical locations; log collection infrastructures must therefore scale to meet the needs of large, distributed heterogeneous networks. They must also deliver secure and reliable audit-quality log collection with traffic management controls, simple deployment and administration.

ArcSight Connector technology addresses these core challenges through a powerful log aggregation and optimization interface layer that also represents the foundation for its broader log management and SIEM platform.

Breadth and Depth of Device Support

The ArcSight library of out-of-the-box SmartConnectors provides source-optimized collection for 275+ commercial products. These products span the entire stack of event-generating source types, from network and security devices to databases and enterprise applications. In addition to the many sources commonly supported, ArcSight Connector technology also uniquely supports:

- Identity and Access Management
- Data Leak Prevention
- Database Activity Monitoring
- Mainframe
- Applications

Furthermore, the ArcSight FlexConnector framework provides a wizard-driven interface to build collection logic and to contextualize logs from legacy and homegrown sources. Each is critical to building use cases such as compliance, fraud and insider threats.

Distributed Processing

Once collected, log data needs to be analyzed in real time and historically to address diverse use cases, such as security monitoring and regulatory compliance. Typically, all processing is left to centralized log management and SIEM components.

However, ArcSight Connectors are architected to efficiently offload the ArcSight log management and SIEM platforms from

centrally processing tasks, which are just as efficiently executed at the point of collection. To this end, ArcSight Connectors can also perform a variety of functions, including:

Collection of raw logs in conjunction with parsing of individual log events, and mapping both their values and schema into a universal event taxonomy. This plays a significant role in enabling cross-device searches, reporting and correlation.

Categorization or additional classification of events using a common, human-readable format, which saves the end user from having to be an expert in reading the output from a myriad of devices from multiple vendors. Categorization also future proofs companies by making all content device independent – so if you need to replace vendors, all reports and rules continue to work seamlessly.

Optional filtering of data that is extraneous to analysis and is not required for retention by regulatory requirements or corporate policies, such as system health alerts.

Audit-Quality Log Collection

Secure and reliable collection of audit logs is essential to ensuring the viability of log data for legal and forensics purposes. However, many sources in remote locations are only capable of generating logs over unreliable and unsecured protocols, such as syslog over user datagram protocol (UDP). ArcSight Connectors offer an easily deployable and manageable localized collection option for remote offices, which ensures end-to-end security and availability of log data.



ArcSight Connectors offer local caching, so in the event of a connectivity loss between remote offices and central log aggregation points, there is no loss of critical event data. ArcSight Connectors also support automated failover to a secondary ArcSight Logger or ArcSight ESM Manager in the event that the primary destination is unavailable.

Log Traffic Management

Remote offices such as retail stores often lack high bandwidth WAN links to data centers. Additionally, any available bandwidth needs to be prioritized for business-critical transactional traffic. To address these challenges, ArcSight Connectors offer granular bandwidth controls, compression of logs in transit, as well as prioritization and batching of log data by time and severity.

Adherence to Hardware and Software Deployment Policies

Distributed, localized deployment of log collection infrastructure is critical for secure and reliable log collection. Yet organizations struggle with the headaches of deploying additional infrastructure at remote locations. Rack space is often limited and existing servers cannot be overloaded with additional agents for log collection. Furthermore, IT staff is often limited and cannot deploy and manage log collection infrastructure at remote offices. To address these constraints, ArcSight Connectors are available in a range of plug-and-play appliances that can be easily deployed and remotely managed. ArcSight Connector Appliances provide a localized, yet agent-less, collection option, reduce the net cost of acquisition and eliminate delays due to hardware selection, procurement and testing.

For locations where no additional rack space is available but where spare computing cycles are available on existing servers, ArcSight Connectors offer the flexibility of software-based deployments while still delivering strong centralized management capabilities.

Centralized Management of Log Collection Infrastructure

There is significant overhead associated with ongoing updates, upgrades, configuration changes and general maintenance of a distributed log collection deployment. Even global organizations with numerous offices prefer to avoid expending valuable IT human resources on managing yet another distributed infrastructure. Therefore, it is not enough for a log collection solution to simply support distributed deployment. ArcSight Connectors minimize ongoing administrative overhead through support for diagnostics, universal and/or selective definition, alteration and roll out of log collection parameters and configuration settings across all appliance and software-based ArcSight Connectors, from a centralized web-based interface.

Content Sharing with ArcExchange

The ArcSight Connector appliance makes information sharing possible with a simple click of a mouse. With the ArcExchange feature, users can download and upload custom-built connectors directly to Protect 724, the ArcSight online user community. Connectors developed and shared by this community allow the collection of event data from customized and advanced applications, databases, devices, etc. This capability, along with out of the box support for 275+ products, makes the ArcSight platform the broadest available SIEM solution on the market.

Highlights

- Complete visibility with collection support for any event source from the physical layer through the application layer
- Ease of analysis through a common event format for all log sources
- Universal content relevance with pre-built, vendor-independent content

ArcSight Platform Integration

Regulatory retention requirements, audit reporting needs, IT operations troubleshooting and SLA management, and proactive monitoring of security threats all represent a continuum in the value chain of extracting context and intelligence from log data. As such, it is logical to leverage a common collection infrastructure across the full range of log collection and archival needs for an enterprise – and that is exactly what ArcSight Connectors offer. As the end device interfacing layer in the ArcSight platform, ArcSight Connectors provide a comprehensive, robust, scalable and easily manageable collection infrastructure that can be used across its log management and SIEM modules, as seen in Figure 1. This is a distinct advantage of the integrated ArcSight platform, and it avoids the deployment of multiple collection infrastructures that would be needed if different vendor solutions were used for log management and SIEM. This benefit applies to both appliance and software-based ArcSight Connector technology deployments.

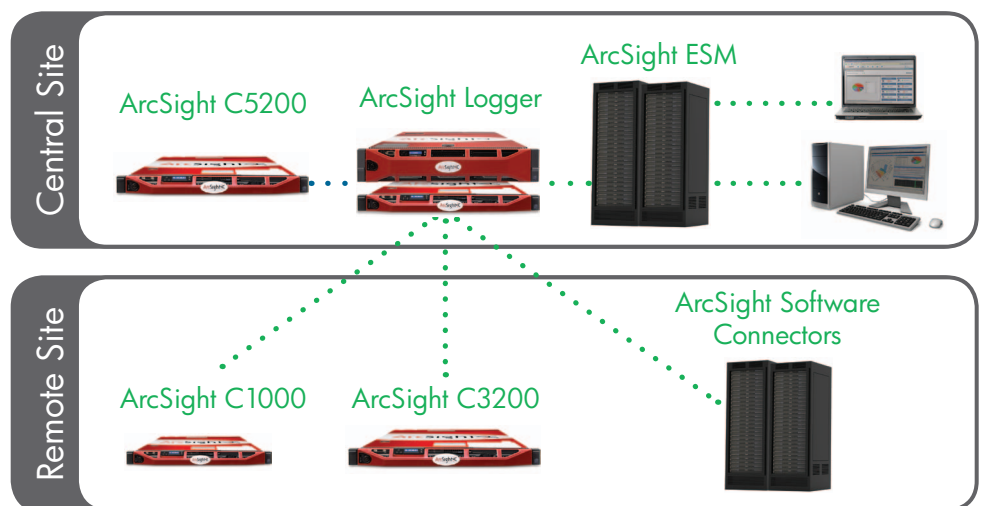


Figure 1: Secure and reliable log collection across all devices and locations

ArcSight Connector Appliance Specifications

MODEL	C1300	C3400	C5400
Management	Web browser, CLI		
OS	Oracle Enterprise Linux 4 64-bit	Redhat Enterprise Linux v5.5, 64-bit	
Max EPS	400	2,500	5,000
CPU	1 x Pentium E5300, dual core, 2.6 GHz	1 x Intel E5620, quad core, 2.4 GHz	2 x Intel E5620, quad core, 2.4 GHz
RAM	2GB	8GB	16GB
Cache	160GB	500GB (Raid 0)	2 x 500GB (RAID 1)
Chassis	Table Top	1U	
Power	280W - Non-Redundant 100 – 240 VAC	1x 460W CS Platinum Power Supply	2 x 460W CS Platinum Power Supply
Ethernet Interfaces	2 x 10/100/1000	4 x 10/100/1000	4 x 10/100/1000
Dimensions (DxWxH)	12.74" x 11.4" x 3.35"	1.70 x 16.78 x 27.25"	1.70 x 16.78 x 27.25"

Actual performance will depend on factors specific to a user's environment.

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

All other product and company names may be trademarks or registered trademarks of their respective owners.

ESP-PRB006-092209-09, Created November 2011

