# Get scalable log collection today

HP ArcSight Connectors

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 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, network, and security devices, hosts, databases, and a 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.

HP 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 HP ArcSight library of out-of-the-box connectors provides source-optimized collection for more than 300 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, HP ArcSight Connector technology also uniquely supports:

- Identity and access management
- Data leak prevention
- Database activity monitoring
- Mainframe
- Applications

Furthermore, the HP FlexConnector framework provides a wizard-driven interface to build collection logic and to contextualize logs from legacy and homegrown sources. Each is critical to satisfying 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, HP ArcSight Connectors are architected to efficiently offload the HP ArcSight log management and SIEM platforms from centrally processing tasks, which are just as efficiently executed at the point of collection. To this end, HP 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 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.

## Highlights

- Provides complete visibility with collection support for any event source from the physical layer through the application layer

- Offers ease of analysis through a common event format for all log sources

- Creates universal content relevance with pre-built, vendor-independent content

## 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). HP 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.

HP 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. HP ArcSight Connectors also support automated failover to a secondary HP ArcSight Logger or HP ArcSight Enterprise Security Manager (ESM) in the event that the primary destination is unavailable.

## Log traffic management

Remote offices such as retail stores often lack high bandwidth wide area network (WAN) links to data centers. Additionally, any available bandwidth needs to be prioritized for business-critical transactional traffic. To address these challenges, HP 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, HP ArcSight Connectors are available in a range of plug-and-play appliances and as software that can be easily deployed and remotely managed. HP ArcSight Connectors provide a localized, yet agent-less collection option, which reduces the net cost of acquisition and eliminates delay due to hardware selection, procurements and testing.

For locations where no additional rack space is available but where spare computing cycles are available on existing servers, HP 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. HP 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 from a centralized Web-based interface. The centralized management capabilities includes all software-based and appliance-based connectors throughout the environment.
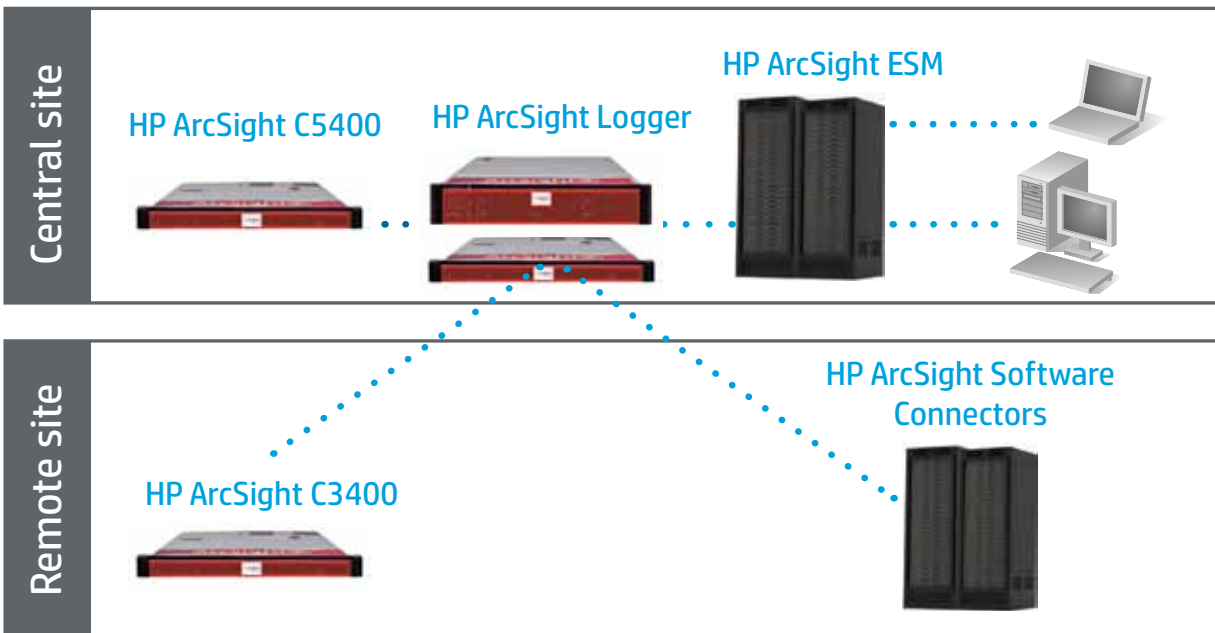
## Content sharing with HP ArcExchange

The HP ArcSight Connectors makes information sharing possible with a simple click of a mouse. With the HP ArcExchange feature, users can download and upload custom-built connectors directly to **Protect 724**, the HP Enterprise Security 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 more than 300 products, makes the HP ArcSight platform the broadest available SIEM solution on the market.

## HP ArcSight platform integration

Regulatory retention requirements, audit reporting needs, IT operations troubleshooting, service level agreement, 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 HP ArcSight Connectors offer. As the data collection layer in the platform, 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 HP 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 HP ArcSight Connector technology deployments.

**Figure 1.** Secure and reliable log collection across all devices and locations



# HP ArcSight Connector appliance specifications

| Model | C3400 | C5400 | Software ConApp |
|---|---|---|---|
| Available as software | Yes | Yes | Software only |
| Management | Web browser, CLI | Web browser, CLI | Web browser, CLI |
| OS | Red Hat Enterprise Linux v6.1, 64-bit | Red Hat Enterprise Linux v6.1, 64-bit | Red Hat Enterprise Linux, CentOS and Oracle Enterprise Linux |
| Max EPS* | 2,500 | 5,000 | Depends on the hardware |
| CPU | 1 x Intel® E5620, quad core, 2.4 GHz | 2 x Intel E5620, quad core, 2.4 GHz | |
| RAM | 8 GB | 16 GB | |
| Storage | 500 GB (RAID 0) | 2 x 500 GB (RAID 1) | |
| Chassis | 1U | 1U | Customer supplied |
| Power | 1 x 460 W common slot platinum power supply | 2 x 460 W common slot platinum power supply | |
| Ethernet interfaces | 4 x 10/100/1000 | 4 x 10/100/1000 | |
| Dimensions (DxWxH) | 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.

## Conclusion

HP ArcSight Connectors deliver flexible, scalable, audit-quality logs in a secure, reliable manner for security and compliance monitoring. Centralized management of all connectors throughout the environment increases operational efficiencies by making deployment and administration simple. HP adapts to customer needs by providing connectors in both software and hardware appliance form factors, thereby, adapting to your requirements and not forcing you to adapt to ours.

## 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.

## HP Software Services

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 **hpenterprisesecurity.com**.

## For more information

To know how you can get audit-quality log collection from all event-generating sources across the enterprise, visit **HP ArcSight Connectors.**

**Get connected**
**hp.com/go/getconnected**

Current HP driver, support, and security alerts delivered directly to your desktop