Hewlett Packard Enterprise

HPE ArcSight SIEM solution

Bigger. Faster. Simpler.

HPE ArcSight SIEM[1] solution is a comprehensive threat detection and compliance management platform with a flexible architecture allowing organizations to easily scale out their existing deployments.

Bigger
This next-generation of data collection and storage engine is based on the HPE ProLiant Gen9 hardware.

ADP supports massive clustering of units, providing load balanced collection, with search queries distributed across the platform.

Faster
HPE ADP now captures raw data at rates of up to 400,000 events per second, compresses and stores up to 480 TB of data, and executes searches at millions of events per second—up to 49 percent faster searches than its predecessor.

Simpler
Introducing Activate Framework, an end-to-end modular content development methodology designed to deploy actionable use cases quickly. It helps facilitate quick, efficient, and less costly deployment of SIEM environments.

The ESM Web user interface (UI) now allows you access to all the dashboards, search functionality, and reports in an easy-to-use UI with just a few clicks.

In addition, we have created a security-rich ecosystem to help security professionals to share, download packages, best practices, and use cases to enable them to get high return on investment (ROI).

[1] Security information and event management (SIEM)

HPE ArcSight SIEM architecture

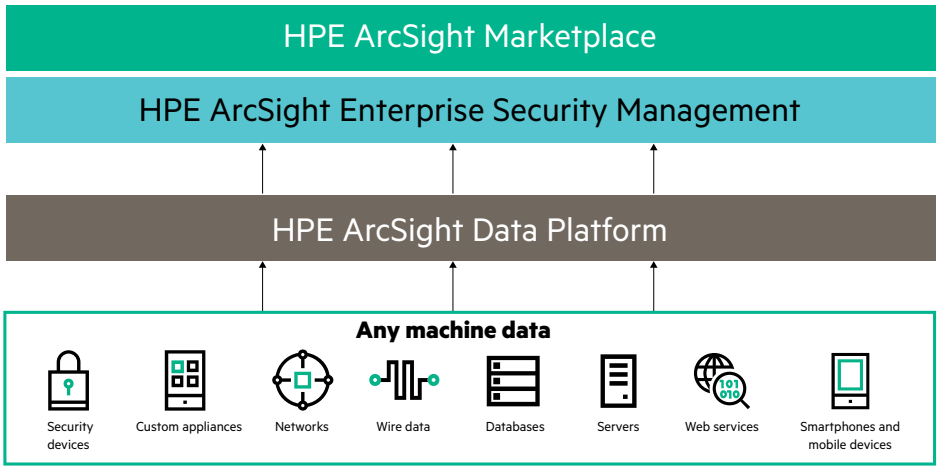

Figure 1: HPE ArcSight SIEM architecture

Whether you are a new security operations center (SOC) implementing your first SIEM solution and starting out with a small staff, or a mature one implementing advanced use cases and forensic queries, Hewlett Packard Enterprise offers you adaptability and flexibility. Our solution simplifies security operations and keeps pace of your growing security needs.

Scalable, high-performance SIEM solution

Next-generation data collection and storage engine

HPE ArcSight Data Platform (ADP) is now architected for breadth, depth, and speed of data collection that Big Data demands. It collects machine data 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 collect, store, search, and report on the data to gain valuable security intelligence across your entire organization.

This next generation of data collection and storage engine is based on the latest HPE ProLiant Gen9 hardware. HPE ADP captures raw data at rates of up to 400,000 events per second, compresses and stores up to 480 TB of log data, and executes searches at millions of events per second—up to 49 percent faster searches than its predecessor.

HPE ADP can be placed on-premise or inside the cloud environment to perform the correlation analysis and send only alerts and incident information back to on-premise systems.

Expansive enterprise security management software
Based on our new Activate Framework, HPE ArcSight Enterprise Security Management (ESM) software allows you to expand your deployment in a hierarchical structure with dedicated ESMs to a particular data source.

Content is triggered by events from specific data sources and you can now create a set of ESM nodes functioning independently of each other. Using a hierarchical deployment, events that need to be correlated across data sources are forwarded to the master ESM node, allowing correlation of up to hundreds of thousands of events per second in real time.

HPE ArcSight ESM offers multi-tenancy and a master console to help managed service providers offer a security intelligence solution in a cost-effective manner.

HPE ArcSight SIEM simplified

Activate Framework for easy deployment
HPE ArcSight Activate Framework, an end-to-end modular content development methodology, makes implementing SIEM easy. The framework provides a standardized approach to creating uses cases or content that can be shared with the community to keep up on the latest IT security threats easily. This results in a robust SIEM that is easier to set up and efficient to maintain.

Hewlett Packard Enterprise has distilled over 15 years of HPE ArcSight SIEM content development experience into this framework. You can now get up and running quickly with effective security use cases and realize ROI as quickly as possible. We do this by leading you through an SIEM maturity path focused on collecting the right data from your feeds quickly realizing value from the investment.

Improved deployment and management
HPE ADP can now be configured, managed, and monitored through a centralized management console, 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.

Monitoring dashboards on the go are now easy with the ADP 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 access to your extended teams, support, or contractors, avoiding unauthorized access.

Improved user experience
Now you can monitor and investigate events from ESM's Command Center Web UI that has added capabilities for the security analysts. You now have the ability to create, edit, delete event channels, apply filter conditions, and add or delete field columns from the channel grid. With this easy-to-use Web UI, you can use the dashboards and search function, create reports, as well as access cases and applications, with just a few clicks.

Simplified pricing and packaging
As part of the strategic direction to integrate analytics and real-time correlation, we introduced a new simplified pricing and packaging structure across the portfolio. The new HPE ArcSight SIEM pricing structure is based on simple traffic ingestion rates of the HPE ADP and ESM.

As part of this price restructuring, the number of SKUs across the portfolio reduced significantly, simplifying the ordering process tremendously.

HPE ArcSight Marketplace—security information ecosphere
With new threats and expanded IT coverage, the uses cases for SOCs are growing rapidly. In order to help SOCs expedite the implementation of use cases and leverage the significant HPE ArcSight community of experts, we have introduced HPE ArcSight Marketplace.

Based on the Activate Framework, Marketplace is a Web-based portal that provides comprehensive and timely content to SOCs. It enables security professionals like you to share or download security packages, trusted use cases, and best practices to help manage your security faster and easier. With Marketplace, you now have as much cutting-edge security information as large companies have to manage their security.

Why HPE ArcSight SIEM solution?

HPE ArcSight SIEM is a solution developed for security experts by the security experts. It has a holistic approach to security intelligence, uniquely unifying SIEM with advanced security analytics for network, user, application, and endpoint monitoring and forensics. It includes out-of-the-box use cases that include real-time threat detection and response, compliance automation and assurance, as well as IT operational intelligence.

HPE ArcSight SIEM solution has been acknowledged as an industry leader 12 years in a row by Gartner and has been deployed in well-known small, medium, and large organizations around the globe.

The HPE Security Intelligence and Operations Consulting (SIOC) practice has been dedicated to defining SOC best practices and helping customers like you to build enterprise-class SOCs since 2007. Combined with, HPE Security Research (HPESR)—an independent, globally recognized security research group that delivers market-leading, vulnerability research and security intelligence, we have the security expertise that is unparalleled in the industry.

Our industry-leading products, proven methodologies, and a decade of experience with one of the largest data set of its kind, make Hewlett Packard Enterprise uniquely qualified to help you achieve security operations excellence.

Learn more at
hpe.com/software/arcsight

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-4463ENW, February 2016