Hewlett Packard Enterprise

HPE ArcSight Enterprise Security Manager

Timely and accurate security intelligence for improved response time and productivity

Fast, powerful, scalable, flexible

- Unify and centralize management, analysis, and reporting of security events
- Identify true threats quickly and accurately so you can take action before critical systems are impacted
- Have the most intelligent and powerful correlation capabilities in the market
- Provide support for multitenancy deployments
- Use the out-of-the-box security correlation rules, use cases, and reports for fast deployment
- Customize rules, use cases, dashboards, and reports based on your unique environment

When minutes mean the difference between a successful or thwarted attack, obtaining the right information at the right time is critical. HPE ArcSight Enterprise Security Manager (ESM) helps to detect and respond to internal and external threats, reduces response time from hours or days to minutes, and gives you the ability to address 10X more threats[1] with no additional headcount.

ArcSight is fast, powerful, scalable, and flexible

ArcSight ESM is a comprehensive and powerful Security Information and Event Management (SIEM) application for security and operations centers. It is part of the **ArcSight SIEM solution**, a threat detection and management platform with a flexible architecture allowing organizations to easily scale out their existing SIEM deployments as they grow their infrastructure.

ArcSight ESM is used in conjunction with **ArcSight Data Platform** or any collection system that uses Common Event Format (CEF). It can easily integrate with investigation and/or remediation tools.

[1] HP (now Hewlett Packard Enterprise) internal testing, 2015

HPE ArcSight SIEM architecture

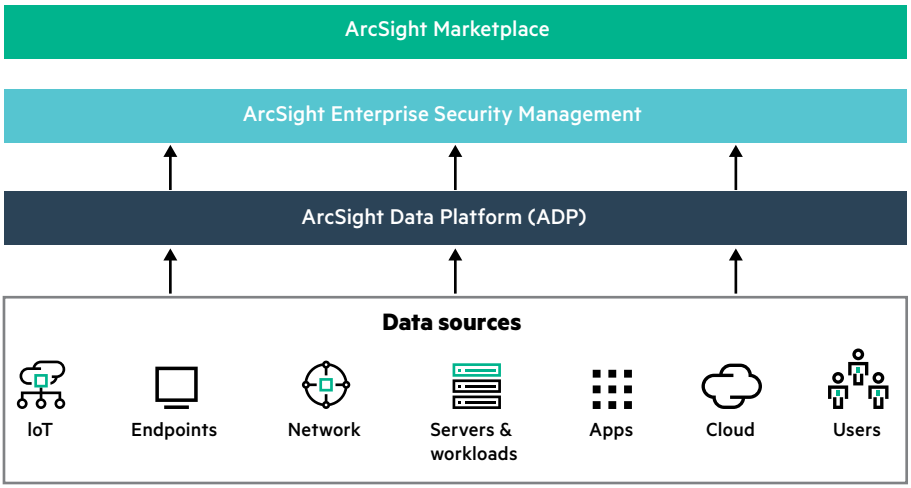

Figure 1: ArcSight SIEM Architecture

"The flexibility of HPE ArcSight is very important for Vodafone NZ. We can use it for our own network, as well as a managed services offering for large government and corporate customers."

– Gerhard Nagele, Product Manager for Security, Vodafone NZ

The multilevel solution that comes with use cases consisting of filters, rules, reports, data monitors, and dashboards make ArcSight ESM ready to use upon installation for first-time security professionals. Yet, with powerful authoring tools, it is also robust enough for advanced professionals even in mature security operations to custom-build complex correlation and long sequence rules.

With ArcSight ESM, you can:

- Monitor systems and infrastructure in real time for potential security threats
- Identify true threats accurately within minutes so you can take action before critical systems are impacted
- Understand contextual information of the events so you can make informed decisions
- Detect indicators of compromise and threats that would otherwise be undetectable
- Improve the efficiency of incident handling activities
- Automate and streamline compliance reporting

Features and benefits

"ArcSight ESM does the log review work of about 5 to 7 FTE's. I really don't think it would be possible to keep up with the threats if we did not have ArcSight ESM in place."

– IT Specialist, Large Enterprise Hospitality Company

ArcSight ESM supports the full range of security information and event management functions—including posture assessment, monitoring, alert and incident handling, breach analysis and response, and event correlation.

Data enrichment

Context information is extremely important for performing advanced correlation.

It is required to make the limited details available within an event or log much more meaningful. We enhance the security data by adding context data at the time of collection, which is critical for understanding the impact of an event. Without data enrichment at the time of collection, the relevant information is lost.

ArcSight ESM enriches the data with user and asset and network information. It gives you the situational and content awareness you need to make an informed, relevant decision during investigation and to accelerate the remediation process.

Categorization and normalization of data
Categorization and normalization convert collected original logs into a universal format for use inside the SIEM product.

We use CEF, a de facto industry standard developed by ArcSight from expertise gained over a decade of building more than 230 connectors across 30 different security and network technology categories.

Categorization and normalization of data helps you quickly identify situations that require investigation or immediate action helping you focus your attention on most urgent, high-risk threats.

Multidimensional real-time correlation
ArcSight ESM has rule-based, statistical, or algorithmic correlation, as well as other methods that include relating different events to each other and events to contextual data (see data enrichment above).

Our correlation engine filters out irrelevant noise while zeroing in on threat risks that matter most. We have the most intelligent and flexible correlation engine with the largest number of correlation algorithms in the industry.

The correlation engine helps you quickly identify indicators of compromise (IOCs), and situations that require investigation or immediate action helping you focus your attention on most urgent, high-risk threats.

"With other products I've used... raw logs and search query results can take from minutes to hours. With ArcSight I can run the same query in seconds."

– Lance Auman, Systems Administrator III, Irvine Unified School District

Ultra-fast investigations and forensics
You can rapidly search terabytes of data using a simple search interface. This feature enables needle-in-the-haystack queries of both active and historical data with a simple search interface. Interesting search patterns can be easily converted into real-time alerts.

The investigation and forensic tools help you obtain the right information at the right time. You can track situations as they develop and query both active and historical data to investigate possible threats.

Out-of-the-box security use cases
ArcSight ESM also comes with standardized templates to build your own advanced queries, correlation rules, and reports customized for your environment.

These trusted use cases can be downloaded via **Marketplace**, a Web-based portal and community for ArcSight security content and SIEM best practices. It provides comprehensive and timely content to security professionals like you, so you can implement your security posture, deploy your SIEM solution quickly, and rapidly realize a return on your investment (ROI).

Workflow automation
Events of interest can be manually or automatically escalated to the right people in the right time frame. The robust workflow framework comes with built in case management and can integrate with your existing processes and systems.

Workflow automation enables members of your team to do immediate investigations, make informed decisions, and take appropriate and timely action.

Optional packages

High availability (HA)—stateful, active or passive HA
Provides backup ESM machine with automatic failover capability should the primary ArcSight ESM machine experience any communication or operational problems.

Threat detector—pattern discovery for automatic pattern detection
Scans for new patterns to stay ahead of new exploitive behavior; instantly uncovers zero-day worms and complex attacks and detect misconfigurations of network devices, systems, and applications so you can triage proactively.

Threat central and reputation security monitor—threat intelligence feeds
Respond to threats based on actionable threat analysis and reputation intelligence from the cloud-based, standards-compliant sharing platform.

Compliance packages—compliance automation and reporting
Easily meet a broad set of regulatory compliance requirements and can ease the cost and complexity of identifying critical issues, helping you avoid risks, prepare for audits and improve productivity and operational efficiency.

Interactive discovery—powerful visual and extensive algorithmic analytics
Explore, correlate, slice, and animate security data across intrusion detection systems (IDS), firewalls, applications, and any other type of security data source, in ways never before possible.

Risk insight—executive level scorecard with insight to security priorities
Combine security intelligence with business risk through rich built-in or customizable dashboards, reports, KPIs, and a heat map capable of showing top priority threats among billion security events.

Learn more at
hpe.com/software/arcsight

Hewlett Packard Enterprise

4AA4-3483ENN, April 2016, Rev. 5