Hewlett Packard Enterprise

HPE ArcSight Enterprise Security Manager

Enriched data and powerful real-time correlation of security events to quickly detect and mitigate threats

Real-Time, Intelligent, Powerful, Scalable, Customizable

- Enriches event data inputs from multiple sources
- Have the most intelligent and powerful correlation capabilities in the market
- Identify true threats quickly and accurately so you can take action before critical systems are impacted
- Unify and centralize management, analysis, and reporting of security events
- Supports multi-tenancy implementations for distributed security environments
- Implement 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

"Another important benefit that HPE Security ArcSight offers is the ability to correlate multiple sources of attacks under a single pane of view. That up-levels investigative efforts, helps shrink remediation time, and boosts the productivity and effectiveness of our security analysts."

– Mike Vamvakaris, Vice President, Managed Cyber Security, Zayo Group

When minutes matter, HPE ArcSight Enterprise Security Manager dramatically reduces the time to intuitively detect, identify, react, and triage cyber-security threats at scale. 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 threats1 with no additional headcount through simplified SOC workflow.

ArcSight ESM is Powerful, Scalable, and Efficient SIEM Solution

ArcSight Enterprise Security Manager is a comprehensive real-time threat detection, analysis, workflow, and compliance management platform with increased data enrichment capabilities. ArcSight detects and directs analysts to cyber-security threats, in real time, helping SecOps teams respond quickly to indicators of compromise. By automatically identifying and prioritizing threats, teams avoid the cost, complexity and extra work associated with being alerted of false positives. ESM allows SecOps organizations the ability to have a centralized, powerful view into their multiple environments creating workflow efficiency for streamlined processes. Through improved detection, real-time correlation, and workflow automation, SOC teams can resolve incidents quickly and accurately.

SC 2017 awards Winner

"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."

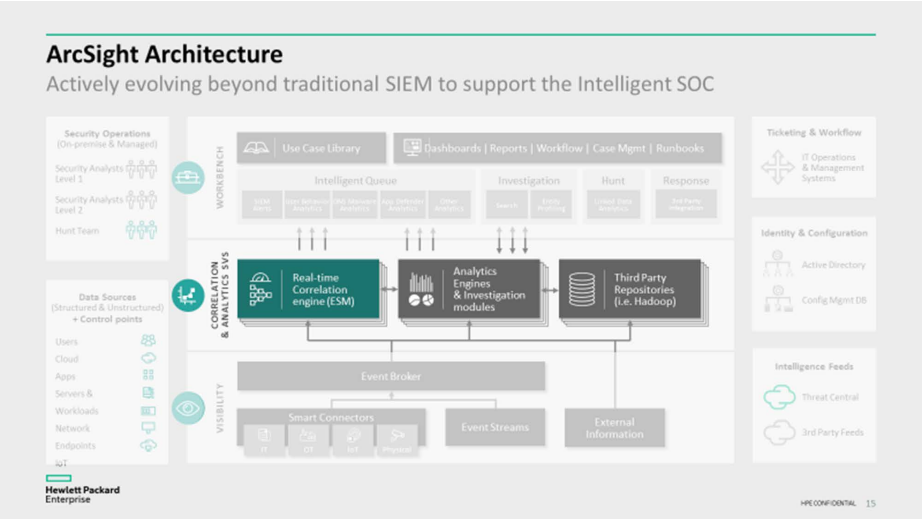
– Gerhard Nagele, Product Manager for Security, Vodafone NZ

"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

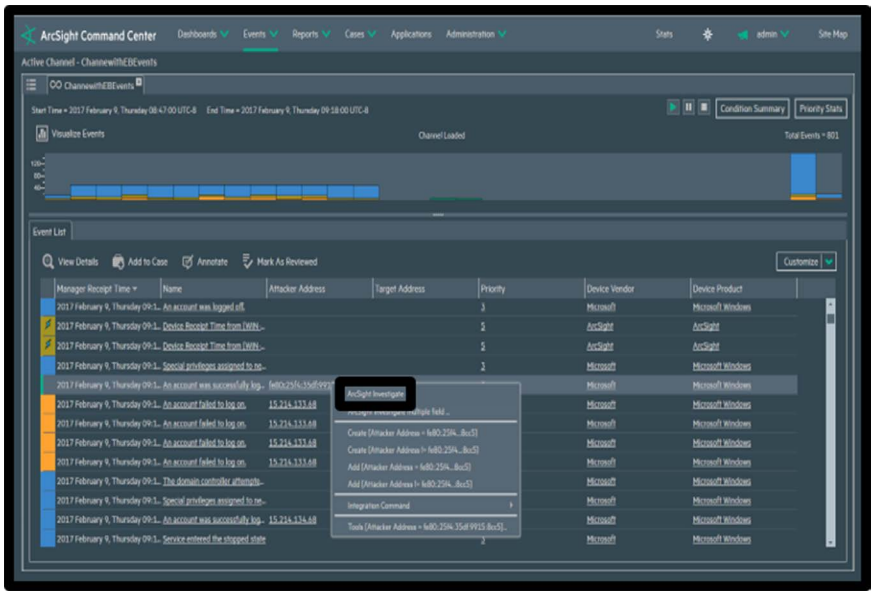
"Our customers have really benefited from having the visibility of the end point, the network, and the data we provide. They're able to do a lot more in HPE Security ArcSight around insider threats and around detecting advanced external threats."

– Marcus Brown, Vice President of Corporate Business Development, Digital Guardian



With ArcSight ESM, you can:

- Monitor your enterprise systems and infrastructure in real-time for potential security threats
- Identify thousands of security threats and variables accurately within minutes so you can mitigate attacks before critical systems are impacted
- Understand enhanced and detailed contextual information of the events so you can make informed security decisions
- Simplify your security operations center's process and workflow to create efficiency and reduce time to mitigation for security threats
- Implement out-of-the-box known security threat rules within minutes to secure your enterprise organization
- Accommodate your growing enterprise systems, assets, and devices and aid your SecOps teams with full IPv6 support
- Integrate with ArcSight Data Platform (ADP) and ArcSight Investigate to create an open, powerful, and intuitive security operations center
- Join the HPE ArcSight security community to share security insights and knowledge



"HPE Security ArcSight ESM reveals security events to us that we were never able to detect before. We're very happy with ESM and confident we can find threats before they compromise our network or disrupt business."

– Mark Beerends, Head of Security Operations Center, Rabobank

"It was very hard for our security analysts previously. Now they are not wasting time on manual tasks."

– Enkhsaikhan Pagva, Manager of the Information Security Unit, Unitel

"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

Features and benefits

ArcSight Enterprise Security Manager (ESM) supports the full range of SIEM functions—including posture assessment, monitoring, alert and incident handling, breach analysis and response, and event correlation.

Data Enrichment
ArcSight ESM collects event information from multiple sources to provide insight into an enterprise's threat landscape. With ESM, the event variables and information that is collected, gets enhanced and enriched to provide more than 400+ individual and specific data points. The enriched data allows ESM to provide event analysis, categorization, and intuitive correlation to determine the threat level.

Categorization and Normalization
Categorization and normalization converts collected original logs into a universal format for use inside the SIEM product. We use CEF, a de facto industry standard developed by HPE from expertise gained over a decade of building more than 300 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.

Powerful Real-Time Correlation
ArcSight ESM correlates events and alerts to identify the high priority threats within environments. The powerful correlation engine of ESM allows for the collection of data and real-time correlation of events to accurately escalate threats that violate the internal rules within the platform. ESM is capable of correlating up to 75,000 events per second within an enterprise.

Workflow Automation
ArcSight Enterprise Security Manager creates an easy way for SOC teams to efficiently and effectively triage detected alerts through the ArcSight Command Center (ACC). Through process implementation and instruction, SOC teams are able to reduce the mean time to respond and escalate incidents to the appropriate personnel for resolution.

Multi-Tenancy
ArcSight ESM allows distributed office environments to utilize one simplified SecOps view. With multi-tenancy capabilities and permissions abilities, enterprises are able to use a centralized set of management abilities including rule-based thresholds and a unified permissions roles, rights, and responsibilities matrix.

Out-Of-The-Box Security Use Cases and Rules
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 **ArcSight 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).

Fast Investigations and Forensics
ArcSight ESM allows SOC organizations to 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.

Compatibility with ArcSight Data Platform (ADP) and ArcSight Investigate
ArcSight ESM is compatible with ADP and Investigate to create a fully integrated open, powerful, and intuitive security operations environment. ESM is able to receive inputs from multiple data sources and ADP's significant open architecture allows for data inputs to be enhanced and more useful for SOC environments. Combining ESM with ArcSight Investigate allows SOC personnel to detect and understand unknown security threats within their enterprise in an intelligent view to quickly remediate any impact or mitigate these security threats before they occur.

ESM Optional Packages

High Availability (HA)—Stateful, Active, or Passive HA
Provides an optimized performance environment with an ESM machine with automatic failover capability should the primary system experience any communication or operational problems.

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
saas.hpe.com/en-us/software/siem-security-information-event-management

Sign up for updates

Hewlett Packard Enterprise

a00007550ENN, April 2017