MICRO FOCUS

Data Sheet
Security

ArcSight Enterprise Security Manager

Distributed real-time correlation with modular content development framework and event triaging

When minutes matter, Micro Focus® ArcSight Enterprise Security Manager dramatically reduces the time to detect, react, and triage cybersecurity threats at scale. ArcSight Enterprise Security Manager (ESM) with its advanced distributed correlation engine, helps security teams detect and respond to internal and external threats, reduces response time from hours or days to minutes, and gives SOCs the ability to address more threats with no additional headcount through simplified SOC workflows and continuously updated threat packages available from the ArcSight Marketplace.

Product Overview

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 security operations 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.

Leverages Arcsight's Powerful Smartconnector and Flexconnector Technology

Benefiting from the Micro Focus advanced event collection, ESM can enrich and analyze data from over 500 different device types. ArcSight's ADP SmartConnectors support every common event format, from native Windows events, APIs, firewall logs, syslog, flat file, Netflow, XML/JSON and direct database connectivity.Beyond those, by using our FlexConnector development framework, custom event parsers can be developed and sent to ESM for indexing and to use in its industry leading distributed correlation engine. More event sources bring more enterprise visibility and the ability to develop more complex use-cases specific to the security needs of your organization.

Categorization and normalization performed by the ArcSight Connectors converts collected original logs into a universal format for use inside the SIEM product. We use CEF, a de facto industry standard developed by Micro Focus from expertise gained over a decade of building more than 400 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.

Real-Time, Intelligent, Powerful, Scalable, Customizable

- The most intelligent and powerful correlation capabilities in the market, now scalable up to 100,000 eps with distributed correlation
- Access to ArcSight Activate threat framework and ArcSight Marketplace content for the most current security correlation rules, dashboards, reports and use cases
- Modular packages allow custom rules, dashboards and other content to be exported and shared across systems or customers
- Eliminate ineffective SOC swivel chair workflows by unifying and centralizing management, analysis, and reporting of all enterprise security events
- MSP/MSSP ready supporting multi-tenancy implementations for distributed security environments
- Ability to incorporate cyber threat intelligence via STIX or CIF standard feeds

Intelligent & Dynamic Event Risk Scoring and Prioritization

ESMs unique priority formula, sometimes referred to as its threat level formula, consists of criteria that each event is evaluated against to determine its relative importance, or priority to your network. The calculation incorporates many data points, such as the defined network & asset model, open ports and imported vulnerability scan results from products like Nessus or Retina paired with corresponding vulnerability databases such as X-Force, CVE, and Bugtraq. For example, a given attack might be known to exploit CVE-1999-0153. If the targeted system exposes that vulnerability and the attacked port is open on the asset, then a system can assume that the attack is likely to succeed and given a higher priority.

Key Benefits

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 100,000 events per second within an enterprise.

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 Micro Focus 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.

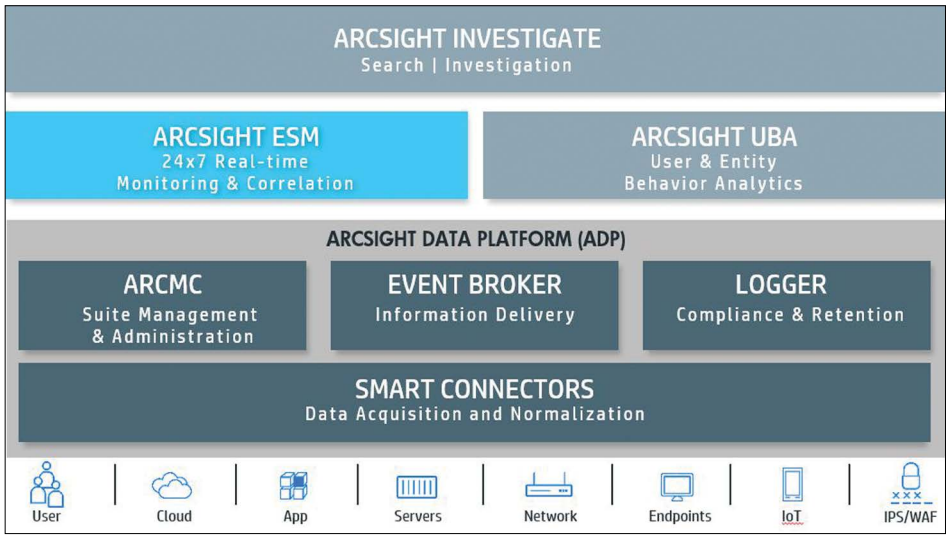


Figure 1. ArcSight Porfolio

Powerful & Modular Content Development

Once custom content (rules, trends, dashboards & reports) have been created to address a security use case, this content can be easily packaged up and deployed on other systems, or shared to other business units or the ArcSight community.In tiered ESM architectures, multiple ESMs can be set to automatically sync content systems dynamically.ArcSight Marketplace and the Activate Framework packages are continuously updated with new security use cases, rules and supported products to keep organizations alerting and triaging defenses current with relevant threats, deploy to your SIEM solution quickly, and rapidly realize a return on your SIEM investment.

**Free access to the ArcSight ContentBrain configurator, allowing customers to track which packages are in testing, production or in review.

Integration with ArcSight Data Platform (ADP) Event Broker

Answering the challenges imposed by Big Data for massive scale, openness, and speed, ArcSight ESM fully integrates with ADP Event Broker: open, massively scalable intelligent data ingestion and delivery bus for the modern SOC.ESM is able to both send and receive events (publisher & consumer) from ADP's EB open architecture, which enables data sharing to third-party applications such as Hadoop, data lakes, or even proprietary in-house applications. This allows the power of an intelligent SIEM, ArcSight ESM, to play a central role among all enterprise security and analytic tools helping to quickly remediate any impact or mitigate these security threats before they occur.

Integration with ArcSight Investigate

ArcSight ESM integrates with ArcSight Investigate to create extremely fast and intuitive search and data visualization within the security operations environment.ArcSight Investigate is a companion next-generation hunt and investigation solution built on a new advanced analytics platform to serve the evolving needs of security teams. 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.

Workflow Automation

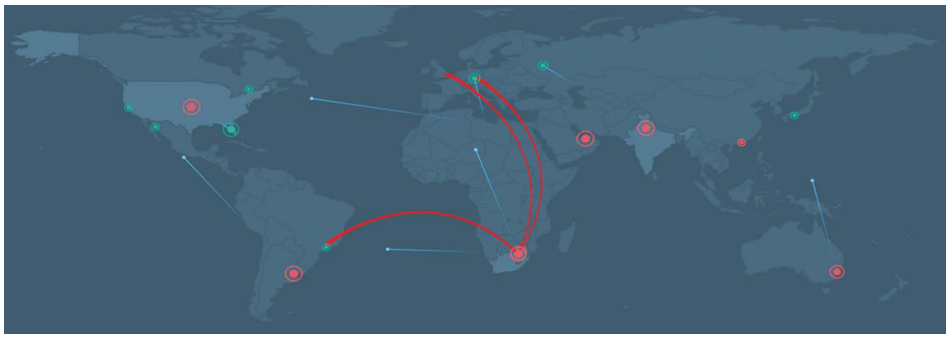
ArcSight Enterprise Security Manager creates an easy way for SOC teams to efficiently and effectively triage detected alerts through real-time triaging channels and its built in case management system.Events of interest (EOI) can be attached to cases and escalated from lower level to upper level responders.Changes to cases create internal audit events allowing close tracking of SLAs and analyst response time metrics. Through these measurable metrics, SOC teams are able to reduce the mean time to respond and escalate incidents to the appropriate personnel for resolution. ArcSight also integrates with 3rd party ticketing systems.

Automated Response within Console or as Rule Actions

Action Connectors (CounterAct) allow integrations between ArcSight and third-party devices; this allows the third-party devices to be controlled from the ArcSight Console. You can execute commands on third-party devices from within ArcSight and send the output of the commands back to the Console for analysts to see. The remote command can also be executed as an action in the correlation rules engine, or as a right-click on the connector. This functionality leads to more cost effective operations as users no longer have to KVM between monitors or switch between detection and action for resolution of events. Not having to leave the ArcSight Console to make changes or to take action is a powerful solution for customers giving them the ability to integrate commands for various applications ESM acting as the central hub for defining, managing, and launching actions, Logger searches, and third-party applications and scripts.

Multi-Tenancy

ArcSight ESM allows distributed business units to utilize one simplified SecOps view.



With multi-tenancy capabilities and access control permissions configurable down to the event level, enterprises are able to use a centralized set of management abilities including rule-based thresholds and a unified permissions roles, rights, and responsibilities matrix. Unique rules, reports, and dashboards can be customized and accessible for target system owners and stakeholders.

Key Features

ESM Optional Packages

HIGH AVAILABILITY (HA)

Provides an optimized performance environment with multiple ESM systems, with automatic failover capabilities should the primary system experience any communication or operational problems.

REPUTATION SECURITY MONITOR (REPSM+)—THREAT INTELLIGENCE FEEDS

Respond to threats based on actionable threat analysis and reputation intelligence from the cloud-based, standards-compliant sharing platform. Threat data is automatically ingested and used in correlation events looking for matches against known bad and indicators of compromise.

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.

Other Features

- **Active Lists**—Dynamic in memory lists capable of holding millions of entries, these can act as watch lists for monitoring suspicious traffic or entity behavior, with the ability to use active lists in any correlation rule
- **Schedule reports**—and deliver results automatically to key stakeholders
- **API**—Retrieve event or case data from ESM with REST based API
- **Trends**—Easily define events of interest to be saved in side tables for extremely fast search and reporting over longer periods of time or outside of the event retention window.
- **Remote Connector Configuration**—Ability to modify configurations on remote connectors from with the ArcSight Console.Aggregation, Event Filtering, Event Time Adjustments, etc.

"Due to the sophisticated collection and correlation capabilities of ArcSight ESM, we have an intelligent system that makes sense of the thousands of events and log records we generate each day—helping us to quickly identify and respond to all of the security incidents that matter."

INFORMATION SECURITY MANAGER NETAPP

Contact us at:
www.microfocus.com

Like what you read? Share it.

- **Custom Image Dashboards**—Overlay dashboards on a custom graphic, such as a map or org chart
- **Format Preserving Encryption (FPE)**—Using Micro Focus SecureData technology, ArcSight can use FPE to retain correlation capabilities, without exposing sensitive data like social security numbers or credit card numbers to analyst or ArcSight users.
- **Data Security**—Protections against the manipulation of data with its immutable data storage for non-repudiation & data integrity purposes

Learn more at
microfocus.com/arcsightesm

Free access to the ArcSight ContentBrain configurator, allowing customers to track which packages are in testing, production or in review at: **https://arcsightcontentbrain.com