



Product Brief: ArcSight ESM

Single Platform for Enterprise-Wide Visibility

Market-Leading Platform for Monitoring Enterprise Threats and Risks

Highlights:

- Store all security information in a single data store
- Build and run powerful monitoring applications
- Reduce the cost of security and compliance

Understand the Who, What and Where behind Every Risk

ArcSight ESM provides the correlation infrastructure to help identify the meaning of any given event by placing it within context of who, what, where, when and why that event occurred and its impact on business risk (see Figure 1). In addition to the ArcSight ESM asset and zone model, the newest version of ArcSight ESM introduces the user model that natively understands identities, roles and groups, and all the accounts that individuals within the organization use. The user model allows administrators to correlate common identifiers like email addresses, login ids and user accounts, and to report on all actions a user has taken across systems, applications, accounts and IP addresses.

Similar to zones that allow IT asset groupings, the user model also includes user categories that map the organizational structure of the organization into custom views, allowing you to monitor groups of users by reporting structure, geography or role.

Correlating user data with asset information enables analysts to focus on the right incidents occurring in the environment. ArcSight ESM gives the highest priority to privileged users performing unauthorized actions on the organizations most critical assets, ensuring that the most critical events are surfaced before they result in a security breach.

ArcSight ESM also correlates user entitlements to event log information and Netflow data. By quickly comparing the actions users are taking with their entitlements, analysts can instantly pin-point privileged role violations and instances of users performing actions outside their authorization. Correlating these disparate pieces of data also allows auditors to definitively attribute any action to a specific person, even when a shared administrative account or dynamic IP address is used.



Figure 1: ArcSight ESM provides a single platform for all your monitoring requirements.

The ArcSight ESM platform is used to secure the world's most demanding organizations. ArcSight ESM monitors all events across the enterprise, and uses powerful correlation and analysis to identify business and technology threats. Built on a flexible, extensible platform, ArcSight ESM enables the monitoring of business objects, transactions and users to mitigate risks to the organization.

Flexible Platform for Building Monitoring Applications

ArcSight ESM is a powerful and flexible threat and risk monitoring platform that can be used to build the sophisticated security management applications necessary to block today's complex threats. The platform features include:

- **ArcSight FlexConnector Development Kit**
Capture any data from any device, system or application using a simple "drag and drop" connector development framework
- **Log Management Framework**
Manage and store every event occurring in your environment securely and efficiently
- **Business-Specific Customization**
Extend the ArcSight ESM platform with industry-specific data types to enable monitoring of very targeted business objects
- **Directory Integration**
Synchronize user, role and entitlement information from corporate directories to find unauthorized user activity, shared account usage and role policy violations
- **Web Services API**
Interface with other IT management frameworks to collect data or deliver intelligent information to analysts, auditors and managers

- **Global Variables**
Author variables from a central location and use them amongst different resources, simplifying the application authoring process
- **Pattern Detection Engine**
Perform heuristic analysis on historic event data with ArcSight Threat Detector to discover subtle patterns, low-and-slow attacks and advanced persistent threats

Using these features to develop sophisticated correlation applications, organizations can maintain a state of continuous situational awareness. Analysts can focus on the few dozen critical events that require review. Real-time alerts show administrators the most critical application, transactional and security events occurring in the environment, along with all of the context necessary to further analyze and mitigate any threat to the business.

Broadest Collection

The ArcSight ESM collection infrastructure offers advanced collection capability for the broadest library of event sources. Logs from over 300 devices and event sources are collected, including OS, network devices (routers, switches), network analyzers (NetFlow data, traffic analyzers, NAC, NBA), security solutions (IPS/IDS, firewalls, VPNs, vulnerability scanners), as well as logs from applications, databases, identity management solutions and Web servers/

web-based applications. Events from different devices in the same family are normalized for easy cross-device monitoring and analysis. Optional solution packages can support and address top-of-mind issues and initiatives such as SOX, PCI, HIPAA, GLBA, user monitoring and IT governance.

Intuitive Dashboards, Robust Reporting

ArcSight ESM offers a range of features that ensure fast, convenient and intuitive access to information. Customizable and graphically rich dashboards ensure business and technical views that are tailored to deliver insights to the appropriate individuals in the organization. The ArcSight ESM console provides a single view of a company's security status based on validated attacks and business risk, while geographic and network map views allow users to maintain awareness in areas of their organizational responsibility.

ArcSight ESM delivers comprehensive technical, operational and trend reports that communicate security status and satisfy regulatory reporting requirements. The reporting framework makes business-level reporting easy through both standard and customizable templates for compliance status, business risk and user profiling. In addition to pre-built reports and templates, the framework allows users to build new reports and templates for ad-hoc and scheduled reporting. The framework melds richly correlated information into comprehensive views that enable stakeholders to identify areas of risk, communicate the value and effectiveness of security operations and easily answer key business questions. Trend reporting enables tracking of events and their impact over time. Through correlation technology, trend reporting can also be used to simulate "what if" scenarios showing the impact that policy changes may make to the organizations overall security and risk posture.

"ArcSight ESM enables us to effectively analyze our log data and know what's really happening on our network. We are able to raise awareness within our organization, comply with our own global IT security policy and meet audit reporting needs – and in the process, we've become a business enabler."

- Marc Seiffert, Senior IT Specialist, BMW Group

Specifications

E7200	
EPS (Peak/Sustained)	5000 EPS/3000 EPS
OS	Oracle Linux (RedHat variant)
CPU	2 x Intel Xeon 5504 Quad Core
RAM	24GB
Interfaces	4 x 10/100/1000 CX
Storage	6 x 600GB - Serial Attached SCSI (SAS) disks in RAID 10
Chassis	2U Rack-mountable appliance
Power	2x 870W - Redundant
Thermal	3000 BTU/hr
Weight	78 lbs. (36 kg)
Dimensions (DxWxH)	26.8" x 17.4" x 3.4"

ArcSight ESM is available either as software or as a rack-mountable appliance. Actual performance will depend on factors specific to a user's environment.

About ArcSight:

ArcSight, an HP company, is a leading global provider of cybersecurity and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the ArcSight Enterprise Threat and Risk Management (ETRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit www.arcsight.com.



ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 (0)844 745 2068
Asia Pac Headquarters: +65 6248 4795

© 2010 ArcSight, Inc. All rights reserved.
ArcSight and the ArcSight logo are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners.
ARST-PB020-081310-02