



Product Brief: ArcSight™ ESM

Delivering Comprehensive Business Monitoring and Protection

Sophisticated Solution for Compliance Requirements and Protection Against External and Internal Breaches

Highlights:

- Comprehensive Monitoring and Protection for all IT hardware and software assets
- Ready to use templates allow faster compliance efforts
- Single platform for security and compliance reports across all assets and users

ArcSight ESM Security Information and Event Management (SIEM) solution is used to secure the world's most renowned businesses. 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, ESM allows content portability from one technology choice to another, within and across organizations.

Reduce Business Risks Across Your Organization

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. ArcSight ESM correlation delivers accurate and automated prioritization of security risks and compliance violations in a business relevant context. The ESM collection infrastructure offers advanced collection capability for the broadest library of event

sources – logs from over 275 devices and event sources are collected including OS, network devices (routers, switches), network analyzers (network monitors and traffic analyzers, NAC, NBA), security solutions (IPS/IDS, Firewall, 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 (e.g. routers) are normalized for easy cross-device monitoring and analysis. Optional Solution Packages can support and address top-of-mind issues and initiatives like SOX, PCI, HIPAA, GLBA, user monitoring and IT governance.

Powerful Correlation and Analysis for Identifying Threats

ArcSight ESM's powerful correlation engine allows organizations to maintain a state of continuous situational awareness by processing millions of event entries in real-time. ESM then focuses on the few dozen





ArcSight ESM can solve multiple problems for multiple users and roles.

critical events that require review by the security administrator. With built-in concepts of network asset and user models, ArcSight ESM is uniquely able to understand who is on the network, what data they are seeing, and which actions they are taking with that data. Real-time alerts show administrators the most critical security events occurring in the environment, along with all the context necessary to further analyze and mitigate a breach.

Flexible 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 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.

| Model | E7100 |
|--------------------------|--|
| Max EPS (Peak/Sustained) | 5000 EPS/3000 EPS |
| OS | Oracle Linux (RedHat variant) |
| CPU | 2x Quad-Core Intel Xeon (2.0GHz) |
| RAM | 16GB |
| Interfaces | 2 x 10/100/1000 CX |
| Storage | 6x 400GB - Serial Attached SCSI (SAS) disks in RAID-10 |
| Chassis | 2U rack-mountable appliance |
| Power | 2x 750W Redundant |
| Thermal | 2700 BTU/hr |
| Weight | 61 lbs (27 kg) |
| Dimensions (DxWxH) | 29.3" x 17.2" x 3.4" |

Actual performance will depend on factors specific to a user’s environment

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of compliance and security management solutions that protect enterprises and government agencies. ArcSight helps customers comply with corporate and regulatory policy, safeguard their assets and processes, and control risk. The ArcSight platform collects and correlates user activity and event data across the enterprise so that businesses can rapidly identify, prioritize, and respond to compliance violations, policy breaches, cybersecurity attacks, and insider threats. 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: +44 870 351 6510
 Asia Pac Headquarters: 852 2166 8302

© 2009 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-PB005-022409-03