



Product Brief: ArcSight Express

Security Expert “In a Box”

ArcSight Express protects your business with built-in solutions for the security and compliance problems that matter.

Highlights:

- Comprehensive monitoring of perimeter, network and server security
- Automated security operations
- Easy-to-deploy and maintain appliance solution

The Network is Still Under Attack

Network security threats continue to rise. Recent studies indicate a 300% growth in malware in 2008 alone. Unfortunately, organizations with smaller security teams and smaller security budgets do not face smaller risks. As a result, most organizations are vulnerable to hackers, viruses, malware, data breaches and identity fraud. Even worse, these firms often do not have a dedicated security team or much security expertise at all. Malware is increasing, breaches are increasing, regulations are increasing, and yet headcount to deal with these issues is shrinking at many firms.

For organizations that face growing threats to their network and their critical information, yet have limited resources and expertise to address these threats, ArcSight Express provides a simple, automated, cost-effective solution.

ArcSight Express brings the power of world-class event correlation and log management to a new range of customers. ArcSight Express analyzes logs from any device or system on your network, determines if a

potentially risky incident is occurring and notifies administrators in time to take action.

ArcSight Express does the heavy lifting of a dedicated security expert, providing meaning to network security events by placing them within context of what, where, when and why each event occurred and its impact on the organization. Real-time alerts show administrators the most critical security and compliance events occurring in the business, along with the context necessary to further analyze and mitigate a breach. ArcSight Express also addresses compliance requirements with the ability to store audit quality logs and provide meaningful compliance reports for fast, easy audits.

Security Expertise, Built Into the Box

ArcSight Express includes the rules, alerts and reports that matter in the protection of the mid-sized organizations. All are pre-built and ready to be used without custom development. Any rule or report can be extended easily using the ArcSight graphical console and rule builder. This expertise addresses the most critical issues faced by customers.



Bot, Worm, and Virus Attacks

- Top Infected Systems
- All AV Configuration Changes and Errors

Bandwidth Hogs and Policy Violations

- Top Bandwidth Users
- Configuration Changes
- Successful and Failed Logins
- Password Changes
- Top Attackers and Internal Targets

Database Monitoring

- Database Errors and Warnings
- Database Access and Configuration

Unauthorized Application Access

- User Authentication, Administration and Configuration Changes

Network Errors and Changes

- Top Connections
- Network Device Errors and Status
- Access and Configuration Changes

VPN Sneak Attacks

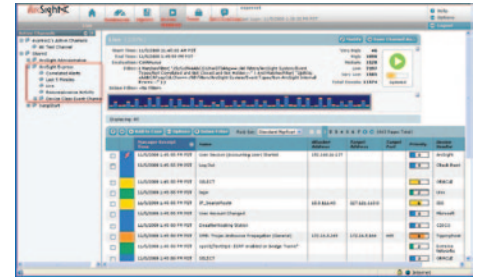
- VPN Authentication Errors
- VPN Configuration Changes
- Connection Activity

Server and Desktop Monitoring

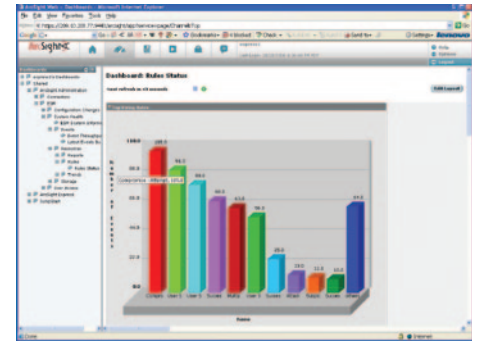
- Privileged User Administration
- Access and Configuration Changes
- Denied Connections
- IPS/IDS Alerts and Bandwidth Usage
- Successful/Failed Login Activity

Compliance Reporting for Multiple Regulations

ArcSight Express delivers a set of common compliance monitoring controls that can be applied to multiple regulations, including Sarbanes-Oxley, PCI DSS, Gramm-Leach-Bliley, FISMA, Basel II and HIPAA. Each can be extended with pre-built Compliance Insight Packs—specialized solution modules designed to deliver full reporting against specific regulations.



The ArcSight Express Web Console allows easy real-time monitoring of your network.



ArcSight Express gives you the critical information you need to react quickly.

ArcSight Express Appliance Specifications

Model	M7200-M	M7200-L	M7200-X	M7200-XL	L3200
OS	Oracle Enterprise Linux 4 64-bit				
Compression	Up to 10:1				
Peak EPS/Flows	500 EPS/ 50K Flows	1000 EPS/ 50K Flows	2500 EPS/ 50K Flows	5000 EPS/ 50K Flows	Same as M7200
Max Devices	750	750	750	750	Same as M7200
MAX Assets	5,000	10,000	25,000	50,000	N/A
Web Users	Unlimited Users				
CPU	2 x Intel Xeon E5504 Quad Core 2.0 GHz			1 x Intel Xeon E5504 Quad Core 2.0 GHz	
Interfaces	4 x 10/100/1000			2 x 10/100/1000	
RAM	24GB			12GB	
Storage	6 x 600GB - RAID 10 Effective 1.6TB			2 x 1TB - RAID 1 Effective 8TB	
Chassis	2U			1U	
Power	2 x 870W 100-240 VAC			1 x 480W 100-240 VAC	
Dimensions (DxWxH)	26.8" x 17.4" x 3.4"			24.7" x 17.1" x 1.7"	



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

© 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-PB005-092109-14

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses, and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit www.arcsight.com.