Data sheet

HP ArcSight Express

Accelerate your SIEM deployment for better security intelligence

Highlights

- **Faster time to value:** Prebundled content enables quick deployment and immediate return on investment
- **Reputation based monitoring:** Alerts when network traffic to and from bad IPs are hitting your network
- **Monitoring straight out of the box:** Preconfigured connections to Windows®, NetFlow, and Cisco

Defending against smarter attacks

The nature of the cyber-attack is evolving, looking more like cyber warfare. Cyber criminals are now selling intellectual property and account user IDs and passwords in online black markets. As a result, organizations are experiencing greater losses by multifaceted attacks, which have become more complex. In the "2012 Cost of Cyber Crime Study" conducted by Ponemon, the loss for an organization ranged from $1.4–$46 million USD per year. Smaller organizations had a higher per capita loss than larger organizations. However, organizations that deployed a security intelligence system were better prepared, able to detect and defend against attacks before attackers successfully exfiltrated the information they were targeting. On average, organizations with better security intelligence were able to save $1.6 million USD annually battling cyber criminals.

However, many organizations lack skills and resources to staff a Security Operations Center. Furthermore, business demands require that the IT environment continue to adapt to new business models with virtualized networks, mobile applications, and Big Data analytics. Each of these requirements makes the organization's environment more porous and more difficult to defend. Security analysts need a solution that helps them quickly deploy a security intelligence management platform, which can help them understand and respond to events that are taking place in their organization. Security intelligence can provide organizations with omniscience like knowledge, giving them the upper hand needed to battle cyber criminals.

Protect what you can see

HP ArcSight Express comes fitted with everything an enterprise needs to give it complete visibility into who, what, and where of an event. HP ArcSight Express incorporates the following features:

- **IdentityView—**Provides identity intelligence enabling early detection of insider threat
- **Threat Detector—**Detects complex threats to the organization, using a heuristic pattern analysis of historical data events
- **NetFlow Analysis—**Understands how network bandwidth is being consumed, so that suspicious activities are correctly prioritized and investigated

HP ArcSight Express also includes a free trial to RepSM, which brings reputation-based intelligence to help security analysts detect and block communication between malicious hosts and infected infrastructure.

Figure 1. HP ArcSight Express provides overall visibility into your security posture

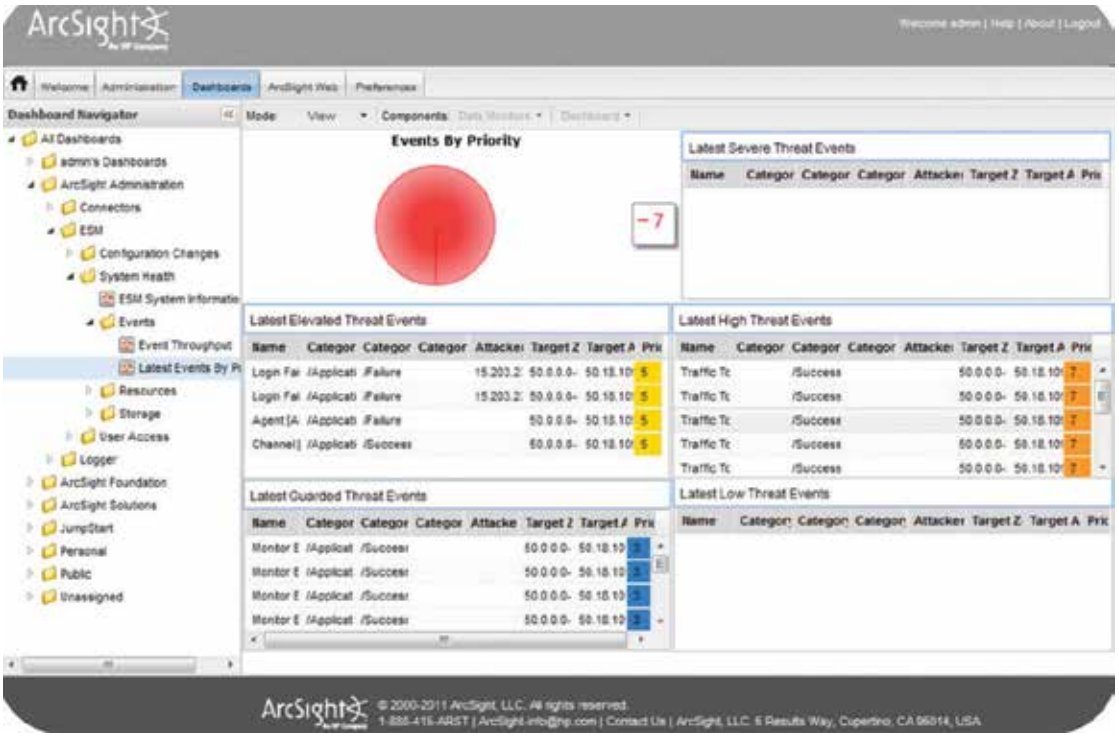
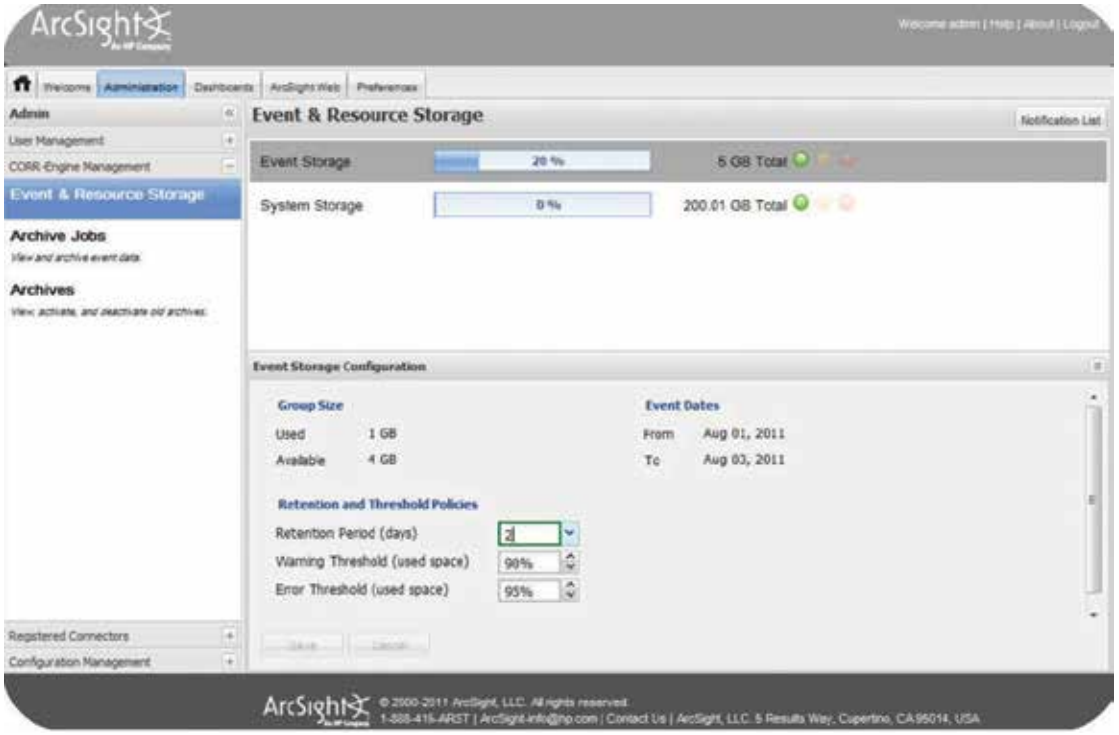


Figure 2. The new HP ArcSight Express management console makes administering and configuring your system a breeze



Prescriptive out-of-the-box content

HP ArcSight Express includes the most commonly used rules, alerts, and reports for perimeter and network security monitoring. All are prebuilt and ready to be used out of the box.[1]

Enterprise level
- Windows Unified Connector
- Top bandwidth users
- Database errors and warnings
- Configuration changes
- Database successful and failed logins
- Successful and failed logins
- Database configuration changes
- Password changes
- Top attackers and internal targets

Database
- Database errors and warnings
- Database successful and failed logins
- Database configuration changes

Network devices
- Network device errors and critical events
- Network device status and "down" notifications
- Bandwidth usage
- Configuration changes by user and change type
- Successful and failed logins
- Top connections

Operating system
- Privileged user administration
- Successful and failed logins
- Configuration changes

Antivirus
- Top infected systems
- All AV errors
- AV signature update stats
- Consolidated virus activity
- AV configuration changes

IPS/IDS
- IPS/IDS alert metrics
- Alert counts
- Top alert sources and destinations
- Top attackers and internal targets
- Access management
- User authentication across hosts
- Authentication success and failures
- User administration configuration changes

VPN device
- VPN authentication errors
- Connection counts
- Connection durations
- Connections accepted and denied
- Successful and failed logins
- Top connections
- Top bandwidth users
- VPN configuration changes

Firewall
- Denied inbound connections
- Denied outbound connections
- Bandwidth usage
- Successful/failed login activity

[1] Additional content can be developed by HP ArcSight Professional Services or Certified Partner

HP ArcSight Express 4.0 Specifications (Appliance)

Model	AE-7506	AE-7511	AE-7526	AE-7551	AE-7566	AE-7581
Peak EPS	500	1,000	2,500	5,000	10,000	15,000
Sustained EPS (enforced)	250	500	1,250	2,500	5,000	7,500
Devices	750	750	750	750	1,500	1,500
Assets	5,000	5,000	10,000	10,000	25,000	25,000
Console users	1	1	1	1	1	1
Web users	25	25	25	25	25	25
IdentityView users	50	50	50	50	50	50
Connector management	Yes	Yes	Yes	Yes	Yes	Yes
Onboard connectors	4	4	4	4	4	4
Remote connectors	4	4	4	4	4	4
System OS	Red Hat Enterprise Linux 6.2 64-bit					
Processor	2 x Intel® Xeon® E5-2650 2.0 GHz 8-core Processor					
Memory	64 GB, 1600 MHz RAM					
Ethernet interfaces	4 x 10/100/1000					
Storage	6 x 600 GB (1.8 TB RAID-10)					
Chassis	2U					
Power	2 x 750W CS Platinum Power Supply					
Dimensions (DxWxH)	29.5" x 17.54" x 3.44"					

Compliance reporting for multiple regulations

HP 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.

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
hp.com/go/hpexpress

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-1163ENW, August 2013, Rev. 4