# HP ARCSIGHT EXPRESS: POWERED BY THE CORR-ENGINE

## Security and Compliance Monitoring for Complex CyberAttacks

HP Enterprise Security Product Brief

## Complex Attack Volumes are Exploding

The recent past is littered with names like Aurora, Stuxnet, Zeus, APT, WIkiLeaks, Anonymous and many more. Organizations are facing growing numbers of increasingly complex threats. A recent U.S. Secret Service investigation report indicates over 800 data breach case reports in 2010. This is about the same case load as the number in the six years prior, with almost 900 data breach cases from 2004 to 2009. The total number of records breached in the Secret Service case load alone has breached one billion, with actual losses of over $500 Million. The Secret Service estimates they have prevented additional losses of over $7 billion.

The former CEO of Google, Eric Schmidt stated that we create as much information in just two days now as we did from the dawn of man through 2003. This unprecedented explosion in data and U.S. Secret Service case numbers reflects three interrelated trends: the consumerization of IT, an explosion in the amount of digital data being created, and the motivation of increasingly sophisticated hackers to profit from theft of this data.

These trends place an enormous burden on IT and security administrators to manage, store and secure this data. IT administrators have to deploy and manage increasing numbers and types of infrastructure devices, systems and applications, all of which generate enormous amounts of log event data. Security analysts have to understand the relationships between these events and stay on top of the increasingly complex, multi-vector attacks that hackers are using to steal sensitive data.

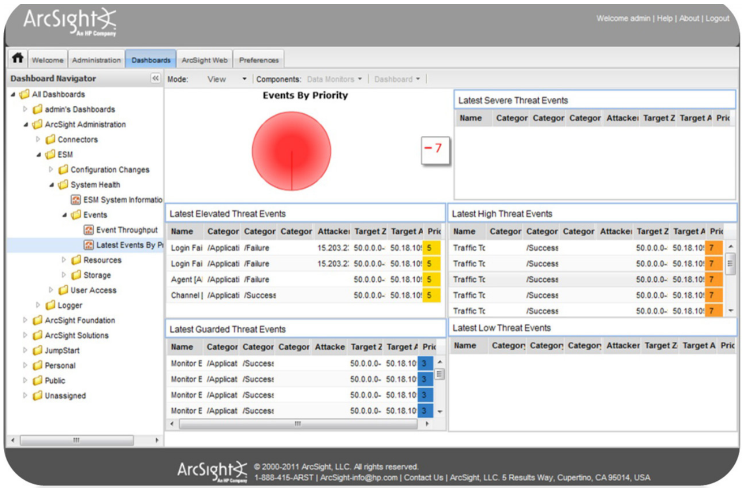
## Correlation at the Speed of Thought

HP ArcSight's Correlation Optimized Retention and Retrieval (CORR) Engine is a breakthrough technology that delivers orders of magnitude improvement in log correlation and storage, helping security administrators thwart the complex threats they face today.

The HP ArcSight Express SIEM solution uses the CORR-Engine as the foundation that helps keep up with the speed needed for today's threat detection, security analysis and log data management. ArcSight Express helps identify the meaning of any given event by placing it within context of what, where, when and why that event occurred and its impact on the organization. ArcSight correlation delivers accurate and automated prioritization of security risks and compliance violations in a business relevant context. Real-time alerts show administrators the most critical security events occurring in the environment, along with all context necessary to further analyze and mitigate a breach.

ArcSight Express also incorporates a new management console that simplifies administrative tasks making the solution easy to deploy, maintain and use (see Figures 1 and 2). Using ArcSight Express administrators and analysts are able to:

- **Detect more incidents**
  The new architecture will allow event correlation rates of up to 5x the current performance using the same hardware.
- **Address more data**
  The new architecture will enable storage capacity of up to 10x the current capacity for correlated events using the same disk space.
- **Operate more efficiently**
  The use of a common data store allows both the real-time correlation application and the log management application to use the same set of data, providing a seamless workflow that includes detection, alerting, forensic analysis and reporting.



Latest Severe Threat Events

| Name | Categor | Categor | Categor | Attacker | Target Z | Target A | Pric |
|---|---|---|---|---|---|---|---|

Latest Elevated Threat Events

| Name | Categor | Categor | Categor | Attacker | Target Z | Target A | Pric |
|---|---|---|---|---|---|---|---|
| Login Fai | /Applicati | /Failure | | 15.203.2: | 50.0.0.0- | 50.18.10! | 5 |
| Login Fai | /Applicati | /Failure | | 15.203.2: | 50.0.0.0- | 50.18.10! | 5 |
| Agent [A | /Applicati | /Failure | | | 50.0.0.0- | 50.18.10! | 5 |
| Channel [ | /Applicati | /Success | | | 50.0.0.0- | 50.18.10! | 5 |

Latest High Threat Events

| Name | Categor | Categor | Categor | Attacker | Target Z | Target A | Pric |
|---|---|---|---|---|---|---|---|
| Traffic Tc | | /Success | | | 50.0.0.0- | 50.18.10! | 7 |
| Traffic Tc | | /Success | | | 50.0.0.0- | 50.18.10! | 7 |
| Traffic Tc | | /Success | | | 50.0.0.0- | 50.18.10! | 7 |
| Traffic Tc | | /Success | | | 50.0.0.0- | 50.18.10! | 7 |
| Traffic Tc | | /Success | | | 50.0.0.0- | 50.18.10! | 7 |

Latest Guarded Threat Events

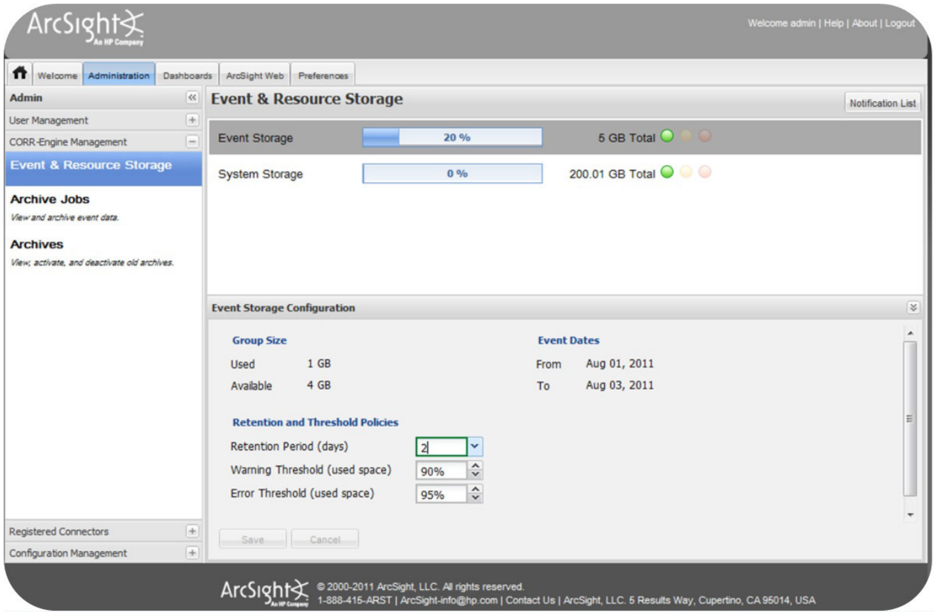
| Name | Categor | Categor | Categor | Attacke | Target Z | Target A | Pric |
|---|---|---|---|---|---|---|---|
| Monitor E | /Applicat | /Success | | | 50.0.0.0- | 50.18.10 | 3 |
| Monitor E | /Applicat | /Success | | | 50.0.0.0- | 50.18.10 | 3 |
| Monitor E | /Applicat | /Success | | | 50.0.0.0- | 50.18.10 | 3 |
| Monitor E | /Applicat | /Success | | | 50.0.0.0- | 50.18.10 | 3 |

Latest Low Threat Events

| Name | Categor | Categor | Categor | Attacker | Target Z | Target A | Pric |
|---|---|---|---|---|---|---|---|

© 2000-2011 ArcSight, LLC. All rights reserved.
1-888-415-ARST | ArcSight-info@hp.com | Contact Us | ArcSight, LLC. 5 Results Way, Cupertino, CA 95014, USA

Figure 1: HP ArcSight Express provides overall visibility in to your security posture.



Event & Resource Storage

Event Storage 20 % 5 GB Total

System Storage 0 % 200.01 GB Total

Archive Jobs
*View and archive event data.*

Archives
*View, activate, and deactivate old archives.*

Event Storage Configuration

Group Size

| | |
|---|---|
| Used | 1 GB |
| Available | 4 GB |

Event Dates

| | |
|---|---|
| From | Aug 01, 2011 |
| To | Aug 03, 2011 |

Retention and Threshold Policies

| | |
|---|---|
| Retention Period (days) | 2 |
| Warning Threshold (used space) | 90% |
| Error Threshold (used space) | 95% |

© 2000-2011 ArcSight, LLC. All rights reserved.
1-888-415-ARST | ArcSight-info@hp.com | Contact Us | ArcSight, LLC. 5 Results Way, Cupertino, CA 95014, USA

Figure 2: The new HP ArcSight Express management console makes administering the system easier.

## Highlights

- Detect More Incidents: Allows more precise prioritization of correlated events
- Address More Log Events: Enables order of magnitude more capacity
- Operate More Efficiently: Frees up security analyst cycles for proactive monitoring

## Prescriptive Out-of-the-Box Content

ArcSight Express includes the most commonly used rules, alerts and reports for perimeter and network security monitoring. All are pre-built and ready to be used out of the box.*

### Enterprise Level

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

### Anti-Virus

- Top Infected Systems
- All AV errors
- AV Signature Update Stats
- Consolidated Virus Activity
- AV Configuration Changes

### Database

- Database Errors and Warnings
- Database Successful and Failed Logins
- Database 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

### Network Devices

- Network Device Errors and Critical Events
- Network Device Status and "Down" Notifications
- Bandwidth Usage
- Configuration Changes by User and Change Type
- uccessful and Failed Logins
- Top Connections

### 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

### Operating System

- Privileged User Administration
- Successful and Failed Logins
- Configuration Changes

### Firewall

- Denied Inbound Connections
- Denied Outbound Connections
- Bandwidth Usage
- Successful/Failed Login Activity

* Additional content can be developed by HP ArcSight Professional Services or Certified Partners.

## 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.

## Call to Action:

For more information about ArcSight Express, visit www.arcsight.com.

## HP ArcSight Express Appliance Specifications

<table>
<tr><th>Model</th><th>AE7405</th><th>AE7410</th><th>AE7425</th><th>AE7450</th><th>AE7465</th><th>AE7480</th></tr>
<tr><td>Max Devices</td><td>750</td><td>750</td><td>750</td><td>750</td><td>1500</td><td>1500</td></tr>
<tr><td>Peak EPS/Flows</td><td>500/50K Flows</td><td>1,000/50K Flows</td><td>2,500/50K Flows</td><td>5,000/50K Flows</td><td>10,000/50K Flows</td><td>15,000/50K Flows</td></tr>
<tr><td>Max Assets</td><td>5,000</td><td>5,000</td><td>10,000</td><td>10,000</td><td>25,000</td><td>25,000</td></tr>
<tr><td>System OS</td><td colspan="6">Oracle Enterprise Linux 5.5 64-bit</td></tr>
<tr><td>Web Users</td><td colspan="6">Unlimited</td></tr>
<tr><td>CPU</td><td colspan="6">2 x Intel Xeon E5620 Quad Core 2.4 GHz</td></tr>
<tr><td>Interfaces</td><td colspan="6">4 x 10/100/1000</td></tr>
<tr><td>RAM</td><td colspan="6">36GB</td></tr>
<tr><td>Storage</td><td colspan="6">6 x 400GB - SAS disks in RAID-10</td></tr>
<tr><td>Chassis</td><td colspan="6">2U</td></tr>
<tr><td>Power</td><td colspan="6">2x 750W CS Platinum 100-240 VAC</td></tr>
<tr><td>Dimensions</td><td colspan="6">27.3"x 17.6"x 3.4"</td></tr>
</table>

ESP-PRB005-092109-19, Created August 2011