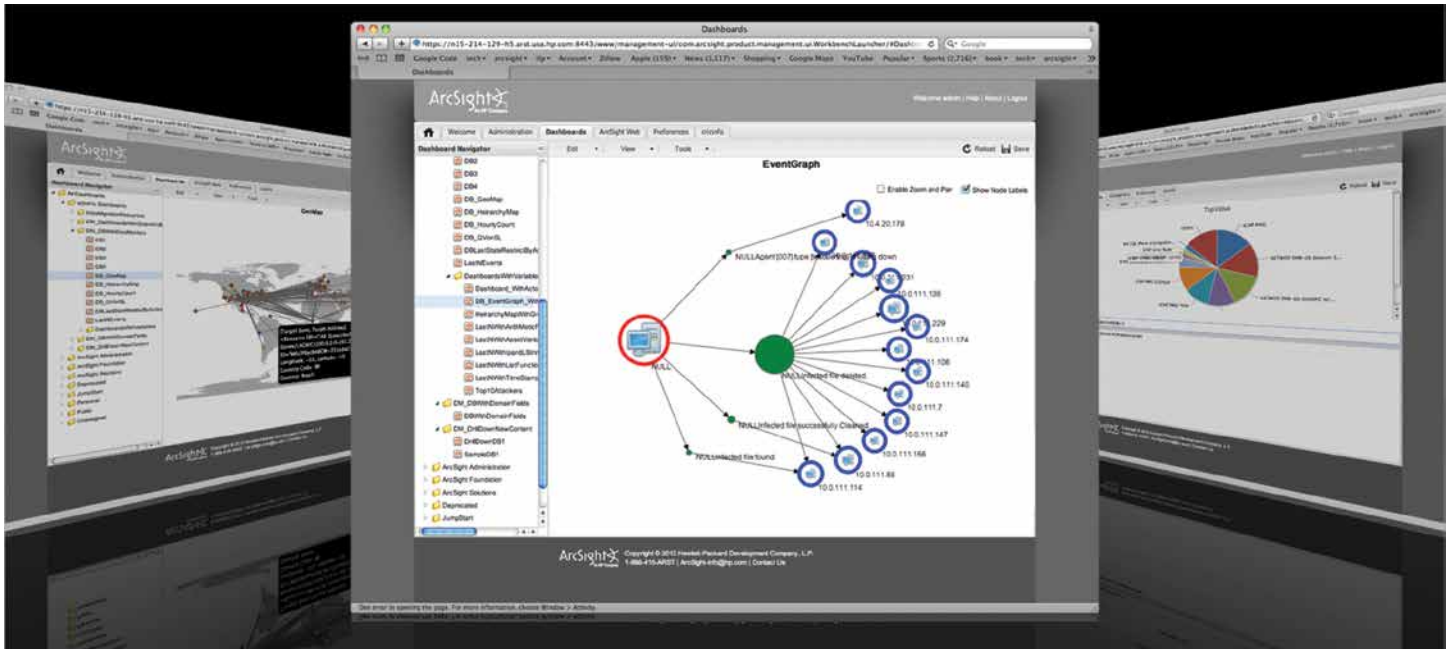
Data sheet

HP ArcSight ESM: powered by CORR-Engine

Simple, intelligent, efficient, and manageable



"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

HP ArcSight ESM is the brain of the HP ArcSight SIEM platform. It analyzes and correlates every event that occurs across the organization—every login, logoff, file access, database query—to deliver accurate prioritization of security risks and compliance violations. The powerful correlation engine of HP ArcSight ESM sifts through millions of log records to find the critical incidents that matter. These incidents are then presented through real-time dashboards, notifications, or reports to the security administrator.

Understand the context of every event

HP ArcSight ESM 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 the context necessary to further analyze and mitigate a breach.

ArcSight ESM also incorporates a management console that simplifies administrative tasks making the solution easy to deploy, maintain, and use. Using ArcSight ESM administrators and analysts are able to:

- **Detect more incidents**
  The new architecture will allow event correlation rates of up to five times the current performance using the same hardware.
- **Address more data**
  The new architecture will enable storage capacity of up to 10 times 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.

Correlation

HP ArcSight 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 ESM solution uses the CORR-Engine as the foundation to help security teams keep up with the speed needed for today's threat detection, security analysis, and log data management.

Highlights

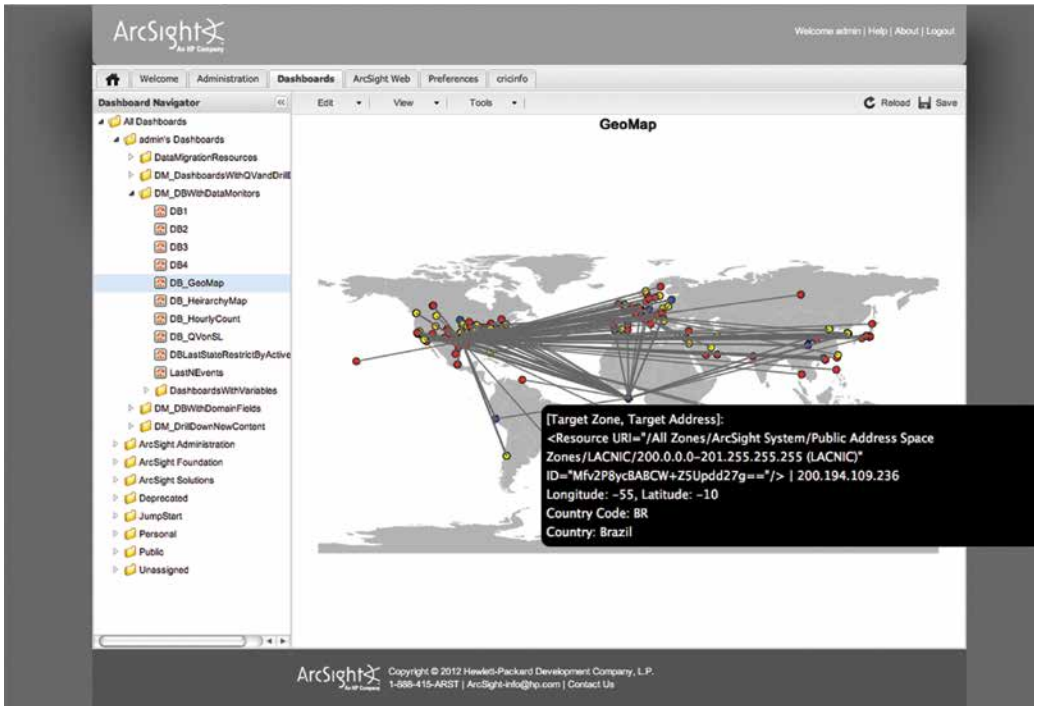
- **Collect everything: log data from any device deployed on premises or in the cloud, including SaaS companies like Salesforce, Box.net and Okta**
- **CORRe Architecture: optimized to run on multiple processors, high data compression, and faster event throughput**
- **Analyze events: high-performance interactive searches, comprehensive drill-down reports, and real-time alerting**
- **Event logs are stored more efficiently so searches and alerts happen much faster**

Features

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

- **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.
- **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 among 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.

Geo dashboard



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

Integration

The ArcSight ESM collection infrastructure offers advanced collection capability for the broadest library of event sources. Logs from any device can be harnessed, normalized for easy cross-device monitoring and analyzed. 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 provide fast, convenient, and intuitive access to information. Customizable and graphically rich dashboards provide 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 organization's overall security and risk posture.

System requirements

Supported operating systems

- Red Hat Enterprise Linux, version 6.2, 64-bit

CPU, memory, disk space

- CPU: 8–32 Intel® Core™ processor or equivalent (2.00 GHz+, 24 MB cache)
- Memory: 16–36 GB
- Disk space: 2–4 TB

Storage

- Average compression of 10:1 (dependent on data type and data source) SAS 15k RPM, RAID 10, 8+ disks

Console platform support

- Windows® XP, 32-bit
- Windows 7, 64-bit

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.

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.

HP Services

HP ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more about HP ESP Global Services at **hpenterprisesecurity.com**.

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop

Share with colleagues

4AA4-3483ENW, Created September 2012