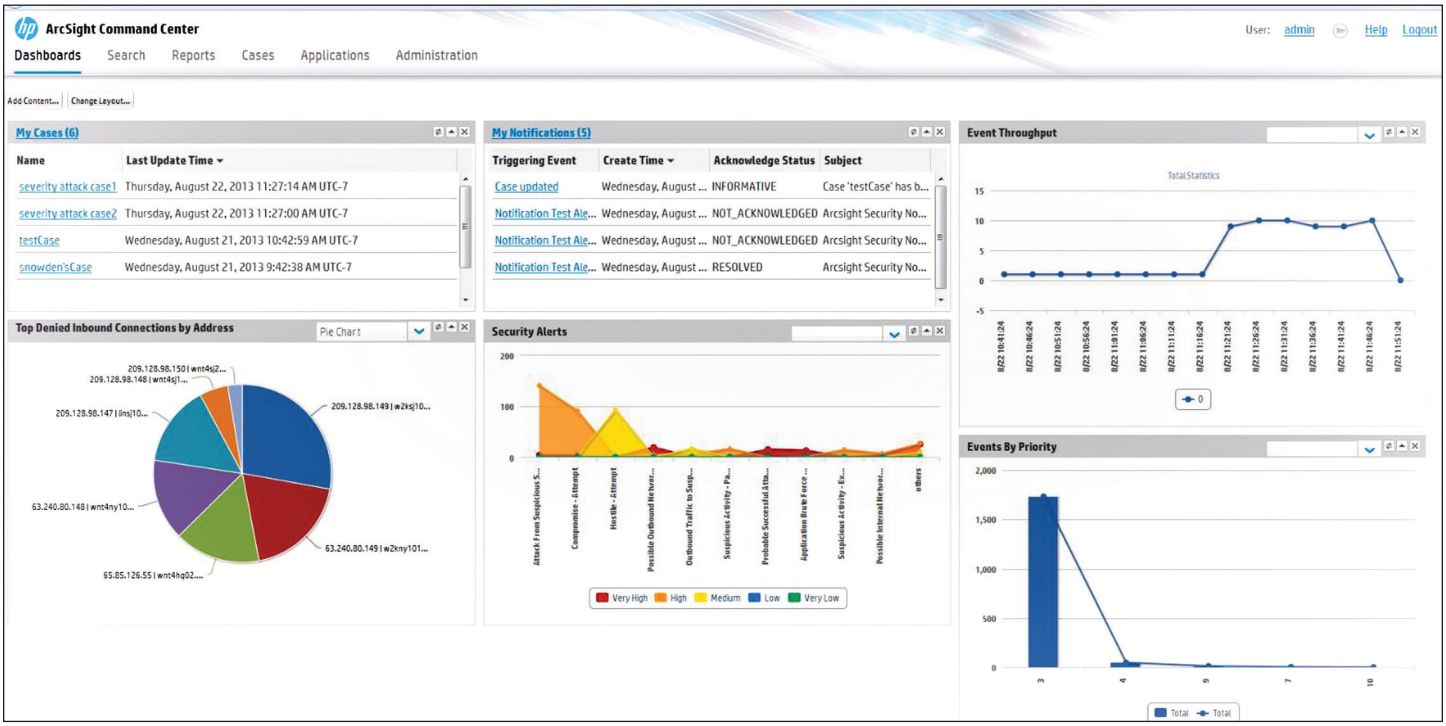
Data sheet

HP ArcSight Enterprise Security Manager

Security and compliance through Big Data analytics



Real-time analytics

HP ArcSight ESM helps you quickly isolate threats so you can triage your responses against the most urgent issues.

Highlights

- Detect and respond to internal and external threats
- Secure your IT
- Automate compliance monitoring and reporting

HP ArcSight Enterprise Security Manager (ESM) provides a Big Data analytics approach to enterprise security, transforming Big Data into actionable intelligence that can reduce the cost of a breach and help minimize risk to business.

In order for businesses to protect their critical data and intellectual assets, security teams need solutions that can provide timely, relevant intelligence to help them quickly detect and respond to breaches. Data volumes have exploded, making it difficult to identify the high-risk anomalies or trends that exist in your event logs. Cyber criminals have become more sophisticated, camouflaging their attacks inside mountains of your data.

Without the right tools, organizations cannot respond quickly, losing valuable time through inefficient analysis of forensic data after a breach. Most often, companies find out about breaches when they are notified by a third party, unaware their security systems had been compromised.

Detect threats in real time

HP ArcSight ESM is a market-leading solution for collecting, correlating, and reporting on security event information. Using thousands of different types of device and application connectors, HP ArcSight ESM provides a central point for analysis of daily business operations. Armed with all this data, the real-time correlation capabilities of HP ArcSight ESM can detect unusual or unauthorized activities as they occur. Finally, the visualization and reporting capabilities of HP ArcSight ESM support personalized dashboards and on-demand or scheduled reports for administrators, managers, or auditors.

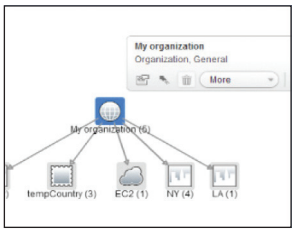
Intuitive dashboards, robust reporting

HP ArcSight Risk Insight
HP ArcSight ESM with Risk Insight delivers comprehensive technical and operational reports that 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.

Figure 1. Prioritize Security Risk using Business Criticality IT Mapping

Heat map

Asset mapping



Risk indicators

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.

Stop threats at the application layer

HP ArcSight Application View
With most threats targeting applications, HP ArcSight Application View can be used to close the security gaps that can result from improper user access and usage of applications. HP ArcSight Application View leverages the insight of HP Fortify into application security to capture the actual events directly from the application, without having to modify the application itself. This data is then correlated within the HP ArcSight platform to help your security administrators gain immediate application security event intelligence without the need for advanced customization.

The intelligence enables fast analysis of database queries, error messages, and other application-related threats that can lead to loss of confidential information or identity theft. The outcome is application security event visibility where previously there was a blind spot for your IT security team.

Automated intelligence and response

HP ArcSight Reputation Security Monitor
HP ArcSight Reputation Security Monitor (RepSM) enhances the capabilities of your HP ArcSight ESM platform by layering threat intelligence onto network flow analysis to filter out communications with malicious networks. This solution includes scenarios to aid in detection and prevention at every stage. Before a breach occurs, HP ArcSight RepSM can detect dangerous browsing of ill-reputed sites. After a breach occurs, HP ArcSight RepSM can identify infected assets or infrastructure trying to communicate with ill-reputed command and control centers. By detecting these communication channels quickly, organizations can protect their intellectual property before it is leaked out of the company.

HP ArcSight Threat Detector
Although HP ArcSight ESM comes with hundreds of pre-built rules and alerts, the agility of your security team to be able to adapt to the adversary is key to detecting advanced threats. Threat Detector enables correlation engine of HP ArcSight to processes historical activity to uncover new patterns. The engine can then auto-create new rules based on these patterns to enable you to detect new threats such as zero-day worms and misconfigurations of network devices, systems, and applications.

Threat Detector gives your analysts the tools needed to determine a suspicious event from a typical event that happens in your network. This helps customize ESM to your specific use-case, reducing the number of resources needed to maintain your security operations center. Threat Detector can look for suspicious activities often found in situations where there is an insider attack or a compromised account. Threat Detector can detect these patterns, and then create rules to catch these activities in the future, so that managers can address potential issues early.

HP ArcSight Threat Response Manager
Once your threats are identified, the race to remove these threats begins. Threat Response Manager (TRM) enables you to automate and reduce the time needed to remediate a threat. TRM gives you a single, integrated, end-to-end network, and security event monitoring solution that enables you to mitigate threats based on actionable events triggered from HP ArcSight, as well as your in-house applications. By shortening your response times, you can manage your business risk in a more proactive fashion, allowing you to reduce costs and increase flexibility in the way you deploy your systems to meet your organization's unique needs.

Add automated security compliance expertise to your team

Designed around best practices, the HP ArcSight Compliance Insight Packages provide a suite of content that delivers event and security monitoring. They help organizations meet a broad set of regulatory compliance requirements and institute a strong IT governance program that includes monitoring of internal controls, access control changes, administrative activity, login monitoring, as well as change and risk management.

They automatically map these technical checks to the relevant standards policy and operational context; this allows organizations to focus on key services and business processes, and address critical audit points. The packages deliver one of the most relevant and comprehensive set of compliance content in the SIEM market today for the following regulatory requirements:

- IT governance based on ISO/IEC 27002:2005
- Federal Information Security Management (FISMA)
- Sarbanes Oxley (SOX) and Japanese Sarbanes Oxley (J-SOX)
- Payment Card Industry Data Security Standards (PCI DSS)
- North American Electric Reliability Corporation (NERC)
- Critical Infrastructure Protection (CIP) 002-009
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Proactive compliance leverages the ongoing event collection and management requirements, and allows organizations to move beyond a "check-the-box" approach. It enables a comprehensive, automated approach for protecting the business, mitigating risk, and addressing regulatory requirements, while at the same time increasing efficiencies and reducing cost.

One unified view—one place to command and control

Universal Log Management
HP ArcSight is designed to efficiently store and analyze large volumes of enterprise log data. This universal log management solution efficiently collects and stores machine data from any log-generating source and unifies the data for searching, indexing, reporting, analysis, and retention. It supports multiple deployments such as an appliance, software, virtual machine, and within the cloud in both Windows® and Linux environment.

HP Services

Security Operation Centers
To build a successful security program, superior technologies need to be paired with a team to help run and implement their security operation centers (SOCs). These functional teams are necessary to detect and respond to attacks and breaches from multiple vectors. Mature SOCs develop and report operational metrics and key performance indicators (KPIs) to demonstrate the value of security investments. Security metrics should measure the efficiency and effectiveness of security operations. Additionally, SOCs with strong support from the business are viewed as key contributors to cost avoidance and risk reduction initiatives within the organization.

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

"The HP ArcSight solution will give us a more comprehensive threat and risk management platform that optimally enables enterprise-wide visibility to identify this type of illegal activity in progress and take prompt, preemptive action."

– Kris Herrin, CTO Heartland Payment Systems

Summary

HP ArcSight provides single view of a company's security status based on validated attacks and business risk. We help enterprises evolve their security operations by combining the best people, process, and technology. By enhancing all three essential components, we help to defend your network and business by keeping your infrastructure monitored for potential threats. Together, we can reduce your overall risk of loss due to a cyber-attack. Securing your business is hard. HP ArcSight gives you the tools to make it easier.

Why HP?

Many Fortune 100 security operations centers run on HP ArcSight technologies and implement HP ESP Global Services. With such unmatched experience in the industry, HP ESP Global Services can help your enterprise to assess the security operations capability and develop a roadmap.

Learn more at
hp.com/go/ArcSight

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-3483ENW, February 2014, Rev. 1