## News Advisory

# HP Helps Customers Disrupt Attacks with Advanced, Real-time Threat Detection

New solutions increase security effectiveness with accelerated big data analytics and real-time, application-level threat detection

Editorial contacts

**Kristi Rawlinson, HP**
+ 1 650 799 7061
kristi.rawlinson@hp.com

www.hp.com/go/newsroom

WASHINGTON, Sept.17, 2013 — HP today announced new and enhanced solutions that help organizations disrupt the life cycle of a cyberattack and improve the overall effectiveness of security operation teams through accelerated big data analytics and real-time, application-level threat detection.

The cyberthreat landscape is evolving faster than security teams can manage, causing many organizations to dramatically increase headcount and training programs. At the same time, the volume, velocity and variety of data is making it increasingly difficult to analyze and understand where security risks exist within an organization. Limited resources and failing signature-based solutions are also limit security staffs' ability to mount an effective defense.

HP delivers advanced, data-driven security technologies designed to empower security operations teams to run more efficiently.  This enables staff to focus on deriving meaningful security intelligence from big data and spend less time on system management, product deployment, risk assessment and manual vulnerability searching. New HP ArcSight solutions identify and prioritize threats faster, combine security intelligence with business intelligence, and close potential blind spots at the application layer, giving customers greater control over their security environments.

*"The exploding volume of data that organizations today must manage presents new security challenges as they try to predict, locate and disrupt cyberthreats," said Haiyan Song, vice president and general manager, Enterprise Security Products, ArcSight, HP. "The newly expanded HP ArcSight portfolio delivers solutions that help security teams and SOCs prioritize risk, automate application-level threat detection and streamline security management to reduce exposure and increase effectiveness of protecting valuable data from internal and external theft."*

**Enhanced visibility to eliminate blind spots, find efficiencies**
While security spending continues to focus on the perimeter, 84 percent of business security breaches originate at the application layer and mobile vulnerabilities have grown by 68 percent.[1] The new HP ArcSight Application View solution closes this gap by

integrating the HP ArcSight Security Information and Event Management (SIEM) platforms—HP ArcSight ESM and HP ArcSight Express—with HP Fortify Runtime to automatically detect and log application security events. This gives security operations teams first-of-its-kind visibility into the application layer, helping to block attacks on applications in real-time and preventing data loss, identity theft and IP loss from occurring.

To help organizations effectively defend against today's targeted threats and manage the increasing volume of security-related data, HP has introduced HP ArcSight Risk Insight. Incorporating key elements originally implemented in the HP ArcSight EnterpriseView product, HP ArcSight Risk Insight is delivered as an add-on to HP ArcSight ESM. The new solution helps security operations teams identify advanced attack targets, analyze current security technology deployments and weigh emerging risk to determine where to focus mitigation efforts. HP ArcSight Risk Insight aggregates the threats identified in HP ArcSight ESM into clear Key Risk Indicators (KRIs) juxtaposed with a hierarchical, business-oriented view of the infrastructure. The solution is designed to marry security intelligence with business risk and provide senior-level management teams with prioritized, strategic insight to security data with actionable intelligence to address risk.

**Streamlined security operations management for better productivity**
Security operations teams are challenged by achieving balance between operational efficiency and conducting security intelligence research, especially as the scope and complexity of their SIEM and logging deployments grow. The HP ArcSight Management Center is an enterprise-grade, centralized security management hub that enables HP ArcSight customers to effectively and efficiently manage large deployments of HP ArcSight Logger, HP ArcSight SmartConnectors and HP ArcSight Connector Appliance from a single console. The HP ArcSight Management Center helps streamline centralized configuration management and compliance, while reducing the time it takes to alter the system or implement a policy change. This allows security operations teams to more efficiently allocate scarce resources, and focus on managing threats rather than disjointed tools and products.

**Intelligence-driven threat detection through security and broader operations data**
Security operations are rapidly evolving to become highly proactive programs that head off and prevent or contain security threats before they occur. These advanced use cases require accurate modeling and binding of large disparate, data sets spanning both human and machine information to be effective.  HP Software utilizes the HP Haven platform for connecting the dots between the various big data sets to address this specific need.

The HP Haven platform consists of Hadoop for raw data storage and batch mode analysis, HP Autonomy for human generated information processing, the HP Vertica Analytics Platform for broader big data analytics, and HP ArcSight ESM for real-time security monitoring and analytics, with applications running over the platform.  A key component of the HP Haven platform is the set of data engines it offers and connects together in a

logical and effective manner, together with more than 700 connectors to a wide array of data sources.  Data collection, storage, monitoring and analysis are now possible under a single umbrella from HP Software.

The openness and flexibility of the HP Haven platform enables security operations teams to use the updated HP ArcSight Enterprise Security Manager (ESM) v6.5c to analyze security events in a broader context when used in conjunction with Hadoop, HP Autonomy or HP Vertica Analytics Platform data stores. This allows customers to benefit from an accurate prioritization of risks and anomalies as well as advanced insider threat patterns. The HP ArcSight ESM solution operates in real-time, sifting through millions of log records, correlating the data at a rate of two million events per second to find the critical events.[1]

HP ArcSight ESM v6.5c incorporates the latest iteration of the highly optimized back-end storage engine that allows faster querying to enable real-time alerts during complex searches, accelerates algorithm performance for correlation event processing and significantly improves data storage efficiency.

## Pricing and availability

- HP ArcSight Application View is available immediately worldwide. A 30-day free trial offer is available, with pricing starting at $2,000 per application following the conclusion of the trial period.
- HP ArcSight Risk Insight is expected to be available this fall.
- The HP ArcSight Management Center is expected to be available in October. A free trial version will be available for evaluation of full capabilities.
- HP ArcSight Enterprise Security Manager (ESM) v6.5c is available as hardware or software, providing flexible deployment options for any environment, and is expected to be available in October.

HP's annual enterprise security event, HP Protect, is taking place Sept. 16-19 in Washington, D.C.

HP's premier EMEA client event, HP Discover, takes place Dec. 10-12 in Barcelona, Spain.

## About HP
HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society.  With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world.  More information about HP (NYSE: HPQ) is available at http://www.hp.com.

(1)  HP Cyber Security Risk Study, 2012.

This news advisory contains forward-looking statements that involve risks, uncertainties and assumptions. If such risks or uncertainties materialize or such assumptions prove incorrect, the results of HP and its consolidated subsidiaries could differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could

be deemed forward-looking statements, including but not limited to statements of the plans, strategies and objectives of management for future operations; any statements concerning expected development, performance, market share or competitive performance relating to products and services; any statements regarding anticipated operational and financial results; any statements of expectation or belief; and any statements of assumptions underlying any of the foregoing. Risks, uncertainties and assumptions include the need to address the many challenges facing HP's businesses; the competitive pressures faced by HP's businesses; risks associated with executing HP's strategy; the impact of macroeconomic and geopolitical trends and events; the need to manage third party suppliers and the distribution of HP's products and services effectively; the protection of HP's intellectual property assets, including intellectual property licensed from third parties; risks associated with HP's international operations; the development and transition of new products and services and the enhancement of existing products and services to meet customer needs and respond to emerging technological trends; the execution and performance of contracts by HP and its suppliers, customers and partners; the hiring and retention of key employees; integration and other risks associated with business combination and investment transactions; the execution, timing and results of restructuring plans, including estimates and assumptions related to the cost and the anticipated benefits of implementing those plans; the resolution of pending investigations, claims and disputes; and other risks that are described in HP's Quarterly Report on Form 10-Q for the fiscal quarter ended April 30, 2013 and HP's other filings with the Securities and Exchange Commission, including HP's Annual Report on Form 10-K for the fiscal year ended October 31, 2012. HP assumes no obligation and does not intend to update these forward-looking statements.