HP Protects the Digital Enterprise With New Security Analytics
Wednesday, September 02, 2015 11:45:00 AM (GMT)

NATIONAL HARBOR, MD--(Marketwired - Sep 2, 2015) - Today at HP Protect, the company's annual enterprise security user conference, HP (NYSE: HPQ) is unveiling new solutions centered on security analytics and designed to help organizations shift from legacy security methods to a modern approach that focuses on protecting the interactions among users, applications and data to help protect enterprises' most valuable assets.

Organizations are inundated with security data on a daily basis and face the challenge of translating this data into meaningful insights to proactively manage threats that pose legitimate risk. With the growing volume and complexity of data, an intelligent security platform is critical -- one that harnesses the power of world-class Security Information and Event Management (SIEM) capabilities for active monitoring with use-case driven security analytics that derive actionable intelligence.

"Breach detection is top of mind for security buyers and the field of security technologies claiming to find breaches or detect advanced attacks is at an all-time noise level," said Eric Ahlm, research director at Gartner, in a recent Gartner press release. "Security analytics platforms endeavor to bring situational awareness to security events by gathering and analyzing a broader set of data, such that the events that pose the greatest harm to an organization are found and prioritized with greater accuracy[1]."

Leveraging Security Analytics to Automate Threat Data Analysis
Organizations receive an average of 17,000 malware alerts per week, and spend an average of $1.27 million annually in time and resources responding to inaccurate and erroneous threat intelligence[2]. Due to the volume of data that enterprise security professionals must monitor, approximately four percent of all malware alerts are actually investigated[2], leaving a significant gap in security coverage. Additionally, traditional endpoint security solutions and manual intervention are not intercepting all critical malware infections, leaving organizations further exposed.

To help organizations automate the analysis of threat data, HP is introducing HP DNS Malware Analytics (DMA), a unique solution designed to identify infected hosts by inspecting an enterprise's DNS traffic. Developed in partnership with HP Labs, HP's central research organization, and HP's internal Cyber Defense Center, this clientless, algorithmic-driven service uncovers infected hosts without endpoint agents, helping customers to quickly detect high-risk threats, reduce data breach impact and enhance overall security posture.

"Organizations today are faced with growing volumes of security data and without the ability to separate the signal from the noise they can fall victim to undetected malware attacks, which can have serious financial and operational impact," said Sue Barsamian, senior vice president and general manager, Enterprise Security Products, HP. "The new HP DNS Malware Analytics solution effectively puts the data science necessary to derive malware detection from voluminous DNS server events into a simple, highly efficient package for customers large and small, and when combined with the powerful HP ArcSight SIEM platform, provides next-generation SIEM capabilities to better protect the enterprise."

HP DMA rapidly identifies malware-infected hosts such as servers, desktops and mobile devices so that they can be contained before gaining a foothold in the network. The solution uses a one-of-a-kind, algorithmic engine -- as opposed to the more common rules-based approach -- to analyze the high volume of DNS records. This enables the detection of new, unknown malware while simultaneously reducing false positives by a factor of 20 over other malware detection systems[3]. This saves valuable IT time and resources, enabling customers to prioritize and remediate based on the highest risk devices.

With simple set-up and cloud reporting, HP DMA can be rapidly deployed to offer continuous threat vigilance. The solution seamlessly integrates with the HP ArcSight SIEM platform, enabling customers to harness the power of SIEM and leverage their HP ArcSight Enterprise Security Management (ESM) deployments to correlate with other contextual data, issue alerts and signal appropriate remediation.

Integrating Application Security Data for Enhanced Intelligence

To further support HP's focus on data-driven security, HP also introduced HP Fortify scan analytics, a first-of-its kind machine-learning technology that harnesses the power of an organization's application security data to improve accuracy and efficiency of application security solutions. Processing an organization's growing collection of historical application security scan results to reduce the number of issues that require an auditor's review, the solution enables customers to focus resources on fewer, higher priority tasks. This analytics technology integrates seamlessly into existing application security testing workflows, which helps to increase both the efficiency of the application security audit process and the relevancy of findings.

Leveraging Predictive Analytics to Accelerate Detection of Insider Threats
The new HP DMA and Fortify scan analytics offerings bolster HP's existing analytics capabilities announced earlier this year around user behavior analytics. HP User Behavior Analytics (UBA) provides customers visibility into user behavior to detect malicious or negligent users, or external attacks that compromise user accounts across the enterprise. Ranking detected anomalies and the associated risk, HP UBA allows customers to focus efforts and resources on the activities, users and applications that pose the greatest risk to the enterprise.

Pricing and Availability

- HP DNS Malware Analytics will be available on September 15, 2015. One-year subscriptions start at $80,000 to analyze up to 5 million DNS packets per day.
- HP Fortify scan analytics is currently available as part of HP Fortify on Demand.
- HP User Behavior Analytics is currently available, with version 1.1 of the solution, UBA Premium, released on August 30, 2015. HP UBA Premium is packaged according to base identities, starting at $250 per identity and decreasing with larger deployments.

Additional information about HP's security analytics solutions can be found at www.hp.com/software/security-analytics. More information about the full portfolio of HP Enterprise Security Products can be found at www.hp.com/go/esp.

HP's annual enterprise security user conference, HP Protect, is taking place this week from Sept. 1-4 in National Harbor, Maryland. Follow HP Security on Twitter @HPsecurity, and keep up with event happenings by following the event hashtag, #HPProtect.

About HP Security
HP enables organizations to take a proactive approach to IT security, disrupting the life cycle of an attack through prevention and real-time threat detection. With market-leading products, services and innovative security research, HP Security brings a global network of security operations centers and more than 5,000 IT security experts to help customers strengthen their security posture to minimize risk and incident impact.

Join HP Software on Linkedin and follow @HPSoftware on Twitter. To learn more about HP Enterprise Security products and services on Twitter, please follow @HPSecurity and join HP Enterprise Security on Linkedin.

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 is available at http://www.hp.com.

[1] Gartner Press Release, Gartner Says Security Analytics May Be Key in Breach Detection, April 2015, http://www.gartner.com/newsroom/id/3030818

[2] Ponemon Institute Study: The Cost of Malware Containment, January 2015

[3] Based on internal testing with production data.

This news release 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 and plans for future operations; 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, clients 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 Annual Report on Form 10-K for the fiscal year ended October 31, 2013, and that are otherwise described or updated from time to time in HP's Securities and Exchange Commission reports. HP assumes no obligation and does not intend to update these forward-looking statements.

Editorial contacts

Kristi Rawlinson
HP
Kristi.rawlinson@hp.com

www.hp.com/go/newsroom

Countries: US
Industries: Computers and Software, Computers and Software:Big Data, Computers and Software:Hardware, Computers and Software:Internet, Computers and Software:Networking, Computers and Software:Peripherals, Computers and Software:Security, Computers and Software:Software
Primary Identifiers: HPQ-US
Related Identifiers: HPQ-US