Hewlett Packard Enterprise

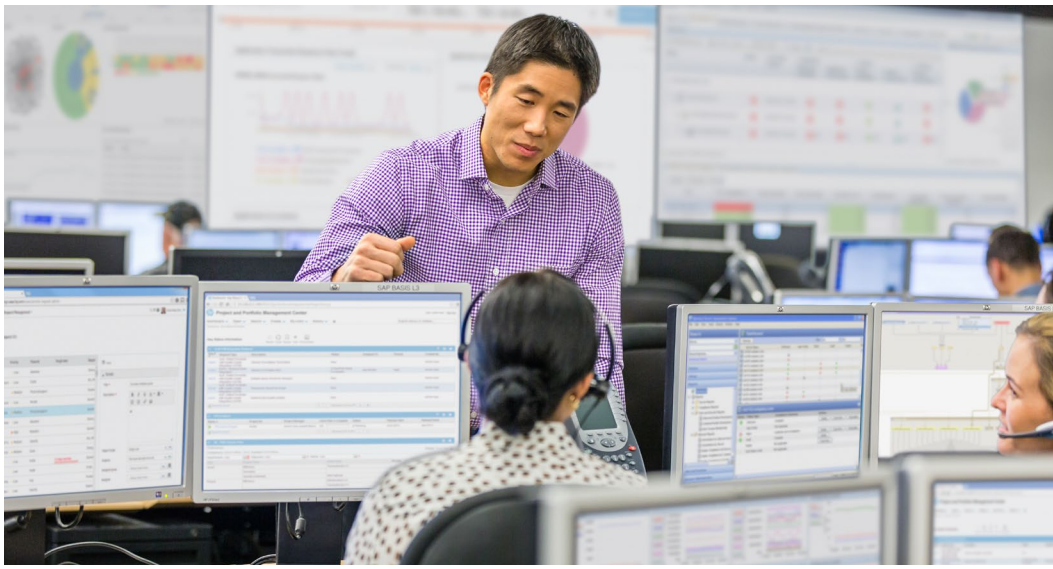
Unify collection, storage and analysis of machine data for security intelligence

HPE Security Logger Channel Promotion

Uncover and develop new prospects for log management solutions that support Security, Compliance, Operations, and Application development teams.

Elevator Pitch:

HPE Security Logger is a universal log management solution that can collect everything, analyze anything and can be used everywhere. It unifies searching, reporting, alerting, and analysis across ANY type of enterprise log data.



Typical Challenges

The log context needed to answer operational, compliance or security questions can come from many devices in the infrastructure; the physical layer (badge in/badge outs) to the host layer (local logins) and up to the application layer (email, web, transactional).

Traditional log management tools cannot be expanded to analyze logs across IT infrastructures based on the following:

- Are limited to the type of sources they can collect from
- Have been designed to solve a specific problem and are not flexible in analysis
- Are not scalable and hence cannot perform under enterprise load

Stretching these first generation log management tools imposes significant tradeoffs between log collection rates, log analysis speed, and log storage efficiency. A universal log management solution must eliminate this classic tradeoff between performance and efficiency and provide enterprise- and infrastructure-wide visibility into logs, anomalies and threats.

HPE Security Logger is the industry's leading log solution that can simultaneously address cyber-security, compliance and IT operation log management needs for enterprises of all sizes.

HPE Security Logger collects machine data from any log-generating source on your network and unifies the data for searching, indexing, reporting, analysis, and retention.

Customer Value and Benefits

HPE Security Logger offers customers:

- Single-pane-of-glass view into all logged events across the network
- Quick and easy deployment
- Simple and cost effective to use
- Supports global regulatory compliance needs
- Optimized forensic analysis for cyber-security and operational issues
- Cohesive log data for IT security, IT GRC, IT operations and log analytics

Target Partners

Partners who resell hardware and/or software can attach this log management component; allowing customers to ensure all event activity is recorded for security purposes.

Target Buyers

IT Directors and Practitioners who are tasked with managing the ongoing optimization of the infrastructure in order to align IT and business with both security and operation focus.

- Directors (IT Operations/ IT security) are focused on finding log management solutions to align with IT operations for log collection, storage, and analysis for IT security, IT GRC, and IT ops.
- Practitioners (IT Managers, IT Security, IT Risk, and IT Compliance Managers) are focused on delivery of the executive-led strategy through the audit, recommendation and implementation of products and services. They are mostly driven by reports and metrics that they can feed it to IT Directors and higher management.

Use Cases

Security Auditing and Forensics

Governments and businesses across the globe are increasingly vulnerable to cyber war, cyber theft, and cyber fraud and cyber espionage by hackers, malware, and malicious insiders. With this evolution of cyberspace, logs are even more important and can be used for forensic analysis of all types of cyber security incidents.

Security Compliance

Most organizations are subject to the cost and effort of complying with numerous industry, state and national mandates such as Sarbanes-Oxley, HIPAA, FISMA, GLBA, PCI, BASEL, the NERC CIP Standards, international data privacy laws and many more.

Streamline IT Operations

With more systems and users connected to the internet it gets difficult for IT operation teams to keep up with the demanding SLAs. In the past, teams could look at device logs in isolation, but current threats require centralized and fast forensic analysis to keep the Mean Time To Repair (MTTR) low.

Proof Points

Figure 1: 2015 Gartner Magic Quadrant for Application Security Testing (AST)

Competitive Differentiator

HPE Security Logger is the industry's preferred log management solution; bringing value through ease of installation and use, ability to scale as organization's needs grow, and strong competitive pricing making it simple to afford and enable a secure and compliant network infrastructure. It is also flexible enough to meet the needs of a small environment to your largest enterprise customer.

HPE Security Logger can be deployed in the cloud (private, public or hybrid solutions) or onsite giving customers flexibility in management and deployment options, which in the end helps manage their ongoing costs of having such a solution.

"HPE Security Logger made a mole hill out of a mountain for us. We are required by law to keep a decade worth of logs generated by thousands of devices. We were blown away by its speed in performing both structured and unstructured queries across terabytes of data."

— Priority Health

HP Security Logger Chosen Against Competitors

A survey of 468 users of HPE Security products answered the following question: "Which other vendor(s) did you consider before selecting HP Logger?"

51% Splunk	14% LogRythm
31% IBM	1% Loggly
26% McAfee	40% Open Source or freeware
16% Loglogic	19% Other

Source: Research by TechValidate June 28 2013
http://www.techvalidate.com/portals/hp-arcsight-logger-collection-of-customer-experiences

Interested in selling HPE Security Logger? Contact your HPE Security Distribution Partner or Area Channel Manager today!

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

PDF Only April 2016 — update