Hewlett Packard Enterprise

Business white paper

A universal log management solution

HPE ArcSight Logger

Table of contents

Hewlett Packard Enterprise is transforming the enterprise security landscape with its Security Intelligence and Risk Management (SIRM) Platform. The SIRM Platform uniquely leverages advanced threat research with the powerful correlation of security events and vulnerabilities. By delivering unparalleled visibility across security assets in context of business-critical processes and applications we help our customers manage their risk and maximize their security investments.

A record of digital fingerprints

Digital fingerprints are generated by employees, customers, contractors, partners, or even intruders as they use enterprise systems, databases, websites, applications, and physical security infrastructure. These digital fingerprints, commonly known as events or logs, can be used in:

- Streamlining IT operations, by capturing and indexing all IT data to help manage applications, servers, and enterprise infrastructure
- Simplifying application development, by providing fast forensic analysis on faults, code exceptions, errors, and connectivity issues
- Combating cyber crime, by allowing unified analysis across all types of data for forensic investigations
- Demonstrating regulatory compliance, through audit-quality data collection, storage, and reporting

Despite these tangible benefits of log management, organizations continue to struggle with the volume and usage of log data for ongoing operations. To date, no single solution has been able to address the differing needs of security, compliance audit, IT operations, and application development teams. Multiple products are typically deployed in an organization to handle each area, resulting in fragmented analysis, IT overspending, and increased business risk. This white paper discusses the requirements for a universal log management solution and specifically describes how HPE ArcSight Logger delivers on those requirements. A recent cyber espionage incident at Boeing Corporation is highlighted as an example.

The growing demand for a universal log management solution

Computer system and application logs have been around for a long time and are older than the Internet, older than the world's first firewall, and essentially as old as any computer system around the globe. They have traditionally been used for troubleshooting. Today, the nature and complexity of our modern networks have resulted in more data, transactions, and users online. Governments and businesses across the globe are increasingly vulnerable to cyber war, cyber theft, cyber fraud, and cyber espionage by hackers, malware, and malicious insiders. With this evolution of cyberspace, logs can now be used for forensic analysis of all types of cyber security incidents. The key requirement is comprehensive collection, centralized storage, and fast analysis of all log events from various devices and applications.

Recent research by the U.S. Cyber Consequences Unit indicates that the destruction from a single wave of cyber attacks on critical infrastructure could exceed $700 billion, the equivalent of 50 major hurricanes hitting U.S. soil at once. The real problem is that over 75 percent of the critical infrastructure is owned by the private sector and is de-regulated (as identified by the Homeland Security Presidential Directive-7). This example clearly shows how and why security and regulatory compliance is interrelated. 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. Most of these regulations require data retention for multiple years, as shown in Table 1. Effective and efficient log management can simultaneously address multiple regulations, and hence, greatly reduce time and cost of regulatory audits.

Effective log management also helps in quick resolution of fault, configuration, accounting, performance, and security (FCAPS) operational issues. Only 20 percent of mission-critical application downtime is caused by technology/environmental failure or a natural disaster; the other 80 percent is caused by people or process failures (Source: Gartner, 2009). For example, a nuclear power plant in the state of Georgia, USA, was forced into an emergency shutdown for 48 hours after a software update was not properly installed (Source: Washington Post, 2008). Part of this 80 percent can be due to cyber security issues, but the balance is simply because of poor change and application management. Since logs maintain an audit trail of all the changes made to various systems, they can help immensely in forensic analysis and faster resolution of IT operations issues.

Historically, log analysis for operations, security, and compliance were treated as separate domains. Log analysis was largely asset-centric, and adoption of commercial tools was specific to an IT group and its managed assets. Solutions were designed to collect logs from specific sources and were optimized to solve a particular problem. However, these tools are inadequate to tackle the current challenges.

Table 1. Data retention requirements for regulated data, as interpreted by HPE ArcSight

REGULATION	RETENTION REQUIREMENT
SOX	7 years
PCI	1 year
GLBA	6 years
EU DR DIRECTIVE	2 years
BASEL II	7 years
HIPAA	6/7 years
NERC CIP-002 TO CIP-009	3 years
FISMA	3 years

Today, the questions that need to be answered through log analysis are increasingly user-centric and can span any and all infrastructure. Traditional log management tools cannot be expanded to analyze logs across the enterprise because they are limited by the type of sources they can collect from; have restricted search/reporting capabilities intended to solve very specific problems; are not scalable; and breakdown under modern loads and scale.

Stretching first generation log management tools imposes significant trade-offs between log collection rates, log analysis speed, and log storage efficiency. A next-generation, universal log management solution must eliminate the classic trade-off between performance and efficiency, and provide enterprise and infrastructure-wide visibility into log data for all teams. Unlike point solutions, it should be flexible enough so that it can be either used by individual teams or expanded into an enterprise-wide log management solution when needed.

Figure 1. Security, compliance, and IT operations are inter-related.

Six requirements for selecting your universal log management solution

A universal log management solution must be flexible enough to simultaneously address the demands of the security, compliance, application development, and IT operations teams. It must be able to capture, store, and analyze all of the log data within an organization. But not all log management solutions are created equal; some treat symptoms in isolation and expose organizations to greater risks. Market conditions demand a single universal log management tool featuring an essential set of requirements to process every event in the enterprise.

Capture and index everything

The first step to any log analysis is comprehensive log collection. Logs are generated in a variety of formats, as shown in Figure 2. For collection, log management solutions should support all the possible methods, including agent-based and agent-less collection. They should not only collect the live feeds but also support collection of past data from file-based storage or from syslog.

Analyze today, prepare for tomorrow

Although logs have proven to be of great value, there has not been much effort to standardize log formats across devices. Each device has its own log format, which might be completely different from a similar device from another vendor, or other devices from the same vendor. As such, no one can humanly understand all the logs from all the devices across the globe. However, log management solutions can play a key role by converting all these different formats into a unified format so that analysts have to learn only one format, rather than a few thousand different formats. This normalizing and categorizing of log formats "future-proofs" all of your audit and monitoring content from vendor swap-outs, and completely removes the need for device expertise. Figure 3 provides an example of what is seen both with and without normalization and categorization of logs. Categorization also simplifies analysis. For example, a simple query on "modify configuration" can return all the logs from all the devices that were impacted by a configuration change.

Figure 2. Comprehensive collection and analysis of structured and unstructured data

Table 2. Normalization and categorization enables "future-proofing" and fast and efficient forensic analysis.

Without normalization

Jun 17 2010 09:29:03: %PIX-6-106015: Deny TCP (no connection) from 10.50.215.102/15605 to 204.110.227.16/443 flags FIN ACK in interface outside

Jun 17 2010 14:53:16 drop gw.foobar.com >eth0 product VPN-1 & Firewall-1 src xxx.xxx.146.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49

WITH NORMALIZATION

Time	Name	Device vendor	Device product	Category behavior	Category device group	Category outcome	Category significance
6/17/2010 9:29	Deny	CISCO	Pix	/Access	/Firewall	/Failure	/Informational/Warning
6/17/2010 14:53:16	Drop	Checkpoint	Firewall-1/VPN-1	/Access/Start	/Firewall	/Failure	/Informational/Warning

Operate without compromise

Most log management tools support fast log analysis only by compromising collection rates and storage efficiency, or by requiring more hardware. Traditional log management solutions have involved this trade-off because of the interdependency among those three things. Products optimized for storage usually involve compression, which slows down the collection and the analysis. On the other hand, fast analysis would dictate indexing, which in turn blows up the storage. An ideal log management solution should eliminate this trade-off and offer fast collection along with ultra-fast analysis and efficient storage.

Store using intelligent storage

Once the decision is made to capture all logs across the enterprise, the data must be stored efficiently and effectively. Organizations that implement homegrown log infrastructures often end up with silos of distributed log servers that are very hard to manage. Given regulatory requirements for data retention, an organization's log infrastructure can quickly reach multi-terabytes. Log management solutions should also allow leveraging of external SAN/NAS/DAS storage, and any bundled storage should come with built-in RAID protection for failover. To be completely flexible, the solution should support popular protocols like NFS and CIFS for archiving of old data. Finally, retention policies should be automatically enforced based on the device type and duration mandated by specific regulations, with the ability to extend the life of the logs in the event of impending litigation.

Collect securely and reliably

Logs are increasingly used during audits and litigation; therefore, organizations must be able to demonstrate the confidentiality, integrity, and availability of log data in transit and at rest. To easily demonstrate audit quality, collection has to occur close to the event-generating sources, which highlights the importance of distributed collection. Log collection infrastructure in remote locations should provide buffers and reliable transfer to prevent data loss when network connectivity to the data center is lost. Once the connectivity is restored, bandwidth controls help in prioritization of real-time transactional logs over transfer of stale log events.

Also look for the ability to preserve logs in their original form. The ability to prove that captured logs haven't been modified or tampered with is another key audit quality best practice. When received, raw unaltered log data collected from across the enterprise is subject to integrity checks using the NIST 800-92 (log management standard) approved SHA-1 hashing algorithm. Finally, high availability measures such as failover capabilities from one data center to another can further minimize data loss.

Correlate, investigate, remediate

Log management is frequently used in conjunction with real-time, cross-device correlation of events for detecting perimeter and insider threats. It is therefore critical that your log management infrastructure integrates seamlessly with your security information and event management (SIEM) investment because very often the users are the same, and certainly the underlying data (logs) is the same.

The integration should be bi-directional, allowing the log management solution to forward the relevant subset of events to the SIEM tool for further analysis. In turn, your SIEM tool should be able to send events representing detected (i.e., correlated) threats back to the logging appliance for search, reporting, and archival. To enable a chain of custody, communication between the log management and SIEM infrastructure should be reliable and secure. Finally, both investments should leverage a common collection infrastructure to avoid unnecessary deployment and maintenance overhead.

The first universal log management solution

HPE ArcSight Logger is a universal log management solution that unifies searching, reporting, alerting, and analysis across any type of enterprise log data—making it unique in its ability to collect, analyze, and store massive amounts of data generated by modern networks.

The solution provides an easily searchable, high-performance log data repository to aid in faster forensic analysis of cyber security, application development, and IT operations issues, and efficient and intelligent storage to simultaneously address multiple regulations. The solution enables any type of organization to:

- Streamline operations, by capturing and indexing all IT data to help manage applications, servers, and enterprise infrastructure
- Simplify application development by providing fast forensic analysis on faults, code exceptions, errors, and connectivity issues
- Combat cyber crime, by allowing unified analysis across all types of data for fast detection and mitigation of cyber attacks
- Demonstrate compliance, through audit-quality data collection, pre-packaged reporting, and efficient storage of years' worth of regulated data

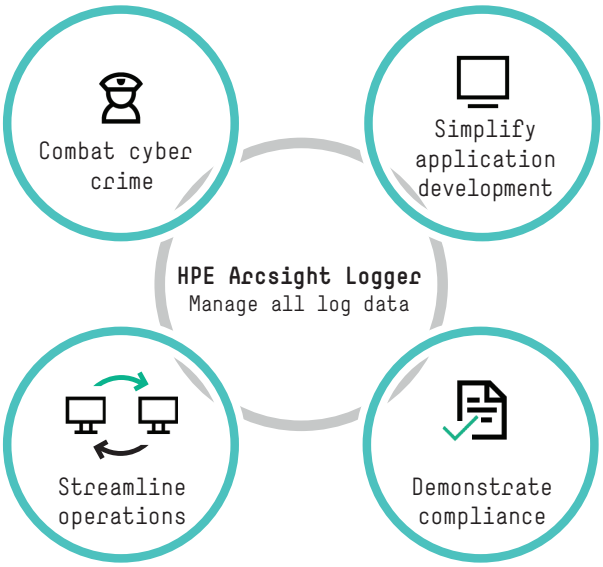


Figure 3. HPE ArcSight Logger is the universal log management solution for preventing cyber crime and addressing compliance, application development, and IT operations issues.

HPE ArcSight Logger is the industry's first universal log management solution and it supports both appliance and software deployment options.

HPE ArcSight Logger delivers:

- Fast collection—captures log data at sustained rates in excess of 100,000 EPS per instance
- Comprehensive log aggregation—raw log data as well as optimized out-of-the-box collection for over 300 distinct sources
- Audit—quality log retention—secure collection and storage, integrity checks, fine-grained access controls, and automated retention policies
- Powerful analytics—high-performance interactive searches across all data formats, comprehensive reporting, and real-time alerting engine with pre-packaged cyber crime, compliance, application development, and IT operations content
- Cost-Effective storage—captures, stores, and searches up to 42 TB of effective log data per instance with an average compression rate of 10:1, enough for years of reporting
- Advanced protection—complies with emerging federal requirements for cryptography (FIPS 140-2) and unified access (CAC)

Streamlining your IT operations

Traditional log management solutions have focused primarily on search of unstructured data for IT operations scenarios. HPE ArcSight Logger combines unstructured search with structured search to enhance the power of investigations. HPE ArcSight Logger can capture and index all IT data to bring silos of logs into a centralized location for efficient searching, reporting, and alerting and faster resolutions of fault, configuration, accounting, performance, and security (FCAPS) issues.

This helps to keep the mean time to repair low, and also helps in key use cases such as:

- Application management
- Usage and user management
- Change management
- Network and infrastructure management
- Virtualization management

HPE ArcSight Logger leverages the HPE ArcSight Common Event Format (CEF) that does not require familiarity with source-specific log formats—thereby avoiding the need for device- or vendor-specific analysis or knowledge.

For example, a simple search of "modify configuration" on HPE ArcSight Logger returns all the logs from all the devices that were a result of a configuration change (see Figure 4).

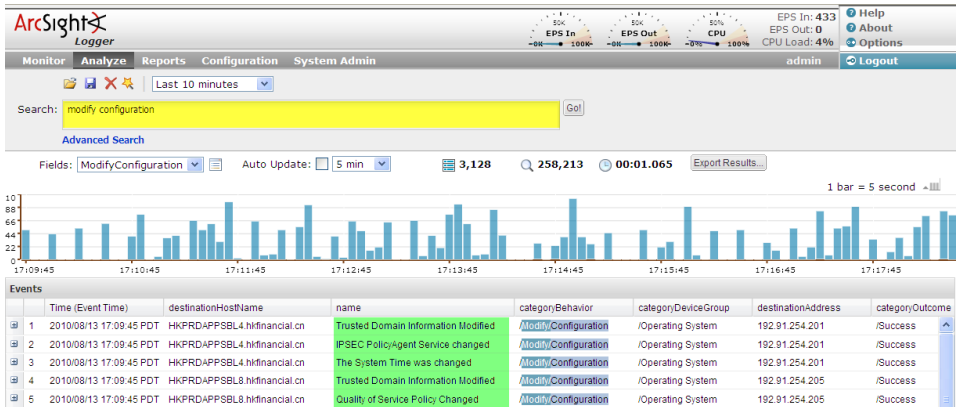


Figure 4. With HPE ArcSight Logger, users can simply search on "modify configuration" to return all logs that were a result of a configuration change.

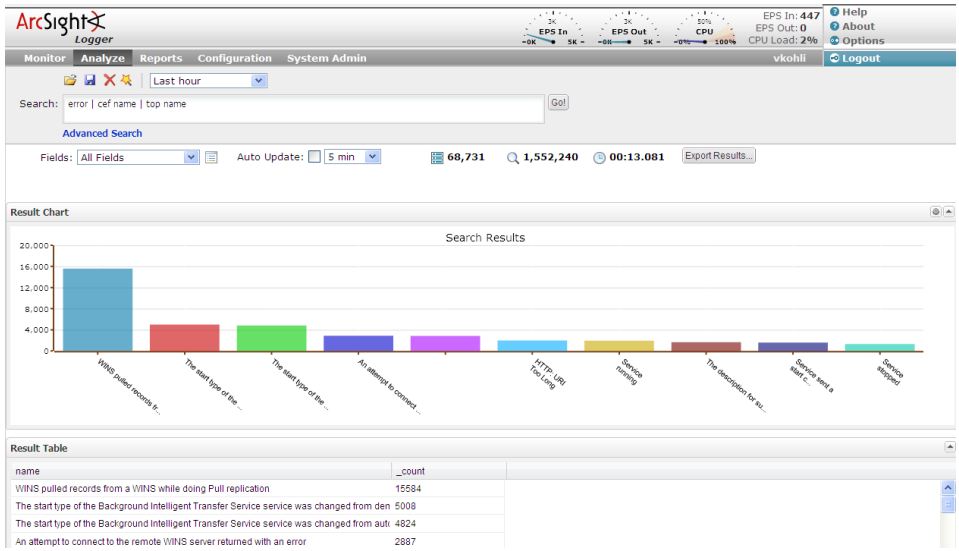


Figure 5. An example of a quick search using HPE ArcSight Logger

Simplifying application development

HPE ArcSight Logger assists in managing already-deployed applications, as well as the deployment and development process itself. It can be used for fast forensic analysis on faults, code exceptions, errors, connectivity issues, etc. HPE ArcSight Logger provides additional value by converting proprietary application log formats into a simple, plain English language that eliminates the need for experts at every level of analysis. For example, Figure 5 shows a quick and simple search on "error | cef name | top name," which returns a chart displaying the top errors and their descriptions.

Built to combat cyber crime

Three main features make HPE ArcSight Logger unique in its ability to combat cyber crime.

- **Universal event collection**
  HPE ArcSight Logger supports collection of raw or unstructured logs from any syslog or file-based log source, and also leverages the vast library of HPE ArcSight Connectors to collect structured data from over 300 distinct log-generating sources. Additionally, the HPE ArcSight FlexConnector framework extends log collection capabilities to custom sources and in-house applications.
- **Simple and fast investigation**
  HPE ArcSight Logger enables unified analysis across all types of data (structured and unstructured) in a "single pane of glass" via a Google™-like interface. In addition to simplicity, HPE ArcSight Logger provides ultra-fast searching (millions of events per second) and reporting capabilities, handling terabytes of data in seconds.
- **Real-time alerts and bi-directional SIEM integration**
  Detection of subtle and sophisticated cyber attacks often requires powerful multi-event correlation. To handle the broadest array of cyber security scenarios, HPE ArcSight Logger provides a series of real-time alerts, as shown in Figure 6, and can integrate with any SIEM offering. More specifically, HPE ArcSight Logger integrates bi-directionally with the market-leading enterprise threat and risk management offering, HPE ArcSight ESM, and is packaged along with HPE ArcSight ESM into HPE ArcSight Express. HPE ArcSight is unique in offering a tightly integrated platform for both log management and SIEM, which together leverage a common collection infrastructure for low total cost of ownership and high return on investment.

When compliance counts

HPE ArcSight Logger is shipped with built-in rules, reports, and dashboards that can be used for compliance, cyber security, application development, and IT operations monitoring. Additional content specific to regulations, such as PCI and SOX, are available as solution packages and are mapped to well-known standards, such as NIST 800-53, ISO-17799, and SANS. For faster audits, HPE ArcSight Logger provides role-based or personalized dashboards that combine relevant reports into a single console. From these summary dashboards, users can drill into specific reports and simulate audit workflow (see Figure 7). The logical flow across different forms of analysis eliminates the need to build new content at each stage of an investigation. Lastly, HPE ArcSight Logger supports multiple data retention policies that can be automatically enforced.

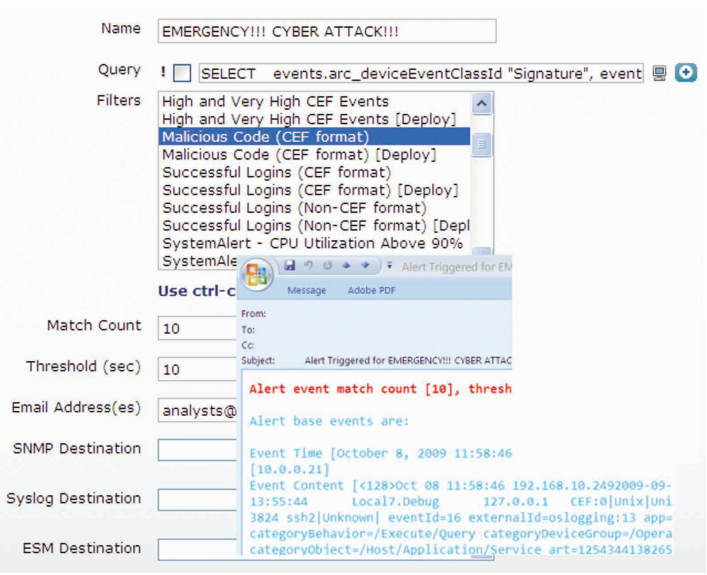


Figure 6. Real-time alerts over SNMP, SMTP, syslog, and Web console

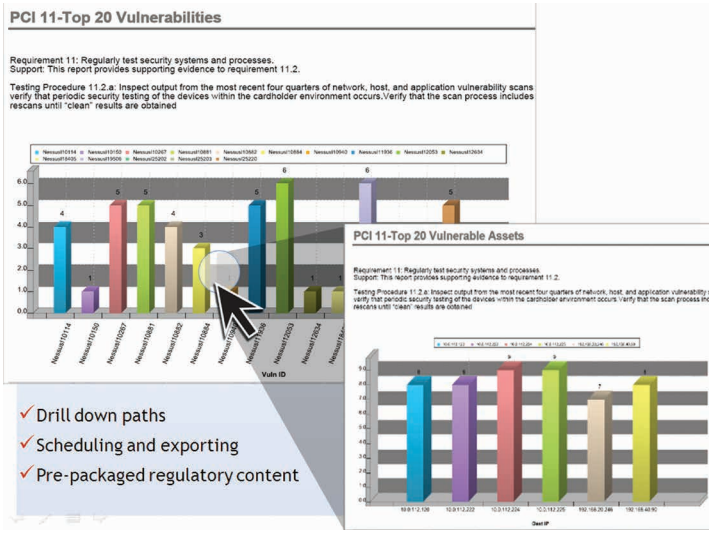


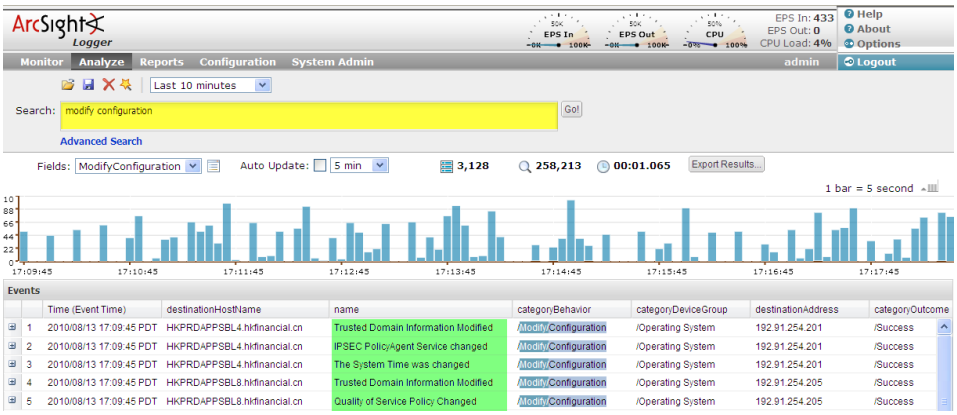
Figure 7. Automated audits with HPE ArcSight Logger

Digital fingerprints paint the complete picture

Global enterprises are leveraging the capabilities of HPE ArcSight Logger, both within and beyond the security, compliance, application development, and IT operations units. The following section highlights a use case where HPE ArcSight Logger, with its unique combination of structured and raw-text advanced search capabilities, might have been used to avoid a cyber espionage incident.

A case for universal log management

In July, 2009, a former Boeing engineer, Dongfan "Greg" Chung, was found guilty of economic espionage for giving aerospace trade secrets, including data about the space shuttle, to the People's Republic of China. Chung joined Boeing as a part of an acquisition, retired after working for more than 30 years, and then returned as a contractor. This example exposes two classic angles within cyber espionage-contractors and "trusted" employees.



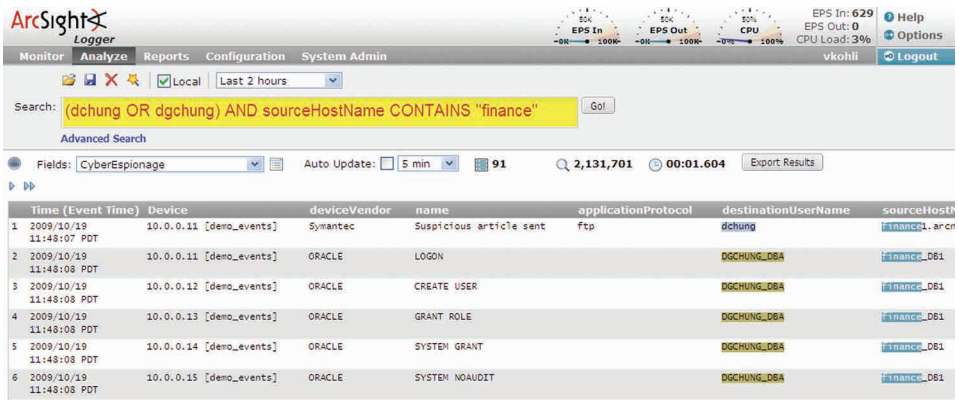
Step 1. All activities by Greg Chung using any of his identities, via unstructured search

The next level of analysis could require reviewing the employee's activity to look for trends of unauthorized or confidential systems access. This search would be both difficult and time-consuming for an organization with a large volume of event logs generated across data centers and consolidated at many discrete locations. An employee can generate a lot of activity within a short timeframe, and that data would most likely be distributed throughout the enterprise's IT network and various system components. Centralized collection by HPE ArcSight Logger simplifies this tedious task to a simple search, as shown in Step 2.

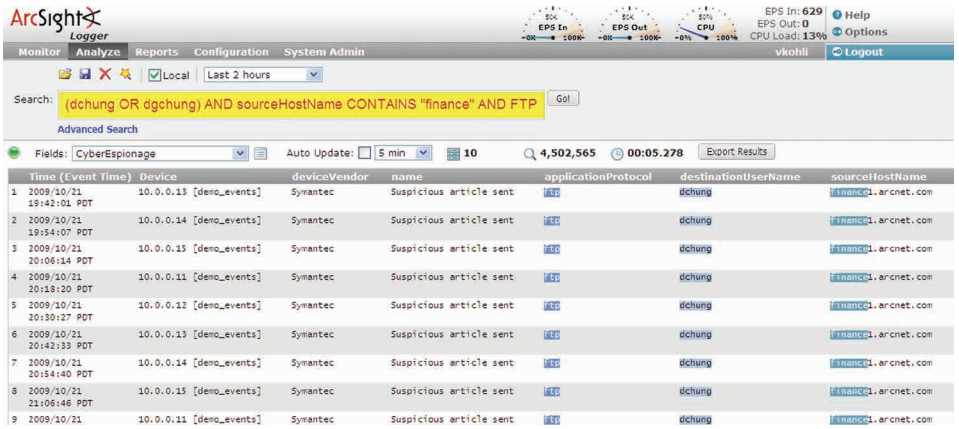
For obvious reasons, senior management would need visibility into systems and data that Chung accessed to find the total scope of the problem. At first glance, this may appear simple: scanning logs to determine what files were downloaded and what hosts and applications were accessed by Chung. However, it soon becomes clear that many types of network activity need to be analyzed to determine if Chung also changed configurations, planted hidden executables, opened a backdoor to the network, or did something unassociated with his normal level of access.

In such investigations, the request will typically show up as, "Show me all activity conducted by the employee during the last week/month/year." This search might be impossible to do in absence of a centralized log repository, but it is extremely easy with HPE ArcSight Logger, as shown in Step 1.

The last analysis step might be to find out from these logs where Chung uploaded something using FTP, as shown in Step 3.



Step 2. All activity related to Step 1 AND financial system being sourceHostname, via structured search



Step 3. All activity related to Step 1 AND Step 2 AND Protocol being FTP, via unstructured search

HPE ArcSight Logger can collect, efficiently store, and provide interactive searching and reporting capabilities across the entire log data set. The search can span all HPE ArcSight Logger appliances distributed across the organization. As shown in the three steps, this particular request would entail one simple search on potential user names or identities that Greg Chung held, combined with the logs for when he accessed confidential systems and uploaded financial documents using FTP. Results are presented as exportable, audit-quality data that can then be drilled into for further analysis or saved as real-time alerts for future notifications. Depending on the type of forensic analysis, users might want to switch back and forth between structured and unstructured data searches. Whether analysts need to go back a few weeks or a few years, HPE ArcSight Logger makes it simple to fulfill any ad hoc search against enterprise log data. The described scenario is a classic security example; HPE ArcSight Logger is being used by enterprises around the world for numerous use cases around cyber security, compliance, application development, and IT operations.

Getting started with HPE ArcSight Logger

Download, install, and get instant value with HPE ArcSight Logger at hpenterprisesecurity.com/products/hp-arcsight-security-intelligence/hp-arcsight-logger/. The downloadable version 1 of HPE ArcSight Logger provides access to all enterprise features for a full year. Using this version, organizations can collect up to 750 MB of log data per day and store up to 50 GB of compressed logs. The product also comes with 90 days of phone and email support and access to the HPE ArcSight Logger user community. At anytime during the year, customers may upgrade to an enterprise version.

The end of the piecemeal approach

Logs contain the secrets of everything that happens within an enterprise and can be of great value if utilized to their full capacity. Log management has become critical to use cases around security, compliance, application development, and IT operations. Therefore, a piecemeal approach, using one product for IT search, one for application development, and another for security and compliance, simply wastes resources and increases risk. The ability to rapidly access and search log data anywhere in the enterprise provides the contextual information needed to augment evidence collection; gain visibility into network, system and application health, and availability; and improve network and system troubleshooting activities.

About HPE Enterprise Security

HPE is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market-leading products from HPE ArcSight, HPE Fortify, and HPE TippingPoint, the HPE Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats. Visit HPE Enterprise Security at hpenterprisesecurity.com.

HPE ArcSight Logger is the industry's first universal log management solution. It helps organizations to capture everything, analyze anything, and can be deployed everywhere. HPE ArcSight Logger stores the log data efficiently with compression and data protection, integrity and access controls; and is easy to deploy, use, scale, and maintain.

For the download availability of HPE ArcSight Logger in your country, please visit hpenterprisesecurity.com/products/hp-arcsight-security-intelligence/hp-arcsight-logger/.

Learn more at
hp.com/go/getconnected

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

© Copyright 2012, 2015 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google is a trademark of Google Inc.

4AA4-1796ENW, November 2015, Rev. 1