HP ArcSight Application View

Prevent the application security threat visibility gap

In many organizations, Security Operation Center teams have little to no visibility into application security events, especially for custom applications. It's a huge problem because your security teams can't protect your organization from what they can't identify. HP ArcSight Application View solves this by helping your organization gain greater application visibility and security intelligence through the combined security capabilities of HP Fortify Runtime Application Logging and HP ArcSight Enterprise Security Manager (ESM).

Application event logging

The best place to detect, understand, and mitigate threats to applications lies in the software itself. That's the focus of HP ArcSight Application View. This unique solution automatically monitors your applications to provide you with threat intelligence feeds that help you defend your applications and data against threats that would otherwise be unknown.

HP ArcSight Application View combines application-level security event logging for virtually any application, which is especially valuable for legacy or custom applications. The solution leverages and enhances the logic in your software to accurately capture, identify, and correlate threat-related events. It also provides user behavior and transactional logging for security analysis. With out-of-the-box content, your security administrators can immediately see application-level events, reports, and correlated dashboards that shine a light on what has often been an application blind spot in terms of security event visibility.

Your visibility extended

With the HP ArcSight Application View solution, your security administrators can gain immediate application security event intelligence without the need for advanced customization. If you're an existing HP ArcSight ESM or Express customer, Application View truly extends the value of your investment by further leveraging ESM with correlated application security data for your IT security operations center (SOC) team.

No other solution on the market can provide true application-level visibility of security events that are then analyzed and correlated to identify irregular internal or external application usage that would otherwise go undetected. The intelligence provided enables fast analysis of database queries, error messages, session login/logout, and other application-related threats that can lead to loss of confidential information, identity theft, and other malicious activities.

User access and application usage

With the evolution of threats targeting applications as the weakest link in the security ecosystem, HP ArcSight Application View can be used to help close the security gaps that can result from improper user access and usage of applications. For example, it might be acceptable for a user to access an application during regular business hours, but why is the user accessing it 100 times Saturday at midnight?

HP ArcSight Application View reconciles that problem by capturing the events from the application and integrating the data into dashboards and reports within ESM. Why did a user log in twice just five minutes apart from two different locations? Do you know? Is that a threat? With HP ArcSight Application View you will know and can take action based on that data. This capability helps you prevent data theft, IP theft, and other potentially fraudulent activities.

Figure 1. HP ArcSight Application View provides a new level of security event visibility
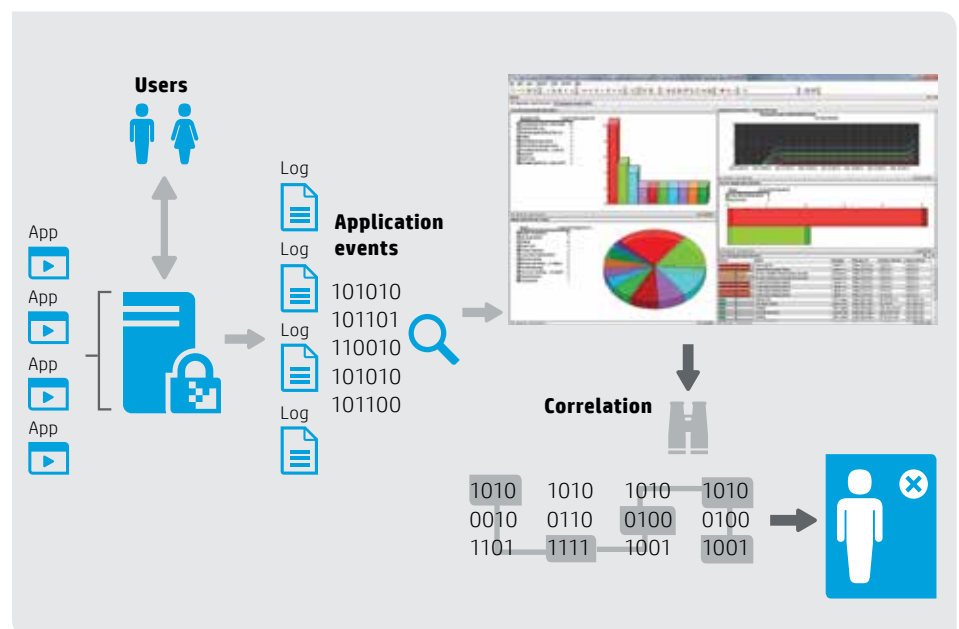
Uniquely HP

While other solutions might be able to monitor an application and layer 7, they cannot capture the actual events from the application, events that are then correlated within ESM for unparalleled application security event intelligence. Other solutions might be able to tell you that you have a headache, Application View can tell you exactly what is causing your headache. Which level of detail do you prefer for your organization?

Key benefits: HP ArcSight Application View

Building on the power of HP Fortify Runtime and HP ArcSight ESM, HP ArcSight Application View:

- Makes existing ESM deployments more valuable by feeding in application security events for correlation and analytics
- Immediately increases visibility and reporting of security-related application events with out-of-the-box content rules
- Enhances borderless collection from virtually any application, especially custom applications, with ESM logging capability
- Captures application security events through extensible contextual content rules

Key capabilities: HP ArcSight ESM and Express

HP ArcSight ESM and Express:

- Provides comprehensive log and data collection from virtually any device or application with more than 350 connectors available
- Supports detailed compliance reporting and audit reporting for SOX, PCI, HIPPA, and other regulatory requirements
- Offers advanced data normalization capabilities to identify contextual behavior across systems
- Enables in-depth correlation from user roles to anomaly detection to identify today's advanced threats
- Provides enterprise-level management console visibility and event scalability (terabytes of log data)

Powered by the HP Fortify Runtime Platform

- Provides advanced application logging rules and integration with ArcSight ESM for event visibility
- Monitors sessions and user behavior from the application itself for the deepest level of event security
- Enables custom applications with logging capabilities to remove the application blind spot
- Facilitates continued research and rules from HP Software Security Research for user activity, file access, security exceptions, and more
- Supports security event feeds to HP Fortify Software Security Center

How HP ArcSight Application View can help you; consider these benefits

Application security event visibility
With HP ArcSight Application View, you gain visibility into application misuse and threats. The Application View solution leverages market-leading HP Software Security Research, integrated rules, and predefined analytics to tell your security teams exactly what security events are taking place within your organization's applications.

Custom application logging
Many custom or legacy applications were not designed with application logging capabilities. HP ArcSight Application View provides logging capabilities immediately without the need for any customization. You gain immediate application security event visibility and intelligence where there was previously a blind spot for your application security team.

Prebuilt reports and dashboards
HP ArcSight Application View provides out-of-the box reports, dashboards, and drill-down capabilities so that your security team can immediately assess security threats without the need for customization.

Identify and prevent unauthorized user access to applications
Identifying threats based on user access to applications is a challenge that HP ArcSight Application View solves. By capturing user-related events for applications, the Application View solution provides details on potentially fraudulent activities, such as brute-force login attempts, geo-location user discrepancy, data leakage, and more.

About HP Enterprise Security

HP 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 HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats. Find out more at hp.com/go/SIRM.

About HP Fortify

HP Fortify offers comprehensive SSA solutions featuring the broadest line of products and services in the market today. HP Fortify solutions help you build trust in the software you depend on by helping you find, fix, and fortify applications in less time and for less cost than comparable tool-centric strategies. Find out more at hp.com/go/Fortify.

About HP ArcSight

HP ArcSight offers a suite of products designed to help organizations understand who is on their network, what information they are seeing, and which actions they are taking with the information. Three hundred sixty degree security monitoring to detect incidents empowers a level of visibility that can protect the business while reducing operating costs. Find out more at hp.com/go/arcsight.

Learn more at
hp.com/go/appview

Sign up for updates
hp.com/go/getupdated

Share with colleagues   Rate this document