SOLUTIONS DATA SHEET

DIGITALGUARDIAN™
Data Protection Integration with HP ArcSight

DATA EVENT VISIBILITY ACROSS ALL ENDPOINTS

Key Benefits

- Closes visibility gap on the endpoint by delivering a rich event data stream to uncover insider and outsider attacks
- Quickly and effectively delivers prevention and containment controls stopping threats uncovered in ArcSight

THE NEED

Correlating network and system vulnerability models with data sensitivity and usage enables a single reporting view for enterprise data protection. Combining events, logs, and information from the network and endpoints, including user trending, endpoint risk scores, and data-at-rest information, allows enterprises to detect and contain insider and outsider threats to sensitive information.

THE DIGITAL GUARDIAN SOLUTION

Digital Guardian is a scalable platform that protects sensitive business data against insider and outsider threats while enabling secure data sharing and collaboration across physical, virtual, mobile, and cloud environments. Digital Guardian endpoint agents classify data as well as audit and control data usage to provide contextual awareness of endpoint and user activity.

Digital Guardian classifies data based on content, context, and user input and tags files accordingly. Data classification enables a data-centric approach to security that allows differentiated policies to provide effective controls without breaking business processes or affecting user productivity.

Digital Guardian endpoint agents enforce data access control policies using a number of mechanisms, including user warnings and blocking, as well as enterprise encryption. Digital Guardian's key management capabilities can transparently encrypt and decrypt information as it is used in normal authorized business processes. File encryption ensures that sensitive data is secure on user devices and removable media.

HP ARCSIGHT

The HP ArcSight Security Intelligence platform is a unified security solution that helps safeguard businesses by giving complete visibility into activity across the IT infrastructure, including outsider threats such as malware and hackers, insider threats such as data breaches and fraud, risks from application flaws and configuration changes, and compliance pressures from failed audits.

ARCSIGHT AND DIGITAL GUARDIAN 1+1=3

With ArcSight CEF integration, Digital Guardian provides a rich event data stream from laptops, desktops, and servers. Forensic logs of data usage events include the users and applications that accessed the data, the data events that occurred, and the classifications of the data itself. Exporting this data stream into ArcSight allows correlation with other security event data from the network, enterprise applications, and other backend systems, dramatically increasing visibility for detecting insider threats and malware, and satisfying containment use cases.

DIGITALGUARDIAN™
by VERDASYS

For more information, visit
www.digitalguardian.com

INSIDER THREAT USE CASE

Digital Guardian provides ArcSight with a rich stream of data usage events and alerts, delivering visibility into user and data event activity on endpoints, including:

- File names
- Data types and sensitivity
- User names and groups
- Applications used to access data
- Types of actions (such as email, upload, print, copy)
- Other contextual attributes

This data enables ArcSight users to answer questions such as "Where does my sensitive data reside? Who is moving this data outside the enterprise? What applications are they using?" By correlating Digital Guardian events and alerts, ArcSight enables detection of advanced insider threat scenarios such as a malicious user transferring a number of sensitive files one by one to different cloud storage solutions to evade detection. Digital Guardian's data classification and persistent tagging means that even attempts to obfuscate the data through encryption or by hiding the data within other non-sensitive files are detected and reported to ArcSight. This capability is essential for US Government agencies that need to comply with Executive Order 13587.

OUTSIDER THREAT USE CASE

Unlike legacy, signature-based antivirus that can only address known threats, the Digital Guardian solution can detect and block malware behavior as it unfolds, in real time on the endpoint.

Digital Guardian provides ArcSight visibility to malware activity on host systems, including:

- Process activity – including accessing file acess, accessing networks, and starting or stopping processes
- Data events – including file operation type, destination, and classification of file
- System context - including user, application, time, OS, network, and more

RISK MITIGATING CONTROLS VIA ACTION CONNECTOR

Organizations that detect outsider attacks in ArcSight can apply controls on host systems directly from the ArcSight console using Action Connector integration. Digital Guardian rules that validate and contain existing malware infections and prevent further infections can be initiated by right-clicking on a malware event in the ArcSight console. Also, ArcSight can instruct HP Tipping Point to lock down network activity for the affected endpoint, further containing malware at the network level and enabling a multi-layered approach on and off the corporate network.

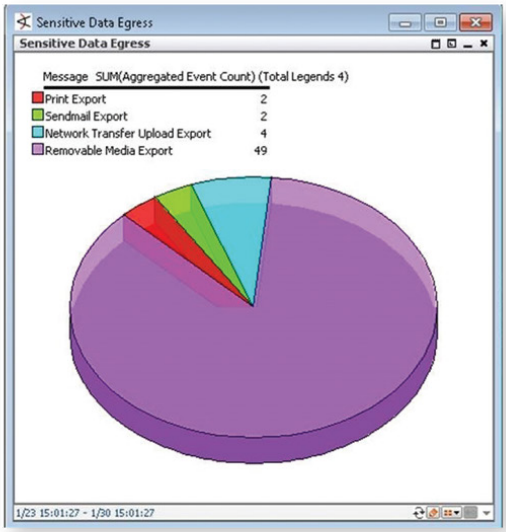

Fig. 1: Egress events of sensitive data by channel

Manager Receipt Time	Attacker User Name	Device Custom String1	Device Action
22 Jan 2013 17:38:50 EST			
22 Jan 2013 17:38:48 EST	demoverdasys\cking	NTU06 - PII-PHI File Uploads	Prompt
22 Jan 2013 17:38:28 EST	demoverdasys\cking	NTU01 - Classified File Uploads(CMK)	Prompt
22 Jan 2013 17:29:55 EST			
22 Jan 2013 17:29:55 EST			
22 Jan 2013 17:29:53 EST	demoverdasys\cking	NTU01 - Classified File Uploads(CMK)	Prompt
22 Jan 2013 17:29:53 EST	demoverdasys\cking	NTU06 - PII-PHI File Uploads	Prompt

Fig. 2: Correlated alerts for specific user over time period

Radar

Manager Receipt Time	Name	Device Custom String1	Destination Host Name
1 Feb 2013 14:33:14 EST	File Move	GS - Google Drive	
1 Feb 2013 14:33:14 EST	File Move	GS - Google Drive	
1 Feb 2013 14:01:04 EST	Network Transfer Upload	NTU01 - Classified File Uploads(CMK)	mail.google.com
1 Feb 2013 14:01:04 EST	Network Transfer Upload	NTU01 - Classified File Uploads(CMK)	mail.google.com
1 Feb 2013 12:46:54 EST	Network Transfer Upload	APT - Application Operation Profiling	mail.google.com
1 Feb 2013 12:46:54 EST	Network Transfer Upload	NTU01 - Classified File Uploads(CMK)	mail.google.com
1 Feb 2013 12:46:54 EST	File Open	APT - Application Operation Profiling	
1 Feb 2013 11:15:44 EST	File Copy	APT - Application Operation Profiling	
1 Feb 2013 11:15:44 EST	File Rename	APT - Application Operation Profiling	
1 Feb 2013 10:32:44 EST	File Open	APT - Application Operation Profiling	

Fig. 3: Data event stream in ArcSight

ABOUT DIGITAL GUARDIAN

At Digital Guardian, we believe in data. We know that within your data are your company's most valuable assets. The sum total of innovations, plans and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

SHARE