SOLUTION BRIEF

Verdasys Digital Guardian— Enterprise Information Protection (EIP) Integration with HP ArcSight

Advanced application and data event visibility across all end points delivering risk intelligence for insider and cyber threat detection and mitigation

KEY BENEFITS

- Visibility of sensitive data usage and policy violations (insider threat) from the laptops, desktops and servers
- Classification and location of data-at-rest across host systems
- Visibility of endpoint specific data access and movement by malicious code (cyber threat)
- Visibility into gold image and rogue application download and usage
- Exceed current and future data security compliance audit requirements

The Solution

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

Verdasys Digital Guardian

Verdasys' flagship product, Digital Guardian (DG), is a scalable platform that protects intellectual property and other sensitive business data against insider threat and malware attacks while enabling secure data sharing and collaboration across physical, virtual, mobile and cloud environments. DG endpoint agents classify data, as well as audit and control data usage, to provide contextual awareness of the endpoint and end user activity.

Digital Guardian classifies data based on content, context and/or user input and tags files accordingly. Using data classification enables a data-centric approach which allows for differentiated policies that provide effective controls without breaking business processes or impacting user productivity.

The Digital Guardian endpoint agent enforces data access control policies using a number of mechanisms including user warnings and blocking as well as enterprise encryption. Digital Guardian's enterprise key management capabilities mean that information can be transparently encrypted and decrypted as it is used in normal authorized business processes. Digital Guardian file encryption also ensures that sensitive data is secure, on end 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: external threats such as malware and hackers; internal 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 and actor/asset model importing, Digital Guardian is able to provide a rich data stream from laptops, desktops, servers and mobile devices, including a forensic log of data usage events, such as the user and application which accessed the data, the data event that occurs, and the classification of the data itself. Taking 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 insider threat, malware detection and containment use cases.

Insider Threat Use Case

Digital Guardian provides ArcSight a rich stream of data usage events and alerts delivering visibility to user and data event activity on the end point including:

- Name of file
- Sensitivity/type of data
- User Name, User Group
- Application used to access data
- Type of action: email, upload, print, CD burn, etc.
- Other contextual attributes

This data enables ArcSight users to answer questions such as "Where does my sensitive data reside and who is moving this data outside the enterprise and what applications are they using." By correlating Digital Guardian events and alerts, ArcSight enables detection of advanced insider threat scenarios such as when a malicious user transfers 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 radical attempts to obfuscate the data through encryption or 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 (government response to WikiLeaks).

Cyber Threat Use Case

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

- Download and activation of rogue applications
- Processes accessing sensitive data
- Processes communicating with external IP addresses
- Malware trait reports from active memory scans

Upon detection of potential malware activity on host systems, Digital Guardian, through automated policy will scan active memory for malware traits for effective detection of zero day threats. Digital Guardian passes the end point's malware threat score to ArcSight for further correlation with other indicators.

Risk Mitigating Controls

Organizations which detect Insider and cyber attacks in these ways are able to apply controls on host systems to stop users and processes accessing or transferring sensitive data. Further ArcSight can instruct HP Tipping Point to lock down network activity for the respective end point or user.

About Verdasys

Verdasys provides Enterprise Information Protection (EIP) solutions to secure the value and integrity of proprietary data within highly collaborative and mobile business processes for Global 2000 companies. **www.verdasys.com**

Companies serious about information protection choose Verdasys.

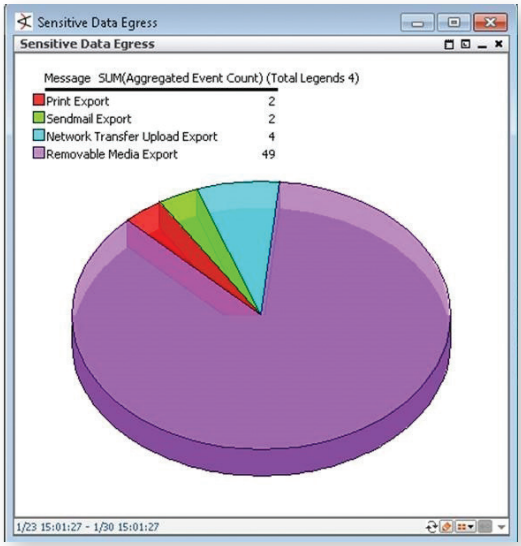
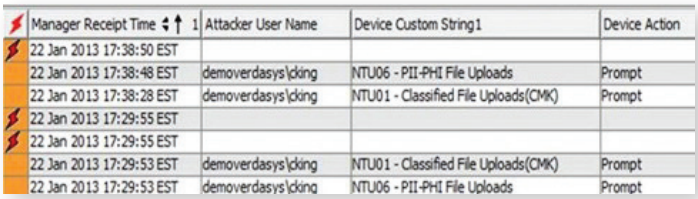
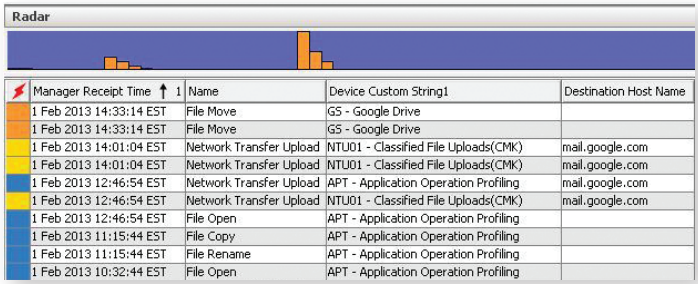


Fig. 1: Egress events of sensitive data by channel



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\dking	NTU06 - PII-PHI File Uploads	Prompt
22 Jan 2013 17:38:28 EST	demoverdasys\dking	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\dking	NTU01 - Classified File Uploads(CMK)	Prompt
22 Jan 2013 17:29:53 EST	demoverdasys\dking	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

VERDASYS

860 Winter Street, Suite 3
Waltham, MA 02451 USA

+1 781-788-8180

info@verdasys.com
www.verdasys.com