SOLUTIONS DATA SHEET

DIGITALGUARDIAN®

Data Protection (DLP) & Advanced Threat Protection (ATP) Integration with HP ArcSight

DATA, USER and SYSTEM EVENT VISIBILITY ACROSS ALL ENDPOINTS

Key Benefits

- Provides deep visibility of data, user, and system activity on the endpoint to power detection of insider and outsider attacks
- Delivers endpoint response to quickly and effectively stop threats uncovered in ArcSight

THE NEED

Attackers, whether insiders or outsiders, target the endpoint as their ultimate goal. The endpoint is the point of risk for data loss, it is where threats land and begin to propagate throughout the network. Visibility of user and system activity on the endpoint including access to and movement of sensitive data is key to being able to prioritize threats and respond. Digital Guardian provides granular visibility of all activity on the endpoint, including pre-correlated behavioral alerts which can detect anomalous behavior by users and processes. This visibility can be correlated with network based alerts from other security tools to prioritize threats and then respond appropriately on the endpoint.

THE DIGITAL GUARDIAN SOLUTION

Digital Guardian is a next generation data protection platform designed to stop data theft. The Digital Guardian platform performs across the corporate network, endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years, it has enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Digital Guardian's unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, enables you to protect data without slowing the pace of your business.

Digital Guardian classifies data based on context, content, and user input and tags files accordingly. This classification enables a data-centric approach to security that allows differentiated policies to provide effective controls without breaking business processes or impacting user productivity. Digital Guardian endpoint agents enforce data access control policies using a number of mechanisms, including user warnings and blocking, as well as encryption.

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

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 and responding to insider threats and advanced external threats.

Digital Guardian offers advanced ArcSight content on the HPE ArcSight Marketplace (https://marketplace.saas.hpe.com/arcsight/content/digital-guardian-7x) including dashboards, reports and data mappings which leverage Digital Guardian's endpoint visibility for threat detection.

DIGITALGUARDIAN®

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.

OUTSIDER THREAT USE CASE

Unlike legacy, signature-based antivirus that can only address known threats, the Digital Guardian solution can detect and block unknown threat behavior as it unfolds, in real time on the endpoint. Digital Guardian provides ArcSight visibility to malware activity and hacking attempts on host systems, including:

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

RESPONDING TO THREATS ON THE ENDPOINT VIA ACTION CONNECTOR

Organizations that detect attacks in ArcSight can apply controls on host systems directly from the ArcSight console using Action Connector integration with Digital Guardian. 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. Action connector controls include quarantining an endpoint and blacklisting a process.

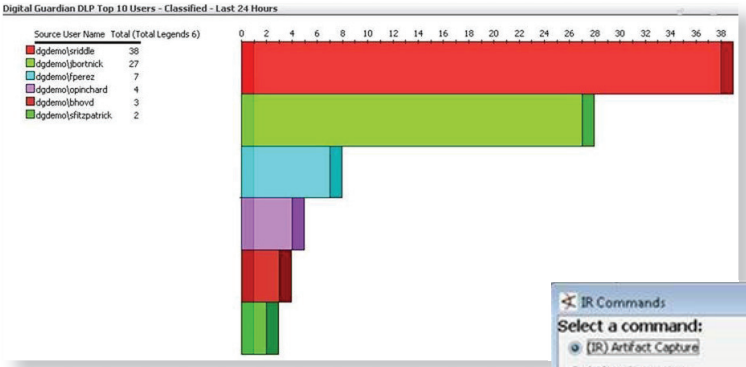

Fig 1. Insider Threat Dashboard

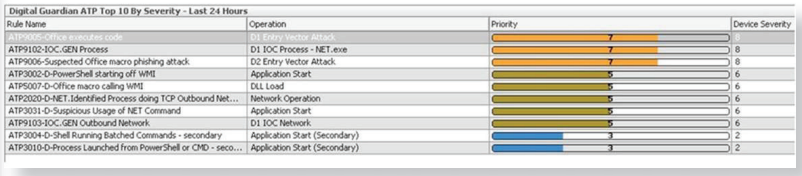

Fig 2. Outsider Threat Dashboard

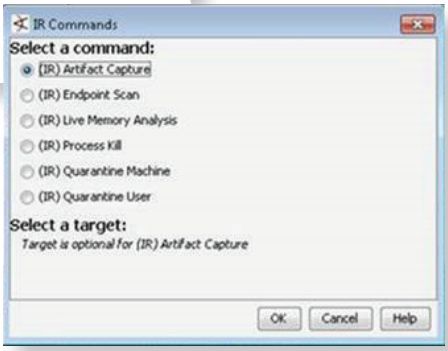

Fig 3. Action Connector

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE