SOLUTIONS DATA SHEET

DIGITALGUARDIAN®

QRadar®

The Digital Guardian App for IBM QRadar

DELIVER ENDPOINT VISIBILITY AND RESPONSE INTO QRADAR FOR ENTERPRISE DATA PROTECTION

Key Benefits

- Enterprise wide visibility of system, data, and user events on the endpoint computer for detection of insider and outsider attacks in the QRadar console.
- Immediate endpoint response to detected threats directly from the QRadar console.

Data, User, and System Event Visibility Across all Endpoints and Throughout the Enterprise

THE NEED

Regardless of the threat, internal or external, attackers target your sensitive data, looking to monetize your information assets. Traditionally, organizations have aggregated events from multiple network security solutions into their Security Operations Center for correlation. However, attacks on the endpoint via malware, hacking or malicious insiders have become increasingly frequent, necessitating prioritization. Organizations need detailed and granular visibility of what is happening on their endpoints and in particular what is happening to their sensitive data to elevate alerts as needed. Once endpoint threats have been detected, SOC staff must respond immediately to stop sensitive data exfiltration or prevent the lateral movement of attackers looking for more valuable targets.

Digital Guardian provides granular visibility of all activity on the endpoint, including correlated behavioral alerts which can detect anomalous behavior by users and processes, identifying potential malware. 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 (DG) App for QRadar allows QRadar customers to leverage Digital Guardian's deep visibility of insider threats and advanced external attacks on the endpoint in QRadar and then respond to these threats by deploying endpoint controls including quarantine. The App features filterable dashboards of Data Loss Prevention (DLP) and Advanced Threat Prevention (ATP) events from endpoint computers which include visibility of egress of sensitive data.

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. The platform enables 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.

IBM QRADAR

IBM QRadar SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It normalizes and correlates raw data to identify security offenses, and uses an advanced Sense Analytics engine to baseline normal behavior, detect anomalies, uncover advanced threats, and remove false positives. IBM QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

For more information, visit
www.digitalguardian.com

THE DIGITAL GUARDIAN APP FOR IBM QRADAR

The Digital Guardian Management Console exports event data in LEEF format to QRadar which parses the information via a built-in DSM (Device Support Module). This rich event data can be viewed, searched and correlated in QRadar via standard QRadar dashboards. The Digital Guardian App for IBM QRadar provides the user with flexible drill down dashboards which allow operators to explore Data Loss Prevention (DLP) and Advanced Threat Prevention (ATP) events from endpoint computers which include visibility of egress of sensitive data.

USE CASES

The Digital Guardian App for IBM QRadar is designed for incident handlers and SOC operators who have high level responsibility for enterprise security but may not be subject matter experts in Digital Guardian. From an operational perspective these operators need to evaluate threats to endpoints and sensitive data and take appropriate actions to stop exfiltration of sensitive information and stop spread of detected threats from within the context of the QRadar console. The Digital Guardian App for IBM QRadar provides easy access to alert data relevant to insider and outsider attacks from Digital Guardian with the ability to drill down and right click to remediate.

Fig 1. Digital Guardian App for IBM QRadar, DLP Dashboard showing Sensitive Data egress trends.

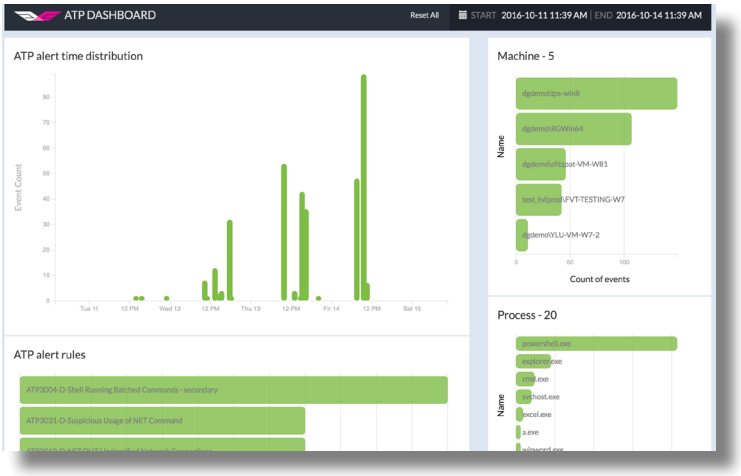

Fig 2. Digital Guardian App for IBM QRadar, ATP Dashboard showing top Advanced Threat Alerts and affected machines, processes, etc.

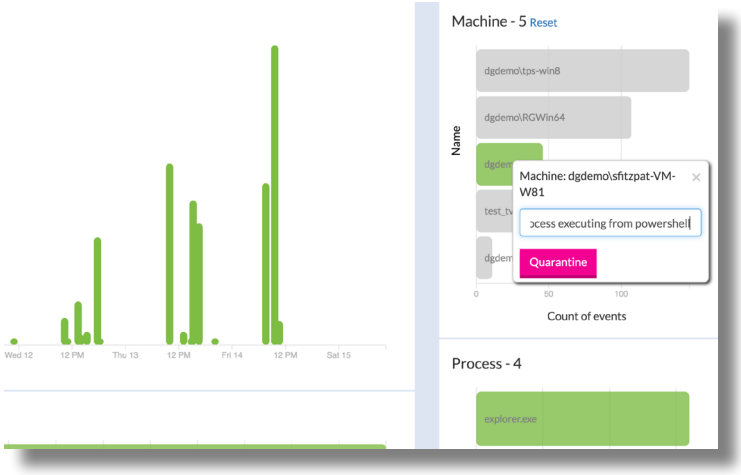

Fig 3. Digital Guardian App for IBM QRadar, Quarantine Action of infected endpoint

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