FORTRA™

DATASHEET (DIGITAL GUARDIAN)

Data Protection Integration with FireEye

Combining Network and Endpoint Defenses to Stop Malware

The Need

Advanced threats easily bypass signature-based detection solutions such as antivirus software and network-based intrusion prevention systems. To successfully prevent, detect, and contain   advanced cyber threats, enterprises need multi-layered defenses at both the network level and the endpoint. This "kill chain" defense collects and correlates attack intelligence, identifies anomalies, and challenges malware at each step of an attack. By integrating network and endpoint defense mechanisms, security organizations can quickly investigate, confirm, and stop advanced threats.

The Digital Guardian Solution

Fortra™'s Digital Guardian® Digital Guardian is a scalable platform that protects intellectual property and other sensitive data against insider threats and outsider malware attacks. Digital Guardian provides visibility into data movement to detect malware and it provides controls to prevent malware from compromising critical systems and data.

Unlike antivirus software that can only detect known threats, Digital Guardian detects and blocks malware behavior as it unfolds in real time. Digital Guardian even protects host systems when users are off the company network and unprotected by corporate network defenses.

Digital Guardian recognizes and correlates compound process events from system, application, and user activity, including:

- Process activity - including file and network access, and starting and stopping processes
- Data events - including file operation type, destination, and classification of file
- System context - including user, application, time, OS, and network

KEY BENEFITS

Reduce Investigation Time

- Quickly determine if threats discovered on the network by FireEye have infected endpoints
- Verify that threats have been contained on the endpoint
- Submit threats discovered on endpoints for detonation and validation in FireEye's Malware Analysis System (MAS)

Reduce Containment Time

- Contain malware on infected hosts
- Prevent new infections using Digital Guardian rules based on Indicators of Compromise received from FireEye

Digital Guardian also provides a wide range of policy controls to stop malware and protect sensitive information:

- Block code from executing
- Block access to files and networks
- Alert administrators and incident response teams to policy violations and malicious activity
- Prompt users to acknowledge company policies and justify their actions
- Encrypt sensitive data automatically based, based on policy, user permissions, and activity

Digital Guardian uses a broad set of malware detection rules to identify malware threats without using signatures. Unlike application whitelisting, which can only compare process characteristics to a predefined list, Digital Guardian correlates individual system, application, and data events against a proprietary set of rules to establish the risk level of process actions and detect malware activity. Based on the risk level, Digital Guardian can implement control responses ranging from passive alerting, to blocking process actions, to locking down the host.

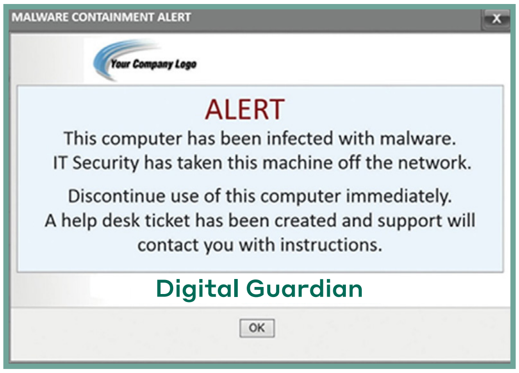
FireEye Malware Protection System

FireEye has developed a purpose-built, virtual machine-based security platform that provides real-time threat protection against the next generation of cyber-attacks. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including web, email, and files. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber-attacks in real time.

FIREEYE AND DIGITAL GUARDIAN 1+1=3

The Digital Guardian server receives FireEye Alerts and converts new IOC discovered by FireEye into rules for endpoint agents to confirm the extent of an infection, quickly contain that infection, and block new infections.

Further, Digital Guardian can submit suspicious malware artifacts collected on host systems for analysis in the FireEye Malware Analysis System (MAS). Results of the analysis are passed back to Digital Guardian for containing and preventing new infections.



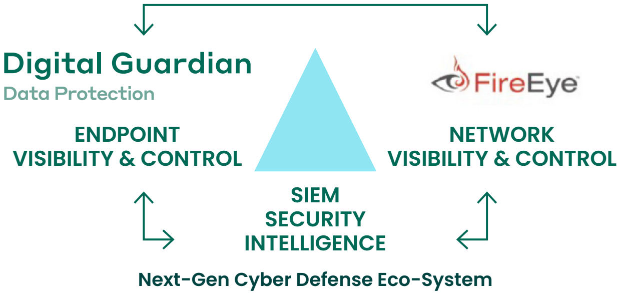
MALWARE CONTAINMENT ALERT

ALERT

This computer has been infected with malware.
IT Security has taken this machine off the network.

Discontinue use of this computer immediately.
A help desk ticket has been created and support will contact you with instructions.

Digital Guardian



Use Case

Validate & Report the extent of FireEye-discovered threats within the endpoint estate. Contain existing endpoint infections and Prevent further endpoint infections.

When FireEye discovers a new threat on the network, administrators need to determine if another layer of defense has already stopped the threat, and if not, which endpoint systems the threat has reached and infected. FireEye passes IOCs of detonated threats to Digital Guardian, which automatically deploys rules to enable administrators to track if and where the malware has landed, create containment and prevention rules, and accurately report the extent of the incident and its containment. These containment rules include the ability to lock down the endpoint to stop malware from infecting other computers on the network, block access to sensitive data, prevent exfiltration, and prompt the user to warn of an infection.

USE CASE

Correlate FireEye and Digital Guardian events in the HP ArcSight SIEM to verify whether an incident is under control at the endpoint.

Many customers aggregate security events in the ArcSight SIEM. Correlating different indicators of malware activity from the network and host systems in ArcSight allows security organizations to recognize threats faster. In ArcSight's single pane of glass, security operations teams can respond to alerts from Digital Guardian, FireEye, and third-party systems. The ArcSight Action Connector for Digital Guardian initiates the conversion of correlated alerts into prevention and containment rules.

USE CASE

Upload suspicious executables and documents captured on the endpoint by Digital Guardian to the FireEye Malware Analysis System (MAS) for analysis to prioritize the incident and respond appropriately.

When Digital Guardian detects malware activity through its Cyber Defense Rule set, it captures relevant documents and executables created by suspicious processes. These files can be automatically submitted to the FireEye MAS service for analysis. FireEye MAS then returns the IOCs discovered through detonation for monitoring and containment on the endpoint by Digital Guardian.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.