SOLUTIONS DATASHEET

Detecting and Containing Advanced Malware with Verdasys Digital Guardian and FireEye Malware Protection System

Combining next-generation defenses on the network and the end point to stop malware in its tracks

KEY BENEFITS

- Reduce investigation and containment time by verifying whether threats discovered on the network by FireEye have infected systems and if they have been contained on the end point.
- Contain malware on infected hosts and prevent new infections by Digital Guardian rules based on IOCs received from FireEye
- Decrease time to investigation and containment by submitting threats discovered on the end point for detonation and validation in the FireEye Malware Analysis System (MAS)

THE SOLUTION

Advanced zero-day threats are able to bypass signature-based detection mechanisms such as end point Anti-Virus and network based Intrusion Prevention Systems. In order to successfully prevent, detect, and contain advanced cyber threats, enterprises need to use multi-layered defenses at both the network and the end point to follow a kill chain defense methodology. By integrating the network and end point defense mechanisms, security organizations can quickly investigate, confirm and stop advanced threats in their tracks.

VERDASYS DIGITAL GUARDIAN

Verdasys' flagship product, Digital Guardian (DG), is a scalable platform that protects intellectual property and other sensitive data against insider threat and malware attacks on the end point. DG end point agents provide the most complete visibility and control on host systems to detect advanced malware and prevent it from compromising critical systems.

Unlike legacy, signature-based AV which can only address known threats, the Digital Guardian solution is able to detect and block malware behavior as it unfolds in real time on the end point. Digital Guardian also protects host systems when they are most vulnerable: when users are off the company network unprotected by corporate network defenses.

The Digital Guardian agent has the ability to recognize and correlate compound

process events from system, application and user activity on the end point:

- Process activity incl. file and network access, start & end of process,
- Data events incl. file operation type, destination and classification of file,
- System context incl. user, application, time, OS, network etc.

It also has the widest set of end point control mechanisms for stopping malware and protecting sensitive information:

- Blocking code from executing,
- Blocking access to files and networks,
- Alerting,
- User prompting,
- Encryption of sensitive data

Digital Guardian uses a broad set of end point malware detection rules which identify zero-day threats without signatures. Unlike application whitelisting solutions which can only compare process characteristics to a pre-defined list, Digital Guardian actually correlates individual system, application and data events such as process starts, communication with IP addresses outside the corporate network, and access to sensitive data against a proprietary set of rules to establish the risk level of a process action and detect malware activity. Based on risk level, Digital Guardian can then implement a range of control responses from passive alerting, to blocking of process actions, to full lockdown of the host.

FIREEYE MALWARE PROTECTION SYSTEM

FireEye® has invented 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 IOCs 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 is able to 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 containment and prevention of new infections.

USE CASE:
Validate & Report extent of FireEye-discovered threat within the end point estate, Contain existing end point infections and Prevent further end point infections

When FireEye discovers a new threat on the network, administrators need to understand if the threat has already been stopped by another layer of defense and if not, which end point systems it 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 end point to stop malware moving laterally, to block access to sensitive data to prevent exfiltration as well as prompting the user to warn of an infection.

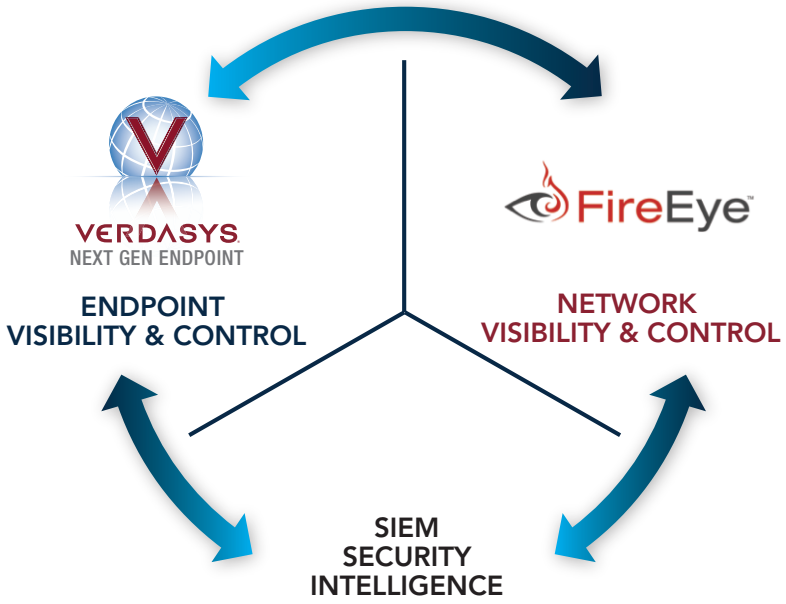
USE CASE:
Correlate FireEye and Digital Guardian events in the ArcSight SIEM to verify whether incident is under control at the end point

Many customers aggregate security events in the ArcSight SIEM. Correlating different sources of visibility to 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 preventative and containment rules.

USE CASE:
Upload suspicious executables and documents captured by Digital Guardian on the end point to the FireEye Malware Analysis System (MAS) for analysis in order 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 end point by Digital Guardian.

Digital Guardian controls stop malware by isolating endpoint systems thereby blocking lateral movement, C&C calls, compromise of credentials, and access to sensitive data.



Next-Gen Cyber Defense Eco-System

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.

VERDASYS

860 Winter Street, Suite 3
Waltham, MA 02451 USA

+1 781-788-8180

info@verdasys.com
www.verdasys.com