Verdasys Digital Guardian 6—
The Next Generation of Endpoint Security

Detect and stop both cyber and insider threats

KEY BENEFITS

- Gain full visibility into insider and cyber threats from a single platform

- Dynamically detect advanced malware behavior as it unfolds on endpoints without signatures

- Combine deep visibility of user and malware events with data classification to know exactly when your most valuable assets are under attack

- Stop insider and cyber threats before they compromise sensitive information and critical systems

- Build a proactive solution ecosystem to stop known and unknown targeted attacks

THE CHALLENGE

Advanced malware is able to bypass signature-based endpoint anti-virus and network-based intrusion prevention systems. In order to successfully prevent, detect and contain advanced cyber threats, enterprises need broad visibility and control on the endpoint which can recognize unknown malware as it unfolds. At the same time, malicious insiders have greater access to data and more channels to exfiltrate that data than ever before. Security departments are challenged to respond to insider and cyber threats using inadequate tools which have no understanding of the sensitive information targeted by these threats.

VERDASYS DIGITAL GUARDIAN

Verdasys has been protecting the sensitive data of the world's largest and most security conscious organizations for over 10 years. Verdasys' 250+ enterprise customers include global powerhouses and household names in manufacturing, high-tech, oil & gas, financial services and government. Verdasys Digital Guardian is a technology leader in the Gartner Magic Quadrant for Data Loss Prevention (DLP) and was called out by Gartner as being number 1 in Intellectual Property (IP) protection.

Deployed globally to millions of systems the Digital Guardian product is an endpoint security solution which helps customers protect their sensitive information against today's two largest security threats:

- Insider threat (data loss through malicious or unintentional actions of insiders)

- Cyber threat (data theft through advanced malware attacks).

Digital Guardian is unique in its ability to see and stop malicious actions by users and malware on the endpoint computer (the point of use). The Digital Guardian agent has kernel level visibility of system, application and data events as well as user and malware behavior. With this high level of visibility, Digital Guardian can put data events into context and apply a granular set of rules to protect data against both insider and cyber threats. Digital Guardian runs on Windows, Linux and Macintosh on real and virtual desktops and servers.

UNIQUE ENDPOINT AGENT CAPABILITIES

Building on many years of experience in protecting sensitive information against Insider Threats (DLP), Verdasys has created a Cyber Defense rule set which specifically monitors for malware behavior and blocks malicious actions. Unlike legacy, signature-based Anti-Virus which can only address known threats, or application whitelisting solutions which have proved too complex to scale on endpoint systems, the Digital Guardian solution is able to detect and block malware behavior as it unfolds in real time on the endpoint. 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 endpoint:

- 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.

DG also has the widest set of endpoint control mechanisms for stopping malware and protecting sensitive information:

- Blocking code from executing

- Blocking access to files and networks

- Blocking risky data actions (incl. cloud storage, webmail, etc.)

- Alerting and user prompting

- Encryption of sensitive data

Based on risk level, Digital Guardian can implement a range of control responses from passive alerting, to prompting the user, to blocking of process actions, to full lockdown of the host.
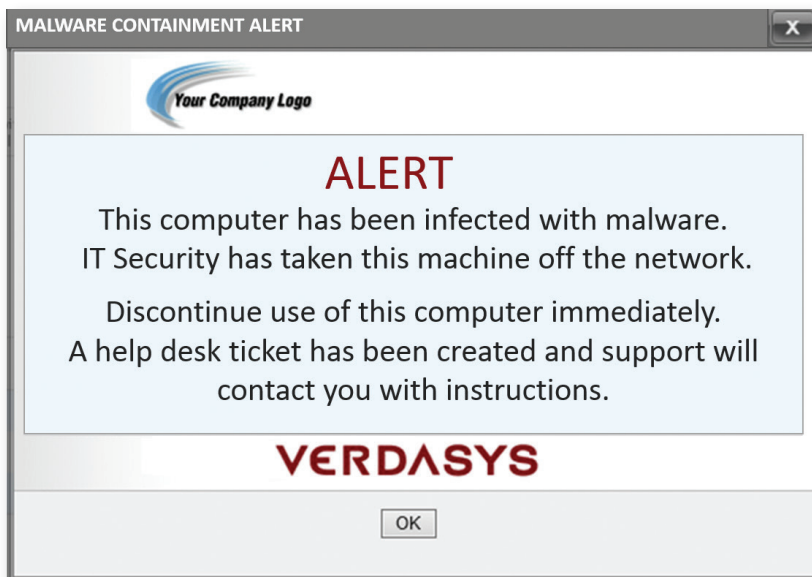
Digital Guardian integrates with market leading SIEM solutions and adds significant value to existing SIEM installations. Digital Guardian's event stream allows customers to fill the end point visibility gap in their SIEM to correlate user and malware behavioral events with other events from the network and backend systems thus dramatically increasing the ability to detect and stop Insider and Targeted Cyber Threats. Digital Guardian also integrates real-time malware alerts from leading network security solutions such as FireEye to immediately find and contain zero-day attacks on end point systems.

The Digital Guardian solution can be deployed on premise or as a fully managed service from the cloud. Digital Guardian agents work autonomously on the endpoint and do not send sensitive information over the network. Verdasys offers two managed services: Managed Service for Information Protection (MSIP) for insider threat and Managed Service for Cyber Defense (MSCD) which can be bought individually or as a combined service for a monthly per endpoint fee.
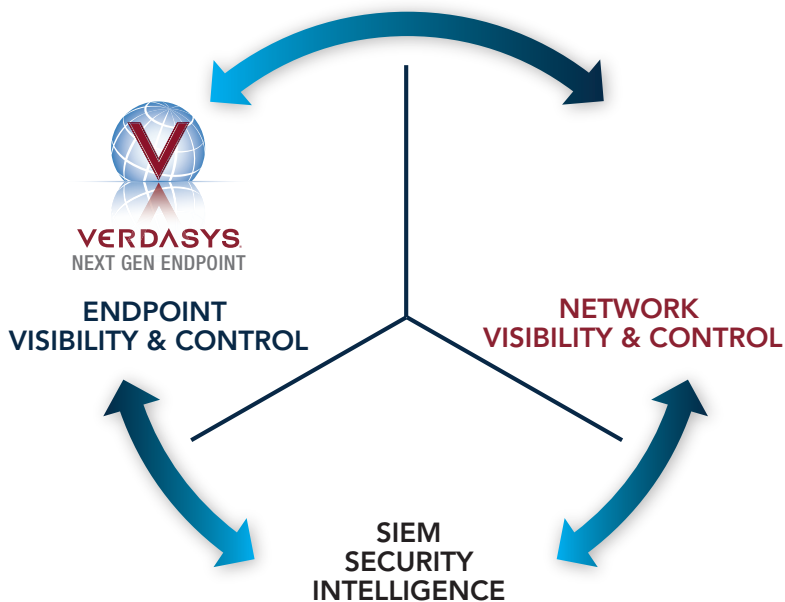

MALWARE CONTAINMENT ALERT

Your Company Logo

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.

VERDASYS

OK

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

VERDASYS
NEXT GEN ENDPOINT

ENDPOINT VISIBILITY & CONTROL

NETWORK VISIBILITY & CONTROL

SIEM SECURITY INTELLIGENCE

Verdasys Digital Guardian integrates with leading SIEM solutions and next generation network security solutions to create a proactive, real-time defense against Cyber and Insider Attacks

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