FORTRA™

DATASHEET (DIGITAL GUARDIAN)

Digital Guardian for Windows

Digital Guardian Fills the Windows Data Visibity Gap

Microsoft Windows® is the most widely deployed operating system in the world, and consequently the most vulnerable to security threats. Critical patches and security updates are issued frequently, but this reactive approach leaves you poorly equipped to defend your organization's sensitive data against both insider and advanced threats.

The DG Windows Agent has been protecting data in the Windows operating system for more than ten years. It's a kernel-level agent that automatically identifies, classifies, and protects your most sensitive data based on contextual awareness - what data is being accessed, by whom, and how it is being used. And since it's software-based, you can install Fortra™'s Digital Guardian® on Windows desktops and laptops with a small memory footprint.

Unmatched Protection for Windows

Digital Guardian is the only data protection solution with:

Full Visibility into Windows Data Movement

Digital Guardian agents monitor all file movement at the origin using an advanced, noninvasive approach. This provides real-time visibility of all data movement and data transmission methods across online, offline, physical, and virtual environments, including email, cloud storage, removable media, print, and FTP.

Effective Data-Loss Risk Management

Full visibility to all data provides enforcement of policies based on data use "context"; what data is affected, which user or process is taking action on data, and how the data is being used. This allows Digital Guardian to stop "known threats," such as moving sensitive data to removable drives, and exposes "unknown threats," such as synchronization of sensitive data to the cloud via Dropbox or other methods.

Noninvasive, Context-Aware Protection

Digital Guardian protects your sensitive data without disrupting legitimate data use. It automatically blocks and controls only those behaviors that pose a threat to your organization based on user, event, and data type. Legitimate data use continues without interruption.

Key Features for Windows

Digital Guardian takes full advantage of kernel-level and user-mode visibility to deliver:

Broadest Security Coverage

Digital Guardian provides organizations with a single solution to monitor and protect over 300 file types and 90 languages, controlling data use and movement by individuals and applications. Information protection policies are based on user role and usage rights — even if users write their own custom script to manipulate data.

Tamper-Resistant Protection — Online or Offline, On or Off the Corporate Network

Sensitive data isn't static, and needs to be used on and off corporate networks. Digital Guardian ensures active protection at all times. Kernel-level classification and enforcement cannot be removed or tampered with – even if the file type is changed or data is copied to another file. Policy enforcement can be hidden from users, or made visible to reinforce data protection policies and influence user behavior.

Privileged–User Monitoring

Digital Guardian protects data from misuse, even from users with full local-administration (root access) privileges — independent of the operating-system security model in place. It separates device privileges from data privileges, monitoring and controlling access and use of sensitive data, even if administrators have full root access to the device.

Data Protection in Windows Case Studies

INSIDER THREAT PROTECTION

Jabil, a Fortune 200 manufacturer with over 60,000 employees needed to protect sensitive data and formula against data theft. Simply locking down the information would not work. The company's competitive edge depended on ready access to this information to drive efficiency and collaboration.

Digital Guardian was used to build actionable and risk-aware information usage policies and controls. Sensitive IP could reside only on Digital Guardian secured workstations, blocking the ability to transmit IP to any computer or server that lacked a Digital Guardian Agent. This created a virtual community of trust, and contained information by governing its use at the endpoint. Aggressive policies regarding device control (USB drives) and printing of confidential IP were also deployed. In less than three months, the team executed a full phase one deployment to safeguard corporate intellectual property.

CUSTOMER DATA PROTECTION

A multi-national financial services company, with over 50 million credit card customers worldwide, was subject to the Payment Card Industry Data Security Standards (PCI-DSS). Using Digital Guardian's contextual data awareness and content inspection technology, Windows endpoint agents could identify and classify sensitive data, monitor all user actions and enforce controls - including automatically encrypting sensitive files when those files are moved to network file servers. Digital Guardian also prevented decryption of PCI PAN and social security data by unauthorized users, including system administrators with root privileges.

REMOVABLE MEDIA DATA PROTECTION

An international financial services company required users to move sensitive data to USB memory drives, but needed to ensure the security of those devices and the data stored on them. Digital Guardian Windows agents on the endpoints identified and classified all data, and automatically encrypted any sensitive data moved to removable drives. Digital Guardian also ensured that only approved removable drives were used. Digital Guardian's granular controls allowed devices to be identified by brand, model, and serial number, to ensure that only company-approved devices were used to store protected data.

INTELLECTUAL PROPERTY PROTECTION

One of the world's leading research based pharmaceutical and healthcare companies needed to more effectively monitor and control their IP without impeding the productivity of their users.

Since Digital Guardian recognizes over 300 data types and 90 languages, it proved simple to automatically classified sensitive data from four discrete technical applications. DG Windows endpoint agents then tracked all use of the IP by employees, third party individuals and clinical research partners, preventing misuse based on corporate polices. This provided the organization with visibility into what R&D scientists were doing with sensitive data, protected data as it moved between users and applications, and enhanced worker productivity.

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.