COMPANY OVERVIEW

DIGITALGUARDIAN™

Complete Data Protection Against Insider and Outsider Threats with One Agent

THE CURRENT APPROACH TO DATA PROTECTION ISN'T WORKING

The nature of data protection has changed dramatically in the past few years. It used to be that an IT-controlled network contained all your organization's sensitive data. You knew exactly where your data was going and who had access.

But changes in the security landscape have dissolved the network perimeter. And as the security landscape has changed, so have the types of threats your sensitive data faces. Insiders and outsiders are increasingly gaining access to and stealing sensitive data using sophisticated and hard-to-detect tactics, making even a layered defense ineffective. We need to change our approach to data protection. **We need security that starts at the source, with each piece of data, and travels with it.**

DIGITAL GUARDIAN - SECURITY'S CHANGE AGENT™

Digital Guardian is Security's Change Agent—the only patented data protection platform trusted on millions of endpoints to secure against insider and outsider threats.

Installed in the kernel of the OS, the Digital Guardian agent sees and classifies every piece of data as it is in motion. The agent then automatically adds a security tag to each individual piece of data that dictates customized permissions, taking into account the type, content, and author of the data. This means your data is protected and context-aware. The DG agent will automatically prompt or block an activity depending on the context, then log and audit the event for forensic follow-up. This data-centric approach streamlines incident response and containment, cutting security cycle times from days or hours to minutes.

You'll design policies that won't block benign actions and employees can continue to enjoy ease of use because the data is made intelligent. For example, if an employee needs to copy a sensitive work document onto a USB to work on at home, they will be permitted to do so, but only if the data is safely encrypted. If you want the CEO to have unrestricted access to all company data, just set up the policies and Digital Guardian will do the rest.

The DG tag persists no matter where the data goes, giving the agent constant visibility and control throughout your entire organization— guarding your sensitive data against insider and outsider threats at the point of greatest risk.

Why Digital Guardian?

THE DIGITAL GUARDIAN PLATFORM IS THE ONLY DATA PROTECTION SOLUTION THAT:

AUTOMATICALLY CLASSIFIES AND TAGS SENSITIVE DATA

Only Digital Guardian can put you on the path to meaningful data protection immediately. The instant sensitive data leaves a protected application or shared network, Digital Guardian is on the case, automatically identifying, classifying, and tracking it. You don't have to wait to complete a lengthy data discovery and classification project.

COMPATIBLE WITH WINDOWS, MAC, & LINUX, PROTECTS DATA ON & OFF THE NETWORK

Digital Guardian agents are the only endpoint agents compatible with Windows, Mac, and Linux. They offer the industry's broadest application coverage, recognizing both structured and unstructured data on multiple systems. They even dynamically recognize malware behavior without signatures. You'll have complete data visibility and control regardless of what users are running, what they're running it on, and whether or not they're on the network.

DELIVERED AS A CLOUD-BASED MANAGED SERVICE, INSTALLED ON PREMISE, OR IN A HYBRID MODEL

While the frequency and sophistication of data attacks are on the rise, CISOs continue to face serious budget and resource limitations. And most lack true security expertise in-house. Only Digital Guardian offers complete data protection through an on premise, managed services, or hybrid model. Our cloud-based managed services are the answer if you have more IP than IT. As an extension of your team, we'll expertly develop, deploy, and manage all of your policies enterprise-wide as if they were our own.

SCALES TO 250,000 USERS USING A SINGLE MANAGEMENT SERVER

Digital Guardian is as robust as it is stable, designed to be easily and efficiently deployed across your entire user base. It's the only agent-based technology covering 250,000 employees using a single management server, and one of the largest and most respected companies in the world has deployed over 300,000 agents.

AT DIGITAL GUARDIAN, WE BELIEVE IN DATA

We know that within your data are your company's most valuable assets. The sum total of innovations, plans, and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss by securing their endpoint devices. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

Office Locations

United States
860 Winter St., Suite 3
Waltham, MA, 02451 USA
Phone 781-788-8180
Fax 871-788-8188

Europe
11 Leadenhall Street
EC3V 1LP London
United Kingdom
Phone +44 (0) 207-469-0940

Japan
Shiodome Plaza Bldg. 9F
2-11-4, HigashiShimbashi
Minato-ku, Tokyo,
105-0021, Japan
Phone +81-3-6435-6207
Fax +81-3-6435-6204

www.digitalguardian.com

SHARE

WE PROTECT YOUR DATA FROM INSIDER AND OUTSIDER THREATS

Your data faces numerous and varied threats every moment of the day.
Digital Guardian agents are always on guard, always protecting your sensitive data.

RISK		SOLUTION
	REMOTE WORKER ACCESSING SENSITIVE DATA	
	**INSECURE PUBLIC WIFI NETWORKS** Dan from Finance attempts to use the free wireless network at a coffee shop to download sensitive business documents. 9 AM **TRUSTED NETWORK AWARENESS** Dan is denied access and advised to use a secure VPN connection via a Digital Guardian real-time user prompt.	
	INCOMING PHISHING EMAIL	
	**INSECURE ADVANCED MALWARE** Jen from HR receives a phony email, seemingly from her bank, saying there's an account issue and providing an attachment to learn more. 10 AM **REAL-TIME PHISHING DETECTION** Digital Guardian alerts Jen that the attachment is suspicious, blocks her from opening it, and alerts IT of the suspected malware attack.	
	UPLOADING SENSITIVE DATA TO A CLOUD APPLICATION	
	**INSECURE WEB APPLICATIONS** Tricia, a designer, attempts to upload sensitive files to her Dropbox so that she can access them from her own laptop at home. 11 AM **WEB APPS AND CLOUD CONTROL** Digital Guardian recognizes that she's trying to send sensitive data to an unauthorized web application and blocks the upload.	
	SYSTEMS ADMINISTRATOR DOWNLOADING SENSITIVE FILES	
	**UNRESTRICTED INSIDER ACCESS** Joe, an IT administrator with root access, is leaving the company and tries to download sensitive design documents to take with him. 12 PM **PRIVILEGED USER CONTROL** Digital Guardian allows proper file access for the privileged user, but blocks his attempt to download the sensitive files and alerts staff.	
	DOWNLOADING CORRUPTED WEB SOFTWARE	
	**DRIVE-BY MALWARE** Susanne in Marketing searches the web for photo editing software. She visits a compromised site and is redirected to a malicious site that starts downloading malware to her machine. 1 PM **APPLICATION CONTROL** The malware attempts to execute a variety of processes on its own. Digital Guardian detects this activity immediately and automatically blocks the malicious application from running.	
	ACCIDENTAL EMAILING OF SENSITIVE DATA	
	**EMAILING SENSITIVE DATA** Kevin from Accounting tries to email payment information and MS Outlook auto-populates an unapproved external recipient. 2 PM **EMAIL CONTROL & ENCRYPTION** Kevin clicks send and a real-time Digital Guardian prompt alerts him of the unapproved recipient and requests justification for the action.	
	COPYING ENGINEERING DRAWINGS TO A USB DRIVE	
	**INSECURE EXTERNAL DEVICES** Michelle from Engineering downloads a sensitive CAD file to her USB device to work on it from home later. 3 PM **DEVICE CONTROL & ENCRYPTION** Digital Guardian automatically encrypts the file prior to copying it to the USB. The file now can only be opened with a decryption key.	
	MALICIOUS INSIDER MODIFYING CONFIDENTIAL FILES	
	**MODIFYING CONFIDENTIAL FILES** A manager named Bill is interviewing with a competitor, so he maliciously copies confidential information from a file on a shared network drive and saves it as a new file on his machine. 4 PM **AUTOMATIC DATA CLASSIFICATION** Digital Guardian recognizes that the data was copied from a sensitive file and applies the "Confidential" tag from the source file. The new file is protected and can't leave the company.	

SECURITY'S CHANGE AGENT™

DIGITALGUARDIAN™

by VERDASYS

52 MILLION TERABYTES

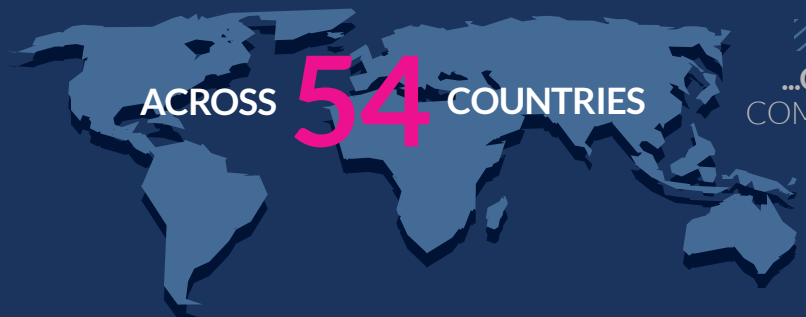
OF SENSITIVE DATA IS PROTECTED DAILY BY DIGITAL GUARDIAN AGENTS

OVER

2 MILLION

AGENTS DEPLOYED WORLDWIDE

TRUSTED DAILY BY MORE THAN **250** OF THE LARGEST BRANDS IN THE WORLD



ACROSS **54** COUNTRIES

...ONE OF THE LARGEST AND MOST RESPECTED COMPANIES IN THE WORLD HAS DEPLOYED OVER

300,000

AGENTS

INCLUDING...

7 OF THE **TOP 10** PATENT HOLDERS

AND **5** OF THE **TOP 10** AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING 250,000 EMPLOYEES USING A SINGLE MANAGEMENT SERVER

WE ARE THE **DATA PROTECTOR OF CHOICE** IN

- ENERGY
- FINANCIAL SERVICES
- GOVERNMENT
- TECHNOLOGY
- HEALTHCARE & LIFE SCIENCES
- MANUFACTURING

BECAUSE WE'RE FOCUSED ON PROTECTING **ONE THING:**

DATA