PRODUCT DATA SHEET

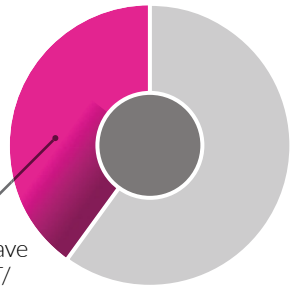
DIGITALGUARDIAN™
for Outsider Threat Protection

TURN YOUR DATA PROTECTION STRATEGY INSIDE OUT

The Convergence of Insider and Advanced Outsider Threats

For over ten years Digital Guardian has been helping some of the most innovative global companies protect their sensitive data from insider threats. This data-centric security strategy leverages deep data and process visibility along with flexible controls to ensure the data that matters most is never compromised.

Many of our clients now leverage these same strategies to protect against advanced outside attacks. The sophisticated outsider's ultimate goal, after all, is to become an "insider." Once outsiders penetrate the physical and/or virtual perimeter and access the corporate network, they look like a valid insider. That means theft of your sensitive data is just a few clicks away.



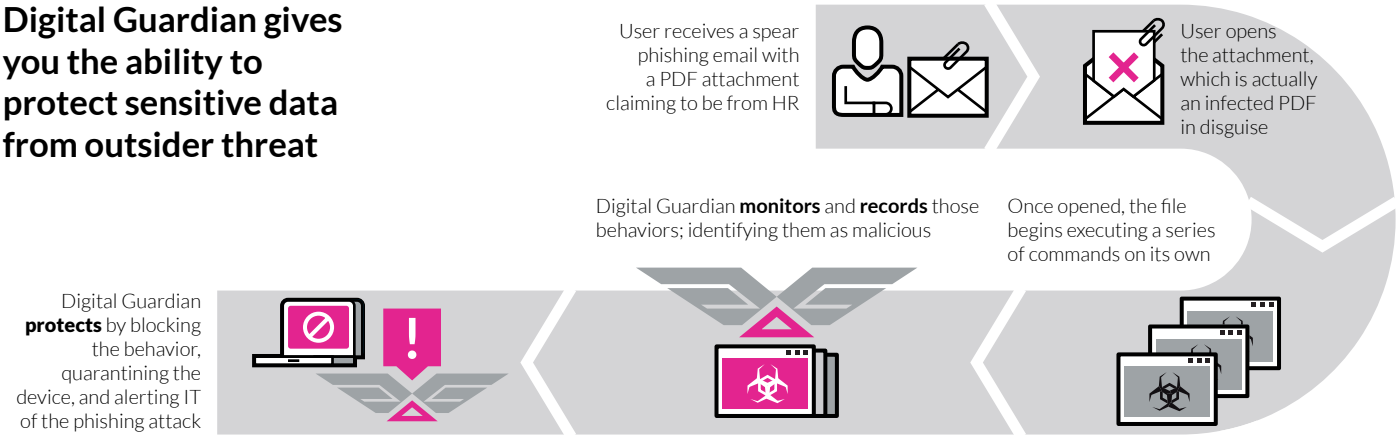
40%

of security professionals surveyed say their endpoints have been the entry point for an APT/ targeted attack in the past 12 months

PROTECT THE DATA FOR THE BEST DEFENSE FROM OUTSIDER THREATS

The question isn't whether to focus on the insider or outsider threat; it's how to defend against each equally well. Digital Guardian is security's most advanced endpoint agent. Its data-centric approach combines deep data visibility and knowledge of process-level malicious behaviors to protect against the loss of your sensitive data — whether the threat originates inside or outside your organization.

Digital Guardian gives you the ability to protect sensitive data from outsider threat



For more information, visit
www.digitalguardian.com

ENDPOINT THREAT DETECTION

The "network" now extends to wherever employees are, wherever data is, and wherever data can be accessed from. In this environment, keeping pace with constantly evolving attack vectors is a challenge for security professionals — and an opportunity for insider and outsider threats. Digital Guardian can detect, understand, and stop threats as they unfold at the endpoint, before sensitive data is compromised. Because the DG agent is autonomous, your endpoints are protected whether they are on your corporate network, on a third-party network, or have no network access.

PROCESS EXECUTION

The DG agent identifies process starts, dynamic library loads, and other system-level behaviors that — independently or in combination — signal an attack on your data. When an attack is identified, Digital Guardian stops it in its tracks and immediately alerts your incident response (IR) team about what has happened. The compromised machine may then be quarantined from the network to stop the lateral spread of the malware.

VISIBILITY

The DG agent has knowledge of all kernel and higher-level activity related to file access, and reports the activity to the Digital Guardian console. By seeing key data interactions from all endpoints, your IR team can perform forensic analysis on intelligence from the full range of potential attack vectors across your endpoints.

DATA CLASSIFICATION

Industry leading, automated data classification ensures the focus is always on the data that matters most. As you respond to threat alerts, you can prioritize those that threaten your most valuable data assets.

A PLATFORM APPROACH

The Digital Guardian Platform is extensible, built for scale, and is centrally managed for unified policy and consistent data controls. Tens or even hundreds of thousands of agents can be monitored from a single console. This is particularly important since breaches often stem from the same weaknesses regardless of whether they result from insider actions or a bad outside actor.

NETWORK INTEGRATION

DG offers APIs for direct integration with network security providers and threat intelligence services. This provides additional analysis capability and a choice of actions based on the intelligence information. For example, automatic submission of a file hash that's deemed a threat could result in all endpoints being set to block and alert should the threat be seen by any endpoint, whether on or off the network.

"With Digital Guardian, our IR Team, can stop would-be data thieves in their tracks, ultimately preventing the crime. Other endpoint threat prevention products only allow them to investigate the crime after it happened. After my data has been stolen."

- CISO, Fortune 50 Global Manufacturer

DIGITAL GUARDIAN STANDS UP TO GARTNER'S REQUIREMENTS FOR ENDPOINT THREAT DETECTION AND RESPONSE (ETDR)

- **Collect endpoint data** such as running processes
- **Centralize the data** by near-real-time collection and make it quickly available
- **Post-process the data** to identify anomalies such as rare processes
- **Provide an interactive data UI** that allows one to explore the data
- **Alert based on patterns** such as new process or connection or "anomaly score"

Gartner

ABOUT DIGITAL GUARDIAN

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 at the endpoint. 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. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. 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.

SHARE