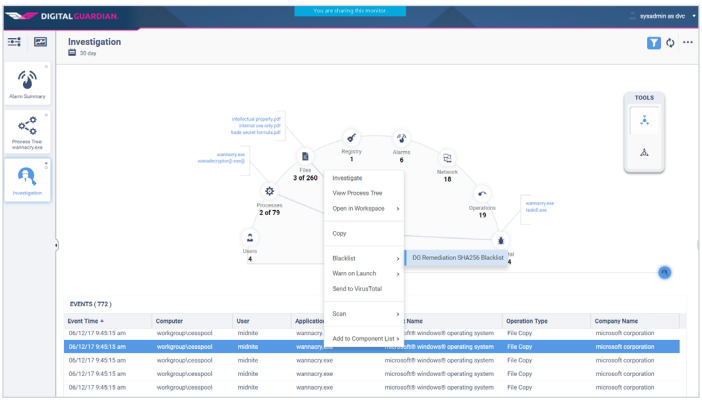
DATASHEET

DIGITAL GUARDIAN®

Digital Guardian Endpoint Detection & Response

Protect the Data for the Best Defense Against Advanced Threats

Digital Guardian delivers the first and only data-aware endpoint threat detection and response (EDR) solution. Digital Guardian's incident responders and threat hunters developed a series of workspaces to guide analysts and hunters to the events that matter for identifying and stopping anomalous and suspicious activity. Analysts can easily drill down to follow an investigation and determine next steps or create custom dashboards, reports and workspaces.



Deepest and Broadest Visibility

Deepest Visibility of Advanced Threats

Only Digital Guardian combines real-time visibility into system, user and data events with the ability to use historical detection to search across the enterprise for any existing infections or attack activity that may have occurred in the past. This provides you the needed context of data movements to enable faster and more accurate determination of the attack, its motivation and impact.

Built-In "Human Learning" Driven Endpoint Detection Automates Detection and Response

Only Digital Guardian Analytics & Reporting Cloud packages over 150 man-years of "human-powered" incident response and threat hunting best practices into preconfigured, behavior-based rules available out of the box.

One Console and One Agent For Data Visibility and Endpoint Detection & Response

Only Digital Guardian uses one console and one endpoint agent for data visibility, data protection, and endpoint detection & response. Reduce complexity. Reduce time to incident resolution. Reduce risks.

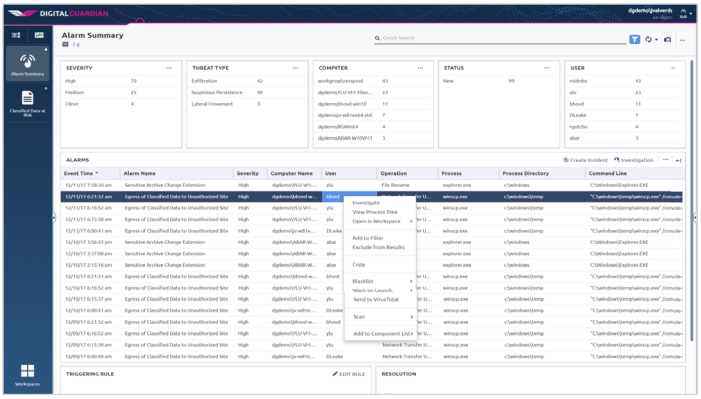
Key Benefits

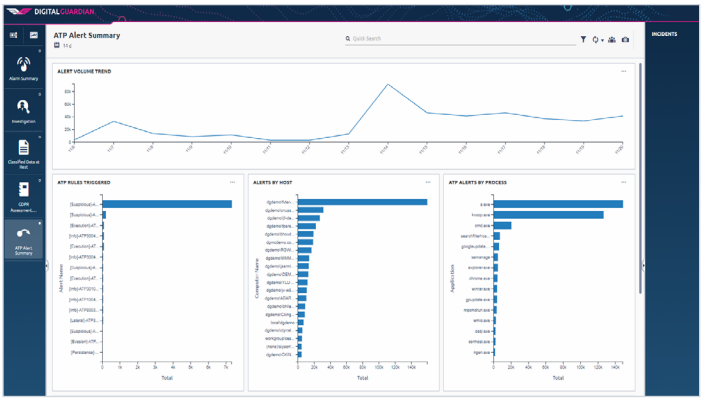
Filters Out the Noise So You Focus On Real Threats

Security teams today are overwhelmed with alerts from ineffective products that lack any context or prioritization of attacks; so they end up missing the real threats targeting their data. Digital Guardian quickly filters through potential anomalies and only triggers alarms for the high fidelity incidents that warrant additional investigation.

Detects and Blocks Advanced Threats Accross the Attack Lifecycle

What differentiates Digital Guardian is its ability to not only detect, but also easily block activity in real-time. Digital Guardian starts blocking at the attack's initial entrance vector (e.g. phishing) and keeps blocking across the entire attack lifecycle. This includes exploit installation, execution and the command and control phase; ultimately preventing data compromise.



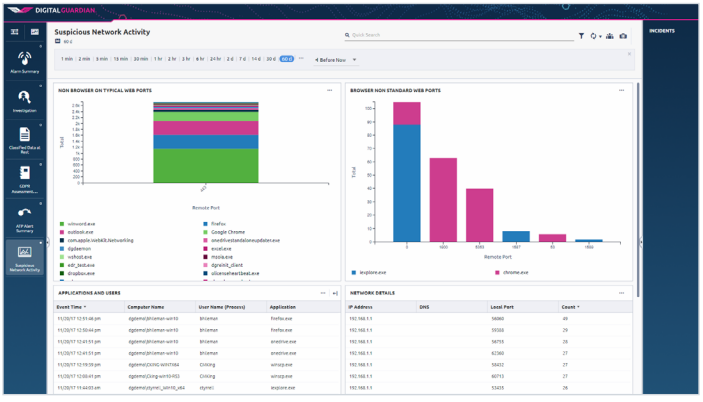


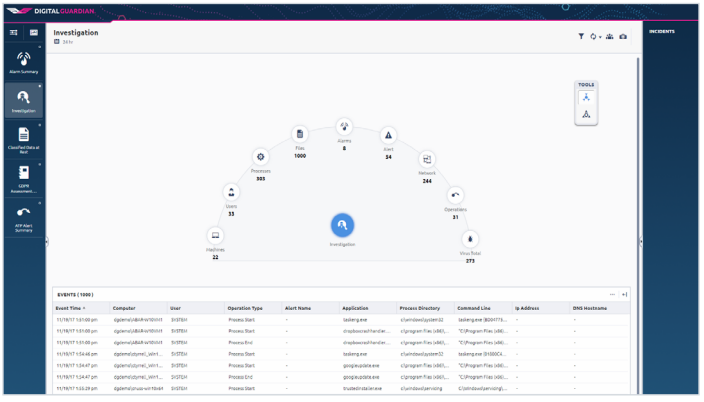
Incident Response and Threat Hunting Managed Service

With our Threat Detection and Incident Response Managed Security Program you can leverage our experts who proactively identify new threats and work with your team to quickly remediate incidents before they turn into a breach.

Comprehensive Protection from Multiple Attack Sources

Digital Guardian's behavior-based rules can automatically detect and block multiple sources of attacks - ransomware, malware, malware-free attacks and other suspicious data movements. It stops threats even if there are no IOC signatures.





ABOUT DIGITAL GUARDIAN

Digital Guardian's threat aware data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats.

By harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.

DIGITALGUARDIAN®

SHARE