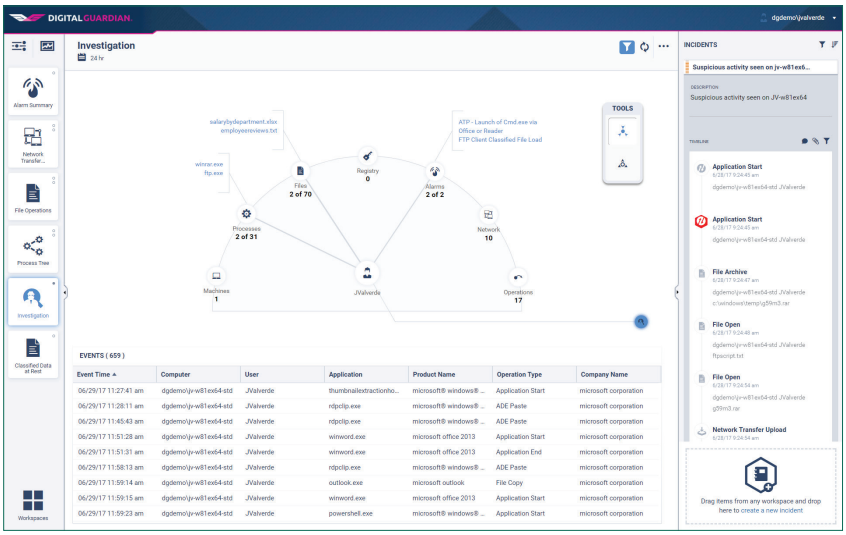
FORTRA

DATASHEET *(Digital Guardian)*

Digital Guardian Analytics & Reporting Cloud

Empower your security teams with cloud-delivered, no-compromise data protection.

Digital Guardian Analytics and Reporting Cloud (DG ARC) is an advanced analytics, workflow and reporting cloud service that delivers no-compromise data protection. Leveraging streaming data from Digital Guardian endpoint agents and network sensors, ARC provides the deepest visibility into system, user and data events. That visibility powers security analyst-approved dashboards and workspaces to enable data loss prevention and endpoint detection and response - all within the same console.



DG ARC Investigation Workspace

A Different Approach to Data Protection

Data Loss Prevention

Endpoint Detection & Response

First and Only Solution to Unify DLP and EDR

This unified solution delivers the product consolidation CISOs must demand. DG ARC puts your most sensitive information assets at the center of all data protection, activity monitoring, and endpoint detection and response activities.

Built-in "Human Learning" Endpoint Detection Automates Detection and Response

Only DG ARC packages over 150 man-years of data defense techniques and threat hunting practices into preconfigured, behavior-based rules available out of the box. These rules can detect lateral movement and elevated privilege to reveal an attack before it can do any damage.

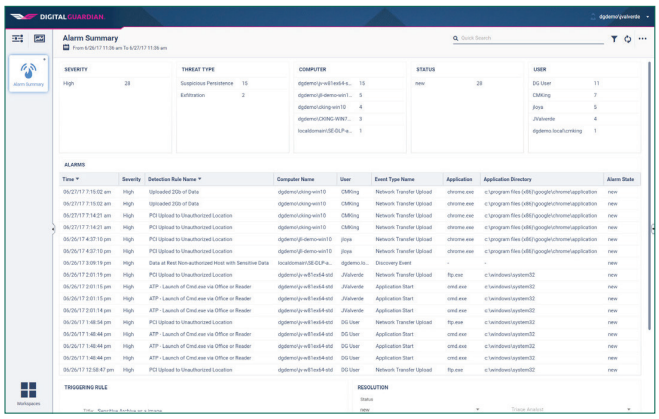
Cloud Delivered Big Data SaaS Architecture Scales With Your Enterprise

DG ARC's centralized reporting in the cloud removes storage limitations on the endpoint agent and gives you the ability to aggregate, analyze and query system, user and data related events across the network and endpoints over longer periods of time. You get big data security analytics without investing in a big data infrastructure.

Key Benefits

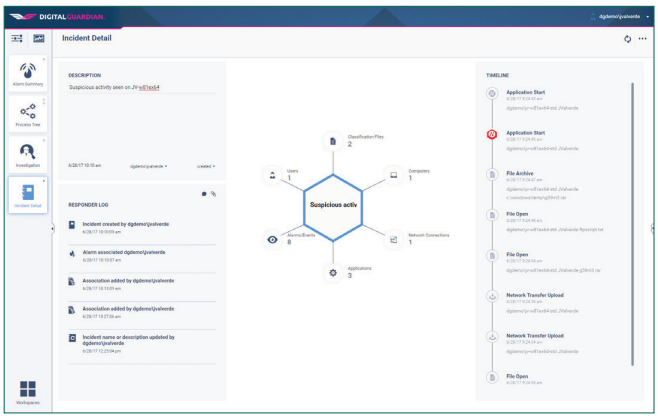
Analytics that Filter Out the Noise

DG ARC monitors the most comprehensive set of events about your systems, users and data, quickly filtering through potential anomalies. It only triggers alarms for the high fidelity events that warrant additional investigation by InfoSec and/or SOC Analysts.



Drag and Drop Incident Management

Analysts can simply drag and drop to create new incidents, add events or alarms. It's easy to add comments and artifacts. A timeline automatically builds out as you investigate an incident and work towards remediation, accelerating response time.

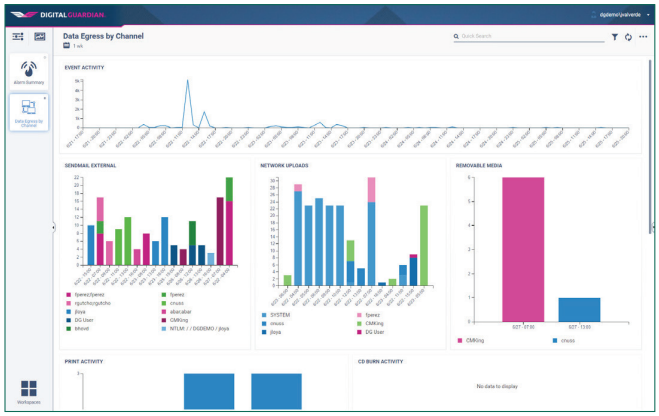


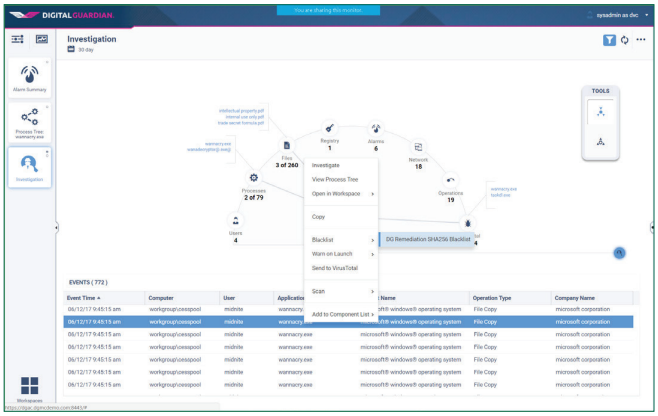
Security Analyst-Approved Workspaces

DG's experienced threat hunters and information security analysts developed workspaces to guide security professionals to the events that matter for identifying anomalous and suspicious insider and outsider activity. Analysts can easily drill down to follow an investigation and determine next steps or to create custom dashboards, reports and workspaces.

Right Click Remediation in Real Time

Security analysts can blacklist processes across the enterprise from virtually any screen for real time remediation of threats identified during incident response or threat hunting. Remediation options include blacklist, scan, warn on launch, send to VirusTotal, and more.





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.