

# 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.

The screenshot displays the Digital Guardian Investigation Workspace. The main area features a network diagram with nodes for 'File', 'Process', 'Network', and 'Operations'. Below the diagram is a table of events with columns for Event Time, Computer, User, Application, Product Name, Operation Type, and Company Name. The incidents panel on the right lists various events such as 'Application Start', 'File Archive', 'File Open', and 'Network Transfer Upload'.

Event Time	Computer	User	Application	Product Name	Operation Type	Company Name
06/29/17 11:27:41 am	dgdemo\j-w81-e854-st4	JValverde	thumbnailextractio...	microsoft® windows® ...	Application Start	microsoft corporation
06/29/17 11:28:11 am	dgdemo\j-w81-e854-st4	JValverde	rdpclip.exe	microsoft® windows® ...	ADE Paste	microsoft corporation
06/29/17 11:45:43 am	dgdemo\j-w81-e854-st4	JValverde	rdpclip.exe	microsoft® windows® ...	ADE Paste	microsoft corporation
06/29/17 11:51:28 am	dgdemo\j-w81-e854-st4	JValverde	winword.exe	microsoft office 2013	Application Start	microsoft corporation
06/29/17 11:51:31 am	dgdemo\j-w81-e854-st4	JValverde	winword.exe	microsoft office 2013	Application End	microsoft corporation
06/29/17 11:58:13 am	dgdemo\j-w81-e854-st4	JValverde	rdpclip.exe	microsoft® windows® ...	ADE Paste	microsoft corporation
06/29/17 11:59:14 am	dgdemo\j-w81-e854-st4	JValverde	outlook.exe	microsoft® outlook	File Copy	microsoft corporation
06/29/17 11:59:15 am	dgdemo\j-w81-e854-st4	JValverde	winword.exe	microsoft office 2013	Application Start	microsoft corporation
06/29/17 11:59:23 am	dgdemo\j-w81-e854-st4	JValverde	powershell.exe	microsoft® windows® ...	Application Start	microsoft corporation

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.

SEVERITY	THREAT TYPE	COMPUTER	STATUS	USER
High	Suspicious Persistence	sgpnet01-wf164-4	New	DG User
High	Malware	sgpnet01-wf164-4	New	DG User
High	Unauthenticated Location	sgpnet01-wf164-4	New	John
High	Unauthenticated Location	sgpnet01-wf164-4	New	JYVince
High	Unauthenticated Location	sgpnet01-wf164-4	New	sgpnet01-wf164-4

Time	Severity	Detection Rule Name	Computer Name	User	Event Type Name	Application	Application Binary	Alarm State
06/22/17 7:14:02 am	High	Updated EDR of Data	sgpnet01-wf164-4	CGMing	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/22/17 7:14:02 am	High	Updated EDR of Data	sgpnet01-wf164-4	CGMing	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/22/17 7:14:23 am	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	CGMing	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/22/17 7:14:23 am	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	CGMing	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/20/17 4:25:10 pm	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	John	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/20/17 4:27:10 pm	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	John	Network Transfer Upload	chrome.exe	c:\program files (x86)\google\chrome\application	new
06/20/17 3:08:18 pm	High	Data at Rest Non-authorized Host with Sensitive Data	sgpnet01-wf164-4	JYVince	Discovery Event	-	-	new
06/20/17 2:05:16 pm	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	JYVince	Network Transfer Upload	File.exe	c:\windows\system32	new
06/20/17 2:05:16 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	JYVince	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 2:01:15 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	JYVince	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 2:01:14 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	JYVince	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 1:48:48 pm	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	DG User	Network Transfer Upload	File.exe	c:\windows\system32	new
06/20/17 1:48:48 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	DG User	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 1:48:48 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	DG User	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 1:48:48 pm	High	ATP - Launch of Cmd.exe via Office or Reader	sgpnet01-wf164-4	DG User	Application Start	cmd.exe	c:\windows\system32	new
06/20/17 1:25:47 pm	High	PC Unauth to Unauthenticated Location	sgpnet01-wf164-4	DG User	Network Transfer Upload	File.exe	c:\windows\system32	new

**DESCRIPTION**  
Suspicious activity seen on **JYVince**

**RESPONSE LOG**

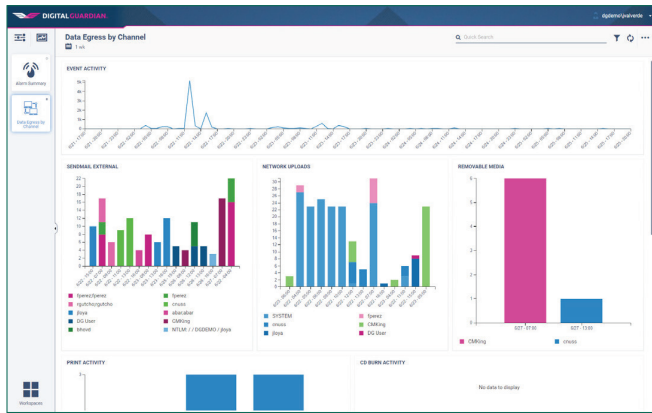
- Incident created by sgpmnet01-wf164-4
- Association added by sgpmnet01-wf164-4
- Association added by sgpmnet01-wf164-4
- Association added by sgpmnet01-wf164-4
- Association added by sgpmnet01-wf164-4
- Association added by sgpmnet01-wf164-4

**TIMELINE**

- Application Start
- Application Start
- File Access
- File Open
- File Open
- Network Transfer Upload
- Network Transfer Upload
- File Open

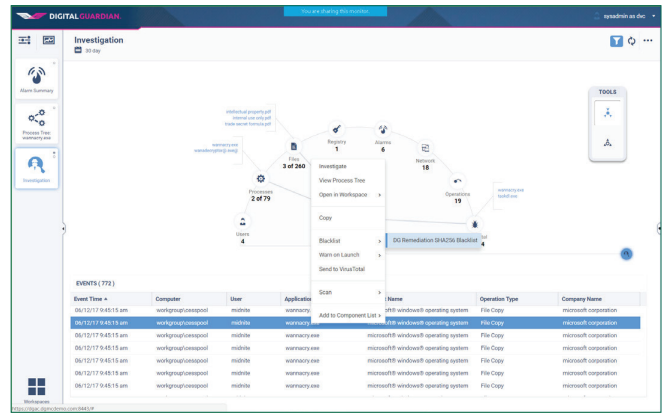
### Security Analyst-Approved Workspaces

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.



**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](https://fortra.com).