Combine Risk Analysis and Risk Discovery to Improve DLP

Justin Bortnick - VP Solutions Engineering

Justin Bortnick – VP Solutions Engineering

- VP Solutions Engineering 12 years; 6 years with Digital Guardian
  - Assisted in implementing and deploying over 40k agents in 2 weeks
- Passionately solving problems for customers by understanding their business and security needs
- Expert in data protection from all threats

DIGITALGUARDIAN®
by HelpSystems

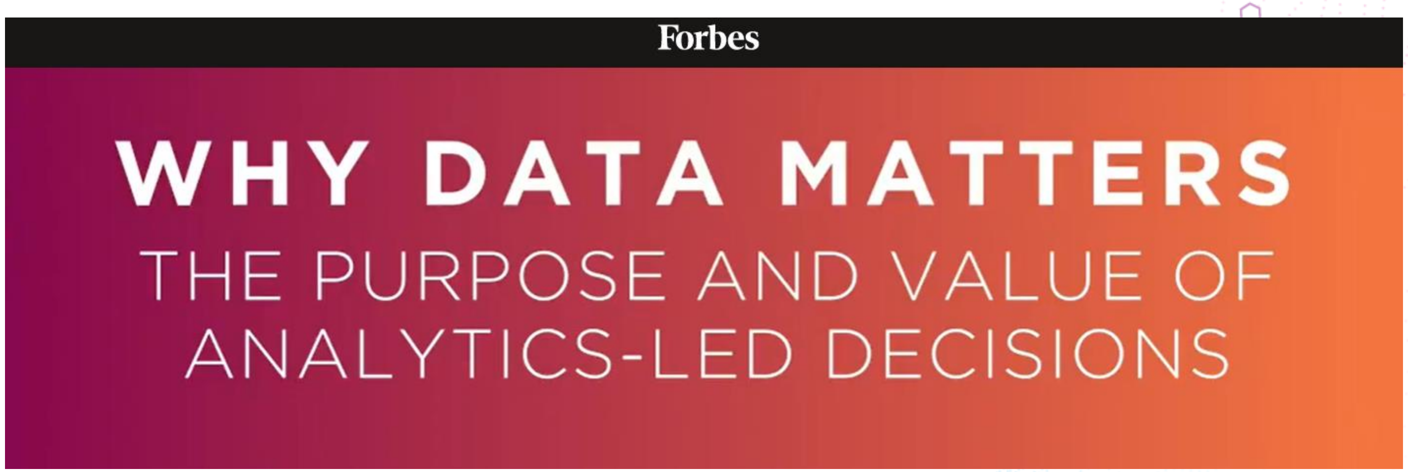
Bill Bradley – Director of Marketing

- Leads Global Marketing for Digital Guardian Data Protection
- 20+ years of Marketing & Sales Experience
  - Field Sales, Competitive Analysis, Product Marketing & Management
- Previously at Rapid7 and General Electric

Agenda

- Top Challenges With Protecting Key Data Types
- Guiderails vs Guardrails for Data Protection
- Why Both Risk Discovery and Risk Analysis
- About Digital Guardian
- Questions

Feeding Your Business Growth Engine



Forbes

WHY DATA MATTERS

THE PURPOSE AND VALUE OF ANALYTICS-LED DECISIONS

“In the world today, ***data is probably the thing that matters most****. It can tell you before the airplane’s brakes fail. It can predict the onset of a natural disaster or forecast when you might suffer a heart attack. This isn’t fantasy or a future state. It’s happening today.”*

Source: https://www.forbes.com/sites/teradata/2020/10/15/why-data-matters/?sh=247b33706886

Feeding Your Business Growth Engine

Forbes

WHY DATA MATTERS

InfoSec leaders must protect the data to feed the actionable insights needed for growth!

“In the wor … ***ost****. It can*
tell you bef … *t of a*
natural disaster or forecast when you might suffer a heart attack. This isn’t fantasy or a future state. It’s happening today.”

Source: https://www.forbes.com/sites/teradata/2020/10/15/why-data-matters/?sh=247b33706886

Data Protection Would be Simple…

Well trained
Motivated
Accurate

Intellectual Property

Regulated Data

Data Protection Would be Simple if it Weren’t For…

Intellectual Property

Stressed

Untrained

Well trained
Motivated
Accurate

Not motivated

Sloppy

Disgruntled

Compromised

Regulated Data

Guiderails and Guardrails to Protect Your Data

- Guiderails
  - Soft limits
  - Provide coaching, feedback
  - Allow for self-correction
  - Lower impact

- Guardrails
  - Hard limits
  - Prevent more serious incident
  - Automatic after exceeding guidelines
  - Higher impact

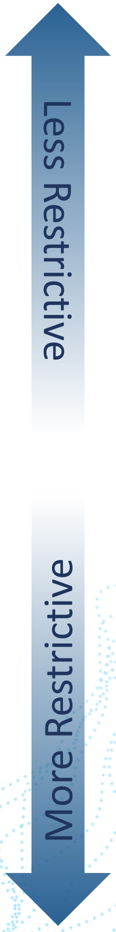
Effective data protection relies on both
The balance varies based on your business

Source: https://aashtojournal.org/2019/05/31/aashto-issues-second-edition-of-low-volume-roads-guidelines/

Source: https://www.maxpixel.net/photo-6114995

Guiderails and Guardrails in Data Loss Prevention

- DLP Guiderails & Guardrails are a Business Wide Decision
  - No surprises for end users or business unit leaders
  - Provide coaching and education about policies
  - Automated action can prevent greater damage
- Graduated and Aligned with the Business
  - Today and tomorrow



Log

Alert

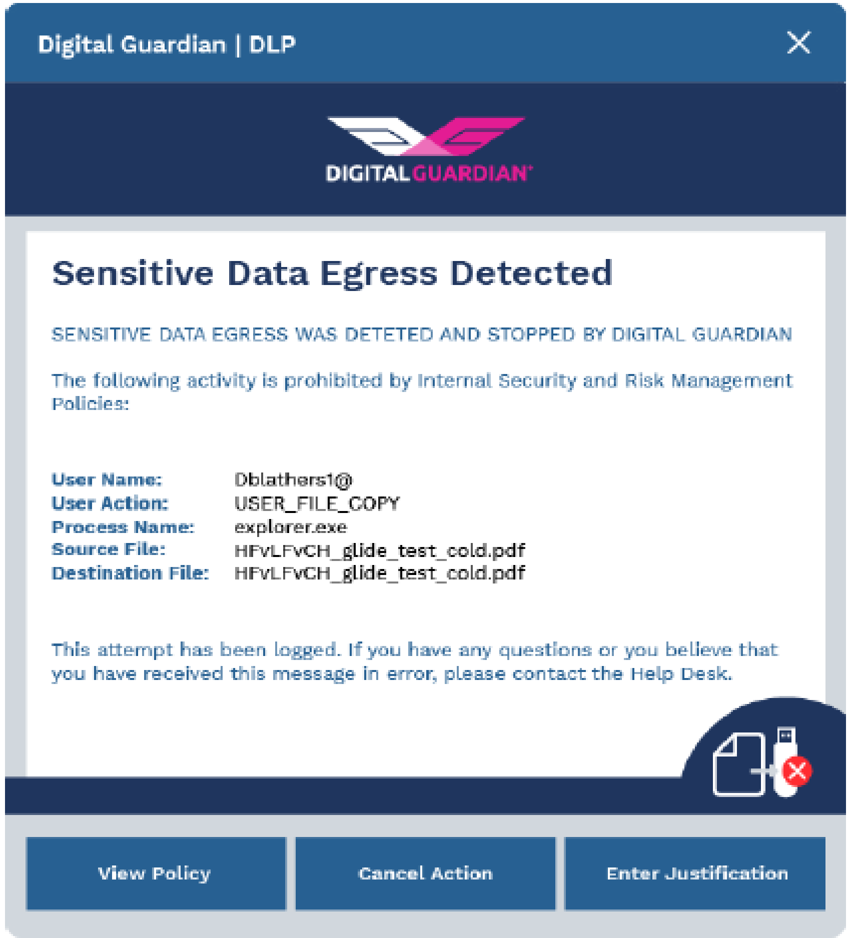
Prompt

Justify

Encrypt

Quarantine

Block



Sensitive Data Egress Detected

SENSITIVE DATA EGRESS WAS DETETED AND STOPPED BY DIGITAL GUARDIAN

The following activity is prohibited by Internal Security and Risk Management Policies:

User Name:	Dblathers1@
User Action:	USER_FILE_COPY
Process Name:	explorer.exe
Source File:	HFvLFvCH_glide_test_cold.pdf
Destination File:	HFvLFvCH_glide_test_cold.pdf

This attempt has been logged. If you have any questions or you believe that you have received this message in error, please contact the Help Desk.

Secure Business Processes; Reduce Impact & Risk

Known Risks: Visibility & Analysis

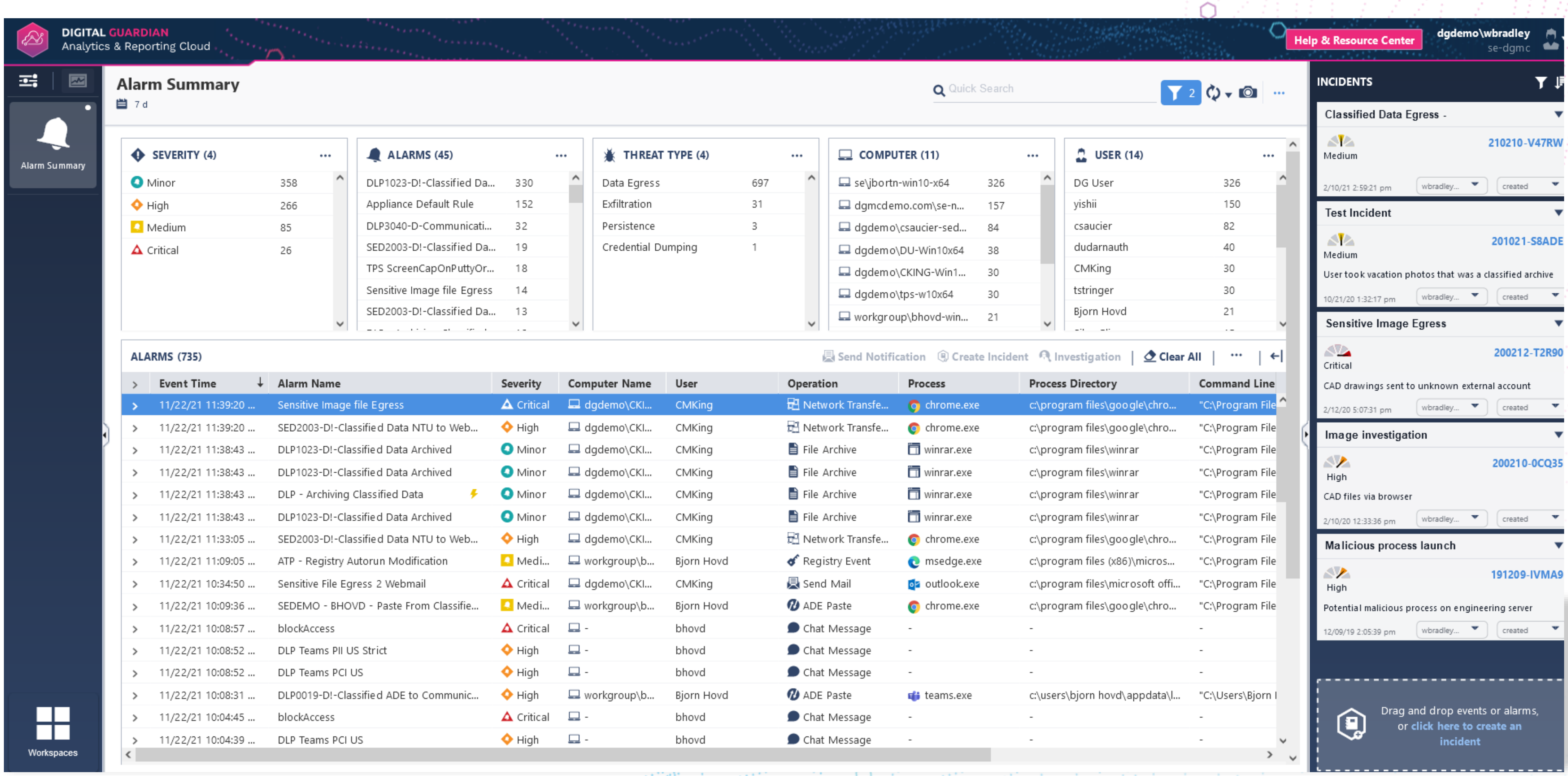
- Use-case based approach
- Compliance or IP protection
- Understand and secure existing business processes
- Focus on known data types, flows, groups & risks

← Continuous Risk Management →

Unknown Risk: Discovery & Quantification

- Know what I don’t know
- Locate data hotspots; learn data flows
- No policy; no problem
- Focus on unknown data types, flows, groups & risks

DG Platform Demo



Alarm Summary

7 d

Quick Search

SEVERITY (4)

Minor	358
High	266
Medium	85
Critical	26

ALARMS (45)

DLP1023-D!-Classified Da...	330
Appliance Default Rule	152
DLP3040-D-Communicati...	32
SED2003-D!-Classified Da...	19
TPS ScreenCapOnPuttyOr...	18
Sensitive Image file Egress	14
SED2003-D!-Classified Da...	13

THREAT TYPE (4)

Data Egress	697
Exfiltration	31
Persistence	3
Credential Dumping	1

COMPUTER (11)

se\jbortn-win10-x64	326
dgmcdemo.com\se-n...	157
dgdemo\csaucier-sed...	84
dgdemo\DU-Win10x64	38
dgdemo\CKING-Win1...	30
dgdemo\tps-w10x64	30
workgroup\bhovd-win...	21

USER (14)

DG User	326
yishii	150
csaucier	82
dudarnauth	40
CMKing	30
tstringer	30
Bjorn Hovd	21

ALARMS (735)

Send Notification | Create Incident | Investigation | Clear All

Event Time	Alarm Name	Severity	Computer Name	User	Operation	Process	Process Directory	Command Line
11/22/21 11:39:20 ...	Sensitive Image file Egress	Critical	dgdemo\CKI...	CMKing	Network Transfe...	chrome.exe	c:\program files\google\chro...	"C:\Program File
11/22/21 11:39:20 ...	SED2003-D!-Classified Data NTU to Web...	High	dgdemo\CKI...	CMKing	Network Transfe...	chrome.exe	c:\program files\google\chro...	"C:\Program File
11/22/21 11:38:43 ...	DLP1023-D!-Classified Data Archived	Minor	dgdemo\CKI...	CMKing	File Archive	winrar.exe	c:\program files\winrar	"C:\Program File
11/22/21 11:38:43 ...	DLP1023-D!-Classified Data Archived	Minor	dgdemo\CKI...	CMKing	File Archive	winrar.exe	c:\program files\winrar	"C:\Program File
11/22/21 11:38:43 ...	DLP - Archiving Classified Data	Minor	dgdemo\CKI...	CMKing	File Archive	winrar.exe	c:\program files\winrar	"C:\Program File
11/22/21 11:38:43 ...	DLP1023-D!-Classified Data Archived	Minor	dgdemo\CKI...	CMKing	File Archive	winrar.exe	c:\program files\winrar	"C:\Program File
11/22/21 11:33:05 ...	SED2003-D!-Classified Data NTU to Web...	High	dgdemo\CKI...	CMKing	Network Transfe...	chrome.exe	c:\program files\google\chro...	"C:\Program File
11/22/21 11:09:05 ...	ATP - Registry Autorun Modification	Medi...	workgroup\b...	Bjorn Hovd	Registry Event	msedge.exe	c:\program files (x86)\micros...	"C:\Program File
11/22/21 10:34:50 ...	Sensitive File Egress 2 Webmail	Critical	dgdemo\CKI...	CMKing	Send Mail	outlook.exe	c:\program files\microsoft offi...	"C:\Program File
11/22/21 10:09:36 ...	SEDEMO - BHOVD - Paste From Classifie...	Medi...	workgroup\b...	Bjorn Hovd	ADE Paste	chrome.exe	c:\program files\google\chro...	"C:\Program File
11/22/21 10:08:57 ...	blockAccess	Critical	-	bhovd	Chat Message	-	-	-
11/22/21 10:08:52 ...	DLP Teams PII US Strict	High	-	bhovd	Chat Message	-	-	-
11/22/21 10:08:52 ...	DLP Teams PCI US	High	-	bhovd	Chat Message	-	-	-
11/22/21 10:08:31 ...	DLP0019-D!-Classified ADE to Communic...	High	workgroup\b...	Bjorn Hovd	ADE Paste	teams.exe	c:\users\bjorn hovd\appdata\l...	"C:\Users\Bjorn I
11/22/21 10:04:45 ...	blockAccess	Critical	-	bhovd	Chat Message	-	-	-
11/22/21 10:04:39 ...	DLP Teams PCI US	High	-	bhovd	Chat Message	-	-	-

INCIDENTS

Classified Data Egress -
Medium — 210210-V47RW
2/10/21 2:59:21 pm — wbradley... — created

Test Incident
Medium — 201021-S8ADE
User took vacation photos that was a classified archive
10/21/20 1:32:17 pm — wbradley... — created

Sensitive Image Egress
Critical — 200212-T2R90
CAD drawings sent to unknown external account
2/12/20 5:07:31 pm — wbradley... — created

Image investigation
High — 200210-0CQ35
CAD files via browser
2/10/20 12:33:36 pm — wbradley... — created

Malicious process launch
High — 191209-IVMA9
Potential malicious process on engineering server
12/09/19 2:05:39 pm — wbradley... — created

Drag and drop events or alarms, or click here to create an incident

DIGITALGUARDIAN®
by HelpSystems

Digital Guardian for Data Protection

Classify, Control, and Secure All You Sensitive Data

Digital Guardian is Now a Part of

helpsystems

DIGITAL GUARDIAN®
by HelpSystems

HelpSystems for Cybersecurity

DATA SECURITY

IDENTITY & ACCESS MANAGEMENT

INFRASTRUCTURE PROTECTION

DIGITAL GUARDIAN®
by HelpSystems

Data Protection Suite

Data Security Platform Designed for Today’s Hybrid Reality

Classify

Understand what data is sensitive so you can prioritize protection

+

Control

Enterprise-wide **data protection** across the entire threat landscape

+

Secure

Collaborate securely with encrypt and control access to files

titus

DIGITALGUARDIAN®
by HelpSystems

vera

DIGITALGUARDIAN®
by HelpSystems

Digital Guardian for No-Compromise Data Protection

powered by aws

Cloud-Delivered

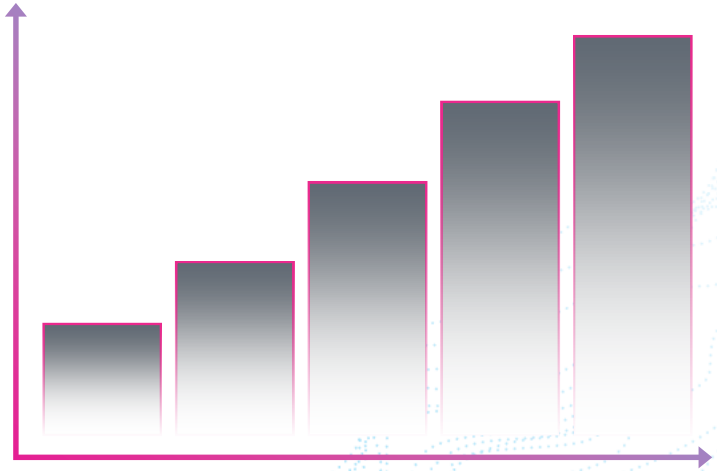
Cross Platform

Flexible Controls

DIGITAL GUARDIAN®
by HelpSystems

Cloud-Delivered for Simpler, Better Data Protection

Simpler

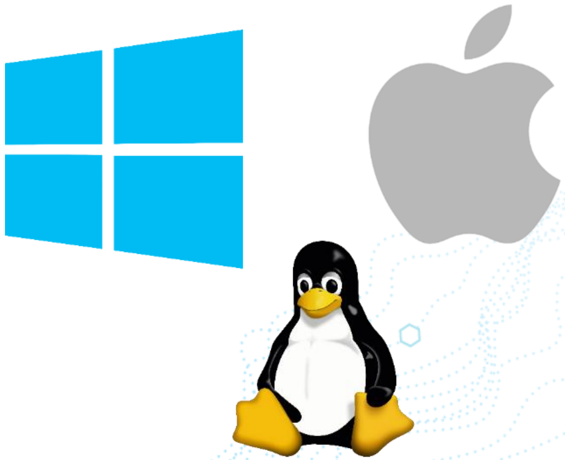


Scalable

Aggregation of Intel

Comprehensive Cross Platform Coverage

Browser or Application



Operating System

On & Off Network

Controls that STOP Data Loss

Monitor

Prompt

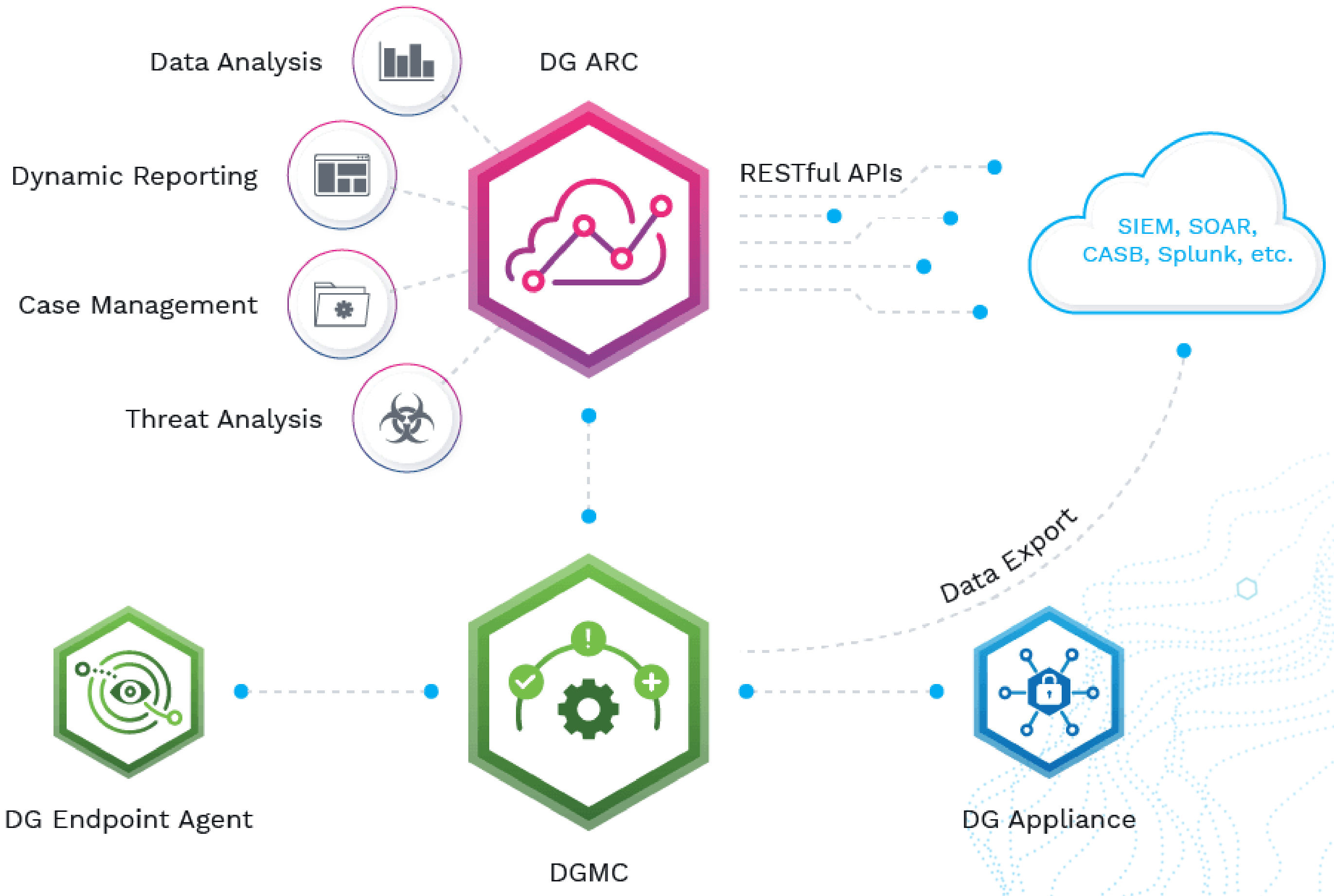
Block

Flexible

Powerful

DIGITALGUARDIAN®
by HelpSystems

Data Protection Portfolio



- Analytics & Reporting Cloud (ARC)
- Endpoint Agent
- Network Appliance
- Applications
  - Discovery
  - Classification
  - DLP
  - MDR
  - DRM
- Management Console

DIGITALGUARDIAN®
by HelpSystems

Digital Guardian Software as a Service (SaaS)

Digital Guardian Managed Security Program

powered by aws

DIGITAL GUARDIAN®
by HelpSystems

Questions

DIGITAL GUARDIAN®
by HelpSystems