FORTRA

How Digital Guardian Helps Organizations

Overcome 7 Data Protection Challenges

How Digital Guardian Helps Organizations Overcome 7 Data Protection Challenges

As the world faces cyber challenges previously unknown, the field of data protection needs to keep pace with the exploits of today. The burgeoning of artificial intelligence, machine learning, and large language models has created new obstacles in an already complex environment filled with hyperconnected machines, hyperdistributed workflows, and an infinitely expanding attack surface.

Many companies already have a tool in place to monitor data. That alone is only part of the solution. A comprehensive data protection platform like Fortra's Digital Guardian is needed to secure all facets of digital data today, at scale, across any environment, and within evolving compliance boundaries.

7 Data Protection Challenges Solved by Digital Guardian

1

Solutions that Create Both False Negatives and False Positives

2

Products that Sacrifice Either Security or Productivity

3

Limited Visibility

4

Failing to Keep Pace with New Compliance Regulations

5

Siloing Reporting, Which Complicates Understanding of the Attack Chain

6

Failing to Service the Cloud; Instead Deploying Directly On-Premises or on the Network

7

Requiring Dedicated Resources that are in Thin Supply for Most Organizations

Where Data Loss Prevention (DLP) Stands Today

We're living in a world where data is big and getting bigger. IDC estimates that by 2025, 463 exabytes of data will be created every single day. While this means wonderful things for business, sprawling amounts of information can quickly become a beast too difficult for traditional data defense tools to wrangle. And that means internally or externally, intentionally or unintentionally, more data than ever is now at risk for loss or theft. The stats tell the story:

- The most recent Verizon Data Breach Investigation Report recorded over 5,000 confirmed breaches in the past year, and over 16,000 incidents where data was compromised.
- With each data breach now costing nearly $4.5 million USD, it's safe to assume that the average company would be unable to withstand the blow.
- The digital landscape has shifted dramatically in the past several years, with the hybrid workforce model here to stay and 89% of organizations migrating data to the cloud in the past twelve months.

What we see is that it is more important than ever to provide strong and coordinated protection across all user touchpoints with sensitive data, and yet concurrently harder and more complicated to do so.

Much has been made of the drawbacks of legacy DLP over the years, especially as many enterprises have embraced digital transformation and adopted cloud technology. Digital Guardian, with 20 years experience protecting valuable data and IP, can help organizations overcome 7 of the biggest data protection challenges facing businesses today, including:

1. Solutions that create both false negatives and false positives
2. Products that sacrifice either security or productivity
3. Limited visibility
4. Failing to keep pace with new compliance regulations
5. Siloing reporting, which complicates understanding of the attack chain
6. Failing to service the cloud; instead deploying directly on-premises or on the network
7. Requiring dedicated resources that are in thin supply for most organizations

In today's evolving environment, most status-quo DLP solutions are hard to set up, scale, and maintain. They offer insufficient operating system, browser, and application coverage, and those limitations can be disruptive to end users. Additionally, they are not understood and supported properly by business leaders, lessening their effectiveness even more. "DLP lite" alternatives have hit the market, touting "easy to install" agents, but they have no teeth. These lighter offerings offer no controls to stop the loss of sensitive data; after all, data loss detection is very different from data loss prevention. Integrated DLP offerings manage to leverage existing investments, but they, too, leave critical vectors open to sensitive data egress due to an inherently siloed approach.

These fits and starts have only played into the years-long debate over whether DLP is really dead. Comprehensive DLP (which includes Endpoint DLP (eDLP), Network DLP (nDLP), and a host of other cloud-delivered functionalities) is taking over at a time when the industry needs it the most and Fortra's Digital Guardian is proud to be leading the charge.

1

Solutions that Create Both False Negatives and False Positives

Solutions that Create Both False Negatives and False Positives

The problem: Companies today handle complex data across highly connected environments. Typical data classification (DC) policies are unable to keep up, and current DLP solutions strain under the weight as resources scale and manually crafted policies show their limitations. Insufficient policies create mistakes, and teams are barraged by thousands of alerts generated in error. Security analysts spend up to a quarter of their time chasing false positives, and even pre-pandemic, 70% reported that up to 75% of the alerts they investigate each day are moot. The cost, complexity, and resources required to follow up on false positives is not sustainable, and too much time is spent continuously tuning DC policies. Fewer false positives would originate if your data was easier to find, track, and organize. Additionally, false negatives can occur when data governance tools fail to catch leaked data than has left the network, resulting in an even more critical situation.

The DG Solution: Digital Guardian's approach to data protection, leveraging a unique context-based approach, ensures data is reliably and automatically classified, then labelled and marked appropriately. This ensures that at the point of enforcement, accurate decisions are automatically made and minimizes false positives and the need for human interaction.

- **Accurate data classification.** Digital Guardian combines content, context, and user-based classification for a three-tiered approach, classifying data immediately after installation, eliminating the need for up-front discovery scans.
- **Content-based classification.** Digital Guardian detects important keywords when the file is in use, then labels them accordingly. This can include numbers that resemble social security numbers, bank account information, medical keywords, and more.

- **Context-based classification.** Digital Guardian identifies critical file shares, cloud shares, databases, and applications and classifies files when saved from those locations to the local system. This aggregates based on file metadata such as file type, keywords in the file name, or whether the file originates from a certain website.
- **User-based classification.** Digital Guardian extends what was previously possible in a data classification solution, allowing Digital Guardian to offer the most unique and comprehensive data classification solution.

Additionally, Digital Guardian can utilize our unique data classification solution (Fortra's Data Classification Suite) to augment the accuracy of each DLP detection, as well as improve alert quality across other areas of your ecosystem. DCS offers the deepest metadata support for data labeling for more accurate DLP.


Digital Guardian
Classified Data at Rest -
60 d
Quick Search
Alarm Summary
Classified Data at Rest -
FILE DISCOVERY TIMELINE
H D W M
60k
50k
40k
30k
20k
10k
0
Sat 23 Mon 25 Wed 27 Fri 29 Mar 3 April Wed 03 Fri 05 Apr 07 Tue 09 Thu 11 Sat 13 Mon 15 Wed 17 Fri 19 Apr 21 Tue 23 Thu 25 Sat 27 Mon 29 May Fri 03 May 05 Tue 07 Thu 09 Sat 11 Mon 13 Wed 15 Fri 17 May 19
REPOSITORY NAME
dgdemo\tps-w10x64 (119,441)
examplecompany\LCA_AWS_W2019server (88,388)
examplecompany\CLIENTB2 (75,563)
se\DGDemo_JM (64,937)
tituscloud\rthomas-dg (60,416)
dgdemo\jgourlaouen-w10 (53,536)
workgroup\DESKTOP-UEGNAJD (52,303)
CLASSIFICATION RULE (21)
Classification Name Total
DLP1000-Context Classification-Restricted 72,579
PHI1001-Content Classification-PHI Low 1,314
PHI1004-Content Classification-PHI Simple 971
PCI1001-Content Classification-PCI Low 664
PII1002-Content Classification-PII Med 460
PCI1002-Content Classification-PCI Med 410
PHI1003-Content Classification-PHI High 291
PHI1002-Content Classification-PHI Med 234
PII1001-Content Classification-PII Low 203
Titus t_class_3 167
PII1049-Content Classification-PII PERU 162
PII1003-Content Classification-PII High 133
PCI1003-Content Classification-PCI High 76
Titus t_class_4 61
Titus t_class_2 40
Titus t_class_1 34
PII1010-Content Classification-PII AUSTRIA 9
CLASSIFICATION CONTENT PATTERNS (34)
Classification Name Pattern Frequency Total Files
address 649,340 31,592
custom_phonenumber 270,637 31,440
custom_person 359,107 23,108
custom_ccn_keywords 179,486 22,678
cc_custom_any_v04 357,075 20,046
custom_ssn_keywords 89,592 17,544
custom_ssn_dash_v02 303,767 12,773
email_address 199,303 12,126
custom_ssn_nodelimiter_v02 97,516 9,500
dx_codes 44,836 8,594
custom_ssn_space_v02 14,783 7,508
custom_phikeywords 37,025 4,937
hcpcs_codes 3,865 2,155
IPData-DemoData (Unstructured) 952 952
DU Passwords (Pattern Match) 101,037 678
CCN (Pattern Match) 87,200 120
peru_dni 3,752 106

2

Products that Sacrifice Either Security or Productivity

Products that Sacrifice Either Security or Productivity

The problem: Your security teams constantly juggle between stringent security protocols and day-to-day effectiveness. All too often, one of the balls drops. While DLP solutions aim to protect sensitive data, they sometimes hinder productivity due to limited processing power and lack of policy flexibility. That makes balancing things like collaboration and large batch transfers difficult to reconcile with gapless security.

The DG Solution: Digital Guardian enables organizations to define rules and exceptions based on user roles, the level of data sensitivity, and what AI-based tools can learn via machine learning. Granular controls, from "log and monitor" to "block," automatically protect data before it's lost, saving your team time and oversight. And if time for creating policies runs short, our "risk discovery" approach lets your team see where data resides and flows, as well as its risks.

Additionally, our support for all operating systems and any browser (without installing an extension) helps minimize time to value and eliminate potential efficiency-sapping snags along the way. For instance, other DLP providers would be unable to detect data theft over Chrome if the browser was recently upgraded to the latest version, resulting in a Help Desk ticket and a session with a support engineer who would then require the user to install an extension on their machine. With Digital Guardian, teams benefit from flexible deployment options that work wherever they do, saving them time upfront and along the way.

3

Limited Visibility

Limited Visibility

The problem: Most DLP solutions build rules around known instances of data loss, producing alerts in a limited "letterbox" view. However, this leaves the organization vulnerable when an unknown risk pops up, causing customers to capture transmitted data for further analysis. While this may help, it requires dedicated analytic resources, with raised privileges and additional stores of sensitive data that need to be secured and protected.

At this point, complex environments are still preventing traditional DLP policies from grasping the full picture of each incident. Recent research by ESG confirms that the majority (78%) of organizations only have a "strong awareness" of less than 80% of their assets. If companies struggle to keep track of the assets themselves, how will they be able to navigate what's being done to them or create sufficient policies to secure them?

The DG Solution: Digital Guardian can gather vast amounts of data activity events by default, without policy triggers. This allows all the data activity before and after that "letterbox" view event to be analyzed, giving greater context and understanding without the need to see the sensitive data. To prevent data loss at scale, deep visibility is required that doesn't compromise the integrity of the data itself.

It does this in two ways:

- Real-time visibility into system, user, and data events such as file save-as, file rename, file/document delete, file copy, cut, paste, system reboot, and content copy.
- Historical detection searches across the enterprise for existing egress and attack activity that may have occurred in the past.

Digital Guardian's endpoint engine performs this analysis in real-time, stopping risky activity and preprocessing alerts so they are immediately actionable when they hit the management console.

Using our advanced analytics engine, you can:

- View high-level snapshots of sensitive data usage across the enterprise
- Drill down to relevant information at the user, machine, or file level
- Target investigations by users or groups using our integrated forensics capabilities
- Integrate Digital Guardian event logs with SIEMs and other event aggregators

Behind our advanced analytics and reporting capabilities is Analytics and Reporting Cloud (ARC), powered by AWS, which leverages streaming data from endpoints and appliances to provide deep visibility into systems, data, and user events to provide the context you need to identify and remediate threats.


Insights
Top Egress by Channel
REMOVABLE
PRINT 55 Alarms
UPLOAD 1.0k Alarms
FILE COPY 298 Alarms
FILE MOVE 75 Alarms
EMAIL 253 Alarms
Top Data Egress by Users
RISKIEST USERS
Name | Sensitive File Egress | Non Sensitive File Egress | Sensitive Data Egress | Non Sensitive Data Egress
cgray | 71 | 7 | 26.61 MB | 5.05 MB
ylu | 36 | 10 | 9.68 MB | 3.26 MB
mitch.cha... | 8 | 0 | 7.91 MB | 0 B
Bob | 6 | 8 | 3.90 MB | 111.92 KB
bob | 44 | 70 | 3.56 MB | 17.20 MB
Top Data Protected by User
TOP USERS
Name | Files | Egressed | Blocked
cgray | 159 | DG Protected | 107.96 MB
mchapman | 80 | DG Protected | 90.03 MB
Bob | 37 | DG Protected | 30.79 MB
DG User | 114 | DG Protected | 20.26 MB
lcaleiras | 159 | DG Protected | 17.78 MB
Web
Email
Print
Removable Drive
DATA PROTECTED 0.3 GB
NON SENSITIVE DATA EGRESS 0.2 GB
SENSITIVE DATA EGRESS 59.6 MB
Data Protected
Non Sensitive Data Egress
Sensitive Data Egress
Security Analytics in Action
825 Events
Policies Applied
5.81 Agent Alerts
0.3 GB Data Protected
7.38 Alarms
18 Incidents Logged
1 Critical
2 High
15 Medium
10 Closed
8 Created
Top Suspicious Processes
THREAT INTEL
No matching results
Adjust time range selector or filter
Policy Violations
Data Protected
Mar 17 Mar 24 Mar 31 Apr 07 Apr 14 Apr 21 Apr 28 May 05 May 12
Policy Violations
Top Rules Protecting Your Data
TOP POLICIES
Name | Triggered | Sensitive Data Egress | Non Sensitive Data Egress
DLP2004... | 243 | 3.35 MB* | 0 B
SED200... | 111 | DG Protected | 0 B
SED200... | 78 | 57.14 KB* | 0 B
SEDEM... | 73 | 699.13 KB* | 0 B
SED200... | 71 | 33 KB* | 0 B
* It is recommended to review the blocking action for each rule

4

Failing to Keep Pace with New Compliance Regulations

Failing to Keep Pace with New Compliance Regulations

The problem: Organizations must keep up with the constantly changing government, industry, and often private security requirements of an evolving digital climate. To be compliant, all data pertaining to a particular compliance requirement must be identified and accounted for on a regular and ongoing basis. However, complex internal environments and hyperdistributed ecosystems make it difficult to locate, and therefore protect all relevant information. Almost 33% of security leaders say that their ability to comply with regulatory requirements could be negatively impacted by a lack of visibility of sensitive data. Nearly nine in ten report not having that visibility.

The DG Solution: Compliant data is visible data. Locating compliance-sensitive content becomes simpler, easier, and more automated when data is classified. Digital Guardian makes it possible for you to gain visibility into your organization's sensitive information on day one and understand exactly where your company's PII, PCI, IP, and PHI data reside (and more), along with how it's being used. Plus, get the added benefits of device control and encryption to help you maintain control of your compliance-sensitive information.

Use Digital Guardian to help you comply with regulations in between with and such as GDPR, HIPAA, PCI DSS, ITAR, DPDP act and many more.

Monitor PII, PHI, IP, PCI, and PHI data autonomously:

- DG agents immediately start classifying and tagging compliance-relevant data via automatic content inspection.

- Tags remain with the data no matter its movement, giving you persistent visibility.

Provide Real-time visibility of data transmission:

- Get near real-time reports on the movement of data based on its classification.
- Set alerts for policy violations.

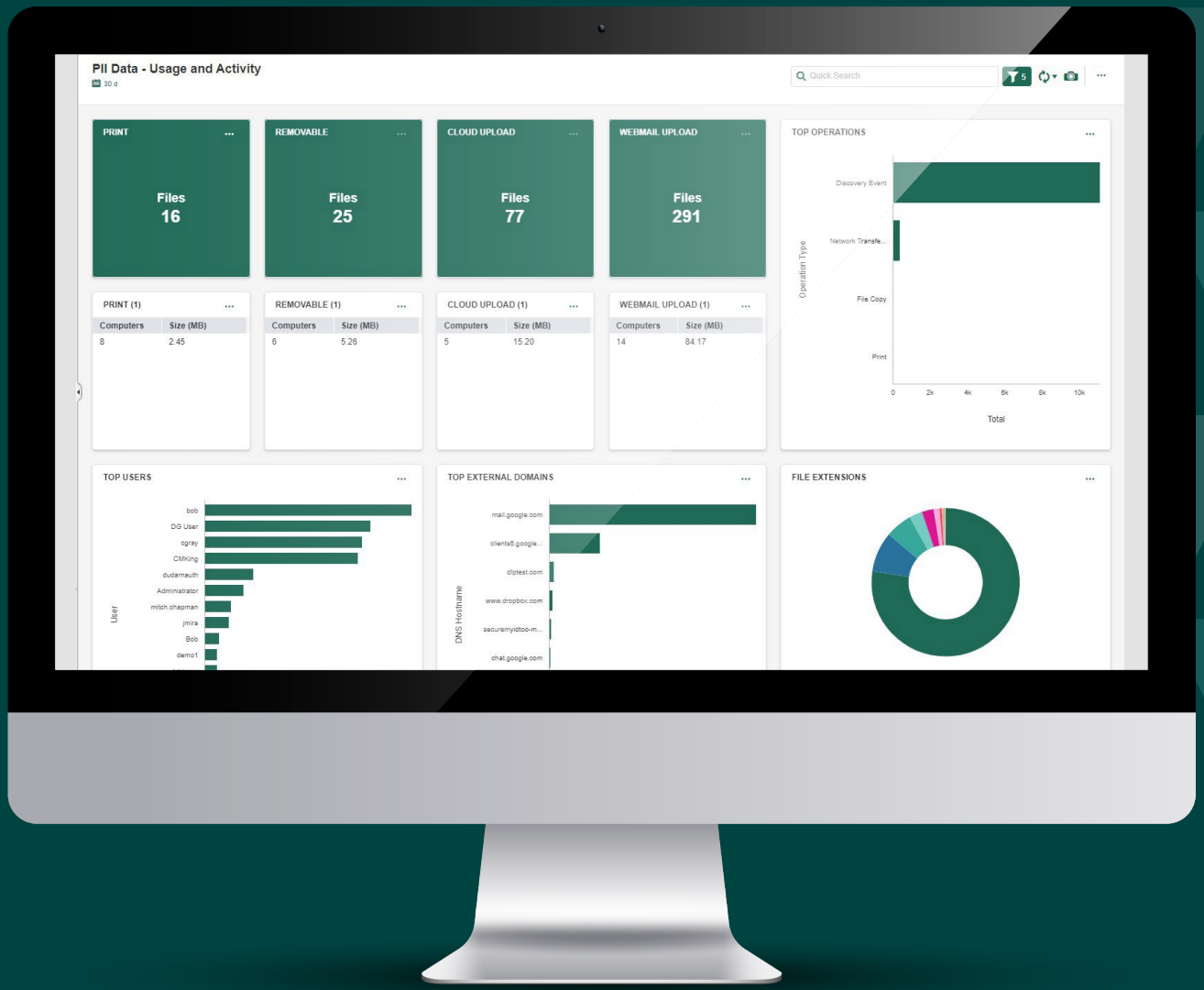
Enforce device encryption policies:

- Requires information written to removable devices to be encrypted using FIPS 140-2 level 2 validated encryption.
- Control who can access devices or media, inside or outside of your organization.

Stop data theft by enforcing device use policies:

- Block, encrypt, or prompt when user tries to copy data to a USB device.
- Identify all removable devices connected to your endpoints by type, manufacturer, model number, and MAC address.
- Control removable devices via endpoint ports like USB, FireWire, eSATA, and webcams.

One global aerospace company called on Digital Guardian to help them meet upcoming ITAR requirements that required it to secure several unguarded attack vectors on an aggressive deadline. With current security resources tied up in day-to-day operations, the firm chose Digital Guardian's Managed Security Program (MSP). With Digital Guardian experts managing both internal and external threats, ITAR-specific data classifications were put in place and sensitive data guarded within the timeframe, all without adjusting the capital budget or adding any additional servers, software, or personnel.


PII Data - Usage and Activity
30 d
Quick Search
PRINT
Files
16
REMOVABLE
Files
25
CLOUD UPLOAD
Files
77
WEBMAIL UPLOAD
Files
291
TOP OPERATIONS
Discovery Event
Network Transfe...
File Copy
Print
Operation Type
0
2k
4k
6k
8k
10k
Total
PRINT (1)
Computers
Size (MB)
8
2.45
REMOVABLE (1)
Computers
Size (MB)
6
5.26
CLOUD UPLOAD (1)
Computers
Size (MB)
5
15.20
WEBMAIL UPLOAD (1)
Computers
Size (MB)
14
84.17
TOP USERS
bob
DG User
cgray
CMKing
dudamauth
Administrator
mitch.chapman
jmira
Bob
demo1
User
TOP EXTERNAL DOMAINS
mail.google.com
clients6.google...
dlptest.com
www.dropbox.com
securemyidtoo-m...
chat.google.com
DNS Hostname
FILE EXTENSIONS

5

Siloing Reporting, Which Complicates Understanding of the Attack Chain

Siloing Reporting, which Complicates Understanding of the Attack Chain

The problem: Typical DLP reporting can be siloed, separating factors that work in concert during an attack. Multiple reports need to be combined to give cybersecurity decision-makers the full picture, slowing down investigation, complicating compliance, and hindering remediation.

The DG Solution: Digital Guardian combines system, user, and data events in a single report. This allows you to see risky behaviors within the context of normal noise and have the context required to stop them at the time of abuse. This enterprise-wide intelligence provides a full timeline of events and a defensible chain of custody in the logs which document file movement.

Events that get generated by the classification software and consolidated into the reporting database include:

- Sending an email with (or without) a selected label value
- Saving a document with (or without) a selected label value
- Sending an email that contains a policy violation after reviewing the warning
- Downgrading or upgrading a classification level, or attempting to
- Using a classification application on identified computers

Event forensics are recorded by time, user, system, application, file type, file classification, and network operation. Correlated events are bundled, hashed, time-stamped, and cryptographically signed for investigative analysis. Lastly, deep visibility reporting presents a full picture of all compliance-related assets.

6

Failing to Service the Cloud; Instead Deploying Directly On-Premises or on the Network

Failing to Service the Cloud; Instead Deploying Directly On-Premises or on the Network

The problem: Most organizations manage an array of disparate tools and applications to protect their business. Many require them to stand up server infrastructure, deploy applications, and then maintain and update them. This incurs expensive infrastructure and management costs, more resources as the platforms scale, ongoing OS and application version maintenance, and intangible reparations as dedicated internal resources are diverted to "feed and water" the services. The overhead burden of deploying a new technology is causing many to look to cloud-based solutions as an alternative. SaaS adoption has grown a sizeable 32% in the last two years, with BetterCloud predicting that 85% of all business apps will be SaaS-based by 2025.

The DG Solution: DG provides a vendor-run SaaS solution, MSP, and on-premises options. We pride ourselves on flexibility of deployment and are one of the few organizations to support all operating systems.

Our team is responsible for backups, patching, uptime, scalability and all the day-to-day maintenance of the DLP solution. Additionally, Fortra's Digital Guardian takes the utmost care with our customers' sensitive data, and at no point stores the actual data itself. This ensures that the only the clients themselves are the ones with access to the raw data, as designated by them.

This was the case with Genesys, a global leader in workforce management engagement. With thousands of endpoints to protect, a mix of OSs, browsers, and applications, a constantly evolving pool of data, and a lean in-house IT staff, they chose Digital Guardian's SaaS deployment option to implement granular data protection controls that could fit their needs today and scale with future growth. After a simple purchase and rapid deployment, the company gained instant visibility into all data movement from endpoint to cloud, without additional internal resources. Deployed on thousands of machines, Digital Guardian was the only DLP solution that could provide full coverage for their diverse environment.

7

Requiring Dedicated Resources that are in Thin Supply for Most Organizations

Requiring Dedicated Resources that are in Thin Supply for Most Organizations

The problem: Aside from operations-level maintenance, many companies struggle to find or maintain the dedicated resources required to analyze all security instances at scale. Dedicated experts with specific expertise are required to make sense of all the data generated by DLP engines and turn alerts into language the business can then act upon.
As cybersecurity skills continue to be in high demand, organizations are challenged to staff their security needs. According to data by labor analyst firm Lightcast, companies currently only have enough trained cybersecurity professionals to cover 72% of demand.

The DG Solution: Digital Guardian's Managed Security Programs (MSP) remove the resourcing pain point by supplying skilled expertise where it is needed most. We make it a point to align with the business processes of our customers, minimizing the impact of adoption and ensuring rapid return on investment.

With Digital Guardian MSP, you get:

- **Fully managed data protection infrastructure** | Get your data protection infrastructure deployed, hosted, and managed by Digital Guardian.
- **Visibility, reporting, and threat alerts** | Get notified of real-time threats with live and configurable dashboard views that provide to-the-minute insights on critical data usage and threats.

- **Immediate access to our experts** | Get instant access to Digital Guardian experts boasting over a decade of experience implementing mission-critical data security, incident response, risk, and compliance programs for the government and Global 2000 companies.
- **Time to value** | Get up and running with a phase-one deployment in 90 days or less.
- **Cost savings** | Use the money you save on upfront technology and staff investment elsewhere.

Digital Guardian offers three MSP offerings:

1

MSP for Endpoint DLP

Let our security experts host, administer, advise and run your DLP program for faster time to value, giving you time to run your business.

2

MSP for Detection and Response

Our incident responders leverage the latest defense strategies and intelligence to hunt, detect, and respond to attacks in real-time.

3

Fortra's Data Protection Select

DP Select is easy data protection for midsized companies. Get a bundle of data protection managed services and software for organizations with fewer endpoints to protect, priced to match.

Conclusion

Digital Guardian can protect critical data wherever it lives. Our three core pillars form the foundation of our industry-leading data protection architecture.

You can look forward to **fast deployment and results**. Our out-of-the-box dashboards enable our customers to see results quickly, coupled with an integrated rapid startup. Plus, our SaaS offering, powered by AWS, presents an option that simplifies and speeds up security while reducing overhead costs and burden to you.

You'll get **cross-platform coverage** for your hybrid environment, including your endpoints, corporate network, and any cloud applications running on Microsoft Windows, Apple macOS, and Linux. To get less than complete visibility of data usage across the three primary operating systems would leave gaps in your data protection program.

Lastly, secure your critical information with **comprehensive controls** based on the sensitivity of the data itself. By providing soft and hard limits on data usage, Digital Guardian helps organizations educate their users on appropriate data use and enables your teams to not only monitor but block outright actions. Stay compliant with pre-built policies and protect data no matter where it goes, on (or off) the network.

Digital Guardian is regularly named a Forward Mover and Top Player in Market Quadrant for Enterprise DLP reports. Currently, Digital Guardian secures sensitive data across 5.5 million agents and is trusted by more than 600 diversified blue-chip customers worldwide. Learn more about our industry-leading data protection platform and MSP solutions here.

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.

fta-dg-ebook-0924-r2-as