

MANAGED DLP FOR THE MID MARKET

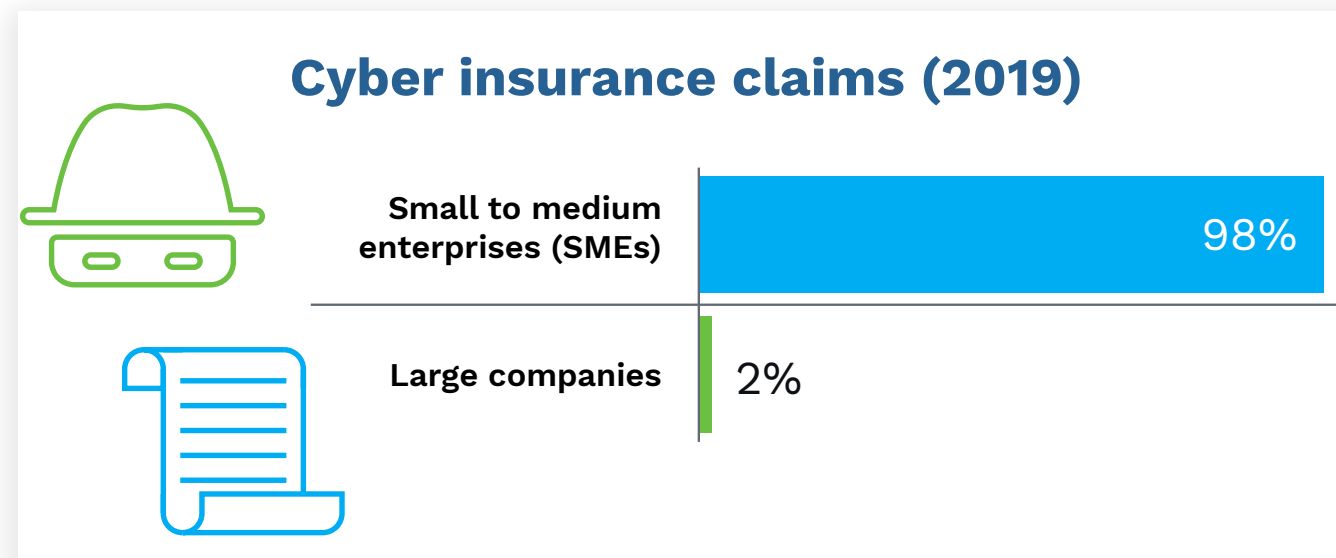
GET A TEAM OF DATA
PROTECTION EXPERTS
WITHOUT THE HASSLES



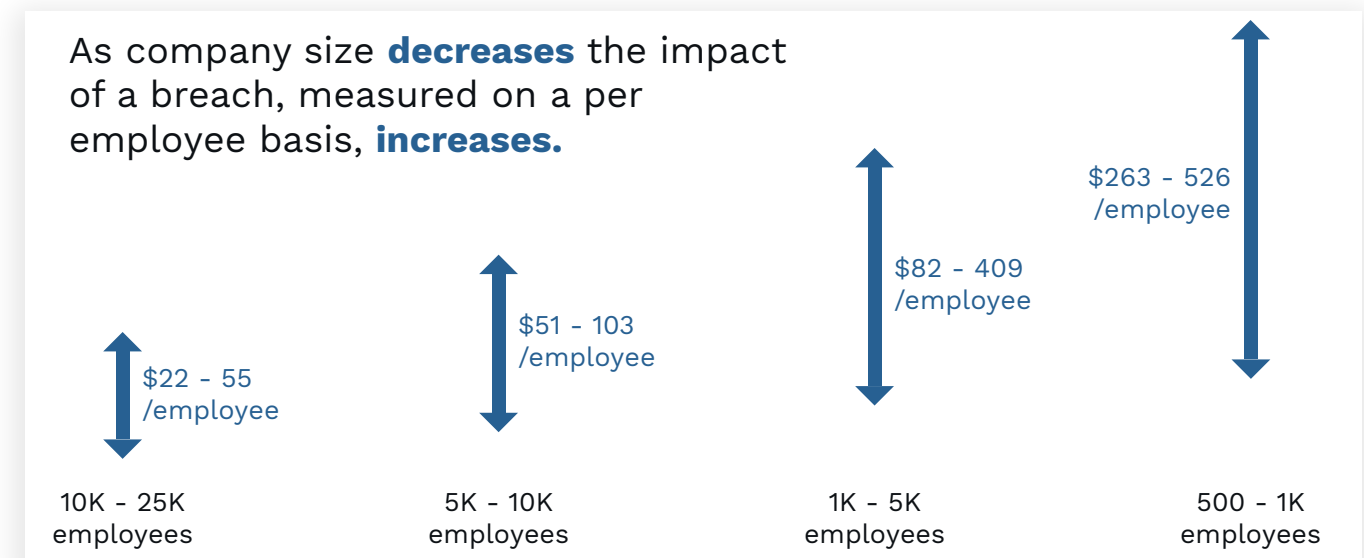
WHY READ THIS EBOOK

SECURITY LEADERS IN MID-SIZED BUSINESSES MUST PROTECT ENTERPRISE VOLUMES OF DATA, BOTH IP AND REGULATED, BUT:

- Lean IT/IS teams are stretched to the limit to protect this growing pool of data
- The repercussions of an incident can have a disproportionately larger impact
- Hiring and maintaining cybersecurity talent continues to be a challenge



Source: Net Diligence 2020



Source: IBM Security, Cost of a Data Breach Report 2021

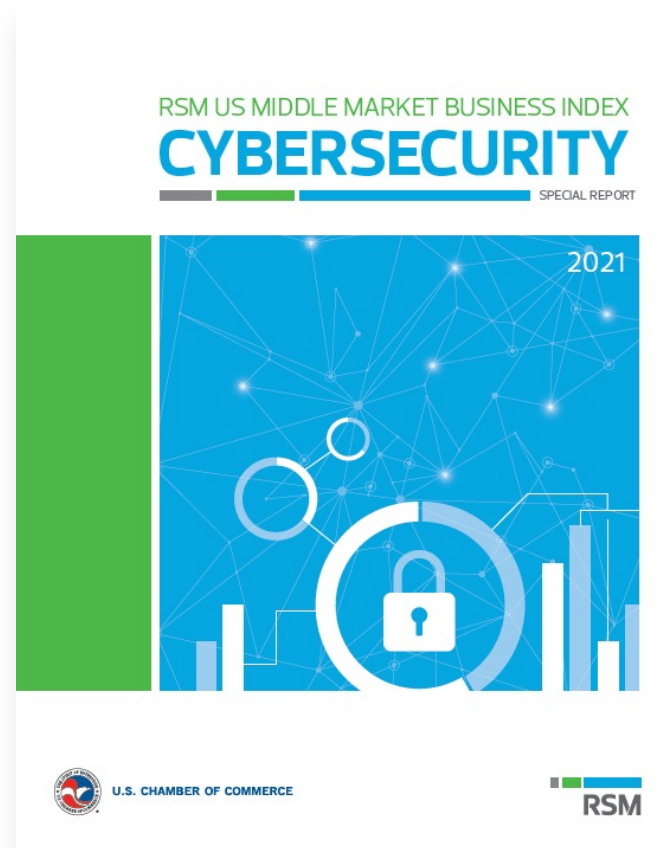
Learn how Managed Data Loss Prevention for the Mid-Market can simplify your information security program

TABLE OF CONTENTS

- 04** The Mid-Market Still has Big Challenges
- 06** Cyberinsurance Trends in the Mid-Market
- 07** Enterprise Demands on Mid-Market Organizations
- 10** Designing a DLP Program for the Mid-Market
- 18** Digital Guardian Managed Security Program for the Mid-Market
- 26** Why Digital Guardian

THE MID-MARKET CHALLENGE

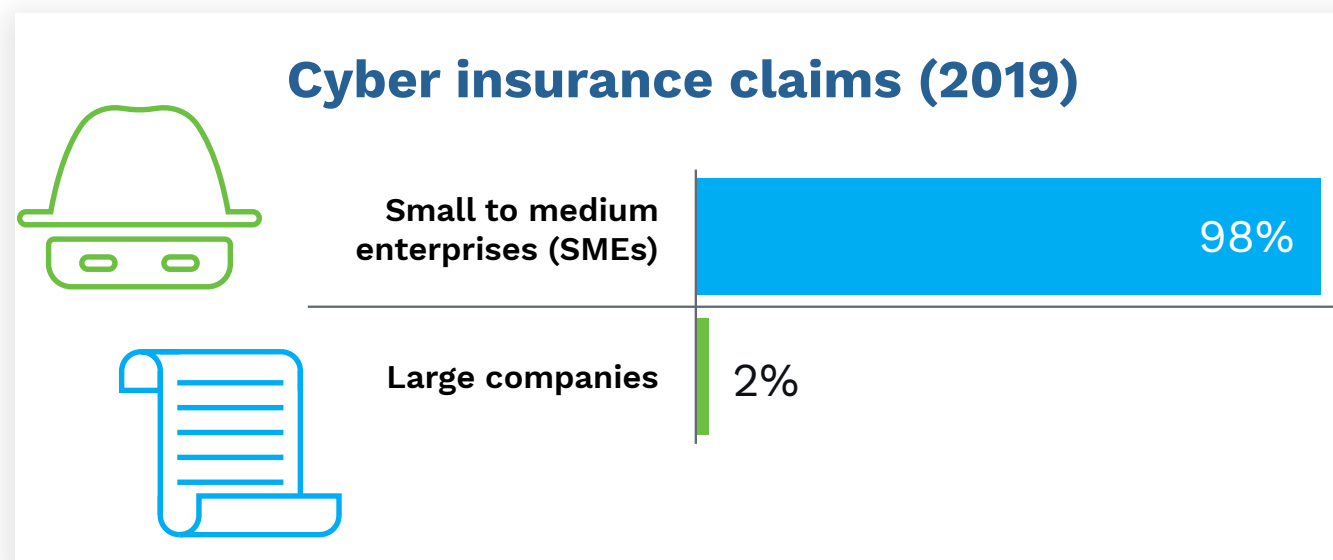
THE MID-MARKET STILL HAS BIG CHALLENGES: QUANTIFIED



QUANTIFYING THE MID-MARKET CHALLENGE:

- 28% of middle market executives claimed that their company experienced a data breach in 2020, up from 18% in 2019.
- 42% of executives at larger middle market organizations reported a breach, compared to 16% at smaller counterparts.
- The middle market has the exposure and digital assets to make them an attractive target for data theft.
- The expectation to know the cybersecurity market.
- They also struggle to lure or maintain cybersecurity talent and balance the resource constraints of a mid sized business.

THE MID-MARKET STILL HAS BIG CHALLENGES: CYBERINSURANCE



Source: Net Diligence 2020

- Cyberinsurance is still maturing with actuarial models evolving, in some cases causing rapid swings from year to year for rates and coverage.
- The mid-market has driven the bulk of claims submitted, though what this means for the future isn't certain, but given the disproportionate share of claims going to mid-market firms one can conclude the market will adjust to a more even distribution.
- To get there, will firms see their rates increase? Coverage decrease?
- Security leaders need to take steps to reduce their reliance on insurance claims.

MID-MARKET BUSINESSES RELY ON THE SAME SENSITIVE DATA AS GLOBAL ENTERPRISES

Just because your organizations lives in the middle, it doesn't mean the types and volumes of sensitive data are any simpler to protect than the large enterprises. As a security leader you need locate (Data Discovery) and understand (Data Classification) all the data in your business to deliver the protection (Data Loss Prevention) for secure growth.

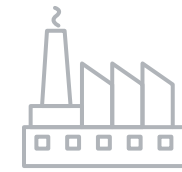
While there are commonalities, each industry and business will have unique data types or data type combinations.

**Finance**

- PCI
- Shares and Repositories
- PII
- Web Sites

**HealthCare**

- HIPPA
- Medical Records
- PCI
- Web Sites

**Manufacturing**

- Compliance (like ITAR)
- Repositories
- Intellectual Property

**Technology**

- PII
- Source Code
- CCPA
- Web Sites

**Retail**

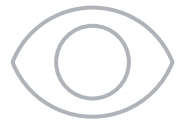
- PCI
- Employee Data
- Customer Data
- File Types

**Legal and Consulting**

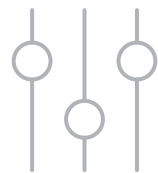
- PII
- Customer Data
- Documents
- Shares and Repositories

MID-MARKET REQUIRES DATA GOVERNANCE

Once you've discovered and classified your data, the next step is the control and retainment of your data as part of your overall governance program.



Organization wide **visibility** is paramount. Data lives on endpoints, in storage repositories, in the cloud, and moves among them. Real time visibility and analysis of the movement delivers the insights to spot data risks or trends that can become data risks. Blind spots here cause big problems.



Visibility without **control** is useless. Telling you data left without an ability to stop it delivers minimal value. Data protection solutions *must* be able to automatically stop the activities your team deems the highest risk.



Balancing the conflicting interests may take adjustments and is driven by industry, regulatory environment, and corporate culture. Over time you will need to modify where the line between too strict and too lenient is. A data protection program must evolve to stay relevant.

SECURITY STAFFING IS BIGGER ISSUES FOR THE MID-MARKET

Of the big three, People, Process & Technology, people come first. Without the right team, few solutions can be effective. Mid-market security leaders have the task of hiring and maintaining their team when the lure of larger companies can decimate a lean team. A mid-market company may have 2-3 dedicated security people, losing 1 really hurts!

In a mid-market company, the team needs to function well. Conflict in a team of only a few people can kill communication and effectiveness in no time. This lack of good process is what leads to missed alerts and alarms... and leads to data loss.

The good side of a small team is it's easy to know who to talk to for local knowledge. It's rarely more than a few people away. That unique setting in the firewall can be explained...but that if that person leaves and the local knowledge goes too, then what?

DESIGNING A DLP PROGRAM FOR THE MID-MARKET

DESIGNING A DLP PROGRAM FOR THE MID-MARKET

Accepting the reality that not all the answers to all your cybersecurity challenges exist inside the (virtual) walls of your business is the 1st step.



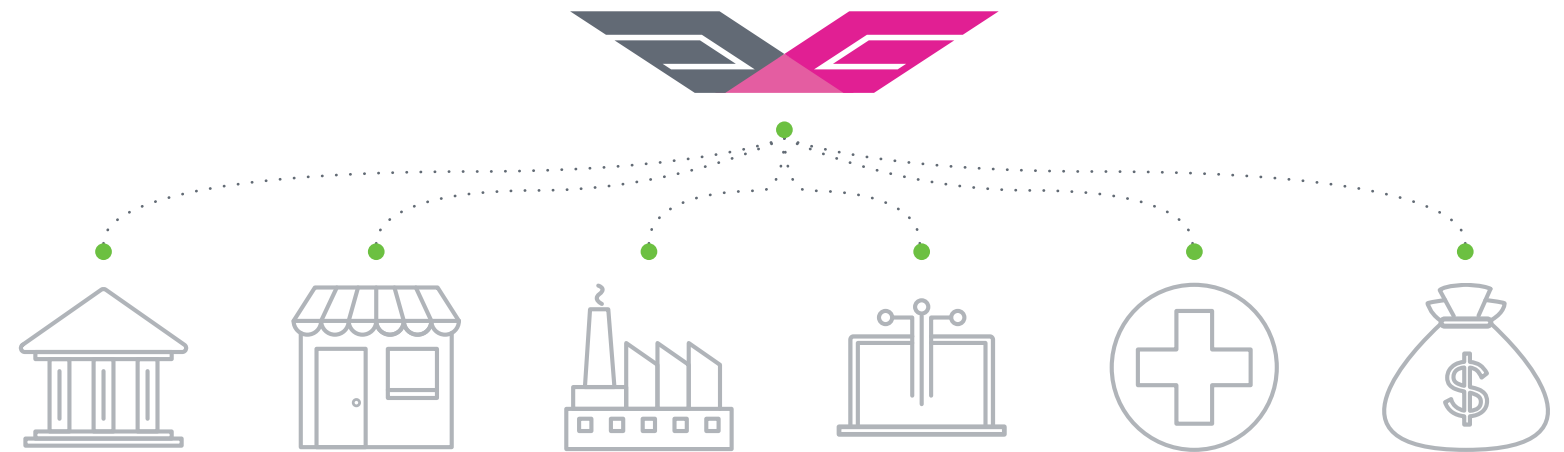
“Among organizations with 1,000–9,999 employees, **only 23 percent** said they rely most on internal staff for security expertise.”

Source: Cisco Cybersecurity Series – The Security Bottom Line October 2019

There are new tactics, techniques, and procedures that organizations need to stay on top of. Many security teams are lean, and in the case of mid-market enterprises, often handle information technology and information security, the challenge doubles. There simply isn't enough time in the day to do your job and stay fresh on the changing environments. New malware, new ransomware, new steal-your-data-ware.

DESIGNING A DLP PROGRAM FOR THE MID-MARKET

DG has a broad collection of customers in our managed services program - manufacturing, high tech, healthcare, financial services, business services, etc. They all rely on us to protect both their intellectual property and their regulated data.



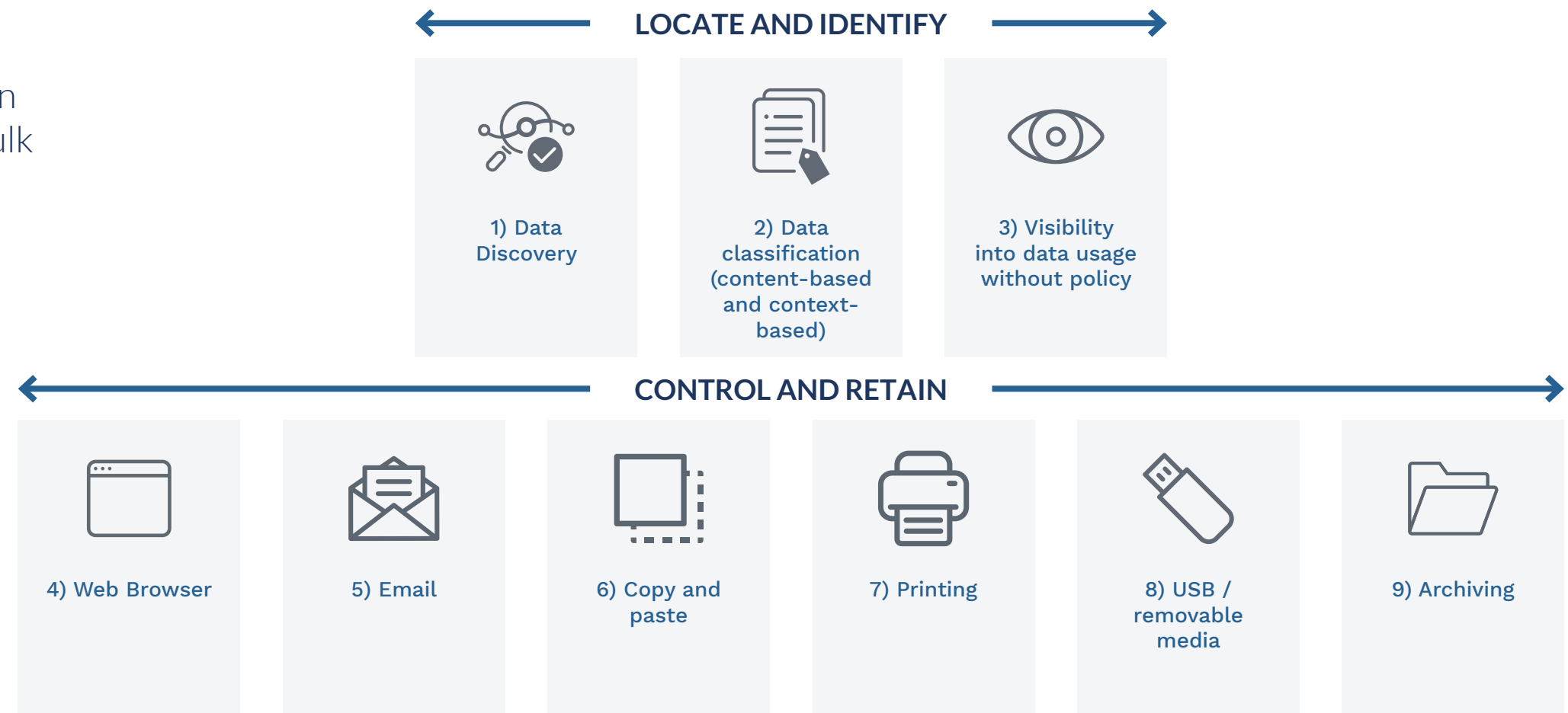
DESIGNING A DLP PROGRAM FOR THE MID-MARKET

We analyzed all those customers to see how they were using DG, looking for patterns across industry size, vertical, etc. We found a core set of control rules and types of controls that tracked data egressing through a core group of channels. We also noticed the data had a pattern of classification categories. All these combined for a data-driven data protection solution.



DESIGNING A DLP PROGRAM FOR THE MID-MARKET

From our data, 9 core uses cases in 2 broad categories covered the bulk of what customers needed.*



*If your data protection needs fall outside of this, Digital Guardian also offers a full and customizable suite of Data Loss Prevention options to protect your organization.

DATA PROTECTION USE CASES

Locate and **identify** is where we start. The adage goes, if you can't see it, you can't protect it. And a corollary to that, if you can't understand it, you can't effectively protect it.

1st priority is the find and classify your data. This includes data movement that you are unaware of too, Visibility into data usage without a policy is something only DG delivers. It's rare for a company to have 100% knowledge of 100% of their data.

← LOCATE AND IDENTIFY →



1) Data Discovery

It's as simple as it sounds, find all the data, but can be a complex challenge with endpoint data, NAS data, cloud data, etc. You need a baseline of your data to design a proper data protection program.



2) Data classification (content-based and context-based)

Once you found it, you need to organize it into discrete, meaningful categories. Here, more isn't always better. Starting with 3 (Regulated, Internal, & Public) is where we recommend you start



3) Visibility into data usage without policy

Being able to track data movement without a policy is unique to DG, and yields the most complete view of data movement. From here you can build a data driven, and far more effective program.

DATA PROTECTION USE CASES

Next, **Control** and **Retain**, is the proactive data protection that can stop data loss before it happens. This can be from either a user simply trying to get their job done and inadvertently putting data at risk, or intentional and malicious actions.

← CONTROL AND RETAIN →



4) Web Browser

More and more apps are browser based, many of these touch sensitive data, or can be used to transmit sensitive data. Seeing data in these apps can help safeguard it.



5) Email

We're in email almost all day, and with this familiarity comes complacency. Entering sensitive data into email can be a potential data loss vector when auto-fill grabs the wrong address or you are simply sending what you shouldn't.

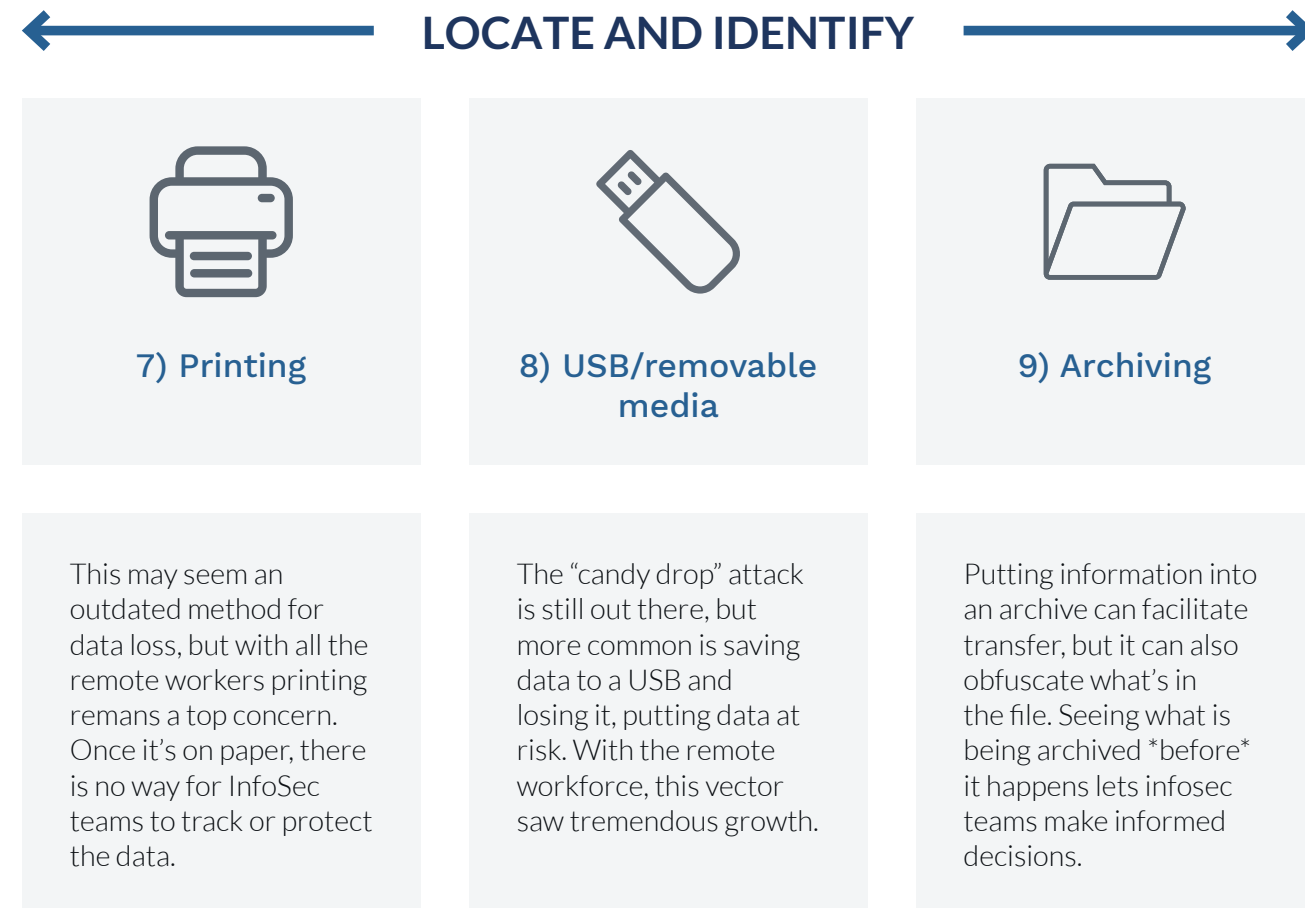


6) Copy and Paste

Yes, it saves us time during the day, but can also speed up the data loss process. Grabbing a large chunk of text may include sensitive data that shouldn't be shared externally.

DATA PROTECTION USE CASES

Part 2 of **Control** and **Retain** expands upon the common data protection use cases we see and rounds out the 9 core use cases we saw in the data analyzed.



DG MANAGED SECURITY PROGRAM FOR THE MID-MARKET

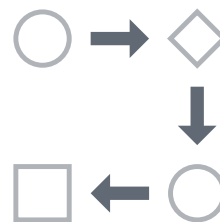
DIGITAL GUARDIAN'S EXPERIENCE DRIVES SUCCESS

The Digital Guardian Managed Security Program (MSP) for Midsize Companies is specifically designed to meet the unique data protection challenges of midsize companies. We rely on our data protection experience to provide the people, process, and technology you need to simplify and improved your cybersecurity program.



PEOPLE

- Our team is an extension of your business, we work for you and your data. We're both focused on protecting your sensitive data.



PROCESS

- DG's insight-driven framework eliminates getting bogged down in policy debates. We get your program operational, then can optimize as needed.

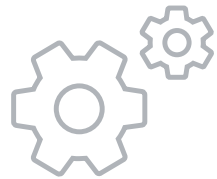


TECHNOLOGY

- AWS cloud delivered data protection for scale & simplicity
- Gartner, Forrester Leading Enterprise DLP Technology
- SC Media Best DLP 2020
- The only DLP selected by cyberinsurers to reduce risk

WHAT YOU GET FROM DG

We combine the People, Process, and Technology into an offering that delivers the essential use cases in a package that cost-effectively delivers our award-winning MSP service to midsize companies. You get data protection expertise without the complexity of staffing up and maintaining your team.



FULL MANAGED DATA PROTECTION

- Rely on our security experts to run your endpoint data protection and data discovery program
- 24x7 global analysts live, eat, and breathe data protection
- Contain insider threats before sensitive data gets out

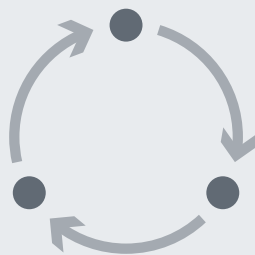


SUSTAINABLE PROTECTION IN RECORD TIME

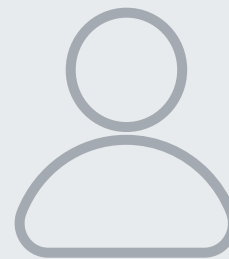
- Rapid time to value
- See data flows, understand business processes (and deviations)
Identify and stop risky behavior

WHAT TO EXPECT FROM DG

When you become a customer, you join the other organizations that rely on DG to protect their most sensitive data. From kick-off to go-live, we'll be with you all along the way to ensure you get coverage for your business, know who to go to for questions, and can see the metrics that define your data protection program.



Implementation
Process



Your
Analyst



Reporting &
Analytics

IMPLEMENTATION PROCESS

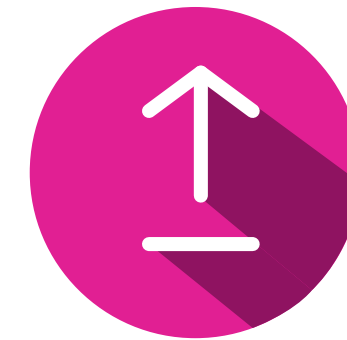
We'll work together to define the timeline that meets your goals.



YOUR ANALYST

The most important person is your assigned DG data protection analyst. This person is your data's advocate, they will work to ensure risks are spotted and data is kept safe. Regular communication is part of what makes this successful.

- Reviewing your data regularly for potential incidents
- Creating cases in Analytics & Reporting Cloud (ARC) for you & your team to triage
- Building a relationship to truly understand:
 - Your data
 - Risks in your environment
 - Best ways to mitigate those risks with our controls

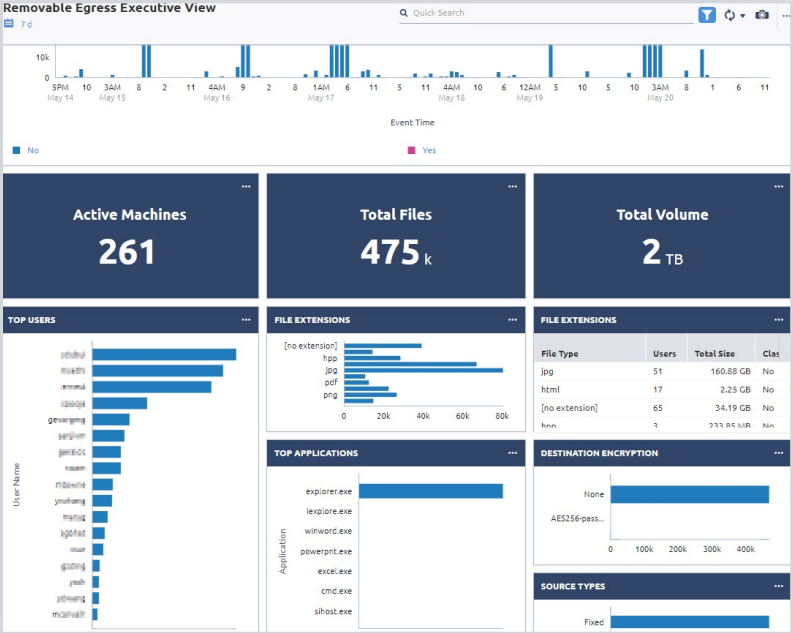
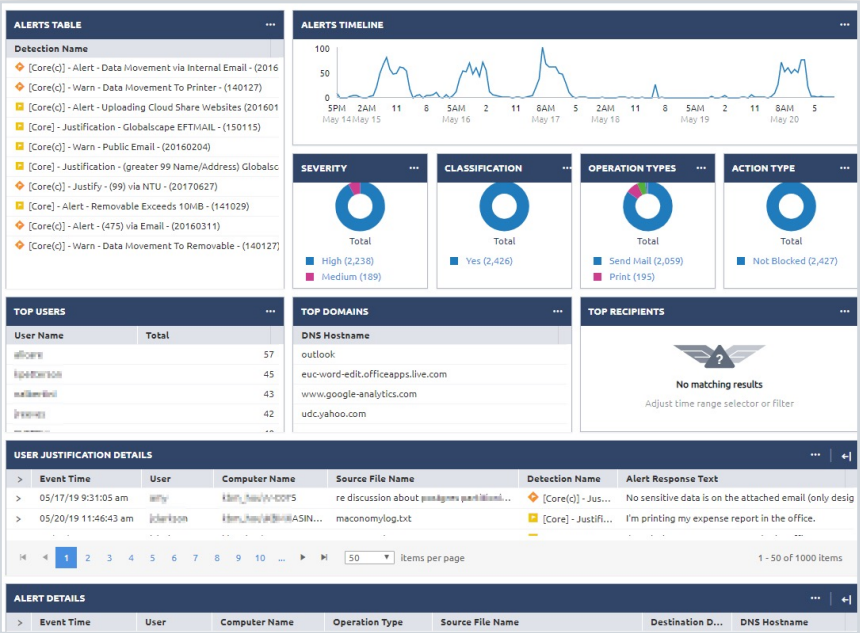


WATCH VIDEO

Learn more about a day
in the life of your analyst

REPORTING AND ANALYTICS

If you can't measure it, you can't manage it. That's why our MSP for Mid-Market Companies relies on the same Analytics & Reporting Cloud that powers all our data protection solutions. You can see all the data centric events throughout your business; your analyst relies on this intelligence to report out on data flows, emerging trends, and how best to modify policies.



WHY DG FOR MIDSIZE COMPANIES

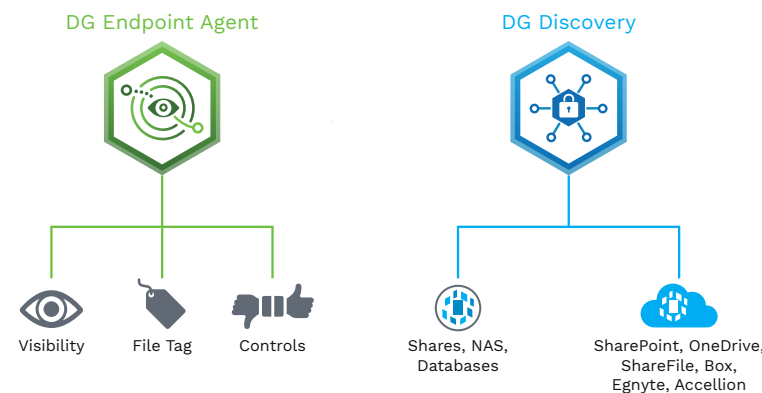
Each business is unique, but these are the key things we hear when our customers talk about the MSP for Midsized Companies.

- 1** Solves the Security Talent Gap Problem
- 2** Delivers DLP for the Long Term
- 3** Adds or Replaces DLP with Rapid Time to Value
- 4** Relies Upon Field Proven, Prescriptive Policies & Protection
- 5** Leverages DG's Programmatic Best Practices

WHY DIGITAL GUARDIAN?

FULLY MANAGED, CLOUD BASED DATA PROTECTION FOR YOUR BUSINESS

Your sensitive data needs enterprise level the protection, Digital Guardian's team of Managed Security Program Analysts rely on the same data protection platform used by some of the most data intensive enterprises across the globe. You get the endpoint to cloud visibility, multi-platform, -OS, and -browser coverage, and the flexible controls powered by Digital Guardian's Analytics and Reporting Cloud. You also get the 24x7 support of a cybersecurity team, dedicated to your data protection needs.



IN YOUR BUSINESS:

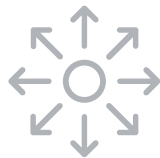
Data collection agents and appliances (physical or virtual) see all the data events and deliver the metadata to the DG experts.



IN THE DG CLOUD

Our Analytics & Reporting Console, powered by AWS, aggregates and filters through these events to surface the most critical ones to the DG analysts who triage and respond as needed.

NO-COMPROMISE DATA PROTECTION THAT STOPS DATA LOSS



CLOUD-DELIVERED

Powered by AWS, Digital Guardian delivers simplified deployment, low overhead, and elastic scalability for increased return on your security spend.



CROSS PLATFORM

Coverage for your Windows, macOS, or Linux operating systems and all your applications, both browser based and native.



FLEXIBLE CONTROLS

Fine-grained controls, ranging from log & monitor to automated blocking, help protect data before it's lost.



DEEPEST VISIBILITY

We see everything that happens to your organization's sensitive data.
Cross Platform



NO POLICY, NO PROBLEM

Our "unknown risk" approach enables you to see where sensitive data is located, how it flows, and where it is put at risk - all without policies.



COMPREHENSIVE CLASSIFICATION

Only Digital Guardian provides content, user, and context-based data discovery and classification.



FULLY MANAGED

Our team of experts are your data protection team. We plan, deploy, manage, and support the whole program for you.

INCREASING SPEED TO LEND; REDUCING DATA LOSS RISK FOR RE INVESTORS

SITUATION

A rapidly expanding, private financial services firm with a focus on real estate investors, needed to reduce information security and regulatory compliance complexity without sacrificing protection of their clients' sensitive data. Their existing data protection platform was driving up support costs, slowing down lending times, and costing them customers. They needed a better way to protect PII and PCI data.

SOLUTION

The organization, working closely with their data security channel partner, deployed the DG Managed Security Program DLP for Mid-Market across their entire organization. The CIO was sold on the data-centric view the platform provided along with the fully cloud hosted delivery model. They were able to eliminate the on-site complexity of their previous data loss prevention solution and gain access to the 24x7 cybersecurity experts, both helping to offload work from their IT/IS team.

RESULTS

During the deployment, DG helped the IT/IS team improve upon their data protection rules, ensuring sensitive data could safely move as needed to speed their business processes. Their DG analyst instantly became a part of their security team, bringing the DLP expertise they needed. Finally, with the cloud-based solution, the customer went through the planning and deployment process in a few weeks.

MANAGED DLP FOR THE MID MARKET

GET A TEAM OF DATA PROTECTION
EXPERTS WITHOUT THE HASSLES

QUESTIONS?

1-781-788-8180

info@digitalguardian.com

www.digitalguardian.com



©2021 Digital Guardian. All rights reserved.

