FORTRA™

The Quick Guide to Data Loss Prevention Managed Security Services for Midsize Businesses

Table of Contents

Three Reasons Why Midsize Businesses Should Care About Data Protection 3

What Should a Midsize Company with Stretched IT Do? 6

What is a Managed Security Services Provider? 7

What is a DLP Managed Security Program? 8

Four Things to Look for in a DLP Managed Security Program 9

Why Consider the Digital Guardian DLP Managed Security Program 10

Three Reasons Why Midsize Businesses Should Care About Data Protection

#1 – Small and Midsize Businesses are Now the Preferred Target for Cybercriminals

Small and midsized businesses are attractive targets for cybercriminals because they tend to be less secure and because automation now permits cyber criminals to mass produce attacks for little investment. Criminals can buy malware kits for as little as $40.

According to multiple experts interviewed by CSO Online, SMBs are so attractive to cybercriminals for all of the following reasons:

- Lack of time, budget and expertise to implement comprehensive security defenses.
- No dedicated IT security specialist on the payroll.
- Lack of risk awareness.
- Lack of employee training.
- Failure to keep security defenses updated.
- Outsourcing security to unqualified contractors or system administrators
- Failure to secure endpoints.

Source: CSO Online, Why Criminals Pick on Small Business, Taylor Armerding

62%

"Of all data breaches last year were at small and medium businesses"

- PWC'S GLOBAL STATE OF INFORMATION SECURITY

"We think threat actors are beginning to target medium-tier businesses because they typically cannot match the sophisticated cybersecurity technologies and processes of the largest companies."

- DAVID BURG, GLOBAL AND US ADVISORY CYBERSECURITY LEADER, PWC

Three Reasons Why Midsize Businesses Should Care About Data Protection

#2 – Cybercriminals See Small and Midsize Companies as a Back Door into Valuable Corporate Data

Sophisticated cybercriminals have identified SMB third party suppliers as the vulnerability point of major corporations. The massive breaches of both Target and Home Depot were both initiated by criminals who stole third party vendor log-on information. The breach of Target was traced back to network credentials that were stolen from Fazio Mechanical, a 100 person HVAC subcontractor. Similarly, Home Depot said the criminals initially broke in using a user name and password stolen from a small business third party vendor.

" Sophisticated adversaries often target small and medium-size companies as a means to gain a foothold on the interconnected business ecosystems of larger organizations with which they partner."

- PWC'S GLOBAL STATE OF INFORMATION SECURITY

" Regulators are also paying closer attention to SMBs. In the retail world, the latest version of the Payment Card Industry Data Security Standard (PCI DSS), which took effect Jan. 1, requires more rigorous security standards for third-party vendors or contractors, which have been a weak point for major companies."

CSO

Three Reasons Why Midsize Businesses Should Care About Data Protection

#3 – Midsize Companies Will Pay Now or Pay More Later to Protect Sensitive Customer Data

Midsize companies will face increasing pressure to button up their cybersecurity presence from both regulators as well as their customers. Federal and state authorities are now recommending or requiring security audits of third party vendors. Midsize companies that can't demonstrate that they are adequately monitoring and protecting the sensitive data of their corporate customers run the real risk of losing those customers.

" The lack of due diligence into third parties has become so prevalent that an increasing number of regulators now require assessment of partner and supply-chain security capabilities. To catch up, small and midsize businesses might consider outsourcing elements of their cybersecurity programs to take advantage of economies of scale."

- PWC'S GLOBAL STATE OF INFORMATION SECURITY

" Describe your institution's due diligence process regarding information security practices that is used in vetting, selecting, and monitoring third-party service providers."

- NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, INDUSTRY GUIDANCE LETTER TO NY BANKS

What Should a Midsize Company With Stretched IT Do?

Cyber attacks targeting midsize companies are expected to continue to increase in numbers and sophistication. Customer demands to demonstrate and document data security compliance will also increase. But security budgets aren't likely to increase accordingly. Security as a service is a worthwhile option for midsize companies. But there is a wide range when it comes to managed security services, from full service providers to specialists, so let's take a closer look at your options.

"Businesses will have to embrace security as a service."

- EARL PERKINS, RESEARCH VP, GARTNER

Gartner®

" To improve their security posture, one option that small and medium companies might pursue is consideration of managed security services. This can enable them to employ sophisticated technologies and processes to detect security incidents in a cost-effective manner."

- PWC'S GLOBAL STATE OF INFORMATION SECURITY

pwc

What is a Managed Security Services Provider?

Gartner defines Managed Security Services (MSS) as:

"The remote monitoring or management of IT security functions delivered via shared services from remote security operations centers (SOCs), not through personnel on-site."

Core managed security services usually include:

- Monitored or managed firewalls or intrusion prevention systems (IPSs)
- Monitored or managed intrusion detection systems (IDSs)
- Security analysis and reporting of events collected from IT infrastructure logs
- Reporting associated with monitored or managed devices and incident response

Source: Gartner, Magic Quadrant for Managed Security Services, Worldwide

What is Data Loss Prevention Managed Security Program (MSP)?

A Data Loss Prevention MSP focuses on protecting sensitive data, and preventing data theft. It delivers data loss prevention software as a service - without additional hardware or staffing. All hardware and software is hosted at a secure facility. A Data Loss Prevention MSP helps you understand your risk by providing visibility into where sensitive data lives within your organization, and how it's being used. It will continuously monitor data usage and can prompt and block to protect data from unauthorized access or theft.

Data security experts that manage the program will work with you to identify and classify critical data anywhere in your firm, discover user behavior that could put data at risk, and create policies to protect sensitive client information. A top-notch MSP will provide monthly expert reviews of reports and will identify risks and advise actionable steps to protect client data.

Four Things to Look for in a DLP Managed Security Program

1 **How Much Experience Do They Have Protecting Data For Midsize Companies?**

Any qualified MSP can set up the infrastructure. But your employees have unique workflows and industry-specific or industry-tailored applications. You'll want to make sure you work with an MSP that has experience working with companies like yours to minimize business disruptions and spot data usage anomalies that put your company at risk.

---

2 **Do They Provide Regular Reporting And Analysis With Actionable Results?**

The best MSPs will provide you with clear reports on how sensitive data is actually being accessed, stored, and used with respect to your or company's unique policies and restrictions. The reporting should include detailed information on application use, network uploads; data access; printing; email and Webmail events; and all file operations that occur both on and off the network. Security experts should review the reports with you at least monthly to identify risks and advise actionable steps to help manage potential threats from both insiders and external attackers.

---

3 **How Long Will It Take To Get Up And Running?**

The best-in-class MSPs can be deployed and will provide you with much greater visibility into sensitive data usage and risks in 90 days or less.

---

4 **Do They Offer Flexible Support Hours That Include 24x7x365?**

Most companies will be properly covered with support during business hours. But if you need 24x7 support to meet client requirements you'll want to make sure up front that the MSP can provide that.

Why You Should Consider the Digital Guardian Managed Security Program

The Fortra™'s Digital Guardian® DLP Managed Security Program is ideal for midsize companies with resource–constrained IT teams.

Four Ways We're Different:

1 **Instant On**

As soon as our experts have installed the Digital Guardian agents, you will immediately discover—in full forensic detail— where your customers' sensitive data resides, who accesses it, and how it's transacted. Your MSP team will provide you with continuously updated security intelligence and trending reports on data location, usage, and risks.

---

2 **Immediate Access To Security Experts**

With the severe shortage of IT security talent, DG MSP customers leverage the knowledge of experts with 10+ years' experience implementing mission-critical data security, risk, and compliance programs for midsize companies, Global 2000 companies, and government agencies.

---

3 **None Of Your Sensitive Data Is In The Cloud**

Your data remains private and secured at all times. With Digital Guardian's secure, cloud–based delivery option, no sensitive data is ever transmitted, recorded, or stored. Reports are based on metadata, which is encrypted, hashed, and digitally signed before being securely transferred to Digital Guardian's hosting facilities via FIPS 140-2 certified messaging protocol.

---

4 **Exceptional Time To Value**

DG MSP customers repeatedly tell us that they were able to improve their data visibility and data security risk posture faster than they ever could have done by themselves, or with any other vendor.

Case Study:

Compliant with Client Data Protection Requirements in 90 Days

A midsize company providing engineering, IT and staffing services to clients in a range of industries received a challenging demand from one of their largest clients. The aerospace client mandated strict new policies for handling their trade secrets, with a six-month deadline to comply.

Due to the aggressive deadline and limited internal resources, the firm chose Digital Guardian's Managed Security Program (MSP). The MSP offering enabled the firm to focus on existing operations and rely on DG security experts to manage and monitor all threats to their data, from inside or outside the organization.

The client's requirements were unexpected, and therefore unbudgeted, but the decision to go with the Digital Guardian MSP offering minimized out-of-pocket costs, and eliminated the need to adjust their capital budget. No new servers, capitalized software, or added IT personnel were required.

Within 90 days, the service was operational and compliant with the aerospace client's security requirements. The company has not only been able to maintain its reputation as one of the aerospace client's most trusted suppliers; they've been able to use their mature security posture to assist in winning new clients.

About Digital Guardian

Fortra™'s Digital Guardian® is the only content aware security platform designed to stop data theft. The Digital Guardian platform performs across endpoints, networks and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 15 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

For More Information

digitalguardian.com

FORTRA™

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-gd-0523-r1-79d)