FORTRA™

How Managed Services Can Help with Cybersecurity Compliance

Introduction

Meeting cybersecurity compliance requirements is absolutely critical to the success of organizations and agencies. Otherwise, they face steep audit fines and an increased risk of cyberattacks. And there are usually several regulatory requirements to be met simultaneously, putting a huge strain on organizations trying to enforce compliance manually. The 2023 Compliance Trends Report found that 80 percent of organizations face negative outcomes from approaching compliance manually, including sluggish sales cycles, cybersecurity incidents, and regulatory fines.[1]

Several factors contribute to compliance being a major hurdle for the modern enterprise. There are more than 700,000 cybersecurity jobs unfilled in the U.S. alone, leaving many organizations without adequate headcount to ensure a properly run compliance program.[2] At the C-suite level, only 59 percent of companies have a dedicated Chief Compliance Officer, or CCO, to steer their compliance program and communicate its impacts to the board.[3] Luckily, organizations can outsource some of the management of their compliance initiatives using managed service providers.

What Are Managed Services?

Managed service providers are companies to whom you can outsource specific parts of your operational process, such as helpdesk, application management, network administration, cybersecurity, and compliance. In the case of compliance, these providers can run your compliance software for you at peak effectiveness, supply detailed reporting for audits, and even provide compliance program progress to executives and boards. You can think of managed service providers as an extension of your team that delivers robust expertise and saves you from having to find, train, and keep dedicated compliance personnel.

Because of the way they take the burden off internal teams and ensure continuous compliance with as many regulations as are needed, managed services are becoming increasingly popular. Cybercrime Magazine projects 77 percent of cybersecurity spending will go toward managed services by 2026.[4] The benefits of outsourcing compliance with managed services aren't industry specific.

Financial, retail, government, manufacturing, critical infrastructure, and healthcare are just a handful of the heavily regulated industries that can rely on managed services to ensure their resources are well-allocated, their organization is well-protected, and their audits are passed.

Types of Cybersecurity Managed Services

There are several subtypes of managed service providers that operate within the realm of cybersecurity and the compliance mandates that enforce it. Here are a few key types of managed services your organization might want to use, along with a quick explanation of what they do.

Managed Services for Fundamental Security Controls

Most compliance requirements include mandates for essential security controls to be put in place and correctly administered. These include **file integrity monitoring (FIM)**, **security configuration management (SCM)**, and **vulnerability management (VM)**. Managed service providers can implement and run the right software to enforce these security controls. Not only does this put your organization on track to pass your audits—but it also sets an elevated level of security across your digital environment to monitor for unauthorized changes, misconfigurations, and security vulnerabilities that could otherwise result in a breach.

Managed Detection and Response

Managed detection and response (MDR) is a process in which the managed service provider serves as a real-time security operations center to uncover and address security issues within your organization. This can span traditional IT infrastructure and endpoints, SaaS, and other cloud environments. MDR is a sophisticated and practical way to minimize security risk. In addition to 24/7 threat detection and intelligence, MDR services can advance your security compliance program with a team of security experts, compliance monitoring, and audit-ready reporting.

Managed Data Loss Prevention

Data loss prevention (DLP) is the process of tracking what happens to an organization's data, making sure sensitive data isn't lost and intercepting unauthorized users from accessing it and misusing it for their own purposes. Managed DLP providers can host and run DLP software for you, freeing up your internal resources and saving considerable time. They protect data at rest, in motion, and in use with tactics like encryption, alerts, and endpoint control. Data protection is a requirement of most major compliance mandates, including the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and more.

Managed Web Application Firewall

Managed web application firewall (WAF) is a service in which the web application firewall—the filter for web traffic that applies rules for HTTP/HTTPS communications to detect and block malicious traffic—is continuously managed by an expert security team that uses robust processes to ensure optimal protection. Managed WAF provides both advanced application and API threat protection. Features typically include managed virtual patching, emerging threat protection, bot management, DDoS mitigation, and credential attack protection.

Managed Digital Risk Protection

Managed digital risk protection (DRP) protects organizations from brand abuse, account takeover, social media scams, and data leaks, designed to compromise your brand, employees, customers, and digital assets. Managed DRP reduces the workload on your team by delivering comprehensive collection, expert curation, and complete mitigation of digital risks. It provides broad visibility into threats outside of your network, managed curation of data that reduces noise and increases focus on real threats, and quick and complete threat mitigation to reduce risk and help maintain compliance.

How Managed Services Help With Compliance

When an organization puts its compliance program in the hands of a trusted managed service provider, it can rest assured that its systems will be continuously monitored for any deviation from its compliance policies. Managed service providers can then help ensure such deviations are remediated before any issues occur. In addition to monitoring for standard policies such as PCI DSS or HIPAA, adequately advanced solutions also enable your provider to monitor for custom, internal policies created within your organization.

The following are a few other benefits you can expect from managed services for compliance:

- Expert solution management for your cybersecurity and compliance software
- Day-to-day enforcement of the security controls mandated by compliance policies
- Knowledgeable professionals that are up to date with the latest regulations
- Continuous monitoring to ensure continuous (rather than point-in-time) compliance
- Robust reporting for audit preparations
- Minimal downtime due to speedy issue remediation
- Quick time-to-value with your compliance solutions

In addition to these benefits, organizations that entrust their compliance programs to managed service providers can also track their progress over time. Some managed service providers offer personalized guidance on program optimization to help you set and track your cybersecurity and compliance goals over time. This is especially helpful because only 70 percent of companies try to gauge the effectiveness of their compliance programs—and of those, only a third can say they have confidence in their metrics.[5]

You Can Trust Fortra's Managed Services for Compliance

Fortra's portfolio of best-in-class managed services makes it easy to entrust your compliance program to experts you can count on.

The following is a sampling of regulations our managed services support, but keep in mind that we can create custom policies and support additional data protection frameworks, too:

- Egypt Financial Cybersecurity Framework (CBE)
- Federal Information Security Modernization Act (FISMA)
- Federal Financial Institutions Examination Council (FFIEC)
- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Trust Alliance Common Security Framework (HITRUST CSF)
- Internal Revenue Service (IRS) 1075
- National Cybersecurity Authority (NCA)
- North American Energy Reliance Commission Critical Infrastructure Protection (NERC CIP)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Securities and Exchange Commission (SEC)
- Service Organization Control Type 2 (SOC 2)
- Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Trusted Information Security Assessment Exchange (TISAX)
- United Arab Emirates Information Assurance Standard (UAE IA)

Fortra's Range of Services

Whether your primary goal is to achieve strong security configurations, policy compliance, integrity monitoring, or data protection, Fortra provides flexible, effective options developed with organizations like yours in mind.

Fortra's Tripwire ExpertOps

Tripwire® ExpertOps℠ is a managed cybersecurity and compliance service that delivers instant expertise and continuous staffing for your compliance program. Choose from cloud-based or remote deployment and select the subscription tier that best matches your needs—from simple operation and monitoring to customized support from a dedicated Strategic Consultant.

Learn More

Fortra's Alert Logic Managed Detection and Response

Alert Logic® MDR® helps organizations comply with myriad regulatory requirements simultaneously to prevent threats to your critical assets. Using automated security controls, it simplifies the process of detecting vulnerabilities that could endanger your compliance status. With experts filtering out the noise of alerts, you can expect streamlined compliance with minimal disruption and improved security posture.

Learn More

Fortra's Digital Guardian Managed Security Program

Digital Guardian® MSP provides superior data loss prevention as a managed service, with teams of 24/7 global analysts working to contain both outsider and insider threats. Prevent breaches of personally identifiable information (PII) and patient health information (PHI) on your networks and keep endpoints secure with monitoring, analysis, and tuning for your DLP program.

Learn More

Fortra Managed Web Application Firewall

Fortra Managed Web Application Firewall (WAF) helps organizations meet the web application firewall requirement of several compliance mandates, including PCI DSS, HIPPA, and GDPR. For PCI DSS, our Managed WAF exceeds PCI DSS 3.2.1 requirement 6.6, and satisfies the new addition in PCI DSS 4.0, requirement 6.4, by providing continuous detection and prevention against web-based attacks.

Learn More

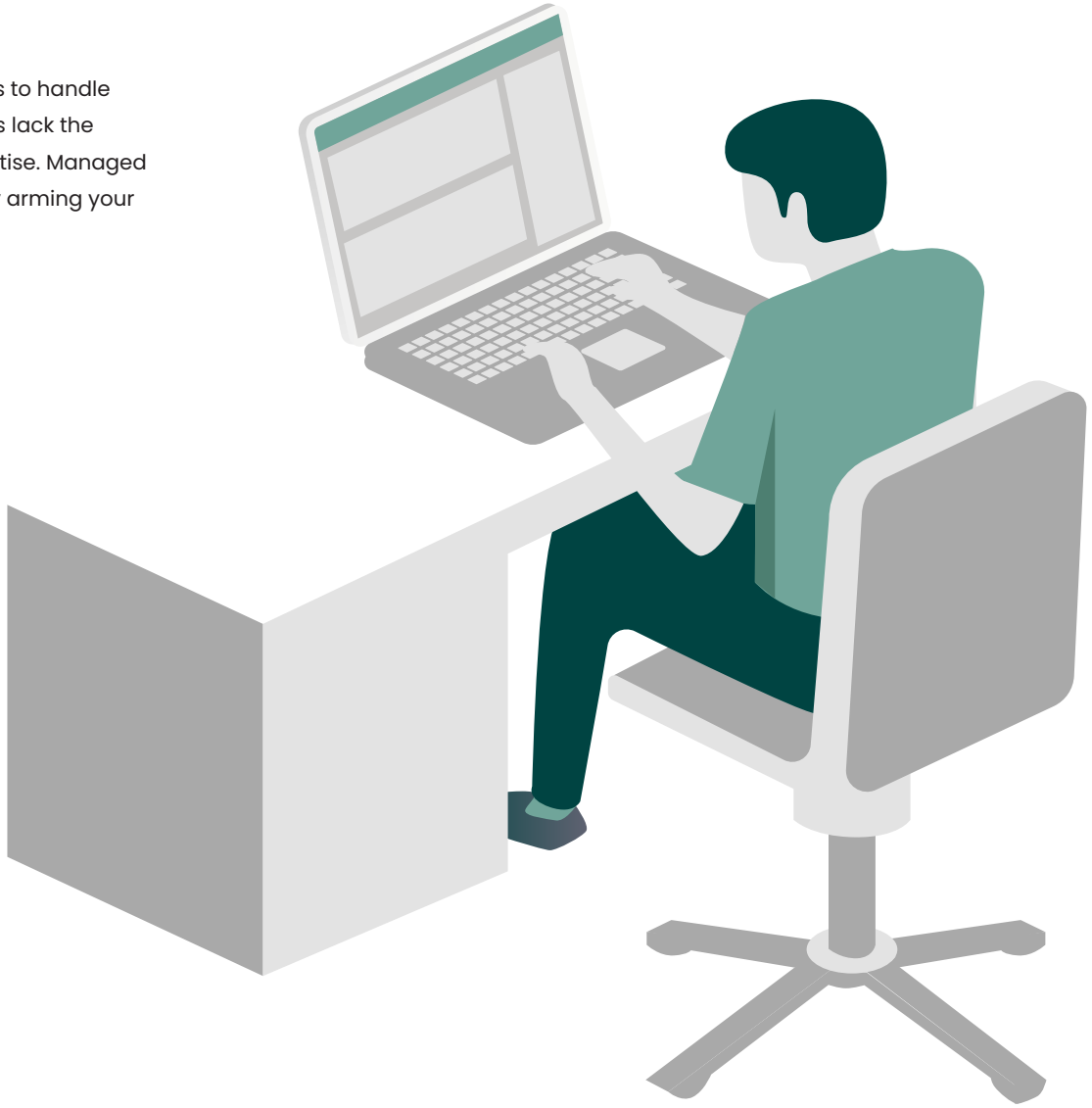
Fortra's PhishLabs Managed Digital Risk Protection

PhishLabs protects organizations from account takeover, social media scams, sensitive data leakage, and more. To protect against the exposure and sale of stolen sensitive data, PhishLabs Dark Web surveillance monitors forum and dark site activity associated with stolen data such as compromised credit card data and personally identifiable information (PII). PhishLabs Managed DRP Service also aligns closely with the Federal Financial Institutions Examination Council (FFIEC) coverage recommendations in several areas pertaining to digital risk management and protection.

Learn More

Summary

Organizations are often overburdened with managing complex tools to handle their most important compliance responsibilities, and in many cases lack the internal headcount to manage those tools with highly-trained expertise. Managed services can solve your security staffing and resource challenges by arming your team with security expertise to maintain optimal compliance.



Sources:

1. https://drata.com/blog/introducing-2023-compliance-trends-report
2. https://fortune.com/education/articles/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/
3. https://www.financierworldwide.com/driving-culture-the-role-of-the-cco
4. https://cybersecurityventures.com/hot-cloud-security-market-fueled-by-msps-and-mssps/
5. https://hbr.org/2018/03/why-compliance-programs-fail

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-tw-gd-0923-r1-hm