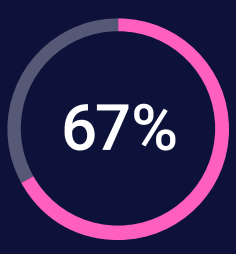
ThreatDown™
Powered by Malwarebytes

# Navigating Compliance for IT service providers and MSPs

**Simplify the complexity. Support your clients. Stay audit-ready.**

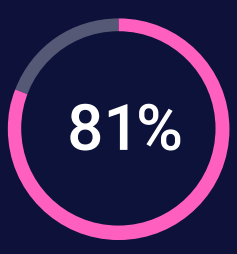
Compliance frameworks can feel overwhelming — especially when your clients span industries and regions. This infographic breaks down the key frameworks, what they typically require, and how MSPs like you can support clients with the right tools.

## Why Compliance Matters



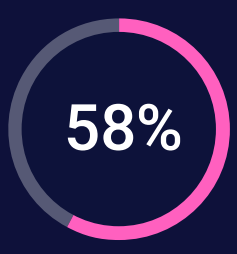

of SMBs say compliance drives cybersecurity spend.[1]

[1] ISACA State of Cybersecurity 2025




of breaches impacted regulated data.[2]

[2] Verizon 2025 Data Breach Investigations Report (DBIR)




of MSPs say compliance guidance is a top client ask.[3]

[3] Channel Futures MSP 501 Report, 2025 Edition

## Key Compliance Frameworks by Region

**North America:**

- HIPAA (Healthcare)
- NIST 800-53 (Gov/Contractors)
- CMMC 2.0 (Defense)
- CCPA/CPRA (Consumer Privacy)

**EMEA:**

- GDPR (All Industries)
- DORA (Finance)
- UK Cyber Essentials (Basic Controls)
- NIS2 (Critical Infrastructure)

**Global:**

- ISO 27001 (ISMS)
- SOC 2 (SaaS, Finance)
- PCI-DSS (Retail, Finance)

## The MSP's Role in Compliance

- Not responsible for certification — but operate the tech that enables compliance
- Provide MDR, EDR, secure config, logging, and response tools
- Contribute to client QBRs, audits, and risk posture

## What's Typically Required

**Encryption**
(Email & Data)

**Policies**
(Access Control, Retention, Use)

**Security Tools**
(EDR, MDR, Patch, DNS)

**Logging & Monitoring**

**Role-based & MFA Access**

**Breach Notification**

**Incident Response Plans**

**Audit Readiness**

## ThreatDown: Your Compliance-Ready Partner

**Tools that help MSPs align with compliance:**

- 24/7 MDR (SOC 2, ISO, NIST)
- Email Security (HIPAA, GDPR, PCI)
- DNS Filtering, Patch Management, App Control (NIS2, Cyber Essentials)

## Join the ThreatDown Partner Program

**Contact us**