How Managed Endpoint Security Can Support Selected Security and Compliance Requirements

Overview

Many regulations, industry standards, and cybersecurity frameworks share the same endpoint security expectations: **protect systems, detect suspicious activity, investigate events, and respond quickly.**

> **TPx Managed Endpoint Security, powered by SentinelOne, supports these common technical requirements through continuous endpoint visibility, behavioral threat detection, investigation context, containment capabilities, and coordinated response.**

How Managed Endpoint Security Helps

- Continuous endpoint visibility
- Behavioral threat detection
- Alert and investigation context
- Platform-based response capabilities
- 24/7 MDR monitoring with the Advanced solution tier
- Analyst-led investigation and triage with the Advanced solution tier
- Approved response actions and coordinated communication

SentinelOne Security

SentinelOne supports customer security, risk management, and compliance efforts through independently audited certifications and attestations, including SOC 2, ISO/IEC 27001, and PCI DSS, and aligns its security program with recognized frameworks and regulatory requirements such as the NIST Cybersecurity Framework (CSF), NIST SP 800-171, HIPAA, and GDPR.

Where These Capabilities Apply

Requirement	What it Expects	Relevant TPx Contribution
NIST Cybersecurity Framework 2.0	Protect systems, detect cybersecurity events, analyze suspicious activity, and coordinate response.	Endpoint protection, behavioral threat detection, investigation context, containment capabilities, and response coordination
HIPAA Security Rule	Technical safeguards that help protect electronic protected health information and procedures for identifying, responding to, mitigating, and documenting security incidents	Detection of suspicious endpoint activity, investigation context, containment support, and service information that may support incident procedures and documentation
FTC Safeguards Rule under GLBA	Safeguards designed to protect customer information, monitor information systems, and support incident response processes	Continuous endpoint monitoring, behavioral threat detection, investigation support, containment, and defined response responsibilities
GDPR	Protection of personal data of individuals in the European Union, which includes technical and organizational safeguards to protect privacy rights, ensuring data processing transparency, and promptly detecting, responding to, and reporting data breaches	Endpoint monitoring, threat detection, investigation support, approved response actions, service reporting, and response coordination
PCI DSS v4.0.1	Protection of in-scope systems from malicious software and processes for responding to suspected or confirmed security incidents	Behavioral threat detection, endpoint alerts, investigation context, containment support, and information that may contribute to incident response processes

Choose the Right Level of Support

Standard Solution Tier (EDR)

Provides SentinelOne-powered detection and response capabilities for organizations with teams that can review alerts, investigate activity, and drive response. TPx manages the platform and support experience.

Advanced Solution Tier (EDR + MDR)

Adds 24/7 MDR monitoring, analyst-led investigation and triage, proactive threat hunting, approved response actions, and coordinated communication.

Complementary TPx Services

Cybersecurity Compliance Management

Helps address the broader governance, documentation, and oversight activities that support compliance efforts. Through gap assessments, ongoing monitoring, quarterly reviews, and expert guidance, TPx helps organizations evaluate their security posture, prioritize risks, maintain supporting policies and evidence, and respond to changing requirements.

Endpoint Management

Supports endpoint operations and device management. When combined with Managed Endpoint Security, it can provide more consistent endpoint coverage, smoother agent deployment and validation, better visibility across managed devices, and stronger coordination between IT operations and security response.

Important Compliance Consideration

TPx solutions can support selected technical safeguards, governance activities, and security processes, but they do not by themselves establish or guarantee compliance or conformity with any law, regulation, standard, framework, contractual requirement, or insurance condition.

Applicability and compliance depend on the organization's environment, scope, risk analysis, policies, procedures, implementation, documentation, and other administrative, physical, and technical controls.