Mantis Protect FAQs for CISOs

blue mantis

Mantis Protect is a managed cybersecurity platform designed specifically for midsized businesses. It combines next generation, enterprise-grade protection with simplified delivery, giving you the tools and expertise you need – in a predictable cost structure – without the overhead of building and managing everything in-house.

The service utilizes User and Entity Behavioral Analysis (UEBA), AI detection and advanced SOAR capability natively built into the platform. Technology coupled with our expert-led security analysts, threat hunters and cyber maturity advisors to prioritize, validate, remediate and proactively assess your alerts reducing the noise of “false positives” and notifying only of current and future credible threats.

Mantis Protect delivers this actionable security intelligence using:

Foundational Security Services

The baseline layer of protection including **email security, user awareness training, multi-factor authentication (MFA), and antivirus.**

AI-Enhanced SIEM with Machine Learning & UEBA

Processes massive volumes of telemetry, analyzes user and entity behavior, and highlights anomalies that matter.

Proactive Threat Hunting

Goes beyond alerts to actively search for hidden risks before they escalate.

Expert SOC Analysts

Human expertise layered on top of AI-driven detection to validate intent, context, and risk.

Managed SSE for Zero Trust

Secure Service Edge (SSE) ensures Zero Trust is consistently applied across users, devices, and cloud applications, protecting data in motion everywhere your workforce operates.

Customized Playbooks

Response workflows tailored to your business, not generic templates.

Compliance Alignment

Continuous monitoring and audit-ready reporting for HIPAA, PCI, SOC2, GDPR, CMMC, and state privacy laws.

What specific capabilities does the Mantis Protect solution offer?

Mantis Protect is a suite of managed detection and response (MDR) cybersecurity tools and services that combine AI-driven detection and security analytics with our 24/7 live security analysts to prioritize and validate customer alerts. This reduces the noise of “false positives” in cybersecurity to ensure that we are only notifying your IT team when we know there are credible threats.
Mantis Protect delivers this actionable security intelligence using:

- **SIEM & Threat Hunting:** Mantis Protect is built on a unified cloud-native security information and event management (SIEM) platform positioned as a Visionary in the Gartner Magic Quadrant for the past three years. This industry-leading platform is the basis for our MDR solution, leveraging user and entity behavior analytics (UEBA) with enhanced machine learning for threat detection. Mantis Protect delivers automated proactive threat hunting capabilities via a combination of AI and dedicated human expert threat hunters. Mantis Protect solutions integrate with your existing IT security investments for seamless deployment and operation.

- **Vulnerability Management:** Mantis Protect offers an optional agent-based solution to deliver regular vulnerability scans across all endpoints, apps, and identities on your network. Vulnerability management in our Mantis Protect solution provides risk-based prioritization of potential software and hardware vulnerabilities along with automated remediation across a customer’s entire attack surface, including on-prem, cloud, and endpoints.

- **Dark Web Monitoring:** Mantis Protect customers can receive the option of proactive identification of leaked credentials, sensitive data, and targeted threats from various dark web sources. Automated detection and analysis of this voluminous data is accomplished using cloud-based AI to provide you with actionable intelligence and recommendations to mitigate threats to your business and reputation.

How does Mantis Protect provide 24/7 support and what does that mean in practice for my team?

Mantis Protect delivers the “R” in MDR with dedicated security analysts who act as an extension of our customers’ IT security teams. Mantis Protect provides 24/7 proactive alerts, threat investigation, forensic analyses, and strategic guidance for a truly holistic managed security solution. Blue Mantis owns and operates a global security operations center (SOC) with constant “eyes on glass” for your IT estate. Our SOC establishes direct lines of communication with your onsite IT along with creating personalized cybersecurity playbooks to handle security events and customized remediation support to reduce the burden on a customer’s internal IT staff along with creating personalized orchestrated and automated cybersecurity playbooks.

What is the onboarding process like for Mantis Protect, and how long does it typically take to see value?

Blue Mantis uses an Assess-Modernize-Manage approach for all customer solutions.
Our comprehensive approach includes repeatable processes that holistically consider the customer’s IT estate, existing tools and technologies and unique regulatory, compliance and cybersecurity risks. This approach not only reduces risk it also enables Blue Mantis to deploy our Mantis Protect solution in a method that seamlessly integrates with and enhances the customer’s existing security tools and tech stack. From the initial customer assessment to system integration, the process generally takes between 30 to 45 days total.

How does Mantis Protect secure the various IaaS, SaaS, devices, and network components that make up my IT estate?

Mantis Protect secures your IaaS, SaaS, devices, and network with an out-of-the-box hybrid approach that unifies cloud and on-prem defenses. By integrating managed Secure Service Edge (SSE) with Zero-Trust principles – least privilege access, explicit verification, and an assume-breach mindset – we enforce consistent, identity-driven security across every environment. This means stronger protection for users, data, and applications wherever they reside, reduced opportunities for lateral movement, and simplified management through one cohesive platform.

How does Mantis Protect help our organization meet compliance requirements (e.g., HIPAA for healthcare, CMMC for DoD, PCI DSS for finance)?

GRC-as-a-Service within the Mantis Protect solution helps organizations support and maintain regulatory compliance across industries – including healthcare, manufacturing, services, finance and others. Whether you're navigating SOC-2, NIST, HIPAA, CMMC, GDPR, PCI DSS, or state privacy laws, our platform simplifies compliance through.

Offload the complexity of policy maintenance, risk assessments, and audit preparation to our experts. We provide oversight, automated reporting, and tailored advisory support – so your team stays focused on strategic priorities.

Will my internal IT and security team lose visibility and control with Mantis Protect?

Absolutely not. Mantis Protect is built with flexibility and designed to enhance your team's visibility and control – not replace it. We operate as an extension of your team, not a black box.

- Shared Visibility: Your team has full access to dashboards, telemetry, and threat intelligence. We provide analyst-verified alerts with business context, so your team sees what we see – and why it matters.
- Collaborative Control: You retain control over escalation paths, containment policies, and response playbooks. We tailor our actions to your environment and governance model, ensuring alignment with your internal policies and protocols.
- Transparent Operations: Every action we take is logged, auditable, and communicated. You'll never be in the dark – and you'll always have the option to intervene, override, or collaborate.

Mantis Protect isn't about outsourcing security – it's about amplifying your team's impact with a true partner.

How is Mantis Protect different than other offers?

Mantis Protect stands apart from traditional MSSP solutions by delivering 360-degree cybersecurity coverage tailored for midmarket organizations. While many MSSP providers offer generic alerting and limited visibility, Mantis Protect provides:

- Full-spectrum coverage across endpoints, cloud workloads, identity, and network — not just what's easy to plug in.
- Human-verified, context-rich alerts reduces noise and delivers actionable intelligence.
- Native, built-in custom playbooks and automated containment aligned to your business and compliance needs.
- Rapid onboarding and seamless integration with your existing IT and NOC services — we carry the operational burden.
- GRC-as-a-Service to support HIPAA, CMMC, PCI DSS, and other regulatory frameworks when internal resources are limited.
- By integrating with our Digital Operations and End User Experience (EUX) services, Mantis Protect transforms cybersecurity from a reactive silo into a proactive, business-aligned engine — delivering faster resolution, deeper visibility, and a seamless user experience.
- Access to Blue Mantis' Professional Services and procurement capabilities, enabling end-to-end support from strategy to execution.
- It's not just MDR — it's a strategic security partnership that bridges detection, response, compliance, and IT operations.

What is the pricing model for Mantis Protect, and how does it compare to other MDR solutions in the market for mid-sized companies?

Mantis Protect is a subscription model competitively priced against leading managed security offerings, especially when compared to either having internal IT teams manage multiple security point solutions or building an in-house security operations center (SOC). The average cost for a company to build and staff a full 24/7 SOC in the USA is now well over $1 million in the first year, with an average of $2 million annual costs related to staffing, training, and software licenses in subsequent years.
An additional advantage of Mantis Protect is our unique ability to extend our value beyond the traditional MDR providers by combining our full suite of Mantis Protect capabilities, as well as our managed IT operational services.