Blue Mantis Protect FAQs for CISOs

What specific capabilities does the Blue Mantis Protect solution offer?

Blue Mantis Protect is a comprehensive framework of 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:** Blue 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 managed detection and response (MDR), leveraging user and entity behavior analytics (UEBA) with enhanced machine learning for threat detection. Mantis Protect delivers managed threat hunting capabilities along with governance, risk, and compliance (GRC). Mantis Protect solutions integrate with your existing IT security investments for seamless deployment and operation.

- **Vulnerability Management:** Blue 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:** Blue 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 Blue Mantis Protect provide 24/7 support and what does that mean in practice for my team?

Blue Mantis Protect delivers 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.

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

Blue Mantis uses an Assess-Modernize-Manage approach for all customer solutions, including Blue Mantis Protect. Our comprehensive approach includes repeatable processes that holistically consider the customer's IT estate. 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 Blue Mantis Protect secure the various IaaS, SaaS, devices, and network components that make up my IT estate?

Blue Mantis Protect secures the various components of your IT estate with a zero-trust security approach. With over 30 years in the industry, Blue Mantis is well known for taking a holistic approach to delivering managed IT solutions based on the National Institute of Standards and Technology (NIST) Zero Trust Architecture framework. This framework removes any implicit trust in devices, services, and users to provide comprehensive security that must be constantly monitored and validated.
Mantis Protect can detect, track, and analyze the various hardware and software components in complex hybrid IT environments for true in-depth defense against persistent cyberthreats.

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

Blue Mantis Protect enables you to achieve and maintain industry and regulatory compliance requirements via comprehensive monitoring, vulnerability management, and forensic reporting capabilities. Governance, Risk, and Compliance (GRC) controls are crucial for many organizations, and Mantis Protect can continually evaluate any changes to customer systems and track how changes may affect compliance.

What level of visibility and control will my internal security team have with Blue Mantis Protect?

Blue Mantis Protect provides real-time security analytics and dashboards to empower your internal teams at all levels with firsthand knowledge of potential cybersecurity threats and risks. These analytics and insights are the same ones used by Blue Mantis analysts in our global security operations center (SOC) to provide you with a high degree of accountability. In addition to granular and highly technical security data, Mantis Protect analytics and reporting is customizable and configurable to provide your C-suite with executive overviews based on business risks.

How does Blue Mantis Protect differentiate itself from other MDR offerings in the market (especially Arctic Wolf, Sophos, and Adlumin given Blue Mantis is partners with them)?

Blue Mantis Protect is a platform-neutral cybersecurity framework with advanced MDR capabilities that are built and operated in-house by Blue Mantis. The underlying next-gen security information and event management (SIEM) technology for our Mantis Protect solution was chosen by Blue Mantis in part because it was named a Visionary in the Gartner Magic Quadrant for SIEM every year since 2022. Blue Mantis has customized the AI-enhanced SIEM to integrate seamlessly with vulnerability management, dark web monitoring, and GRC services to meet the unique cybersecurity needs of customers in the midmarket. Blue Mantis values our partnership with Arctic Wolf, Sophos, and Adlumin – and will continue to offer those products based on customer needs.

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

Blue 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 Blue Mantis Protect is our unique ability to extend our value beyond the traditional MDR providers by combining Mantis Protect with our managed IT operational services. For example, Blue Mantis customers can employ end-to-end vulnerability management with Blue Mantis not only monitoring hardware endpoints and cloud software services for exploits, but also automatically validating and deploying the appropriate hardware and software security patches.