blue mantis

# Behind the Shield: How Blue Mantis Protect Keeps You Safe

# Table of Contents

# Cybersecurity isn't just protection—it's potential. Are you tapping into it?

Cybersecurity is essential for organizations to operate with confidence and protect their critical assets in today's digital economy. For strategic IT leaders, cybersecurity serves as a foundation for scaling operations and adapting to new challenges in a globally connected (and increasingly volatile) business landscape.

As attackers grow more sophisticated and compliance demands tighten, IT leaders face a dual challenge: strengthening defenses while ensuring security doesn't slow innovation. Security strategy is now inseparable from business strategy.

The reality: The cost of a breach is staggering. IBM's Cost of a Data Breach Report 2025 places the global average at $4.44 million with so-called "shadow AI," where employees use unapproved AI tools at work, adding an extra $670,000 to the global average breach cost. Beyond the financial hit, breaches damage trust, disrupt operations, and erode a company's long-term competitiveness.

Meanwhile, IT leaders are tasked with:

- Simplifying compliance
- Unifying fragmented tools
- Protecting sprawling hybrid and multi-cloud environments

## Enter Blue Mantis Protect.

This guide isn't just about a platform – it's a framework for understanding what modern cybersecurity should deliver: protection, compliance, and measurable business outcomes.

You'll learn:

- Why cybersecurity has shifted from a technical concern to a board-level priority
- The principles behind Mantis Protect and how they translate to business results
- How organizations are building resilience and enabling growth with modern frameworks

References: IBM, Cost of a Data Breach Report 2025, July 30, 2025.

# The Shifting Cybersecurity Landscape

Today's security environment is complex, fast-moving, and most of all, unforgiving to the ill-prepared. Challenges include:

### Disjointed Security Stacks

A patchwork of point solutions creates silos, inefficiencies, and blind spots – leaving IT teams reactive instead of proactive.

### Expanding Attack Surface

Cloud adoption, hybrid work, IoT, SaaS, and AI-enabled attacks have stretched enterprise perimeters every new integration becomes another potential entry point.

### The Talent Shortage

With a near 4M+ global cybersecurity skills gap, finding and retaining experts is nearly impossible, especially for mid-market enterprises.

### Compliance & Regulation Pressure

HIPAA, PCI, SOC 2, GDPR, CMMC, and evolving state privacy laws make compliance a business imperative. Manual reporting across fragmented tools only increases strain and risk.

Traditional stopgap approaches can't keep up – but what can?

# Introducing Blue Mantis Protect

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

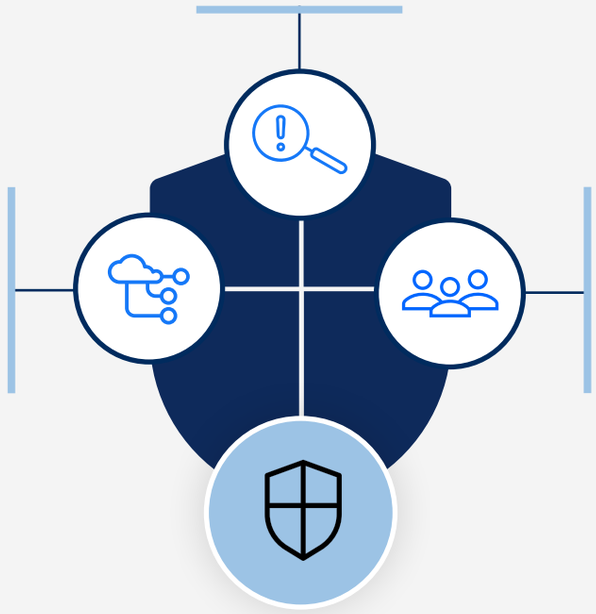
At its core, Mantis Protect rests on three pillars:

### Comprehensive Threat Detection & Response

Leveraging AI-driven analytics, machine learning, UEBA (User and Entity Behavior Analytics), continuous monitoring, and expert-led security analysts and threat hunters, the platform ensures that threats are identified and contained before they can disrupt business operations.

### Cloud-Native Scalability

Designed for modern hybrid and multi-cloud environments, Mantis Protect scales seamlessly with your business, providing consistent protection no matter how your IT landscape evolves.



### Expert-Driven Management

With Blue Mantis' team of experienced cybersecurity professionals at the helm, organizations benefit from around-the-clock oversight, proactive threat hunting, and tailored response strategies without needing to expand internal headcount.

**As MSSP Alerts puts it:**

AI and machine learning are essential for scaling threat detection. It helps us process massive volumes of telemetry and surface anomalies faster than any human team could. But threat hunting isn't just about identifying patterns; it's about understanding intent, context, and risk. That's where our human analysts come in.

Modern-day security isn't just about blocking threats anymore – it should come with the promise of continued resilience and performance. Let's move on to the key offerings of Mantis Protect, all crafted to deliver you the cream of the crop of managed cybersecurity offerings.

# Core Services

Mantis Protect delivers an integrated suite of services that address your most urgent cybersecurity needs.

**Core Service #1:**
**Managed Detection & Response (MDR) with Active Threat Hunting**

## The Pain

Most IT and security teams are stretched thin. Limited staff, after-hours coverage gaps, and the rising sophistication of attacks leave organizations vulnerable. When threats slip past perimeter defenses, every minute counts but without 24/7 expertise, the response is often too little, too late.

## The Solution

### MDR with Active Threat Hunting

Blue Mantis combines AI-, machine learning–, and UEBA-driven detection with proactive human-led threat hunting, all monitored through a 24/7 security operations center (SOC). Our team doesn't just wait for alerts; we actively seek out signs of compromise to stop threats before they escalate.

## What You Gain

- Always-on security operations that never sleep
- A proactive, not reactive, approach to defense
- Rapid detection and response that limits dwell time and damage

## What Makes Mantis Protect Different

Our MDR service is powered by the Gartner Magic Quadrant "Visionary" SIEM platform – Gurucul, bringing enterprise-grade threat intelligence and visibility to every customer engagement.

# Core Services

**Core Service #2:**
**Vulnerability Management**

## The Pain

Patching delays, a sprawl of distributed endpoints, and complex IT environments leave organizations exposed. Meanwhile, auditors demand proof of controls, putting added strain on already overextended IT teams.

## The Solution

### Vulnerability Management

Blue Mantis delivers continuous scanning, risk-based prioritization, and automated remediation workflows. By focusing on what matters most, we help you address vulnerabilities faster while reducing noise and wasted effort.

## What You Gain

- Confidence in audit readiness with documented remediation
- Reduced compliance burden and faster patch cycles
- Lower operational risk and minimized attack surface

## What Makes Mantis Protect Different

Unlike generic scanning tools, we align vulnerability data to business context so your team can focus on fixing the issues that truly move the needle for security and compliance.

# Core Services

**Core Service #3:**
Dark Web Monitoring

## The Pain

Compromised credentials and leaked data often surface on the dark web long before organizations realize they've been breached. Without visibility into this hidden ecosystem, your brand, employees, and customers remain exposed to fraud and reputation risk.

## The Solution

### Dark Web Monitoring

Blue Mantis uses advanced AI to scan over 3.5 million daily dark web events. We detect leaked credentials, sensitive data, and threat actor chatter, then provide real-time alerts so your team can act before attackers weaponize the information.

## What You Gain

- Strengthened visibility into external threats
- Accelerated remediation when leaks are detected
- Optimized use of internal security resources

## What Makes Mantis Protect Different

Our platform doesn't just flag stolen data – it combines findings with actionable intelligence, giving you next steps that help you prioritize responses and protect your reputation proactively.

# Core Services

**Core Service #4:**
**Governance, Risk and Compliance (GRC) as a Service**

## The Pain

Regulatory complexity grows every year, but many organizations lack dedicated compliance staff. The result: audit stress, compliance gaps, and high costs associated with penalties or missed certifications.

## The Solution

### GRC as a Service

Blue Mantis delivers concierge-level compliance management, real-time oversight, and expert advisory support. From policy creation to audit preparation, our GRC experts serve as an extension of your team – scaling up as your needs grow.

## What You Gain

- Always-on compliance monitoring and reporting
- Scalable services that adapt to changing regulations
- Reduced staffing costs without sacrificing expertise

## What Makes Mantis Protect Different

We pair deep regulatory expertise with automation-driven oversight, ensuring your compliance program is both cost-efficient and always audit-ready.

# How Blue Mantis Protect Works

Mantis Protect isn't just another security tool – it's a fully managed service designed to work seamlessly with your existing IT stack. At its core, the platform brings together **advanced AI, machine learning, UEBA-driven analytics, Managed SSE for Zero Trust enforcement, proven processes, and expert human intelligence** to create a multi-layered shield around your business.

Built on the NIST Zero Trust Architecture framework, Mantis Protect removes implicit trust from devices, services, and users.
By continuously validating access across hybrid and multi-cloud environments, it delivers a true defense-in-depth model, ensuring resilience even when your IT estate grows more complex.

## A Smarter Security Stack in Action

**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 our workforce operates.

**Customized Playbooks**
Response workflows tailored to your business, not generic templates.

**Compliance Alignment**
Continuous monitoring and audit-ready reporting for HIPAA, PCI, SOC 2, GDPR, CMMC, and state privacy laws.

## Our Proven Approach: Assess – Modernize – Manage

Every engagement begins with a clear-eyed assessment of your environment. From there, we modernize your defenses with the right mix of automation, analytics, and playbooks, before moving into ongoing management and optimization. The result: a solution that doesn't just keep you safe but is also fully aligned with your business priorities and tailored to improve your pre-existing infrastructure.

## Built to Fit, Not Disrupt

Mantis Protect integrates cleanly into your current IT stack. It's platform-neutral, meaning you don't have to rip and replace tools you already trust. Instead, Protect amplifies their value by bringing centralized visibility, smarter correlation, and hands-on expertise.

# From Protection to Performance: The Value of Blue Mantis Protect

The true impact of cybersecurity is measured not just in what it prevents, but in what it enables. Mantis Protect is designed with that principle in mind, **delivering value far beyond MDR and traditional SOC services**.

**Build Resilience, Recover Faster**

**Every minute counts and response delays have lasting consequences.** Mantis Protect strengthens organizational resilience by ensuring threats are contained and neutralized before they can escalate. **In the event of an incident, Mantis Protect coupled with Blue Mantis data protection services and IR services can accelerate recovery** – minimizing disruption, preserving trust, and keeping the business moving forward.

**Reclaim IT Productivity**

Security should never drain IT resources. By automating routine detection, response, and reporting tasks, Mantis Protect frees internal teams to focus on strategic initiatives that drive business growth. The result: IT staff spend less time firefighting and more time delivering innovation.

**Simplify Compliance and Audits**

Compliance no longer needs to be a scramble. Mantis Protect provides continuous visibility, detailed reporting, and audit-ready documentation. That means demonstrating adherence to frameworks like HIPAA, PCI, and SOC 2 becomes part of the daily workflow – not an annual burden.

**Reduce Risk Through Proactive Defense**

With 24/7 monitoring, advanced analytics, and rapid-response capabilities, threats are addressed before they can create material impact. This proactive posture lowers both the likelihood and cost of incidents, protecting critical assets and reputation alike.

Mantis Protect ensures IT leaders don't have to choose between operational efficiency and security strength. Instead, it creates the foundation for both – where security becomes an enabler of performance, resilience, and growth. With this shift, organizations can stop seeing cybersecurity as a sunk cost and start recognizing it as a strategic advantage.

# Features & Capabilities at a Glance

Unified security dashboard for visibility across environments.

SOC expertise available 24/7.

Pre-built compliance templates and reports.

Scalable Services for growing SMB and midsized organizations.

## Strategic Benefits

Mantis Protect helps organizations move from reactive defense to proactive resilience. The outcomes:

- **Business Resilience**: Minimize downtime and protect continuity.
- **Productivity:** Free IT teams from constant firefighting.
- **Compliance Confidence:** Simplify audits and reduce regulatory risk.
- **Risk Reduction:** Shrink attack surfaces and lower likelihood of breaches.

## Tactical Features

On a day-to-day level, IT teams gain:

- **Unified Visibility:** A single pane of glass across cloud, endpoints, and network.
- **Automation:** Playbooks that shorten response times and reduce manual effort.
- **Cybersecurity Partnership:** Human expertise layered on top of AI and automation.
- **Scalability:** Start with baseline protection, expand as your business grows.

# A Day in the Life: When Threats Strike

**Imagine this**

At 2:14 a.m., your IT team is asleep. But attackers aren't. A malicious login attempt triggers an alert in your SIEM. Normally, that alert might be buried until morning – if anyone sees it at all. By then, lateral movement could already be happening.

With Mantis Protect, here's what happens instead:

**2:14 a.m**

AI-driven detection flags the abnormal login as suspicious.

**2:15 a.m**

The 24/7 SOC validates the alert, cross-referencing threat intelligence.

**2:17 a.m**

An automated playbook temporarily locks the account, preventing escalation.

**2:20 a.m**

A Blue Mantis analyst investigates further, confirming attempted credential compromise.

**2:25 a.m**

Your security team wakes up to a clear incident report, root cause identified, and next-step recommendations.

**The Outcome**

Instead of an active breach waiting for discovery in the morning, the attack was contained in minutes – saving your organization time, money, and reputation.

# Competitive Comparison

**DIY SOC**
Requires heavy staffing, high costs, and constant upkeep.

**One-Size-Fits-All MDR**
Generic coverage that often ignores compliance or midsized-specific needs.

**Blue Mantis Protect**
Tailored to midsized businesses, balancing enterprise-grade security with flexible, cost-effective delivery.

## Why Blue Mantis Protect Outperforms DIY and One-Size MDR

| Criteria | DIY SOC | One-Size MDR | Blue Mantis Protect |
|---|---|---|---|
| **Cost Efficiency** | High upfront and ongoing costs (talent, tooling, 24x7 coverage). | Lower cost but limited flexibility; often includes unused features. | Predictable subscription pricing aligned to business needs; no hidden staffing/tool costs. |
| **Scalability** | Difficult to scale without major investment. | Rigid service tiers; scaling often means paying more than you use. | Flexible, modular services that scale with business growth and evolving threats. |
| **Expertise & Coverage** | Requires hiring and retaining scarce cybersecurity talent. | Generalized monitoring, often lacking deep industry or compliance expertise. | Access to seasoned cybersecurity experts, 24x7 monitoring, and industry-aligned best practices. |
| **Technology & Integration** | Siloed tools, complex integration, high maintenance burden. | Single platform, but limited integration with your unique environment. | Seamless integration with existing IT and cloud infrastructure, based on Zero Trust principles. |
| **Time to Value** | Long ramp-up; months to build processes and achieve coverage. | Faster deployment but minimal customization; gaps often remain. | Rapid deployment with white-glove onboarding tailored to business priorities. |
| **Business Outcomes** | Security drains resources; ROI is uncertain. | Security box is “checked” but may not enable growth or compliance. | Security as a business enabler: compliance readiness, reduced risk, and accelerated innovation. |

Unlike many MDR providers that take a one-size-fits-all approach, Mantis Protect is platform-neutral and tailored for the mid-market. Blue Mantis enables you to leverage many of your existing cybersecurity investments by integrating them into Mantis Protect, while also adding AI-enhanced features and proactive protections. That means you gain the freedom to leverage best-of-breed tools—without being locked into rigid frameworks.

As enterprise technology continues to evolve, 2025 marks a pivotal shift where the importance of network strategy becomes evident as a strategic business enabler, not just a technical necessity.

# Supporting IT Leaders & CISOs

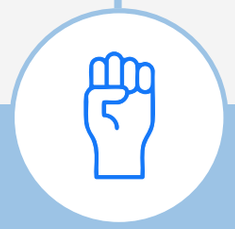
Mantis Protect was built with IT executives in mind – helping them balance security demands with strategic initiatives.

### Transparency you can trust

Gain 24/7 visibility into your security posture through intuitive dashboards and executive-ready reports that make it easy to demonstrate ROI, track compliance, and communicate risk to the board.

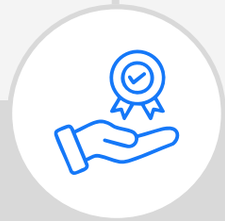
### True partnership, not just a vendor

Our SOC doesn't sit in a silo – we provide direct escalation channels, ensuring your team has immediate access to security experts when an incident occurs.



### Stronger IT, Same Team

Mantis Protect is designed to augment your staff, closing gaps without displacing existing resources.
We strengthen your team's capabilities, allowing them to focus on innovation, transformation, and revenue-driving initiatives.



### Executive advantage

By leveraging Mantis Protect, IT leaders can deliver enterprise-grade security and compliance, while freeing up capacity to align technology strategy with business growth.

# In Conclusion? It's Time to Turn Cybersecurity Into Your Next Opportunity

IT leaders and CISOs are under constant pressure to balance risk, compliance, and innovation while dealing with tight budgets and resource constraints. Traditional, one-size-fits-all solutions rarely meet the mark.

Mantis Protect was built differently. By combining a zero-trust foundation, white-glove support, and decades of industry expertise, it delivers more than security – it delivers confidence, resilience, and efficiency. Whether your goal is to reduce risk, prove compliance, or empower your IT team to focus on innovation, Mantis Protect ensures cybersecurity becomes a strategic enabler rather than a cost burden.

Organizations that understand the critical importance of fortifying the future are the ones that thrive. That's why partnering with Blue Mantis is your next best step. You don't just get protection – you gain a partner committed to your success. **Ready to take the next step?** Contact us and let's start turning your cybersecurity burdens into breakthroughs.

**Let's Meet >**

**Let's meet the future.**

**Email:** contact-us@bluemantis.com | **Phone:** (800) 989-2989

blue mantis