blue mantis

Why Cybersecurity Expertise Should Top Your Managed Services Selection Criteria

Introduction

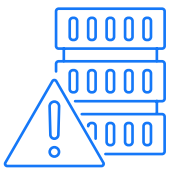
Almost half of all businesses in the United States have fallen victim to a cyberattack.[1] And 66% of respondents to a global survey of 5,600 IT pros said their organization had suffered a ransomware attack the previous year.[2] Whatever the cause, the financial impacts of a cyberattack are incredibly high, with one IBM study finding that the average cost of a data breach in the US was $9.44 million last year.[3]

At the same time, compliance with regulations like Europe's General Data Protection Regulation (GDPR) and even state laws like the California Consumer Privacy Act (CCPA) can incur costly penalties if your customers' private data is stolen or compromised. And subsequent legal expenses from lawsuits due to a breach only add to the costs. A recent CSO Online article stated, "Litigation is a probability, not a possibility."[4] Legal costs often remain an ongoing expense for years.

But IT talent is now scarce, with 62% of organizations stating that they feel they are understaffed regarding security professionals.[5] That means your business, like most businesses, may not be in a position to comply with the data protection regulations under which you operate. Or fend off attacks. That's why cybersecurity expertise should be at the top of your criteria list when reviewing managed services providers (MSPs).

But your list shouldn't stop there. The complexity of managing on-premises data centers, cloud, and hybrid cloud environments can overwhelm internal IT and security teams. Your IT team may not be available 24/7, but the attackers never sleep, often coming at you from distant time zones. The need for continuous coverage that ensures a quick response to security anomalies adds more challenges for smaller teams. Meanwhile, staying competitive in today's fast-paced business environment demands that internal IT teams focus on operations and innovation.

Having an MSP partner that offers a full suite of services—while staying focused on cybersecurity—can be a game-changer for your business, freeing up your IT team to help drive the business forward.



$9.44 million

One IBM study found that the average cost of a data breach in the US was $9.44 million last year.[3]

Cybersecurity Benefits of Working with an MSP

Every company's situation is unique. Understanding your existing IT infrastructure, cybersecurity and data protection measures, and overall security posture is crucial if your MSP is going to put effective mitigation measures in place. They also need to understand your budget restrictions, risk tolerance, and the regulatory requirements under which you operate.

That starts with an assessment that documents these areas and identifies gaps and where improvements are needed. From there, the MSP should produce an IT modernization roadmap specifying changes to your security program and infrastructure and identifying solutions to close gaps. An experienced MSP will also recommend and deploy modern cybersecurity best practices and security tools so you can be confident that your employees and data are protected everywhere and at all times.

It's also important that your MSP partner offers the breadth of services you need to ensure business resilience, from infrastructure-related services to IT expertise specific to your vertical industry. A one-stop shop approach to outsourcing is typically more efficient and cost-effective than going with multiple vendors whose solutions may not be compatible.

Why Choose Blue Mantis?

At Blue Mantis, we focus on customer care because we understand that you trust us to protect your most valuable asset—your data. For over 30 years, we've produced an enviable track record of success, helping our clients with cybersecurity, cloud and hybrid cloud infrastructures, and digital transformation solutions.

We bring deep and broad cybersecurity and managed services expertise to every customer engagement. Every member of our elite team of security experts has 20-plus years of industry experience, including stints as CIOs, CTOs, CISOs, and risk managers.

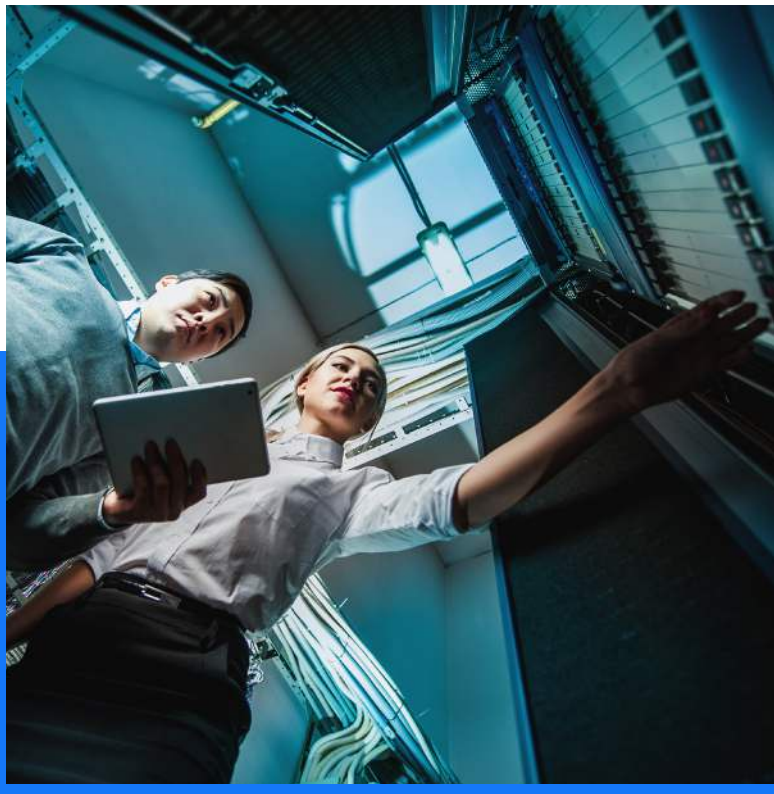
Cybersecurity Simplified

An expert and experienced MSP will recommend the appropriate strategies for securing your business. These strategies should include a multilayered approach to securing your data, devices, identities, networks, and applications.

Look for an MSP with in-depth experience in security technologies like zero trust, governance risk management and compliance, automation and orchestration, and reporting and analytics.

Your MSP partner should aid you in streamlining infrastructure management and cybersecurity and ensure you are aware of ever-evolving threats. And they should offer capabilities that can fulfill all your IT requirements as your business expands.

Blue Mantis is an MSP that has been doing just that for over 30 years.



Our teams work collaboratively across IT disciplines. If a cloud architecture update is needed to support your security requirements, for example, a Blue Mantis cloud expert will help identify the best solutions for your business. And we have deep, direct experience with legacy and leading-edge technologies.

Services, Tools, and Technologies Close Vulnerability Gaps

At Blue Mantis, we stay abreast of the latest innovations, tools, and technologies to ensure that our clients' businesses are secure and resilient. Our service offerings span every aspect of IT.

Gap Assessment Drives Requirements

Blue Mantis holds crucial cybersecurity certifications, including Certified Information Systems Security Professional (CISSP) and Offensive Security Certified Professional (OSCP), among others. We adhere to industry best practices such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27000 information security standards, and others (HIPAA, ISO 27000 PCI, SANS, CIS, and OWASP to name a few).

Blue Mantis has received its SOC 2 certification, and the company is progressing with the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC). This unifying standard and new certification model ensures that DoD contractors properly protect sensitive information—among the highest levels of digital security. To that end, we'll apply those same security principles where appropriate for all our clients.

Blue Mantis client engagements typically begin with an assessment and/or penetration test of your existing infrastructure and threat mitigation measures, including risks involving your partners, vendors, and employees. Any discovered gaps are analyzed.

We then work with you to develop a cybersecurity modernization roadmap for implementing appropriate solutions based on your unique requirements—and your budget. And our CxO-as-a-Service solutions give you access to on-demand cybersecurity expertise to help smooth the development of an effective plan and minimize the hassles of implementation.

Our service offerings span every aspect of IT.

Governance, Risk, and Compliance

We offer a suite of governance, risk, and compliance services that help you put the policies, controls, and technologies in place to ensure that you meet regulatory requirements and mitigate risks wherever possible.

Our penetration testing services help bolster your defenses by identifying attack vectors, vulnerabilities, and threats. And our ransomware readiness program helps block social engineering schemes like phishing and spearphishing, the leading methods for ransomware delivery.

Secure Access

We are also on our own zero-trust journey, continually updating best practices and identifying the most effective technologies for delivering on the promise of zero trust—preventing unauthorized access to user data. Our deep understanding of zero-trust strategies guides our process for strengthening our clients' security posture.

We employ a multilayered approach to cybersecurity that starts with ensuring our clients follow the principle of least privilege, with role-based access controls (RBAC) that limit user access to the applications and data required to perform their jobs and nothing more.

We offer multifactor authentication (MFA) solutions that put up another roadblock to access by unauthorized users. And we are adept at implementing powerful data protection technologies, like immutable backups, which can't be altered or deleted, even by ransomware.

We work with you to implement next-generation endpoint detection and response (EDR) and extended detection and response (XDR) for integrating security across endpoints, networks, servers, and cloud-based applications. Our holistic approach to cybersecurity covers multiple cloud environments and can either integrate seamlessly with your existing IT security team or provide you with trusted cybersecurity experts on call when you need them.

Cloud and Network Security

As a full-service MSP, our cybersecurity offerings extend across your infrastructure. This includes security solutions that harden your cloud environment, protecting cloud workloads while ensuring that you can scale quickly and efficiently as your business evolves. And our network security services protect your cloud and on-premises infrastructure, data, applications, and users.

Incident Management

Blue Mantis helps you immediately respond to attacks by working with you to create an effective incident response and disaster recovery (DR) plan. Our services extend to emergency incident crisis communications, ransomware containment, eradication, recovery, and digital forensics so you understand what happened and can be better prepared in the future.

Application Security

Many of our clients depend on a smooth software development lifecycle (SDLC) process to drive innovation and stay competitive. At Blue Mantis, our site reliability engineering (SRE) services help you secure your continuous integration/continuous development (CI/CD) software pipelines.

We also help you implement application security technologies ranging from static application security testing (SAST) and dynamic application security testing (DAST) to cloud-native application protection platforms (CNAPP). And we support the Open Worldwide Application Security Project (OWASP), tapping into its resources when appropriate.

Managed Security Services

By relying on Blue Mantis for managed security services, you free up your IT team from the burdens of keeping up with the latest threats and mitigation technologies. You also benefit from our robust security and information management (SIEM) solutions, state-of-the-art security operations center (SoC), and managed detection and response (MDR) technologies.

A 360° Cybersecurity Strategy

At Blue Mantis, we take a comprehensive approach to cybersecurity because anything less puts your precious data at risk. Our broad suite of managed and professional services offerings ensures that you have access to the expertise and support you need to combat threats and foster business growth.

Most importantly, we serve as your trusted advisors, closely collaborating with you to put the proper services and solutions in place for your business without taking our eyes off your budget. Our long-term customer relationships are evidence of our commitment and capabilities.

LEARN MORE

“Blue Mantis cares as much about my organization succeeding as they do their own—sometimes more.”

Arthur Harvey, CIO, Boston Medical Center

[1] Hiscox, The Hiscox Cyber Readiness Report 2022.
[2] Sophos, The State of Ransomware 2022.
[3] IBM, 2022 Cost of a data breach report.
[4] Hill M, Cybersecurity litigation risks: 4 top concerns for CISOs, CSO Online, April 2022.
[5] ISACA, State of Cybersecurity 2022 Report.