corsica technologies

BLOG ARTICLE

The Key to Managed Cybersecurity Services

Managed cyber security is an outsourced service that allows an organization to improve their cyber security standing while focusing on their core business. It's an important service for companies of all sizes due to increasing cyber threats and the high cost of hiring cyber security resources on staff.

It can be tough to evaluate **managed security service providers (MSSPs)**. This guide answers many common questions about managed cyber security to help stakeholders in IT and business make the right decisions for their organizations.

Key takeaways:

- Managed cyber security offers comprehensive protection at a lower cost than hiring experts on staff.
- MSSPs protect against every common type of cyber threat, and they scale up with growing businesses.
- The best MSSPs and their teams carry certifications like SOC 2 Type 2, Cisco CCIE Security, and others.
- MSSP pricing varies based on billing model.
- Look for an MSSP with 100% predictable pricing and unlimited service. Use our MSSP Pricing Calculator to compare.

What is managed cyber security?

Managed cyber security is a recurring, outsourced service that gives businesses comprehensive protection against evolving digital threats. Managed cyber security service providers (MSSPs) offer this protection through 24/7 monitoring, threat detection, and response capabilities delivered by specialized security experts.

Managed cyber security often includes additional services like strategic cybersecurity consulting, managed compliance, security policy development, and cyber security training for employees. Some MSSPs, like Corsica Technologies, handle all these offerings in-house. Other providers outsource some of their services to subcontractors.

The managed cybersecurity market continues to grow as businesses of all sizes adopt these services. Markets and Markets predicts that **the global Managed Security Services market will grow from $39.7B in 2025 to $66.83B in 2030**, a compound annual growth rate of 11.15. Clearly, organizations are responding to the rapidly evolving cyber threat landscape, including the rise of AI-driven attacks.

Here are the specific services that are most often included in managed cyber security.

- Strategic cyber security consulting
- Managed endpoint detection and response (MDR)
- Security information and event management (SIEM)
- Security alerting and containment
- Endpoint vulnerability scanning
- Dark Web monitoring
- Managed patching
- Secure internet gateway
- Phish testing and security awareness training
- Managed compliance
- Cybersecurity policy development

For a full rundown on what's included, check out this blog post: **What Is Managed Cyber Security**?

What are the benefits of managed cyber security?

Managed cyber security offers enterprise-class protection with a lower cost and smaller management burden than hiring equivalent experts on staff. This approach allows organizations of all sizes to gain access to an entire team of cybersecurity experts. Companies that use managed cyber security achieve the robust security standing of a global enterprise—often for the cost of one or two staff hires.

> *"The internet is a bit of wild, wild west. Corsica serves as our eyes on cybersecurity and ensures our staff are educated."*
>
> **Sharon Pohly, CEO | Girl Scouts of Northern Indiana**
> See case study →

Here are the specific benefits of managed cyber security:

- **World-class protection.** Many organizations would never gain access to this kind of protection without managed cyber security.
- **Reduced cost of protection.** Managed cyber security is far more affordable than hiring the equivalent experts on staff.
- **Reduced management burden.** Because these services are outsourced, they allow organizations to focus on their core business rather than investing significant staff resources into cyber security.

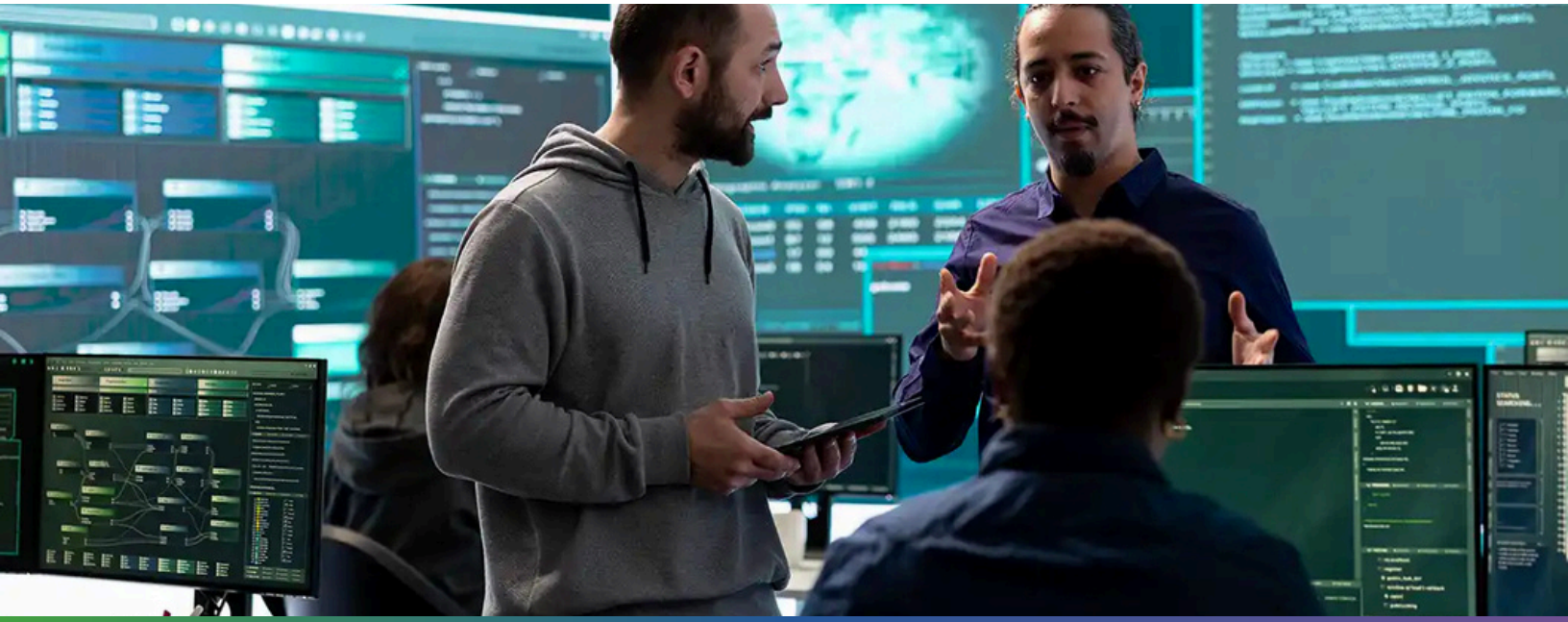
- **Strategic cyber security guidance.** Companies without a CISO (chief information security officer) benefit greatly from the C-level cyber security consulting that comes with managed services.
- **A clear path to regulatory compliance.** Organizations with small IT teams may struggle to achieve and maintain regulatory compliance. An MSSP can provide the necessary additional bandwidth and expertise—plus a clear, proven methodology—to reach compliance and maintain it over time.

Check out this article for details: **What Are the Benefits of Managed Cyber Security?**

How do managed cyber security services differ from in-house security?

Managed cyber security differs from in-house security primarily in operations, cost, and responsibility. A managed cyber security provider will come with established toolsets, policies, best practice recommendations, and contractual commitments. An in-house cyber security program must establish and maintain its own toolsets, policies, best practices, and internal SLAs.

In other words, managed cyber security offers an easier way to establish greater security, while an in-house approach offers total control alongside far greater responsibility and cost.



Here's how the two approaches compare in detail.

	Managed Cyber Security	In-House Cyber Security
Internal responsibility	Lower	Higher
Internal Control	Lower	Higher
Cost	Lower	Higher
Must Establish Toolsets	No	Yes
Must Establish Policies	No	Yes
Must Establish Internal SLAs	No	Yes
Contractually Guaranteed Outcomes	Yes	No

Want to learn more about the difference? Check out this post:

Managed Cyber Security vs. In-House Security.

What specific threats do MSS providers typically protect against?

MSSPs protect against every common type of cyber attack, including malware, phishing, AI-powered attacks, and many others. MSSPs can provide this level of coverage due to their comprehensive capabilities in cybersecurity implementation, system monitoring, threat detection, and response.

Specifically, here are the most common cyber threats and how MSSPs defend against them:

- **Malware.** MSSPs prevent the occurrence of malware by implementing best practices in access, system security, and up-to-date patching. MSSPs also use sophisticated tools to detect malware that has either slipped past these controls or was put in place before the controls were implemented.
- **Phishing.** These attacks can occur through email, phone calls, social media, and SMS messages. MSSPs prevent these attacks through AI-powered detection software and cybersecurity awareness training for users.
- **Password attacks.** MSSPs can help prevent password attacks by implementing and enforcing strong password policies, removing unneeded users, and requiring periodic password changes.
- **DDoS (dedicated denial of service).** In this type of attack, criminals overpower a system or network with traffic to shut it down. MSSPs can detect anomalous traffic, block specific IPs, and assist with backup and redundant systems to keep things running smoothly.
- **Supply chain attacks.** Cyber criminals can exploit vulnerabilities in third-party systems that are integrated with an organization's own systems. This type of exploitation is called a supply-chain attack. MSSPs can assist with preventing and detecting these through in-depth vendor analysis, vulnerability detection, and mitigation.
- **Insider threats.** Internal users will always represent a cyber security threat, whether through intentional or unintentional actions. MSSPs can help mitigate insider threats through creating and enforcing security policies, maintaining proper user permissions, and establishing Zero Trust architectures.

Get more details here: **What Threats Do MSSPs Protect Against**?

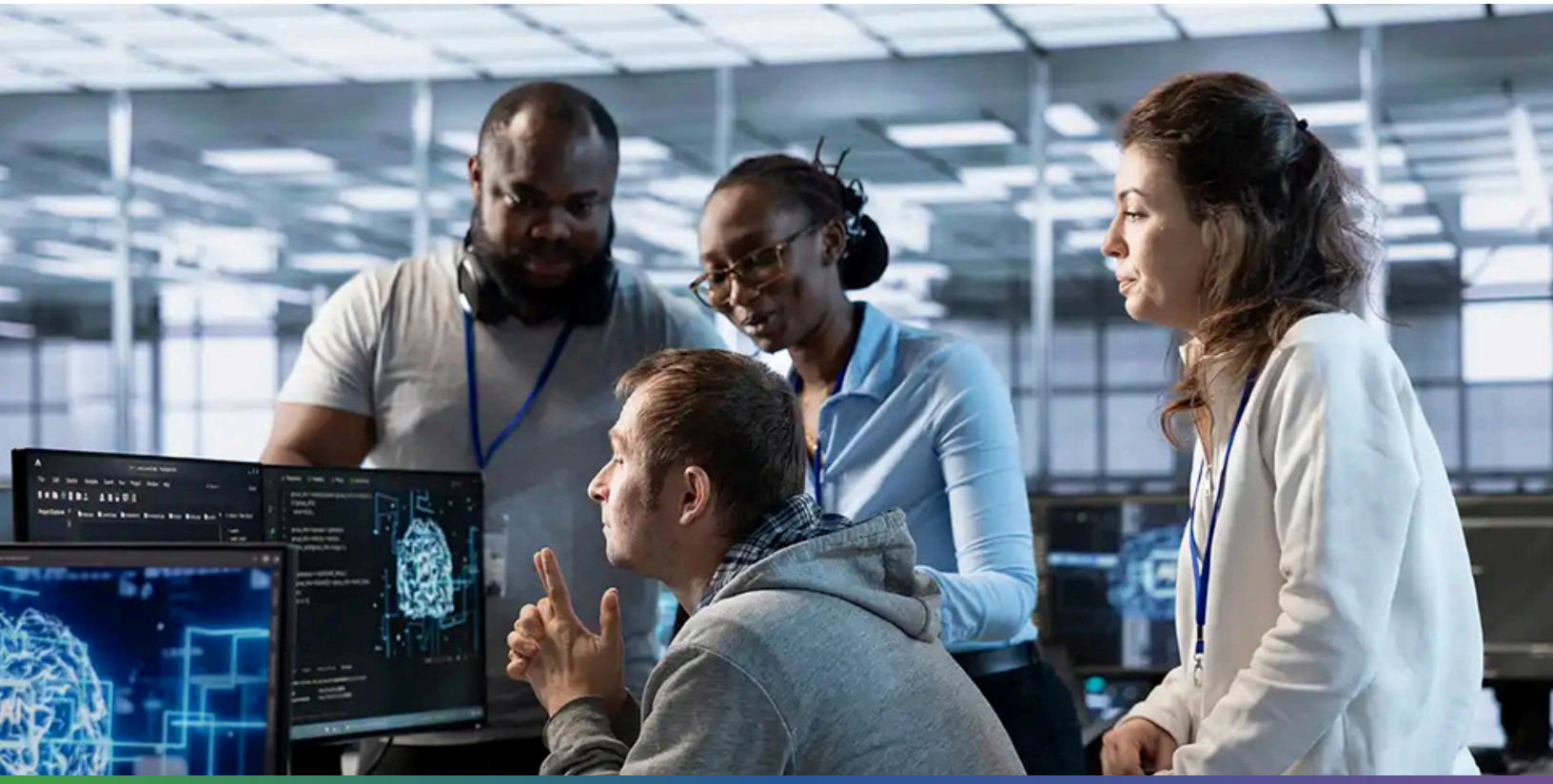
How can managed security services scale with business growth?

Managed security services can scale with business growth through the flexibility and comprehensive capabilities of MSSPs. The best providers have specialists in every cyber security discipline, and they offer flexible contracts and service packages. This empowers their clients to ramp up their service coverage easily as required by business growth.

In contrast, it's more difficult to scale up an internal cybersecurity team to support business growth. Screening candidates, hiring, training, and ongoing management create additional overhead and can slow down the expansion of your cybersecurity capabilities.

Managed cyber security services overcome these difficulties through economies of scale. Whatever additional resources a growing business needs, their MSSP should have those resources available already.

Learn more here: **How MSSPs Scale Their Services for Growing Clients**.



What industries benefit most from outsourced cybersecurity services?

Industries such as healthcare, financial services, manufacturing, government, and education are at significant risk of cyber attacks, making outsourced cybersecurity services especially beneficial in such sectors. However, every industry is vulnerable to attack—especially in the age of AI, in which cyber criminals can scale up their strategies to hit a wide number of organizations.

Ultimately, the benefits gained from outsourced cybersecurity don't depend on industry as much as they do on the organization's internal cybersecurity capabilities. If a company has limited staff resources to dedicate to cybersecurity—or not staff resources at all—then outsourced services are a huge help in strengthening cybersecurity posture and stopping attacks.

Go deeper with this post: **The Power of Outsourced Cybersecurity in Different Industries**.

How do top MSSPs customize solutions for different industries?

Common industries requiring customized cybersecurity solutions include healthcare, criminal justice, and defense contractors. In these industries and others, the best MSSPs tailor their solutions to address regulatory compliance, unique cyber threats, and industry requirements for data security. Here's how MSSPs adapt to solve problems in specific industries.

- **Accounting:** MSSPs help accounting firms achieve compliance with the Sarbanes-Oxley Act (SOX). They also protect accounting companies with phishing awareness training, threat detection and mitigation, and data security measures.
- **Banking:** MSSPs assist banks with regulatory compliance, such as the GLBA (Gramm-Leach-Bliley Act), Computer-Security Incident Notification Rule, and voluntary frameworks such as NIST 2.0. MSSPs also assist with all standard managed cyber security services.
- **Construction:** MSSPs help construction firms with unique cyber risks like corporate espionage, attacks from nation states, and other threats related to building infrastructure.
- **Criminal justice:** CJIS compliance is critical for organizations that handle criminal justice data. MSSPs can help achieve and maintain this compliance in addition to cybersecurity requirements that are common across industries.
- **Government:** Local governments are especially vulnerable to cyber attacks, as they often have aging infrastructure and limited resources. MSSPs can tailor their services to address infrastructure upgrades, applicable regulation, and continuous monitoring.
- **Law firms:** With lots of sensitive information in their files, law firms face unique cyber threats in terms of phishing and ransomware. MSSPs can tailor their offerings to counter these unique challenges and protect confidential information.
- **Manufacturing:** IoT (internet of things) devices, government contracts, and classified information for defense contractors create unique challenges in manufacturing. MSSPs can help with comprehensive monitoring, regulatory compliance, and solutions tailored to manufacturing.

- **Healthcare.** HIPAA regulations create unique cyber security requirements in healthcare. Unfortunately, providers are often targeted because they have patients' sensitive personal information. MSSPs can help with HIPAA compliance and solutions designed to counter the unique attack strategies in healthcare.
- **Nonprofits.** With limited resources, nonprofits often face challenges from older, unsecured technologies. MSSPs can help with roadmaps for required upgrades, better security for existing systems, and continuous monitoring, threat detection, and response.
- **Schools and education.** Budgetary constraints put schools in a tough spot in terms of cybersecurity. MSSPs can help by implementing best practices, securing user accounts, and monitoring systems 24/7 for threats.

Learn more in this blog post: **How Top MSSPs Customize Their Solutions in Different Industries**.

How much do managed cyber security services cost?

Most managed cyber security clients pay between $5,000 and $20,000 or more per month with contract lengths from three months to three years. The exact cost of these services will depend on several factors, such as the client's particular needs, the size of their organization, their regulatory compliance requirements, and the billing model of the MSSP.

Here are the main factors on the client side that contribute to the overall cost.

- The number of employees
- The number of workstations and devices supported
- The complexity of the network environment
- The number of physical locations supported
- Regulatory compliance requirements

The client's environment isn't the only thing that influences cost. The MSSP's approach to billing and service delivery has a significant impact as well. MSSP pricing models fall into two categories:

- **Unpredictable pricing models.** These MSSPs will charge a fee per unit, such as number of users supported, number of devices supported, number of service hours consumed, or some combination of these calculations. This can create fluctuating bills for clients, making it challenging to stick to a budget.
- **Predictable pricing models.** These MSSPs charge one unchanging monthly fee for the duration of the contract. This fee remains stable even as the client's service requirements, user count, and device count fluctuate up or down. This is how pricing works for Corsica Technologies' **Corsica Secure Service Bundle**.

As you can see, the MSSP's billing model has a significant impact on the overall cost of managed cyber security services. You can use Corsica Technologies' **MSSP Pricing Calculator** to input your organization's information and compare unpredictable pricing with Corsica's predictable pricing.

What is the onboarding process for a managed cyber security service provider?

MSSPs typically onboard new clients in four separate phases: 1) Envision and Align, 2) Build and Prepare, 3) Launch and Refine, and 4) Optimize and Grow. Grouping initiatives into these phases allows an MSSP to lay a strong foundation for their partnership with the client, then build on top of it. Here's what happens specifically in each phase.

1. **Envision and Align.** The MSSP will collaborate with the client to create a shared vision for top priorities, create a list of existing gaps in cyber security coverage, and draft a plan for mutual success. While a good MSSP is ready to adjust on the fly, this stage is crucial for setting the course of the MSSP/client relationship.
2. **Build and Prepare.** The MSSP will begin work in your systems, collaborating with your team as determined in the plan. The goal in this phase is to prepare your environment, assign roles, and align the MSSP's team with your internal resources to ensure a strong partnership and meet your strategic goals.
3. **Launch and Refine.** Now your MSSP will deploy, test, and refine any new or modified systems and toolsets. They will also prepare for the support cutover to their team, then execute the cutover, taking full responsibility for the services for which they are under contract.
4. **Optimize and Grow.** MSSP onboarding doesn't end with the launch of the partnership. Cyber threats continue to evolve, and your strategic priorities may change over time. The best MSSPs involve themselves as a strategic partner, setting up a regular cadence to review your cyber security standing as it relates to specific goals, emerging trends, customer expectations, and changing best practices.

Learn more here: **Guide to MSSP Onboarding.**

corsica
technologies

Corsica Technologies offers managed IT and cybersecurity services for businesses throughout the United States. We help companies to align technology with their business goals while minimizing the IT risks to their organizations so they can focus on running their business. One of the nation's leading managed service providers, Corsica Technologies is full service—offering everything from help desk IT support to advanced cybersecurity risk management and compliance.

Ready to learn more about managed technology services?

Schedule a free consultation with our specialists to learn how technology can enable and transform your business.

corsicatech.com (855) 411-3387

Mid-Atlantic
508 Rhett Street
Suite 200
Greenville, SC
29601

Midwest
9921 Dupont Circle Dr. W.
Suite 160
Ft. Wayne, IN
46825

South-Central
7 Office Park Drive,
Suite 200
Little Rock, AR
72211

Southwest
78660 E Hartford Dr.
Suite 110
Scottsdale, AZ
85255

05/26