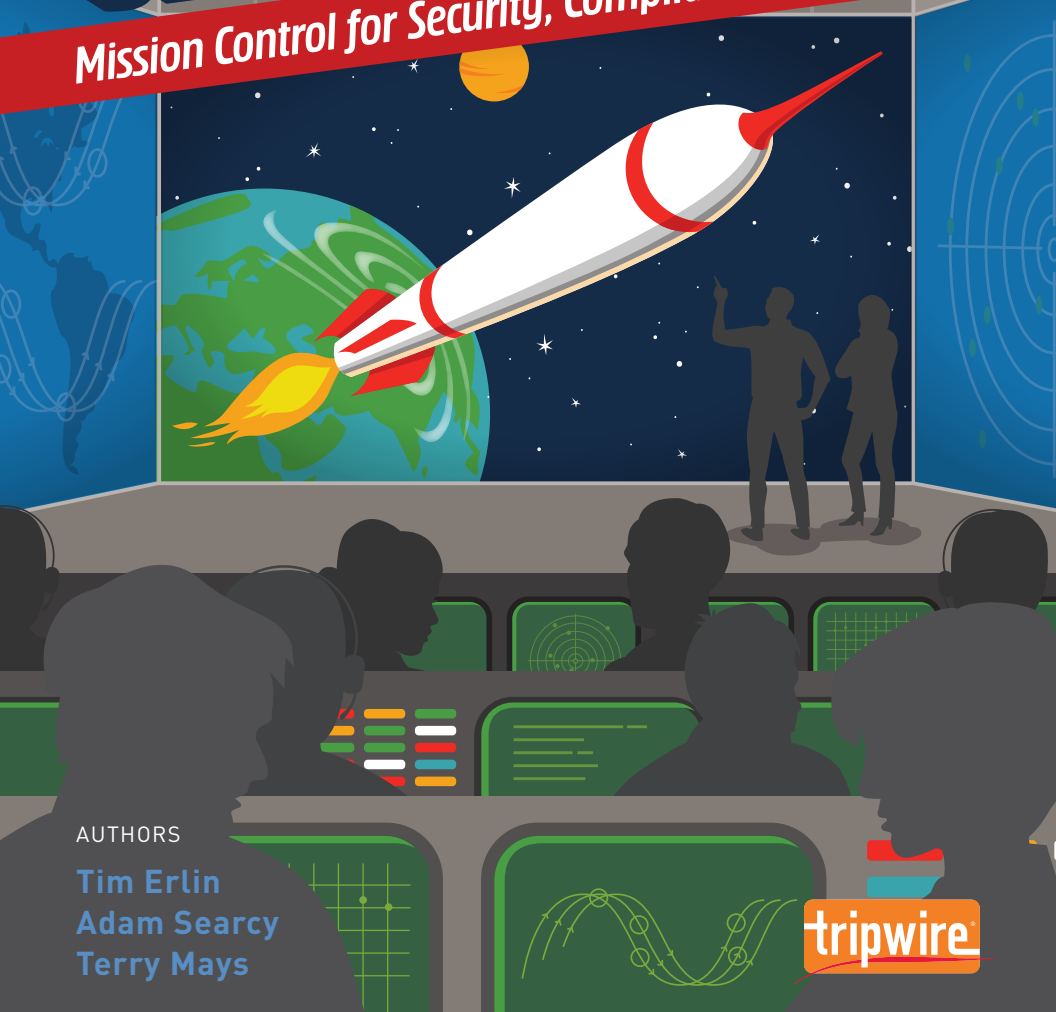


EXPLORING MANAGED CYBERSECURITY SERVICES

Mission Control for Security, Compliance, and Beyond



AUTHORS

Tim Erlin
Adam Searcy
Terry Mays

tripwire

TABLE CONTENTS

CHAPTER 1 • PAGE 4

EXPERTS AT MISSION CONTROL

Why Organizations Go Managed

CHAPTER 2 • PAGE 7



MAPPING THE SOLAR SYSTEM

Types of Managed Service Providers

CHAPTER 3 • PAGE 10

DEEPER INTO SPACE

What Do MSPs Deliver?

CHAPTER 4 • PAGE 17

LAUNCH READINESS

Commencing Countdown, Engines On



INTRODUCTION

Do you have the in-house technology and talent needed to run your cybersecurity and compliance programs? Most organizations don't, at least not at optimal performance.

Even though the idea of failed audits and data breaches is enough to motivate teams to adopt stringent cybersecurity controls, having the internal resources to make that happen effectively is rare.

It's a major challenge to recruit, train, manage, and retain a team adept at keeping up with ever-changing compliance requirements and ensuring systems are hardened against cyberattacks. The global cybersecurity workforce requires an 89 percent staffing increase in order to match the amount of critical assets that need defending.¹

In the year 2021, the number of available cybersecurity jobs hovers around 3.5 million.² We're several years into a global cybersecurity skills shortage; there still aren't enough trained cybersecurity professionals in the industry to tackle all the work that needs to be done. Simply put, there's too much to do and not enough skilled people to do it.

MANAGED SECURITY SERVICES AS MISSION CONTROL

"Managed services" refers to outsourcing particular organizational processes to an external vendor—a managed service provider (MSP)—who provides standards, best practices, and ongoing operations on your behalf.

Common managed services include helpdesk, network & systems administration, application management, cybersecurity, and compliance management. There are also managed security service providers (MSSPs), who focus entirely on cybersecurity, as well as co-managed services, where responsibilities are shared between the customer and the MSP.

That's why managed cybersecurity services are rapidly growing in popularity—it's projected that 77 percent of cybersecurity spending will go toward managed services by 2026.³ Instead of worrying about how to fill your in-house IT and cybersecurity vacancies, you can outsource part or all of this effort and rely on an MSP and their team of managed services engineers (MSEs).



By 2026, Cybercrime Magazine projects 77 percent of cybersecurity spending will go toward managed services.³

Managed service providers help their customers keep up with compliance requirements and administer a broad range of tools with the expertise to reap their full potential. Two of the main concerns propelling managed security services adoption are compliance and cybersecurity.

COMPLIANCE

Compliance is a huge driver for managed services adoption. You can stay audit-ready by making sure systems maintain compliance with regulatory and internal requirements on a continuous basis. Effective managed services providers speed up the discovery and response process so vulnerabilities aren't left floating around for a threat actor to find.

SECURITY

The inhabitants of planet Earth are getting used to reading headlines about cyberattacks on a near-daily basis. Cybercriminals are disrupting supply chains, holding sensitive data ransom or auctioning it off, breaking through the defenses of government networks worldwide, and even attempting double-extortion by threatening to post stolen data on the web.

Organizations are shifting their priorities accordingly, making cybersecurity a top focus in order to stay ahead of these threats—and in many cases it's more advantageous to outsource than to try to develop those capabilities internally. The global market for managed cybersecurity services is blasting off, set to reach \$46.4 billion annually by the year 2025.⁴

You can have the best cybersecurity and compliance solutions money can buy, but without adequate staff and expertise to run them, cybersecurity programs can't achieve escape velocity. You can think of your MSP as your mission control team, managing your solutions on the ground to ensure your spacecraft reaches orbit.



EXPERTS AT MISSION CONTROL

Why Organizations Go Managed



A variety of drivers cause organizations to use the services of an MSP. Depending on the type of organization, their priorities, and their limitations, an MSP can be a great fit. Let's start our voyage into the managed services space with a look at the benefits they can provide.

KEY BENEFITS OF MSPs

1 Do more with less

Organizations choose to utilize an MSP to get more done with less: Less time, less manpower, less worry. It can be a headache for security or IT teams to complete their long to-do lists, especially if the team is lacking in people, knowledge, or resources.

2 Overcome hiring and retention challenges

MSPs make sure your organization runs smoothly even if your team does not have adequate headcount or technical knowledge. Because employees often leave companies for any number of reasons, companies who work with MSPs can insulate themselves from the risk of staff turnover and maintain service continuity over time.

3 Unburden your staff

The reality of being short-staffed leads team members to have to do more than their share of work, often without adequate experience and training. Seventy-four percent of organizations have felt the impact of their team being understaffed—meaning overworked employees, underdeveloped security programs, and less opportunity to align with other business units on security practices.⁵ Utilizing an MSP gives you and your team more time to tackle the strategic goals on your long to-do list.

4 Leverage outside expertise

Companies benefit from the cumulative experience of their MSP that has previously supported dozens, hundreds, or even thousands of other companies that have similar problems and goals. When working with an MSSP that focuses on IT and security, efficiencies are gained that a dedicated in-house team isn't as likely to achieve. Everyone on the team—and even across the entire organization—can feel confident that their security program is in good hands.

5 Pass that audit

Another big reason for organizations to opt for an MSP is to help them more easily pass audits. Audits are daunting for many teams, and failing can result in heavy fines. However, preparing for and passing an audit can involve a lot of time-intensive work that your team might not have the bandwidth to take on. An MSP can alleviate a lot of stress, as they will be able to guide you through the audit process, saving you both time and worry. And since some auditors charge by the hour, speeding up the process by using an MSP can save you money in more ways than one.

WHO USES MANAGED CYBERSECURITY SERVICES?

Every organization needs cybersecurity, and every industry is beholden to its own set of regulatory compliance requirements mandating the use of core security controls such as configuration management, change monitoring, and vulnerability assessment.

These are some of the industries in which it's common to outsource processes to an MSSP:

- » *Financial*
- » *Tech*
- » *Federal Government*
- » *Healthcare*
- » *Critical Infrastructure*
- » *Retail*
- » *State, Local, and Education (SLED)*
- » *Transportation*
- » *Manufacturing*
- » *Oil & Gas*

THE PROS AND CONS OF MANAGED COMPLIANCE AND CYBERSECURITY SERVICES

ALL SYSTEMS GO

Solves recruitment and retention challenges with designated experts

Benefit from specialized technical skills and industry knowledge

Avoid downtime due to fast and sophisticated issue response

Save time and money on audit preparation and response

Validate in-house compliance efforts pre-audit so there aren't any surprises

Compliance isn't a strategic part of most organizations. With an MSE to handle the compliance efforts for you, you'll be able to instead focus on your strategic initiatives

Stay on top of unauthorized changes, vulnerabilities and weaknesses, and drifts from your security policy

Scale expenditures proportionally to staff size and device count to "right size" services

Quick time-to-value, as MSPs can "instantly" mature your IT or compliance department

Remove obstacles to organizational growth

LAUNCH SCRUBBED

Could pose a barrier to employees growing their roles and expertise

Less availability for impromptu requests outside service scope

May not be able to handle unique problems outside their tried-and-true processes

Not the best fit for organizations that want total control of compliance efforts

Some have older systems that don't meet the minimum requirements to be considered for MSPs, or non-standard assets for which a manual approach is preferable

Support may not extend beyond business hours of the MSP's time zone

Your data may be commingled with other organizations' data

Some prefer to keep all services in-house to enable greater oversight or help grow the department

Some organizations are beholden to geographical hosting rules that inhibit MSP adoption

An MSP's approach may seem too mature if your infrastructure is simple enough that a small team of generalists solves all requirements



MAPPING THE SOLAR SYSTEM

Types of Managed Service Providers



When you're first looking for the right type of MSP for your needs, it can quickly seem like there are more options to choose from than there are stars in the sky. The race among vendors to differentiate themselves in the market can be perplexing for customers.

When a company only communicates how it's different, the selection process can easily move from clear to confusing. Understanding the different types of managed service providers can help make the space less nebulous and provide clarity about which type of provider is right for your organization.

MANAGED SERVICE PROVIDER (MSP)

MSPs are capable and interested in managing all of your information technology, including infrastructure and people. An MSP will generally deliver services up to and including systems and network infrastructure, applications, and security. MSPs provide ongoing monitoring, maintenance, administration, and support of all IT assets.

An MSP can provide both remote and on-site resources. They may also host infrastructure and assets in their own data center, a third-party data center, or with a public cloud provider. With a definition this broad, there are, of course, many variations of MSPs in the market. The defining criteria, however, is broad applicability to IT environments and a willingness to manage the technology that you purchase or already have in place.

MANAGED SECURITY SERVICE PROVIDER (MSSP)

Managed Security Service Providers (MSSPs) can be thought of as a specialized subset of MSPs focused exclusively on cybersecurity. MSSP services generally include outsourced monitoring and management of security controls—firewalls, intrusion detection, virtual private networks (VPNs), vulnerability management, file integrity monitoring, log management, endpoint protection, identity access management, incident response, and more.

An MSSP may provide both remote and on-premises services, but there's strong bias toward remote. Because of the nature of the work, most MSSPs offer a 24/7 Security

Operations Center (SOC) for monitoring. The defining criteria for an MSSP are a focus exclusively on cybersecurity, the ability to manage a broad range of security controls, and a willingness to manage cybersecurity technologies that you already have in place or later purchase.

BEGIN TRANSMISSION

HEAR FROM AN MSSP: MSPs vs MSSPs

"MSSPs provide security-focused managed services, which are very different from other MSPs in the industry in that security spans across all aspects of an enterprise (hardware, software, applications, infrastructure, etc.)—whereas MSP could be pertaining to only one aspect, such as cloud. Large enterprises have the internal resources to manage their own security. However, it's the small and medium businesses that neither have the resources nor the right expertise to implement and support IT and OT security. MSSPs provide a robust platform where customers focus on their core business and the MSSP takes care of their 'mess for less.'"

— Premier Federal President Paul Gupta

CO-MANAGED SERVICE PROVIDERS

There's a growing category of service provider that offers a hybrid between a self-managed software-as-a-service (SaaS) solution and an outsourced managed service. These vendors are called co-managed service providers, and their goal is to allow an organization to outsource a specific security capability or function without giving up all of security to an MSSP.

In most cases, the co-managed provider is a vendor with specific expertise around the selected function or capability, or who may focus on removing the administrative burden of operating and supporting a specific tool or set of tools (for example, a firewall vendor offering co-managed firewalls, or a policy compliance vendor offering co-managed policy compliance assessment).

The defining criteria for a co-managed service provider are a focus on a function, capability, or aspect of security, and specific expertise in that domain. Co-managed providers may offer multiple services, but they do not generally offer to manage technology that's already in place. Co-managed providers may also offer different tiers of service that integrate with existing security teams at varying levels.

MANAGED DETECTION & RESPONSE (MDR)

There's a growing trend in the managed security services space specifically for Managed Detection and Response (MDR). The trend, and the differences between this service and others, merits specific mention. MDR service providers focus on the detection, containment, and disruption of efforts by a cyber adversary to limit dwell time and reduce the extent of a potential breach disclosure.

MDR is a managed service focused on threat detection and response to identified threats. In order to deliver this service, MDR providers bring their own curated technology stack to the customer and provide 24/7 "eyes on glass" monitoring of the environment for attacks, along with incident response services.

An MDR provider looks like a co-managed service because they manage their own technology, but they provide more comprehensive services, within the specific scope of threat detection, than a co-managed provider might. In terms of categorization, MDR is typically an even more focused version of an MSSP that sits somewhere between an MSSP and a co-managed service but doesn't fit neatly into either category.

WHAT ABOUT PLUTO?

Some MSPs may also offer a variety of other services that aren't technically managed services. A professional services engagement, staff augmentation services, and project-based engagements are examples of services that aren't included in the managed services definition.

Offerings such as these tend to have a specific scope—often defined by a statement of work—and a limited duration. In contrast, managed services are defined by an ongoing relationship. While these other services are important, they are outside of this book's solar system.



DEEPER INTO SPACE

What Do MSPs Deliver?



In the previous chapter, we covered the different types of managed service providers in the cybersecurity space. But what makes people look for managed services in the first place? To answer that question, we'll launch into the various capabilities offered by MSPs. But first, let's pay a quick visit to Earth to observe a typical day in the life of an overworked chief information security officer (CISO).

A DAY IN THE LIFE OF A BUSY CISO

Let's say it's Thursday on planet Earth, and a CISO named Isabella is in the 11th hour of her workday. A cold slice of pizza sits forgotten on her desk. She doesn't have time to think about dinner because she's too busy trying to address several major priorities that need immediate attention.

Her biggest challenge is an impending PCI DSS audit for which her team isn't prepared, but their time is already tied up trying to mitigate a barrage of system vulnerabilities. It's an unmanageable task to stay on top of, with confusion around which vulnerabilities are most critical. She could allocate more budget toward hiring a dedicated compliance officer or an additional security specialist, but recent turnover in the team makes it so that this new hire would need a very specific and sought-after skill set.

Isabella's situation is typical in that her main motivation for using an MSSP is for automated compliance policy enforcement. She decides to select a vendor who can run the team's cybersecurity solutions on their behalf with a high level of expertise and detailed reporting to make audits quick and painless. This way, her team can attend to other priorities and use their time more strategically.

MANAGED SERVICE CAPABILITIES IN THE CYBERSECURITY SPACE

Regulatory Policy Compliance

The purpose of regulatory compliance is to make it mandatory for organizations to follow a certain set of security controls based on the type of business they do. Without compliance policies, organizations wouldn't be audited against a basic standard of protection for their customers' data.

Many industries are subject to specific regulatory compliance standards. Retailers must align with the Payment Card Industry Data Security Standard (PCI DSS). Healthcare providers are subject to the Health Insurance Portability and Accountability Act (HIPAA). Public companies of all types must comply with Sarbanes-Oxley (SOX). Most industries have a primary compliance standard like these, but some standards are more far reaching, like GDPR (the General Data Protection Regulation).

MSPs can do the ongoing work required to ensure system compliance with mandates such as PCI DSS, SOX, North American Energy Reliance Commission Critical Infrastructure Protection (NERC CIP), and others.

HOW MSPs DELIVER COMPLIANCE AS A SERVICE

- » *Continuous policy monitoring using a solution with pass/fail compliance testing*
- » *Day-to-day enforcement of the security controls mandated by compliance policies*
- » *Presenting compliance status and trend reports to internal stakeholders*
- » *Enforcing multiple compliance policies at once*
- » *Optimizing audit prep activities*
- » *Offering tailored recommendations for compliance program improvements*

Best Practice Framework Enforcement

In addition to mandated compliance policies, managed service providers can make sure your system configurations satisfy cybersecurity frameworks provided by organizations such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST). These frameworks are continuously updated resources you can adhere to in order to maintain a modern, effective cybersecurity program that stays in orbit around emerging best practices.

There are a handful of frameworks available to help you create an effective cybersecurity program, including the CIS Controls, NIST, and MITRE ATT&CK (Adversarial

Tactics, Techniques, and Common Knowledge). An MSP with expert compliance capabilities will be able to enforce multiple policies at once across your infrastructure in addition to best practice frameworks like these.

There can be significant overlap between regulatory policies and best practice standards. In some cases, such as in adherence to internal compliance programs, organizations may undergo a compliance audit against a best practice framework. A managed provider can help take the guesswork out of how to handle multiple policies and multiple audits in an effective way.

CONTINUOUS MONITORING AND CONFIGURATION DRIFT

It's not enough to know that you were aligned with your compliance mandates under the scrutiny of an auditor. The goal should be the ability to know your exact compliance level at any point in time—audit or not.

When new assets are deployed and hardened, the confidence level in the functionality of those assets is usually high. But as users and administrators interact with these assets—software and operating systems are upgraded, settings changed—configurations deviate from their compliant state, a problem known as “configuration drift.” Continuous (rather than periodic) monitoring catches this drift and helps ensure ongoing compliance.

FILE INTEGRITY MONITORING

File integrity monitoring (FIM) is a core cybersecurity control required in most common regulatory compliance mandates (such as the PCI DSS). FIM is the control that monitors and detects changes in your environment to alert you to cybersecurity threats and helps you quickly remediate them.

While it may still be called “file” integrity monitoring, FIM has developed well beyond monitoring only files. FIM solutions also detect changes to system attributes, and to configurations that deviate from their baseline, including changes to servers, network devices, databases, virtual images, cloud service accounts, and more. They do this by continuously monitoring current system states against a secure baseline and alerting on suspicious or unauthorized changes.

MSPs can take the hard work off your security team's plate by running FIM solutions for you, conducting continuous monitoring for change control across your organization, and acting quickly to remediate risky changes that take systems out of compliance or create opportunities for malicious threat actors.

VULNERABILITY MANAGEMENT

Vulnerability Management (VM) is the process of scanning networks for known vulnerabilities (often referring to a list of common vulnerabilities and exposures, or CVEs), then prioritizing and remediating those vulnerabilities in order based on risk severity. Effective security programs have to keep up with a plethora of new vulnerabilities every day.

The Center for Internet Security (CIS) lists continuous vulnerability assessment and remediation as a key part of risk and governance programs—it's prioritized in the CIS Controls: "Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information."⁶

BEGIN TRANSMISSION

THE CIA TRIAD: CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

"In the security world, there is a CIA Triad. I have to admit, when I was a young guy starting out, I thought oh, that means the secret agency. No, it means confidentiality, integrity and this little word the most security professionals forget: availability.

Availability typically has a systems definition, meaning the system is running and available. However, it has another meaning too: accessible, as in people are accessible.'"

— Databank CISO Mark Houtp



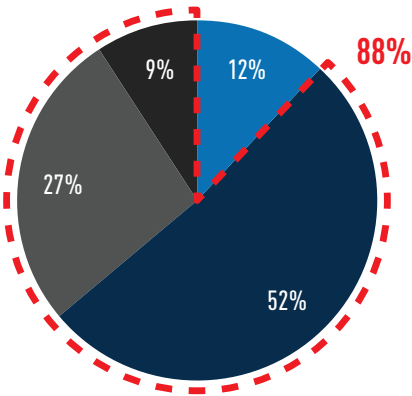
INDUSTRIAL CYBERSECURITY





Industrial cybersecurity revolves around the concept of visibility. Ensuring the integrity of your industrial environment starts with comprehensive asset discovery/inventory, management, and monitoring—those processes will just look different depending on the specific hardware and software within your industrial environment.

Industrial control systems (ICS) are rapidly becoming more connected, a change that brings with it a host of new ways for cybercriminals to gain entry. One example of this is the industrial internet of things (IIoT). In a 2021 Tripwire survey, only 12 percent of cybersecurity professionals stated that their existing teams were adequately resourced for the security needs of IoT and IIoT devices across their company.⁷

88% REQUIRED (OR STILL REQUIRE) ADDITIONAL HELP FOR IoT AND IIoT SECURITY NEEDS

In your opinion, is your team adequately resourced for the security needs of IoT and IIoT devices across your company?



-  Yes, our existing team is more than capable with existing skillsets
-  Yes, but we've required additional help (training, hiring, consultants, etc.)
-  No, but we have a plan to get there
-  No, we don't and we're not sure what we need to do

BEGIN TRANSMISSION

WHAT MSPs DELIVER IN IT vs OT ENVIRONMENTS

Some MSPs have the capabilities to bridge what's called the IT/OT gap: the inherent mismatch between IT security processes and OT equipment. Industrial environments are a complex mix of traditional IT assets as well as unique industrial OT assets such as programmable logic controllers (PLCs), robots, conveyor systems, sensors, etc. MSSPs with OT specialization will implement solutions that can read common industrial protocols—discovering and monitoring industrial assets that can't be scanned with traditional IT tools—and meeting compliance requirements in the process.

In general, MSSPs serving OT networks will not be fully cloud-based, as it's often necessary to have an on-prem footprint to interface with ICS equipment. It's also important to consider the non-technical aspects of an MSP servicing an OT environment. When the assets are different, and the priorities are reliability, resilience, and safety, the MSP needs to bring a different set of skills to the partnership in order to be successful.

— Databank CISO Mark Houpt

OTHER SERVICES MSPs OFFER

- » *Network and connectivity support (routers, switches, firewalls, wireless access points (WAP), internet service provider (ISP), and VoIP*
- » *Desktop support and helpdesk*
- » *Public cloud account configuration management*
- » *Infrastructure monitoring and management for servers, storage, and operating systems*
- » *Mobile device management and application management*

MANAGED SERVICES FAQs

Q: Where will my data be hosted?

A: There are many data hosting options available depending on the specific MSP you're working with. Here's a non-comprehensive list of possibilities:

» *Private cloud* » *Public cloud* » *Self-hosted cloud*

» *Co-location or data center* » *On-premises*

Based on your industry, there are regional data residency laws and regulations that your MSP will need to take into consideration. If your data needs to be hosted in multiple countries, look for an MSP that has a strategy to address these requirements.

Q: What will I still be responsible for when working with an MSP?

A: The division of responsibilities between an organization and an MSP is integral to a successful relationship. That division of responsibilities can vary, so it's important to make sure that the MSP you're selecting is well aligned with your objectives and goals. Review their shared-responsibility matrix if available.

Q: What will the audit process look like when working with an MSSP that has strong compliance competency?

A: If you stay ready, you don't have to get ready. MSSPs can take the pain out of audit-readiness with continuous compliance—versus point-in-time compliance. This means you will always be in an audit-ready state, with clear documentation of exact compliance policy alignment available to the auditor.

Q: What's the benefit of a co-managed service?

A: Some decision makers see compliance as too important (and expensive) to outsource completely. Co-managed services allow you to offload day-to-day operational processes—outsourcing the hassle but not the responsibility.



LAUNCH READINESS

Commencing Countdown, Engines On



Every successful mission depends on preparation. Knowing you have the right information and fully understand the mission objectives will ensure a successful launch. It's crucial to know what your needs are for an MSP so that you will know what to look for while exploring vendors on the market.

ASSESSING WHAT YOU NEED IN A MANAGED SOLUTION

Your organization has a unique set of requirements, goals, and limitations. All will influence what a good MSP will look like to you. Before looking at the options available on the market, you must assess your own craft to figure out what you're looking for by asking questions like these:

- » **What's on your network?** Do you want all of your assets to be managed? Can all of your assets be managed? Understanding your environment will help you choose a solution that will fit all of your mission-critical needs.
- » **What are your biggest challenges?** These obstacles are likely why you've decided to work with an MSP, so you'll want to make sure you know exactly how any MSP you're considering will tackle these problems.
- » **What do you need when it comes to an MSE?** You may have local or global hosting requirements to consider. You also may need to choose vendors with engineers who hold certain certifications—for example, you might be looking for a vendor that is FedRAMP certified. Having a list of must-haves will aid you in your search process.



WHAT TO LOOK FOR IN A MANAGED SOLUTION

Next, let's outline some of the primary capabilities you should be on the lookout for when assessing MSPs. It's important to pick a solution that fits your specific needs and will deliver the best possible service.

Financial Analysis

Price is obviously a huge factor when considering new vendors. Doing a financial analysis will guide you in your decision-making. Depending on your needs, you may want a shorter-term engagement for more flexibility, or a longer one for more stability and predictability. If you are planning to divide the cost between departments and cost centers, you'll want to ensure this is possible.

Does your organization prioritize having the highest quality of service or a more budget-friendly option? Providers may have different tiers of service that will suit your needs and have the pricing that you're looking for. It's important when performing this analysis to include factors beyond software licensing costs.

For example, will engaging the MSP allow you to operate with fewer people? If you were to purchase a self-managed solution, what would you need to spend on hardware, ancillary software, training, professional services, etc.? These additional factors can make a very material difference in an analysis of return on investment (ROI).

Dedicated Support

A top-tier MSP will give you designated and customized support. Having designated support means that when you encounter problems the experts at the MSP you're working with will already understand your needs and will be able to jump in and address them.

Instead of a one-size-fits-all solution, you're getting the exact help that you need. Great service doesn't always mean *more* service, however. Identifying what type of mission support you require and right-sizing the offering is important.

Maturity of the MSP

Working with an MSP that has been around for a while is advantageous. They already know their way around the galaxy—they have great industry knowledge, are likely a stable business, and have probably resolved many of the problems you're facing for others. An MSP that has already been on many successful missions is a reliable choice.

An established MSP offers additional value, as they are more likely to have more advanced internal security resources. This means that they can allocate more dedicated expertise to specific security problems than the average organization. An experienced MSP can provide an organization with the booster rocket needed to reach stable orbit.

Helping You Prove Value

You understand how important cybersecurity is to your organization, and how worthwhile your team's efforts are. However, sometimes the rest of your organization may not, and you may not know how to show your value.

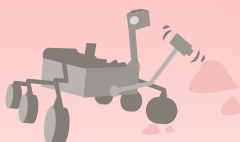
A great MSP will help you change that, by showing you reports that you'll be able to present to leadership to prove ROI. You and your MSP are doing a lot to keep your organization secure—it's crucial to share that your investment was beneficial.

BEGIN TRANSMISSION

HEAR FROM AN MSSP: COMPLEX COMPLIANCE COMPETENCE

An MSSP that handles complex multinational compliance requirements must have well-educated compliance personnel that are experts in the compliance regimens they service. The MSSP should have expert staff that are singly focused on specific disciplines, such as privacy. This staff must have a strong legal background and be backed by a legal team that can render final, legal authority over opinions and decisions.

— Databank CISO Mark Houpt



HOUSTON, WE HAVE A QUESTION

12 Questions to Ask Your MSP

1. *Are there different tiers to your service, and what are they?*
2. *How long have you been in business?*
3. *Are there certain industries in which you specialize?*
4. *Do you host your service locally, globally, or both?*
5. *Where are your company and managed service engineers located?*
6. *What reporting capabilities can you provide?*
7. *What certifications do your managed service engineers have?*
8. *Do you provide a designated point of contact for each customer?*
9. *How do you help me stay in compliance with industry standards and regulations?*
10. *How well trained is your staff on the products they support?*
11. *Do you provide technical support for all the products in your managed portfolio?*
12. *How quickly can I deploy and get value?*

WHEN YOU'RE READY TO LAUNCH AN MSP PARTNERSHIP, TRIPWIRE IS HERE TO HELP

Tripwire, in conjunction with our managed service partners, is able to support a wide range of customer situations. If you're looking for a co-managed services offering, Tripwire® ExpertOpsSM can deliver exceptional expertise and service.

If your needs go beyond a co-managed offering to include more managed security services, Tripwire's partners can deliver broad solutions that include our industry-leading technology and capabilities.

Whether your mission is to optimize specific programs like security configuration, policy compliance, and integrity monitoring, or to send your entire security function to the off-world colonies, Tripwire and our partners can provide flexible, effective, and efficient options.

Learn more about Tripwire ExpertOps

Tripwire ExpertOps provides a unique co-managed experience for customers who need security configuration assessment, policy compliance, integrity monitoring, and vulnerability assessment. It supports customers around the world, across commercial, government, and industrial environments.



Everything You Need

Tripwire ExpertOps includes software, ongoing consulting, professional services, and cloud infrastructure in a single subscription.



Personalized Service

Get tailored advice, incident assistance, and audit support based on Tripwire findings.



Focus On What Matters

Spend less time managing tools and more time protecting your organization.



Measure Performance

Track progress towards your security and compliance goals.

READY TO LEARN MORE?

Download the
Tripwire ExpertOps Services Brief
or request an evaluation now

tripwire.me/demo

THE STATE OF SECURITY

tripwire.com/blog



@tripwireinc

AUTHORS



Tim Erlin, Tripwire VP of Strategy

Tim Erlin is VP of Strategy at Tripwire, and the host of Talking Cybersecurity – The Tripwire Podcast. He previously managed Tripwire's vulnerability management product line. His background as a sales engineer has provided a solid grounding in the realities of the market, allowing him to be an effective leader and product manager across a variety of products. His career in information technology began with project management, and customer service, as well as systems and network administration. Erlin is actively involved in the information security community. His contributions include blogging, podcasts, press, speaking, and television.



Adam Searcy, Tripwire Strategic Product Manager

Adam Searcy is the Strategic Product Manager of the Tripwire ExpertOps managed cybersecurity services division, which launched in 2017. After graduating from Purdue University with a degree in Management and obtaining a series of IT certifications, Adam launched an IT consulting practice in 2002 that focused on serving software development and ASP/SaaS providers. By 2009 the company had evolved into a managed services provider, serving clients with offices spanning San Francisco to Raleigh and Chicago to Tampa. Adam sold the company in 2019 to focus on cybersecurity and worked with a local Managed Detection & Response company before coming to Tripwire. Outside of work, Adam enjoys cycling, racquetball, and spending time with his wife and two daughters.



Terry Mays, Tripwire Global MSP Program Director

Terry Mays looks after the managed service provider business at Tripwire. Terry has demonstrated success focusing on building and growing Tripwire's MSP and MSSP partner segments. He is tasked with brokering relationships, providing ideation strategy and bringing subject matter expertise to our MSP channel partners. He has extensive experience in successfully quarterbacking and managing sales activities with large GSI MSPs and MSSP channel partners. Terry holds degrees in Computer Information Systems Management, Computer Technology, and Telecommunications Management. He enjoys playing tennis and golf, and plays drums in a weekend rock 'n' roll band. Terry and his wife, Holly, reside in Atlanta/Johns Creek, Georgia.

CONTRIBUTORS



Paul Gupta, Premier Federal President

Paul Gupta brings over 35 years of industry and business experience at Fortune 100 US corporations such as divisions of GE, GM, Westinghouse, Allied Signal, and Hitachi Corporations in Cyber Security, Data Analytics, AI, ML, Health IT, and Federal Government (DoD, HHS). For the past 15 years, Paul has started multiple technology companies, and now at Premier Federal, Paul has established successful business partnerships with Cisco, Tripwire, AWS, Alteryx, Microsoft Azure, HP, and IBM, and is currently focused on developing its Cyber Security MSSP practice in partnership with the Tripwire ExpertOps platform for Federal Government and Commercial markets.



Mark A. Houpt, DataBank Chief Information Security Officer

As Chief Information Security Officer of DataBank, Mark brings 30 years of extensive information security and information technology experience in a wide range of industries and institutions. Mark joined DataBank in September of 2017 with their acquisition of Edge Hosting (CISO since 2015). In his leadership position, Mark's responsibilities include strategic planning, oversight of security, and compliance, as well as providing subject matter expertise for developing and maintaining a comprehensive, integrated information security and compliance program. Mark is a successful and sought-after security speaker, blogger, podcaster, and entrepreneur.



ABOUT TRIPWIRE

Tripwire, Inc. protects the world's leading organizations against the most damaging cyberattacks, and we've been doing it for more than 20 years while keeping pace with rapidly-changing technology landscapes to defend against ever-evolving threats. On-prem and in the cloud, our diverse solutions find, monitor, and minimize risks to your digital infrastructure—all without disrupting day-to-day operations or productivity.



ABOUT DATABANK

The data center market has changed. DataBank recognizes this, and that is why we have created the Data Center Evolved. We've invested in the infrastructure, people and frameworks that allow you to configure the solution that best fits your business needs. Whether it's a mission critical never-go-down co-location environment, a PCI DSS compliant private cloud, or a secure on-ramp to multiple public cloud availability zones, DataBank has engineered its data center platform to provide the flexibility, security, and uptime you need.



ABOUT PREMIER FEDERAL

Premier Federal, Inc. specializes in cybersecurity & compliance (CMMC), multi-cloud (hybrid, public, and private), emerging technologies (AI, ML, AR, VR, MR, NLP, 3D, and data science), and infrastructure modernization (migration and virtualization) solutions and services. Premier Federal is a SBA 8(a) certified, minority woman-owned small business located in Atlanta, GA (U.S.). Premier, along with its industry partners (Cisco, Microsoft Azure, AWS, and others), is uniquely positioned to offer its proven custom solutions and services in cybersecurity.

SOURCES

1. [ISC]². [ISC]² 2020 Cybersecurity Workforce Study, 2020, www.isc2.org/Research/Workforce-Study
2. Perhach, Paulette. "The Mad Dash to Find a Cybersecurity Force." The New York Times, 7 Nov. 2018, www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html
3. Cybersecurity Ventures. "Hot Cloud Security Market Fueled By MSPs And MSSPs." Cybercrime Magazine, 4 Aug. 2020. cybersecurityventures.com/hot-cloud-security-market-fueled-by-mcps-and-mssps
4. Panettieri, Joe. "Managed Security Services Market Forecast: How Fast Are MSSPs Growing?" MSSP Alert, 15 Oct. 2020. www.msspalert.com/cybersecurity-research/managed-security-services-market-forecast-size
5. Oltsik, Jon. "Is the Cybersecurity Skills Shortage Getting Worse?" CSO Online, CSO, 10 May 2019, www.csoonline.com/article/3394876/is-the-cybersecurity-skills-shortage-getting-worse.html
6. "CIS Control 7: Continuous Vulnerability Management." CIS, Center for Internet Security, 2021, www.cisecurity.org/controls/continuous-vulnerability-management
7. "IoT and IIoT Cybersecurity Report." Tripwire, 2021, www.tripwire.com/misc/iot-and-iiot-cybersecurity-report

EXPLORING MANAGED CYBERSECURITY SERVICES

Do you have the in-house technology and talent needed to run your cybersecurity and compliance programs? Most organizations don't, at least not at optimal performance. It's a challenge to recruit, train, manage, and retain a team adept at keeping up with ever-changing compliance requirements to pass audits and ensure systems are hardened against cyber attacks.

That's why more organizations are choosing to partner with managed service providers to run their cybersecurity solutions and compliance operations on their behalf. You can have the best cybersecurity and compliance solutions money can buy—but without adequate staff and expertise to run them, cybersecurity programs can't achieve liftoff. You can think of your MSP as your mission control team, managing your solutions on the ground to ensure your shuttle stays in orbit. Discover best practices for using managed cybersecurity services that provide advanced protection.

