novawatch

The Right People, The Right Tools, Always On WATCH

The Ultimate Guide For Choosing The Right MSSP

Optimize Security & Cut Costs with an Managed Security Service Provider Tailored to Your Unique Business Needs.

Table Of Content

Choosing The Right MSSP

Executive Summary

With cyberattacks on the rise, it has never been more important for organizations to bolster their security and compliance posture. However, not all businesses are ready to build their own security teams, and not all cybersecurity solutions can account for their client's unique needs.

That's where Managed Security Service Providers (MSSPs) come in. By outsourcing cybersecurity functions to an MSSP, businesses can get the comprehensive security management they need at a lower cost than building out traditional security infrastructure.

This white paper will explain what MSSPs are capable of and how businesses can find the right one for their unique security and compliance needs.

Key Learning Points

1. MSSPs are information technology (IT) service providers that protect businesses from security threats, maintain compliance, and resolve internal vulnerabilities.

2. Experienced MSSPs provide comprehensive cybersecurity monitoring and management, including virus and spam blocking, and intrusion detection.

3. By outsourcing security to an MSSP, businesses can reduce their security costs by eliminating the need for in-house security specialists and equipment.

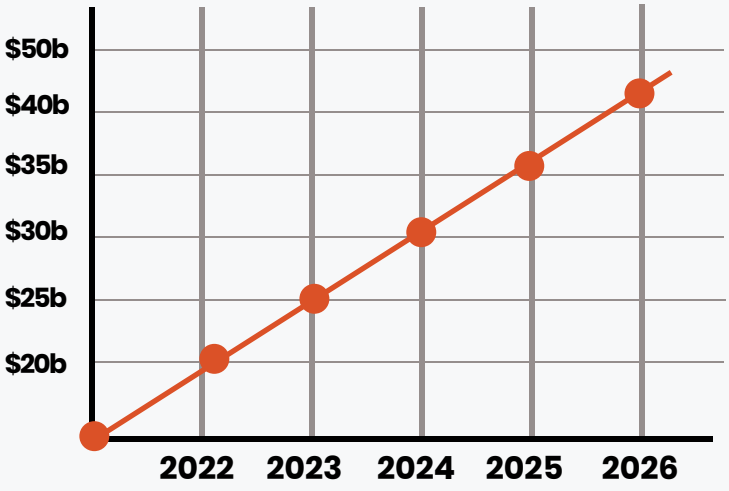
4. Not every service offered by an MSSP is necessary for a specific business or industry. Choosing the right MSSP is vital to achieve optimum security and cost-effectiveness.

What is an MSSP?

An Managed Security Service Provider is a software and IT infrastructure service provider. Businesses can outsource their security needs to an MSSP to keep sensitive data secure, detect existing vulnerabilities, and respond to cyberattacks in real-time.

Some of the services that MSSPs provide include managed firewall, intrusion detection, virtual private network, and vulnerability scanning. MSSPs can also offer security recommendations and help businesses develop compliance policies to safeguard them from internal and external threats.

MSSP Industry Forecast



Why Use an MSSP?

There's a reason the MSSP industry is forecasted to reach $46.4 billion by 2025 – these highly efficient and cost-effective security solutions can defend networks from intrusions, protect sensitive data, and streamline security processes. To accomplish this, MSSPs integrate a variety of services, including vulnerability risk assessment, threat intelligence, intrusion management, access control, and continuous security monitoring.

There's a reason the MSSP industry is forecasted to reach $46.4 billion by 2025 – these highly efficient and cost-effective security solutions can defend networks from intrusions, protect sensitive data, and streamline security processes. To accomplish this, MSSPs integrate a variety of services, including vulnerability risk assessment, threat intelligence, intrusion management, access control, and continuous security monitoring.

Key Benefits of an MSSP

Superior Protection

Since MSSPs keep up with the latest threats and techniques, they can pro comprehensive and up-to-date security services for businesses. After all, it's their job to stay on the pulse of the cybersecurity world and roll out new protections as cyberattacks continue to evolve.

Lower Costs

By outsourcing network security to MSSPs, businesses can avoid hiring a full-time staff of security specialists. The right MSSP will provide exceptional service, superior protection, and 24/7 support – all without the cost of an in-house security team.

Incident Response & Investigation

With far-reaching experience in the current cybersecurity climate, MSSP Incident Response teams can assess real-team security challenges and quickly recommend proper remedies.

Compliance & Risk Management

Because most industries require close monitoring to maintain compliance, experienced MSSPs provide comprehensive risk management and compliance expertise to ensure that each of their clients' assets receives full protection.

Cutting Edge Technology

Experienced MSSPs have access to the latest technologies and will often implement their in-house technologies to provide businesses with the best protection against cyber incidents. At MegaplanIT, our SOC analysts and security consultants are fully certified and have decades of experience helping organizations like yours stay safe from cyber threats. Based out of our state-of-the-art SOC in Scottsdale, Arizona, our Managed Security Solutions is one part of a wider service offering that can meet the specific security and compliance needs of your organization.

MSSPs Mitigate Critical Security Threats

There's no denying that malicious entities are getting more sophisticated. That's why businesses must always stay a step ahead by keeping their security posture up to date. Of course, without a team of experienced cybersecurity specialists, this is a herculean task.

When businesses outsource their security practices to an MSSP, they receive comprehensive and up-to-date cybersecurity monitoring and management without having to start from scratch or build their own security team in-house.

Some of the cyber incidents that MSSPs mitigate include:

Malware and Ransomware – Experienced MSSP platforms deliver immediate and effective virus detection to protect businesses against malware and ransomware attacks, whether endpoints are online or offline.

DDoS Attacks – Distributed denial of service (DDoS) attacks bombard servers and firewalls with fake traffic and requests until the systems are overloaded and crash. To combat this, experienced MSSPs provide anti-DDoS protection to detect malicious web traffic and filter it out.

Dark Web Activity – The dark web is an area of the Internet that's hidden from the public and commonly used by cybercriminals to share or sell stolen data. With dark web monitoring, experienced MSSPs can alert businesses if their sensitive data is leaked on the dark web.

Phishing Attacks – Approximately 90% of cybersecurity attacks begin when an unsuspecting employee opens a phishing email. Experienced MSSPs focus on prevention just as much as response, creating cybersecurity training programs to teach employees the basics of cybersecurity and the importance of awareness.

Malicious Content – To combat phishing and malware downloads, MSSPs can integrate automated filters that remove dangerous web content, preventing business devices from becoming infected.

The Cost of an MSSP

There are many factors to consider while pricing an MSSP. Typically, businesses can expect to pay between $100 to $250 dollars a month for every user. In this way, the cost is largely dependent on the size of the business and the number of services required. In any case, leveraging an MSSP will almost always be more cost-effective than hiring an in-house security team.

Let's look at some of the biggest pricing factors:

Services Required - The complexity of services required is one of the most influential factors in the cost of an MSSP. Less intensive services will have a lower cost per month, while more comprehensive and complex services will have a higher cost per month.

Number of Endpoints - Likewise, the size of your business, as well as the number of assets you need to secure, greatly impacts the price of an MSSP. Businesses with more devices and assets can expect to pay a higher premium per month.

Novawatch HQ - N. Scottsdale, Arizona

Choosing the Right MSSP For You

There's plenty of variation between MSSPs – some offer high-level security services that meet the needs of most small to medium-sized businesses while others offer more nuanced and comprehensive services fit for enterprises. To choose the right MSSP, businesses must consider which solutions and services are integral to their cybersecurity needs.

Here are some of the most important considerations:

Expertise - Businesses must verify that their MSSP is staffed with cybersecurity experts, such as engineers, analysts, and cybersecurity professionals.

Services - Comparing the services offered by an MSSP to current needs is also critical. Scaling businesses should ensure that there's room for growth as their security needs become more complex.

Choosing the Right MSSP (continued)

Specialties - Some businesses must meet certain compliance requirements, such as the Health Insurance Portability and Accountability Act (HIPAA). Finding an MSSP that specializes in relevant compliance frameworks can save businesses a lot of time and money.

Staff - Businesses should also ensure that an MSSP is staffed with a sufficient number of trained employees to provide 24/7 security support.

Security - Looking into how an MSSP handles and maintains a business' sensitive data

Why Partner with Novawatch?

Our Team - At Novawatch, our analysts and security consultants are fully certified with decades of experience in protecting businesses like yours from cyber threats. Based in Scottsdale, Arizona, our MSSP solutions are designed to meet the specific security and compliance needs of your business – no matter where you're located.

Superior Vulnerability Detection - Routine scanning and patching play a crucial role in the security of your environment and must not be relegated to a side-task for an already over-whelmed security team. By letting our VM experts handle the process for you, your routine scans will be reviewed by experienced vulnerability analysts to build a database of historical vulnerabilities and provide regular reports on current vulnerabilities.

Continuous Network Intrusion Monitoring - Identifying network intrusions requires full monitoring of all traffic to spot suspicious activity, such as lateral movements during data ex-filtration and the proliferation of malware. Our security operations team uses the latest network monitoring and intrusion detection (IDS) technologies to identify suspicious traffic inside your network and determine malicious intent. When a malicious presence is identified, containment processes nullify the threat before any damage occurs.

Constant Communication with Your Business - Novawatch's MSSP solutions are equipped with the latest security technologies and are fully staffed at all times to deliver always-on protection and communication for your in-scope systems. If you have a question, you can contact our expert QSAs at any time to solve even your toughest compliance challenges.

MSSP Displacement Program

Novawatch is excited to announce our all new, exclusive up-to 6 months* MSP Displacement Program. This program enables you to get real world experience with our cutting edge tools and 24/7 monitoring, totally free of charge until your existing technology or provider contract expires. Try it totally risk free today.

Service Overview

Cybersecurity Is Hard. Simplify It!

Our exclusive up-to 6 months* Displacement Program gives you the opportunity to get real world experience with Novawatch's cutting edge tools and service without having to pay for the same service twice, regardless of any existing SIEM's,
Antivirus or EDR tools. This program provides your Organization with a 30-day window to evaluate not only our industry leading tools but also our fully PCI & SOC2 Security Operations Center.

You've Got A Lot To Worry About

Don't Let Cybersecurity Be One Of Them

Identify threats fast, respond quickly, and maintain compliance with a cloud-based security monitoring solution that provides total visibility into your IT environment. Our experts are available 24/7 to help you react faster and better mitigate the risk of an attack by giving actionable alerts so you can take immediate action. Beyond Anti-virus, Beyond Security, You Need Managed Security Solutions That Adapt to Your Business.

Solution Offering

Managed Detection And Response (MDR)

You're on the front lines. You know how vital it is to have your network and systems protected. That's why you need a Managed Detection & Response solution that can help you stay current with the latest threats and be ready to respond quickly when an attack occurs.

- **24/7 monitoring of your network and systems**
- **Easy-to-use dashboard that allows you to see the status of all security measures in one place**
- **Weekly reports so you can see how effective your measures are at detecting and stopping threats**
- **Enriched Network Meta-data**
- **Perfect-Fidelity Smart PCAPs**
- **AI Binary Inspection for Zero-Day File Inspection**
- **Received Prioritized Alerts**

Detecting Threats, Delivering Solutions

With our Managed Detection & Response solution, we'll help you identify threats, prioritize them, and then take care of the entire incident response process. We can even help with SOAR (security operations and analysis review), which helps us analyze everything from incident detection to threat prioritization to remediation processes. We'll also help with endpoint detection, vulnerability assessments, and more—all so that when a threat comes knocking on your door, we're ready!

Solution Packages

Managed Detection & Response Services

Offering	MDR Entry	MDR Plus	MDR Pro	MDR Advanced
SIEM / XDR Solution	✓	✓	✓	✓
File Integrity Monitoring	✓	✓	✓	✓
SOAR Integration	✓	✓	✓	✓
Network Detection & Response	Optional	✓	✓	✓
Endpoint Detection & Response	✓	✓	✓	✓
Email Security Monitoring			✓	✓
Threat Hunting			✓	✓
Web Application Firewall			✓	✓
Cloud Infrastructure Security Monitoring		✓	✓	✓
Deception Technology				✓
Security Awareness Training	Optional	Optional	Optional	✓
Managed Phishing	Optional	Optional	Optional	✓
Vulnerability Assessment & Scanning	Optional	Optional	Optional	✓
Ongoing Security Penetration Testing				✓

Hosted SIEM Solution

A tremendous amount of effort goes into deploying and maintaining a SIEM solution, on top of the ongoing training and enablement of your own security team. Let us handle the difficult work for you.

Our dedicated security engineers handle all aspects of a Fully Managed SIEM deployment as well as the monitoring and optimization necessary for effective incident management. We offer a choice of several SIEM solutions tailored to best fit our clients' needs, often eliminating the need for other security tools in your environment

Key Benefits:

- **Fully Managed Security Stack**
- **Early Threat Detection**
- **Real-Time Incident Response**
- **Daily Compliance Reviews**
- **24/7/365 Staffing & Service Availability**

Log Management

Logs are collected from event sources (such as servers, switches, routers, operating systems, and firewalls) throughout the IT environment of your organization. The logs are then forwarded to other Security Analytics devices, where they are stored as meta-data for use in investigations and reports. Let us become your partner solving log management challenges with the latest solutions. We continually evaluate our logging sources throughout the day and validate this information.

with your team each month during our managed security service review meeting. We help coordinate every aspect of logging for your organization, so you can trust your logs will be securely stored, readily accessible, and retained for the specific amount of time required for compliance.

- **Continual validation of logging sources**
- **Keep track of new devices and network changes**
- **Logs are securely stored and readily accessible**
- **Fully Managed Log Retention**

Remove Alert Fatigue

It's one among some ways the protection industry has failed: you shouldn't chase false alerts or get desensitized to real ones. The Novawatch SIEM Solution gives you trustworthy, curated out-of-the-box detections.

- **Deploy and see value within days**
- **Drive efficiencies to form more room in your day**
- **Gain complete visibility of your environment**
- **Respond to threats in just a 1/3 of the time**

SOAR Platform

Integrate your analytics, SIEMs, and threat intelligence solutions in one place so you can easily track and analyze real-time data. With automated alert contextualization provided via a combination of proprietary and open-source intelligence feeds, Novawatch's security team can rapidly triage and drill-down on suspicious activity to identify malicious actors in your environment.

Through additional SOAR integrations, our security team can also incorporate many of your existing security solutions into our response capabilities, and we custom tailor every incident response plan based on your organization's unique business needs and processes.

Key Benefits:

Orchestrate

Connect your teams and tools for clear communication and complete integration across your tech stack.

Automate

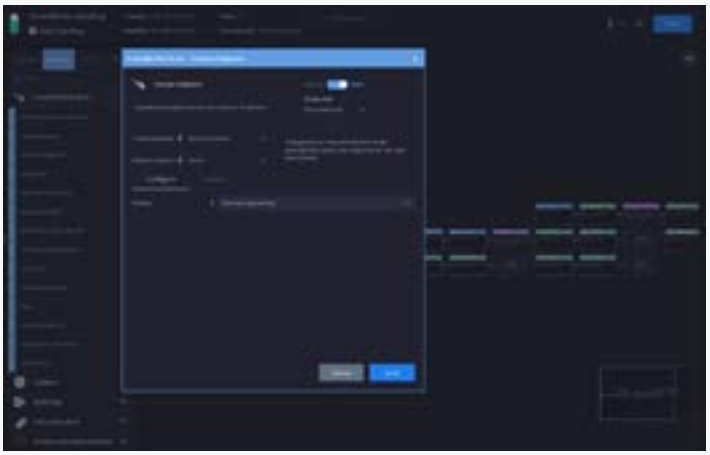
Streamline your manual, repetitive tasks with connect-and-go workflows—no code necessary.

Accelerate

Supercharge your operations with automation that creates efficiency without sacrificing control.

Connect Your Tools

Seamlessly connect your existing security tools with our library 200+ plugins. The result? Each tool is used to its max potential, connecting the dots between them to better inform Novawatch's SOC during an incident giving us maximum ability to prevent any kind of widespread issue.



Automated Workflows

Security tools haven't historically been built to work well together, and without deep programming knowledge, building automation between tools was nearly impossible. With Novawatch's SOAR platform integration, we are able to streamline our operations with workflows and playbooks and ensure that all of your security tools are performing to your expectations. We create workflows from scratch and customize them to meet your team's needs.

Mapping Your PCI DSS Requirements

At Novawatch, we have a keen understanding of the challenge businesses face in passing compliance assessments and remaining compliant over time. Based out of our State of the Art 24/7/365 Security Operations Center in Scottsdale, Arizona, we provide a suite of managed services to ensure your business stays safe from cybersecurity attacks and comply with regulatory compliance requirements.

PCI DSS Requirement	Novawatch Managed Security Services Mapped To PCI DSS
1	• Unified & Correlated Netflow analysis and firewall logs deliver “single pane of glass” visibility into access to cardholder-related data and all cardholder data flows across systems and networks. • Built-In Asset discovery provides a dynamic asset inventory and topology diagrams, cardholder-related resources can be identified and monitored for unusual activity. • Accurate and automated asset inventory combined with relevant security event notifications accelerate incident
2	• Built-in and consolidated asset inventory, vulnerability assessment, threat detection and relevant correlation provides a unified view of an organization’s security posture and critical systems configuration. • Automated assets inventory enumerates all of your PCI in-scope assets.
4	• Unified Netflow analysis and event correlation monitors traffic and issues alerts on unencrypted traffic to & from cardholder-related resources.
5	• Behavior-based solution provides an extra layer of defense against zero day threats (before anti-virus updates are issued) • Unified log management provides an audit trail of anti-virus software use by collecting log data from anti-virus software. • Built-in network detection identifies & alerts on malware infections in the credit cardholder data environment. • Integrated deployment dashboard discovers non-compliant endpoints without active anti-virus installed.
10	• Built-in log management captures all user account creation activities on critical systems, as well as collection and correlation of valid and invalid authentication attempts on critical devices. • Built-in host-based intrusion detection and file integrity monitoring detect and alarm on changes which aggregates to a central logging solution.
11	• Built-in vulnerability assessment streamlines the scanning & remediation process - one console to manage it all. • Built-in host-based intrusion detection identifies the attachment of USB devices including WLAN cards. IDS provides extra layer of defense against zero day threats (before anti-virus updates are issued). • State of the art File Integrity Monitoring alerts when password files and other critical systems files have been modified. • Unified vulnerability assessment, intrusion detection, and event correlation provides full situational awareness in order to reliably test security system and processes.

Mapping Your NIST Requirements

With Novawatch's Managed Security Services, you can identify threats fast, respond quickly, and maintain compliance with a cloud-based security monitoring solution that provides total visibility into your IT environment. Our experts are available 24/7 to help you react faster and better mitigate the risk of an attack by giving actionable alerts so you can take immediate action. Beyond Antivirus, Beyond Security, You Need Managed Security Solutions That Adapt to Your Business. A good place to start is the NIST CSF Framework. Below is a mapping of the NIST CSF Requirements to the services Novawatch offers.

NIST CSF Requirements	Novawatch Managed Security Services Mapped To NIST CSF
PR.AC-5 (1.1, 1.2, 1.3) **PR.PT-4 (all req. 1)**	• Unified & Correlated Netflow analysis and firewall logs deliver "single pane of glass" visibility into access to cardholder-related data and all cardholder data flows across systems and networks. • Built-In Asset discovery provides a dynamic asset inventory and topology diagrams, restricted data resources can be identified and monitored for unusual activity. • Accurate and automated asset inventory combined with relevant security events accelerate incident response efforts and analysis.
ID.AM-1 (2.4) **ID.AM-2 (2.4)** **ID.AM-4 (2.4)** **PR.AC-1 (2.1)** **PR.AC-3 (2.3)** **PR.AC-5 (2.2)** **PR.DS-3 (2.4)** **PR.PT-4 (all req. 2)**	• Built-in and consolidated asset inventory, vulnerability assessment, threat detection and relevant correlation provides a unified view of an organization's security posture and critical systems configuration. • Built-in host-based intrusion detection and file integrity monitoring will signal when password files and other critical systems files have been modified. • Automated assets inventory enumerates all of your in-scope assets.
PR.DS-2 (All of Req. 4)	• Unified Netflow analysis and event correlation monitors traffic and issues alerts on unencrypted traffic to and from business endpoints.
DE.CM-4 (all req. 5) **DE.CM-5 (all req. 5)**	• Built-in host-based intrusion detection provides an extra layer of defense against zero day threats (before anti-virus updates are issued) • Unified log management provides an audit trail of anti-virus software use by collecting log data from anti-virus software. • Built-in network detection identifies & alerts on malware infections in the credit cardholder data environment. • Integrated vulnerability assessment discovers non-compliant endpoints without active anti-virus installed.

NIST CSF Requirement	Novawatch Managed Security Services Mapped To NIST CSF
ID.AM-1 (2.4) **ID.AM-2 (2.4)** **ID.AM-4 (2.4)** **PR.AC-1 (2.1)** **PR.AC-3 (2.3)** **PR.AC-5 (2.2)** **PR.DS-3 (2.4)** **PR.PT-4 (all req. 2)**	• Built-in log management captures all user account creation activities on critical systems. • The system correlates valid and invalid authentication attempts on mission critical devices. • Built-in host-based intrusion detection and file integrity monitoring detect and alarm on changes.
ID.AM-1 (11.1.1) **ID.RA-1 (11.2, 11.3)** **PR.AC-5 (11.3)** **PR.DS-6 (11.5)** **DE.CM-1 (11.4)** **DE.CM-7 (11.1, 11.4, 11.5)** **DE.CM-8 (11.2)** **DE.DP-2 (11.2, 11.3, 11.4)** **DE.DP-3 (11.2, 11.3)** **RS.AN-1 (11.5.1)** **RS.AN-2 (11.5.1)** **RS.AN-3 (11.5.1)** **RS.AN-4 (11.5.1)** **RS.MI-1 (11.5.1)** **RS.MI-2 (11.5.1)** **RS.MI-3 (11.2, 11.5.1)**	• Built-in vulnerability assessment streamlines the scanning & remediation process one console to manage it all. • Built-in host-based intrusion detection identifies the attachment of USB devices including WLAN cards. • Built-in host-based intrusion detection alerts on unauthorized attempts to access cardholder data. • Unified vulnerability assessment, intrusion detection, and event correlation provides full situational awareness in order to reliably test security system and processes. • Built-in file integrity monitoring alerts on unauthorized modification of system files, configuration files, or content.

Effective Collaboration During Assessments

For most organizations, the NIST Cybersecurity Framework is an excellent basis for improving risk-based security.

Framework benefits include:

• Assistance with regulatory compliance

• Potential future improvements in limited legal exposure

• Effective measurement, monitoring, and communications of security posture

Business Requirement for Third Party Suppliers

NIST CSF can be used as a business requirement for companies that provide services to critical infrastructure owners, operators, and providers.

Framework benefits include:

• Protection against potential weak links in the supply chain

• Laying the groundwork for future requests for proposals (RFPs)

• Allows partnerships that require NIST CSF compliance.

Who We Are

Novawatch provides customized 24/7 managed detection and response (MDR) services from our state-of-the-art security operation center in Scottsdale, Arizona. Our team of certified solution experts, engineers, and security analysts will ensure that you are protected from the latest threats and intruders. Novawatch offers a uniquely client driven approach. Unlike other managed security firms, we don't see your organization as just another client. We're committed to building a relationship with your organization that will allow us to find the most cost-effective solution for your business needs.

We understand that easily accessible data is the cornerstone of a productive business environment, which is why our experts employ a practical strategy that won't interrupt your everyday activities. Our experts adhere to strict standards and leading-edge practices that will lead your organization down the most cost-effective path to cyber resiliency.

Novawatch Security Operation Center, Scottsdale, AZ

Novawatch HQ, Scotttsdale, AZ

Cybersecurity Is Hard Simplify It!

Get the visibility and control you need to confidently manage your security operations. we offer 24/7 support—so you can focus less on pushing back the floodwaters and more on building a comprehensive security strategy and implementing it enterprise-wide. You can rest easy knowing that we've got your back, so you can take care of what really matters: Keeping your business running smoothly, and keeping your customers' data safe and sound.

novawatch

The Right People, The Right Tools, Always On WATCH

Novawatch is a world leader in managed security solutions. From our full range of packaged services to our cutting-edge security technologies, Novawatch is committed to providing optimum security solutions for our clients.

Choosing an MSSP partner for your business is by no means an easy decision – but we're here to help. Give your business a brighter future and partner up with an MSSP that meets your existing security and compliance needs and has the capacity to scale with you.

Visit our website today to schedule a complimentary consultation.

Request A Demo

www.novawatch.com

Follow Us: Twitter LinkedIn