nuspire

The Complete Guide to Finding and Working with a Managed Solution Security Provider (MSSP)

nuspire.com

Table of Contents

04 Common Cybersecurity Challenges

08 How an MSSP Can Help

09 What an MSSP Offers

11 The Best Way to Work with an MSSP: A Framework

14 MSSP in Action

16 Industry Acronyms and Their Benefits

19 Additional Resources

nuspire

Cyberattacks are still on the rise

The overwhelming number of cyberattacks isn't abating anytime soon. Cybercriminals are more ruthless as they expand into new vectors and look for more stealthy ways to infiltrate your environment.

Breaches have increased 68% since 2020[i], and the average cost of a breach is now $4.24 million—the highest in 17 years[ii]. The increase in ransomware, especially, is concerning for organizations of all sizes. In 2020, it's estimated that there were 65,000 successful ransomware attacks—that's one every eight minutes[iii]. Additionally, the average time to identify and contain a data breach was 287 days[iv].

In this eBook, we'll discuss why throwing more resources (both human and money) aren't the best approach to outsmart cybercriminals and why a managed security service provider (MSSP) is your best solution for securing your organization's defenses. Consider this your complete guide to what an MSSP is, benefits of working with an MSSP, how to find the right provider, and why a coordinated, multi-layered, multi-faceted approach to security is critical.

> The average cost of a breach is now $4.24 million — the highest in 17 years.

Attackers are always a step ahead

It's not your imagination — attackers are often a step ahead of companies that are trying to protect their perimeters. Researchers at MIT studied why cybercriminals are way ahead in terms of technical innovation. They found that the dark web, a network of websites and servers that use encryption to obscure traffic, is a "value chain" of sorts and the source of many cybercriminal communities. All it takes to be a hacker is a bit of research and some bitcoin to purchase an email-flooding service on the dark web[v].

According to Kela's analysis of dark web forum activity, the "perfect" prospective ransomware victim in the U.S. will have a minimum annual revenue of $100 million and preferred access including domain admin rights, as well as entry into remote desktop protocol (RDP) and virtual private network (VPN) services[vi].

Additionally, attackers use artificial intelligence (AI) to gather personal information from social media sites like Twitter and Facebook to automatically generate phishing emails and posts with open rates as high as 60%[vii].

Common Cybersecurity Challenges

Unfortunately, defending your company against well-organized and well-funded cybercriminals isn't as simple as assigning additional internal IT personnel to combat the issue or buying more security tools.

Severe shortage of cyber experts

Creating an in-house security operations center (SOC) team by hiring cybersecurity experts might seem like an obvious option, but it's not easy to fulfill.

February 2022 saw the largest spike in cybersecurity job openings ever; an increase of 74% over a year earlier. For every 100 cybersecurity jobs openings, there are only 68 qualified candidates[viii], and 2.7 million positions are unfilled globally[ix].

Not only are these professionals scarce, they're also expensive. The average annual pay range for a cybersecurity engineer is $120,000-$210,000 and a cybersecurity analyst is $95,000 to $160,000.

Cybercriminals don't rest and neither should a security team. Full-time security operations require a fully staffed security operations center (SOC). This means you'll need a large team of these experts, probably located across time zones,to provide 24x7x365 coverage. Additionally, if you've purchased cybersecurity insurance, you may find that your insurance company mandates 24x7x354 security operations to limit the risk of ransomware.

For every 100 cybersecurity jobs openings, there are only 68 qualified candidates

Technology sprawl

It's common to purchase more cybersecurity tools to plug security holes. In fact, 30% of organizations deploy more than 50 security tools and technologies, and 45% use more than 20 tools when specifically investigating and responding to a cybersecurity incident[x].

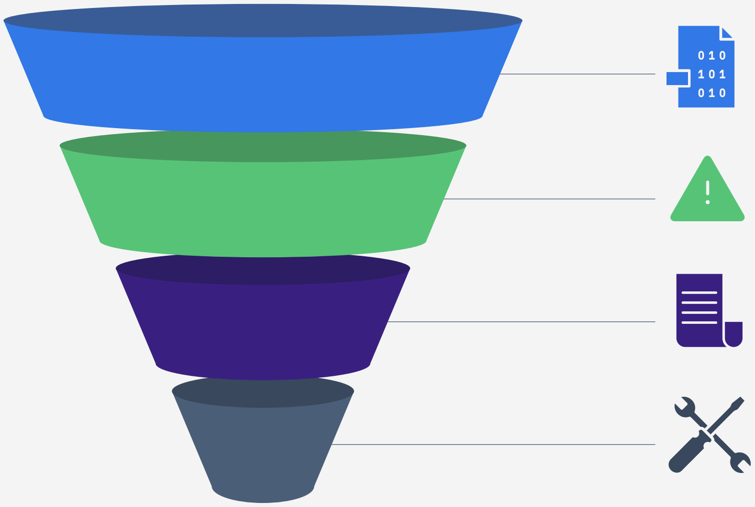
With a multitude of tools, many of which are often isolated from other threat intelligence and security tools, it's nearly impossible for your team to monitor all of them. Your IT team is left spinning a thousand plates in order to decipher information, only to have an unclear picture of your unique threat landscape and specific actions to take.

Alert fatigue

Using multiple cybersecurity tools, each of which sends threat data to your IT technicians, can quickly lead to "alert fatigue," numbing them to which alerts are most critical. Security staff spend an average of 30 minutes for each actionable alert, while 32 minutes are lost chasing each false lead[xi].

When they're potentially receiving thousands of alerts, it's easy to see why true cybersecurity threats can be missed. Alert fatigue can also result in burnout and higher turnover. When new replacements are hired, the cycle starts all over again. It also takes IT technicians away from their other important responsibilities because managing alerts becomes a full-time job.

MSSPs use threat intelligence and analysis to help you focus on the threats that matter



Logs collected
357,961,237,794

Q4 # of Alerts
5,845

Q4 # of Cases
SOC 55 / NOC 117

Q4 Remediation

	SOC	NOC
Priority 1:	1	0
Priority 2:	13	86
Priority 3:	37	25
Priority 4:	4	6

Work from home (WFH)

and bring your own device (BYOD) present unique challenges

As a majority of employees work from home and want to use their personal devices to access corporate resources, companies are presented with unique challenges to ensure their security.

The dilemma lies in giving employees the freedom they desire while ensuring they remain secure. This is a common issue for most organizations, as research from Palo Alto Networks found that 60% of organizations expanded BYOD to enable their employees to work from home. However, as a result, organizations that allow increased BYOD usage have employees who are over eight times more likely to ignore, circumvent or disable security than companies that restricted BYOD access[xii].

Organizations that allow increased BYOD usage have employees who are over eight times more likely to ignore, circumvent or disable security than companies that restrict BYOD access.

Cyberattackers understand this and continually change their methods to fool employees into taking the bait. For example, phishing schemes aren't just limited to email anymore—they're now prevalent via texting and phone calls, too.

Staff turnover opens security holes

The Great Resignation may also have ramifications for cybersecurity. As employees resign, security holes can be left behind if their user accounts aren't quickly deleted or they download sensitive information to take with them.

Current employees also might not adhere to company security policies. IT may be too busy with other responsibilities to train new employees on security processes, which can leave openings for cybercriminals to exploit. Even if employees don't have malicious intentions, they may be lax in following security guidelines such as using easy-to-guess passwords.

Difficulty keeping up with the latest threats

Threat intelligence is just information. But, when it's analyzed and becomes actionable, it becomes intelligence. It's a critical component that allows your organization to keep up with the latest threats, but it can be difficult to access and curate all the necessary threat intelligence sources to understand which ones pose the greatest risk.

It's important to know how to acquire threat intelligence and how to use it to create a smart cybersecurity program. You'll also need a security team that has the skills and experience to consume the output of threat intelligence, create an actionable plan and use it as a meaningful part of your program.

How MSSP Can Help

Rather than navigating the turbulent cybersecurity landscape yourself, it's advantageous to partner with an MSSP, a service provider that specializes in monitoring and managing security devices and systems to protect your organization from cyberattacks.

MSSPs offer a coordinated, multi-layered, multi-faceted approach to security, which is difficult to do on your own. An MSSP shifts cybersecurity risks from your organization to a third-party that specializes in addressing cybersecurity challenges.

What is an MSSP?

A managed security service provider (MSSP) monitors and manages security devices and systems for organizations. Technologies MSSPs use include firewall, intrusion detection, security information and event management (SIEM), vulnerability scanning and endpoint protection services such as anti-virus and endpoint detection and response (EDR).

What an MSSP Offers

Access to experienced cybersecurity experts

One of an MSSPs' biggest advantages is the fact that it employs a team of cybersecurity experts so you don't need to. It eliminates the need for you to find, hire, train and manage security staff, deal with turnover and more.

An MSSP's incident response team typically includes professionals such as:

- **Security intelligence and analytics experts** to identify and diagnose threat actor activities by reviewing data flows and anomalous activity, and hunting for threats.
- **Security incident team (SIT) implementation experts** to deploy tools, tweak existing tools for added visibility or apply security controls/change controls to provide short-term containment.
- **Health, availability, lifecycle and optimization infrastructure and system experts** to support the teams and systems, ensure availability of reports and make sure that change controls are working.
- **Security and incident response team (SIRT)** that is comprised of SOC operations staff and analysts who lead and execute the response process.

Multiple sources of threat intelligence

To thwart attacks, you need to know what is happening throughout your business. And you need to have multiple sources of threat intelligence powered by enough expertise to know what to do with the data. An MSSP has access to these sources so it can be proactive and escalate incidents to your organization in a predetermined process to keep you safe from threats.

The combination of human analytics and threat hunting produces threat intelligence from multiple sources. Analysts enrich information by examining indicators of dark net happenings, industry-specific compromises, threat intelligence platforms and other sources.

Actionable alerts and trained security experts

In general, there are too many alerts and false positives for any human to realistically review them all. Forty-three percent (43%) of organizations experience false positive alerts in more than 20% of cases, while 15% report more than half of their security alerts are false positives[xiv].

An MSSP's trained security experts use their vast experience to sift through alerts to prioritize the most important ones. The MSSP will also use specialized, integrated software that's designed to filter out false positives and highlight those that deserve further investigation.

This type of software is expensive to build and requires in-depth expertise to use effectively. Taken together, an MSSP's human expertise plus specialized software means you'll rarely be sent an alert that's redundant or unusable.

24x7x365 managed support services and scalability

It's a daunting task to build your own team of cybersecurity experts who can monitor your organization's security posture around the clock. An MSSP can easily do this with coverage across all time zones. Additionally, if you need to scale your cybersecurity resources up or down, an MSSP can do that quickly.

Fast incident response time

An MSSP has the capabilities and resources to speed up the response process. The longer threat actors go without being stopped, the more damage they cause. For every incident, an MSSP can provide an incident commander who can pull in resources with different areas of expertise to provide immediate, prioritized and coordinated support. This is the best approach to achieve long-term containment and mitigation.

Support level agreements (SLAs) spell out specifically what an MSSP will do for you and guarantee you'll receive a specific level of support. In general, the average time to respond after detections should be about five minutes.

Utilizes multiple sources of threat intelligence

An MSSP has an experienced security team that specializes in threat intelligence and leverages data from multiple sources, correlates it and enriches the data.

Doing this helps an MSSP provide the best information possible to you by:

- Understanding which threat actors want to attack you and the tactics they use
- Removing false positives
- Enabling a more effective response
- Permitting analysts to weigh and score the threat and make sure it is actionable information
- Enriching and fine-tuning alerts

An MSSP will monitor traffic as it passes through its infrastructure, examine syslogs and perform API analysis for near real-time, customized alerting. These capabilities provide actionable intelligence to help defend networks and systems that are communicating with malicious actors.

The Best Way to Work with an MSSP: A Framework

There are many MSSPs out there, and when you're searching for the right one, you want the best fit for your company. One of the most impartial ways to evaluate an MSSP is to ask if it uses a security framework.

It's critical to use an MSSP that has a clear security framework so you can identify and implement the right controls to build the strongest security posture for your business. The ideal framework addresses your industry, technology, infrastructure, staff, expertise and other variables.

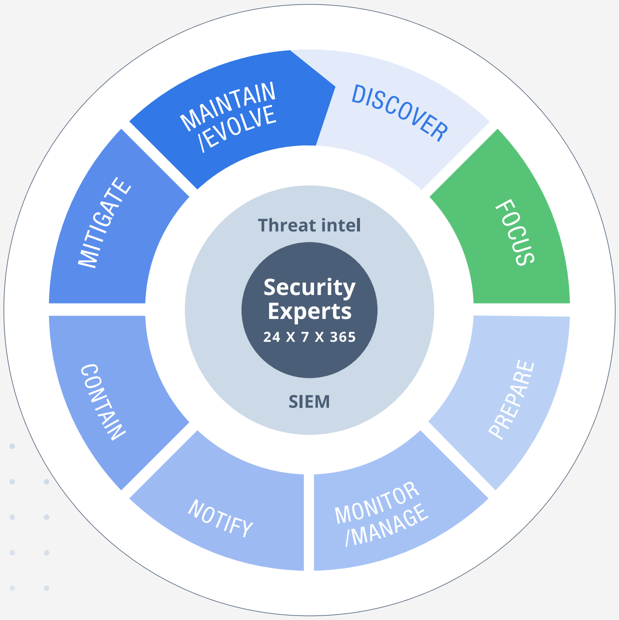
Other industry frameworks often lack two important measures, though:

- **Customization** based on your specific goals, existing technology and services and your industry needs.
- **Continuous improvement** of the security program over time to be sure it fits your needs even as you continue optimizing your security operations.

The Security in Action Framework fills in the gaps of other frameworks, because it's both interactive and customizable and built on a consultative model, so it satisfies your organization's unique requirements, even as they change over time.

Read on to learn about the eight steps of the Security in Action Framework—and the best approach to working with an MSSP to achieve better security and business outcomes.

Securit in Action Framework



The Security in Action Framework consists of eight steps to protect your organization.

Step 1: Discover

Discovery is a great opportunity to be accurate and precise in capturing relevant business objectives, risk factors and security goals and to clarify your threat landscape and implement the right controls and communications.

The process also:

- Sets the tone and expectations for your work with the MSSP.
- Helps build a security program that combines your goals and existing technology with industry and cybersecurity intelligence.
- Builds trust in data from many sources to create a safer environment with appropriate security controls.

Step 2: Focus

The MSSP will apply Discovery findings to prioritize threats and mitigation efforts based on the greatest risks, which helps pinpoint where to optimize your valuable resources.

Gain greater clarity:

- Create a roadmap prioritized by findings for technology and services.
- Receive recommendations from the MSSP's cybersecurity experts.
- View, keep tabs on and manage your roadmap (and ultimately your entire security program).

Step 3: Prepare

The MSSP will maximize threat visibility, close high-risk gaps, eliminate overlaps and/or add required security controls:

- Collaborate on architecture and solution designs.
- Create a security runbook in collaboration with the MSSP's security implementation team (SIT), security operations center (SOC) and network operations center (NOC) teams to be sure you're both on the same page in terms of prioritizing issues.
- Customize your needed services and technology priorities.

Step 4: Monitor/Manage

The MSSP will monitor and proactively manage your IT environment 24x7x365 with the aid of its SOCs and NOCs:

- Eliminate swiveling among multiple screens to get as close as you can to operating with a single point of view.
- Acquire services that align to what you have already and where you need to be.
- Keep track of your entire security program's progress including tickets, potential threats, services and technology.

Step 5: Notify

The MSSP will communicate with you based on the alerts and processes set up during onboarding:

- Reduce false positive alerts.
- Receive threat alerts and detailed information about what to do next.
- Receive instructions for further actions if they are required.

Step 6: Contain

The MSSP helps contain threats and mitigate potential damage:

- Receive assistance from the MSSP’s dedicated experts such as a its SIT, SOC and NOC resources.
- Work with its certified security incident response team (SIRT) to expedite containment.
- Minimize business disruption with automated response options.

Step 7: Mitigate

The MSSP will mitigate threats using proactive response management:

- Respond to threats 24x7x365.
- Remove threats using manual or automated methods.
- Return to steady state as quickly as possible

Step 8: Maintain/Evolve

The MSSP assesses and improves your security posture continuously:

- Make decisions based on metrics and ongoing threat modeling.
- Participate in regular security reviews.
- Adjust your security program and controls to keep up with the changing threat landscape and business/industry requirements.

Most MSSPs miss two crucial elements in their security frameworks: customization and continuous improvement.

The Security in Action Framework adds the crucial areas missing from other frameworks: customization and continuous improvement. All eight steps work together to improve both day-to-day operations and your cyber resilience, so you’ll be ready for anything. Integrated steps also make it easier to balance the human intelligence, technology and processes your organization needs.

When you evaluate MSSPs, map their approach and capabilities to the Security in Action Framework. Then you can determine if it delivers the right service that will improve your organization’s security and business outcomes.

MSSP in Action

It helps to understand exactly how an MSSP can benefit your organization through examples. The following use cases are broken out by industry.

Automotive

An automotive manufacturer needed to protect their brand, customers and data across many independently owned and operated dealerships. An MSSP was able to reach out and recognize the unique needs of each individual dealerships, focus the dealer on security gaps, and prepare them to upgrade their security infrastructure and capabilities. With the help of the MSSP, the OEM, dealership and customers have a customized solution to protect all U.S. dealerships.

Additionally, the OEM now has visibility into its dealer network landscape, enabling it to more effectively prepare for new threats, roll out new technologies, and guide its dealership technology ‘maintain and evolve’ capabilities in the future.

Manufacturing

A leading global manufacturer’s small in-house IT team struggled to provide 24x7x365 support and was constantly fighting fires to support the company’s global operations. The manufacturer’s MSSP provided 24x7x365 access to its IT security experts for network security support and assistance. The MSSP monitors, notifies, and helps contain and mitigate security events. The transition to using an MSSP has reduced costs and complexity while streamlining security configurations. The small internal team now focuses on security projects, bettering the organization and taking a proactive approach instead of firefighting.

Healthcare

A healthcare organization was experiencing difficultly balancing its cybersecurity needs with pressing business priorities. They lacked the focus needed to prepare for today's threats and were not happy with the multitude of vendors providing hardware, hardware management, endpoint technology, and SOC and SIEM services into their environment.

By using an MSSP, the healthcare company now has an experienced provider to manage its firewalls and 300 endpoints 24x7x365 with
an effective SIEM and proven SOC. The MSSP's system was up and running within three days, providing the healthcare company with a streamlined solution for security monitoring, management and response. The benefits came immediately, increasing speed to contain and mitigate threats.

> **"I really appreciate the partnership and service Nuspire is providing. It is a tremendous cost savings to the business to outsource security management to qualified individuals on your side so we can focus internal teams on important business priorities."**
>
> — SVP of IT at a healthcare organization

Franchise

Given that franchises don't own, manage or have authority over their endpoints, it's difficult to maintain their security. A particular franchise's parent organization had a small and busy IT team that didn't have the time to focus on 24x7x365 security monitoring and management across many disparate locations, technologies and groups.

Using an MSSP, the organization now has a partner to help focus each franchisee on their particular needs. The parent organization also has cross-platform visibility across all its franchise locations. The MSSP's 24x7x365 SOC analysts continuously monitor endpoints for unusual activity and block and remediate threats in real-time. Since the MSSP understands "normal" endpoint activity across the entire franchisee landscape, they can better monitor for "unusual" activity. This increases speed to identify, contain and mitigate threats.

Industry Acronyms and Their Benefits

There are so many acronyms in the cybersecurity industry that it can be hard to keep them straight. Here's a guide to the most common terms including how each service can benefit you.

Managed Security Services (MSS)

MSS are delivered by a managed security services provider (MSSP) that monitors and manages security devices and systems for organizations. Technologies include firewall, intrusion detection, security information and event management (SIEM), vulnerability scanning and endpoint protection services such as anti-virus and endpoint detection and response (EDR).

Reasons to use MSS:

- Use the latest security technologies without capital expense.
- Reduce security costs because you don't need to maintain an in-house team.
- Centralize visibility of what's being monitored to address threats faster.
- Access additional services such as threat hunting.
- Tap the expertise of security experts who can help reduce risk.
- Enable 24x7x365 protection and monitoring of the enterprise security posture.

Endpoint Detection and Response (EDR)

An EDR solution uses software such as anti-virus and antimalware to detect threats on fixed and mobile endpoints such as smartphones, tablets, laptops, desktops and servers. Alerts are sent to a security team, which investigates events and initiates action against perceived threats.

Reasons to use EDR:

- Centralize endpoint monitoring and management functions.
- Isolate compromised devices.
- Customize threat watchlists.
- Store logs to support digital forensics.
- Remediate threats using multiple techniques.
- Hunt for new "zero-day" threats.

Managed Detection and Response (MDR)

MDR is a service, provided by an MDR-specific provider or a MSSP, covers endpoints, cloud and networks on-premises and in hybrid environments. Capabilities include 24x7 threat monitoring, threat detection, threat intelligence, threat hunting, advanced analytics and human experts (housed in a security operations center (SOC).

Reasons to use MDR:

- Customize security services and runbooks.
- Implement around-the-clock monitoring.
- Validate incidents in real time to minimize false positives and alert fatigue.
- Obtain advanced analytics with the use of machine learning (ML).
- Receive expert human security expertise in incident investigations.

Extended Detection and Response (XDR)

XDR is a platform that collects the greatest number and types of telemetry from cloud, network and endpoint sources, thus extending threat visibility. Integration, automation and orchestration unify and speed activities including data collection and correlation, data enrichment via threat intelligence, analysis, detection and real-time response.

Reasons to use XDR:

- Broaden visibility across an organization's entire attack surface 24x7x365.
- Integrate multiple security products and domains into a single view.
- Manage detection and response using a single interface.
- Lower overall costs associated with detection and response.
- Increase security efficiency with automated response actions.
- Identify complex and sophisticated attacks.

Security Information and Event Management (SIEM)

A SIEM solution is software that collects, aggregates and analyzes log data from multiple sources to identify abnormal behavior and potential threats. Findings are communicated via alerts to a security team that analyzes
the data to determine if a threat exists and what to do about it.

Reasons to use SIEM:

- Simplify the security view with visual dashboards.
- Detect security events as they occur.
- Manage logs and retain data for investigative and/or compliance purposes.

Security Orchestration, Automation and Response (SOAR)

Known to be complex to build and implement, SOAR platforms allow security teams to integrate disparate security tools and create custom automated runbooks. SOAR automates data analysis, recommendations and response actions; manages workflow; and provides a single access point to threat intelligence and reports.

Reasons to use SOAR:

- Automate manual processes and repetitive tasks.
- Connect SIEMs, firewalls, threat intelligence sources and other security tools.
- Reduce alert fatigue.
- Leverage artificial intelligence (AI) and ML to improve context and threat analysis.
- Enable analysts to keep up with the increasing volume and sophistication of bad actors.

Security Operation Center as a Service (SOCaaS)

SOCaaS monitors and manages an organization's security technology such as endpoint, cloud and network. SOCaaS includes the human experts who specialize in areas such as threat intelligence, threat modeling, threat hunting, forensic and incident response.

Reasons to use SOCaaS:

- Reduce the cost and complexity of maintaining an in-house SOC.
- Lower risk by centralizing and unifying your security program.
- Bring in experts to run your security technology since resources are hard to find.
- Operate in compliance with minimal internal effort and expense.

Endnotes

[i] IBM Cost of a Data Breach Report 2021.

[ii] Cybercrime to Cost the World $10.5 Trillion Annually By 2025, Cybercrime Magazine, Nov. 13, 2020.

[iii] White House Warns Companies to Act Now on Ransomware Defenses, New York Times, June 3, 2021.

[iv] Ponemon, 2021 Cyber Resilient Organization Report.

[v] The Big Business of Cybercrime: The Dark Web, Forbes.com, Sept. 12, 2019.

[vi] Ransomware in 2022: We're all screwed, ZDNet, Dec. 22, 2021.

[vii] 4 ways to defend against the Dark Web's cybercrime ecosystem, according to MIT researchers, TechRepublic, Feb. 19, 2021.

[viii] The Cybersecurity Talent Shortage, Emsi, March 8, 2022.

[ix] (ISC)^2 2021 Cybersecurity Workforce Study

[x] Ponemon, 2021 Cyber Resilient Organization Report.

[xi] 'Alert Fatigue' Can Lead to Missed Cyber Threats and Staff Retention/Recruitment Issues: Study, Forbes.com, Nov. 8, 2021.

[xii] Hybrid Work is here to stay: What does that mean for security?, ZDNet, Aug. 30, 2021.

[xiii] Everyone is burned out. That's becoming a security nightmare, ZDNet, Dec. 8, 2021.

[xiv] Cybersecurity Report Series 2020, Cisco, CISO Benchmark Report.

Additional Resources

Here are links to helpful articles on additional security topics:

Gartner Market Guide for Managed Security Services >

Defining Zero Trust, Plus Steps to Establish a Zero Trust Framework >

On-demand webinar: The Cybersecurity Talent Shortage: Proven Strategies to Attract and Retain Diverse Talent >

On-demand webinar: Security Technology Trends from a CSO and CTO's Perspective >

8 Questions That Cut Through the Lingo of Cybersecurity Incident Response >

Security in Action Framework: The Best Approach to Working with an MSSP >

Take the next step in protecting your company by reaching out to Nuspire. We're ranked highest in client satisfaction among MSSPs with a 97% client retention rate.

Cybersecurity redefined: powered by us, customized for you.

What Makes Nuspire Different >

About Nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @Nuspire

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks