

# MSPs: Your LAST STOP of Defense Against Cyber Threats

45 NORTH NETWORKS | WatchGuard

# Table of Contents


03. MSPs: Your Last Stop of Defense Against Cyber Threats

04. Feeling Outmatched?

05. What You're Up Against: Cyber Threats by the Numbers

06. A Game Plan for Stronger Defense

07. MSPs: Your Cybersecurity MVP

08. Recruiting an MSP to Manage Your Security

09. Searching for Your Last Stop of Defense Against Cyber Threats?










# MSPs:

## Your Last Stop of Defense Against Cyber Threats

In the fast-paced world of ice hockey, a constant barrage of relentless attacks means a strong defensive strategy can make all the difference. Hockey teams often find themselves outnumbered against an aggressive attacking force, but must hold the line and stop opponents from scoring.

The same is true in the cybersecurity arena. Companies of all types and sizes are up against sophisticated threat actors and attack techniques and need a strong defense capable of overcoming the odds. And like hockey and many other sports, success in cybersecurity comes down to sound strategy and teamwork.

With a trusted managed service provider (MSP) at the core of your cybersecurity strategy, serving as the last stop of defense, your team can confidently put cyber opponents on ice.



# Feeling Outmatched?

Protecting a modern organization in today's threat landscape can feel like a losing proposition. Most IT and security teams are underdogs facing steep odds against sophisticated opponents. If any of these challenges seem familiar, you're not alone.

- Insufficient budget for necessary security solutions and staff
- A lack of time and bandwidth to dedicate to critical security tasks
- Difficulties recruiting and retaining cybersecurity professionals due to the ongoing skills gap
- Complex, hybrid workforces and IT environments
- The growing volume of advanced security threats
- The substantial cost of downtime and data breaches
- Increasingly stringent regulatory requirements
- Endlessly evolving and expanding technology options



## Did you know?

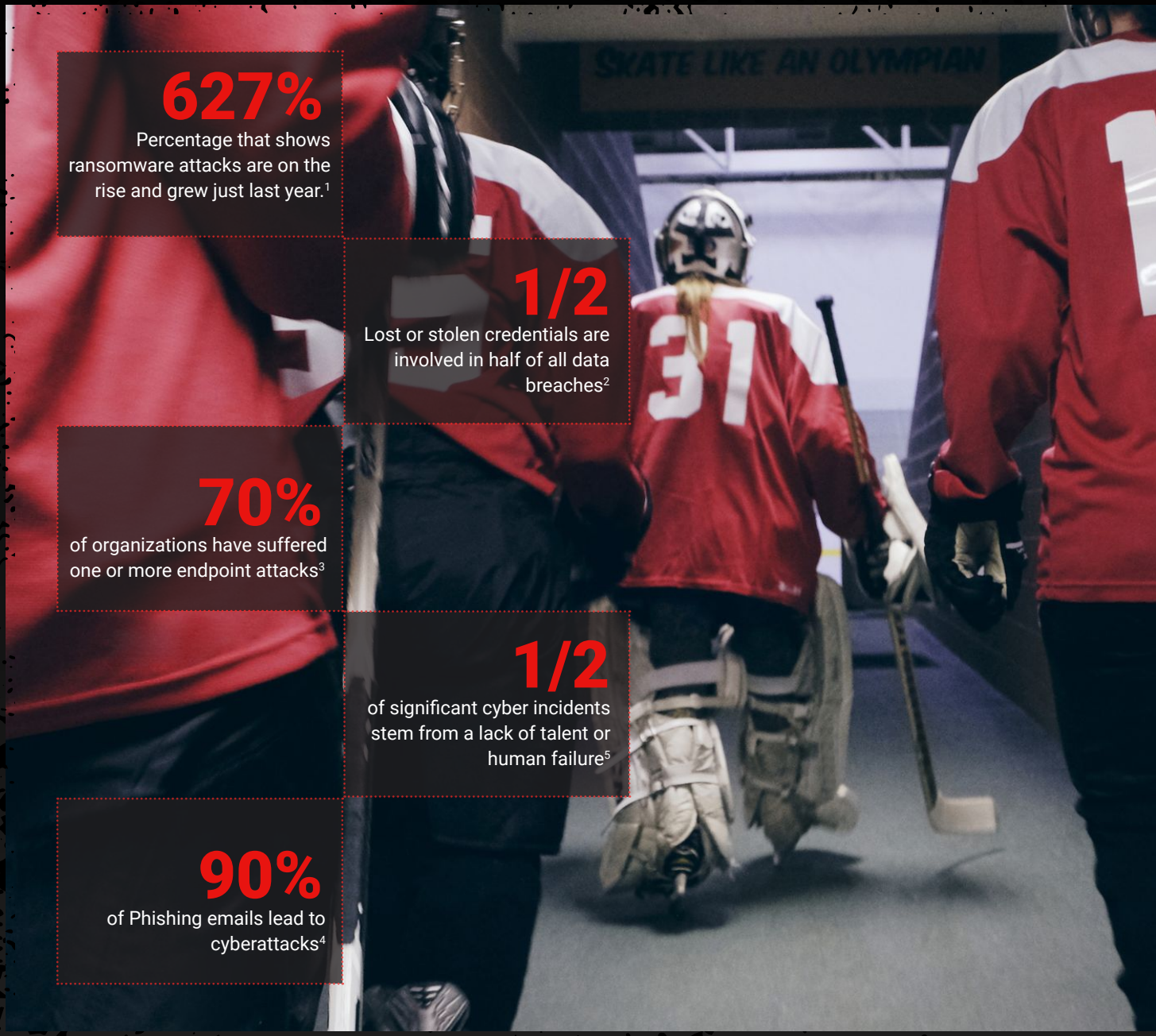
A "penalty kill" in ice hockey is when a team is outnumbered due to one or more of their players serving time in the penalty box. The "short-handed" team is at a significant disadvantage and must focus on defensive strategies to prevent goals. Cybersecurity can sometimes feel like an endless penalty kill.

# What You're Up Against: Cyber Threats by the Numbers

Every day, you're facing off against an expanding and increasingly complex threat surface. Chances are, your teams are often "short-handed" as they work to fend off overpowering cyber opponents who are becoming more sophisticated and ruthless in their attacks.

- Ransomware attacks are on the rise and grew 627% last year[1]
- Lost or stolen credentials are involved in half of all data breaches[2]
- Nearly 70% of organizations have suffered one or more endpoint attacks[3]
- Phishing emails lead to 90% of cyberattacks[4]
- Over half of significant cyber incidents stem from a lack of talent or human failure[5]

The truth is, in order to come out on top against cybercriminals, you need a strategy that covers all of your weak spots, ensures there's teamwork across your entire security stack, and allows for simplified, scalable operations.




**Source:** 1. WatchGuard | 2. Verizon | 3. Ponemon | 4.CISA | 5.Gartner

# A Game Plan for Stronger Defense

What does a winning defensive strategy look like? There are five key elements that deliver a security posture capable of overcoming today's expanding threat surface.

1. **Comprehensive Security** – tightly integrated security solutions that can safeguard your IT environments, devices, and users (network, endpoint, and identity security products and services).

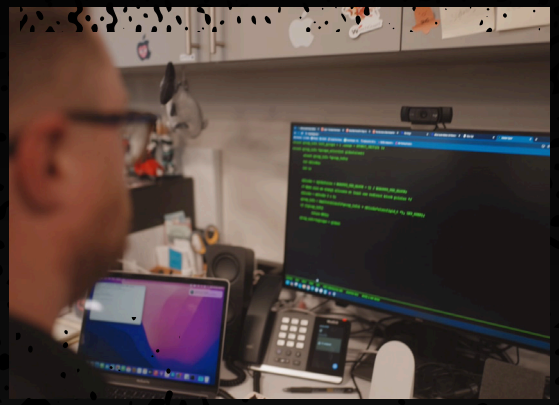
2. **Clarity and Control** – a centralized security management solution that unifies deployment, administration, management, and reporting tasks.

3. **Shared Knowledge** – the ability to share, collect, and visualize security data and alerts across domains and security solutions for correlation, prioritization, and automated or manual remediation.

4. **Operational Alignment** – a robust ecosystem of integrations, APIs, and flexible payment options to enable business requirements and scalable security operations.

5. **Automation** – sophisticated automation capabilities that improve security efficacy and streamline management tasks.

Given the scale and severity of today's threats, relying solely on in-house resources and expertise to source, deploy, and manage these critical security elements can be a losing strategy. The good news is that it's not too late in the game to consider leveraging external support to even the odds.








# MSPs:
# Your Cybersecurity MVP

Managed service providers (MSPs) offer a range of security products and services to help protect businesses from cyberattacks. As threat actors continue to score lucrative breaches, many organizations are turning to MSPs as trusted advisors with the time and expertise to change the game in a variety of ways.

- Bridging the security skills gap with a deep bench of cyber experts
- Delivering ongoing threat monitoring, detection, and remediation
- Providing a cost-effective path to stronger protection
- Unifying and simplifying disconnected security toolsets
- Freeing up time to focus on core business activities

## The stat line doesn't lie – businesses are teaming up with MSPs for stronger security.

**74%**

Percentage of global **IT spending** that goes through the channel[1]

**91%**

Percentage of global **Cybersecurity spending** that goes through the channel[2]

**93%**

of organizations **outsource** all or a portion of their **cybersecurity responsibilities to MSP/MSSPs**[3]





### Did you know?

Choosing to work with an MSP could be the key to unlocking critical security approaches that would otherwise be out of reach. For instance, many MSPs use WatchGuard's AI-enabled Zero-Trust Application Service to deliver true deny-by-default endpoint security at scale, ensuring that only safe applications and processes run on your devices.

**Source:** 1. Canalys | 2. Canalys | 3. Pulse

# Recruiting an MSP to Manage Your Security

Each MSP is different, from the vendors they use to how they transact with customers, what level of managed services they provide, and so on. Similarly, every organization has a unique set of security, business, and operational needs. Add the right MSP to your team and you can rest easy knowing you have a powerful, last stop of defense always working to protect your business.

## Did you know?

MDR (Managed Detection and Response) adoption is expanding rapidly as companies look for ways to elevate their protection while satisfying insurance and regulatory requirements? Many prefer to go with MDR from a trusted service provider to avoid the cost and complexity of building and managing an in-house security operations center.

Leverage this checklist to map out and organize your requirements and use it as a guide when vetting potential MSP partners to ensure they can deliver the level of protection you need, how you need it.

| | |
|---|---|
| **Operating Hours** | |
| | Business Hours (8x5), extended hours for services |
| | Extended Hours (12-24x5 or 12-24x7) |
| | Always On (24x7x365) |
| **Relationship to Customer** | |
| | Solutions expert for purchases, customers remain the owners/operators of security solutions |
| | Consultative security expert; shared responsibility for security services |
| | Owns and operates security solutions on customers' behalf; measured against SLA/SLO |
| **Transaction Model** | |
| | Traditional project-based invoicing |
| | Custom proposals with a mix of project-based invoices and managed security services agreements |
| | Service contracts with monthly or annual payments and hardware and/or software included |
| **Organization Type** | |
| | Large traditional organization with extensive sales and customer service personnel, and a small services product line staffed with admins |
| | Large service organization with security analysts, and less-prominent traditional organization |
| | Entirely services-based, with tiered security analysts, threat hunters, client services staff, etc. |
| **Product Packaging** | |
| | Product-based bundles with significant customer modification allowed, and some managed services option |
| | Standard packages with some add-on and customization options; willing to sell some specific point products on top of services contracts |
| | Standardized managed security packages with few add-on or customization options |
| **Service Delivery Method** | |
| | Product resell from vendor or distribution with limited managed services; delivers basic security monitoring services via admins checking alerts/logs |
| | Primarily managed services packages; offers some SOC capabilities via outsourced SOC or vendor-managed services |
| | Managed services packages exclusively; delivered via in-house SOC with a highly standardized tech stack for advanced security offerings |

# Searching for Your Last Stop of Defense Against Cyber Threats?

Today's threat actors are some of the toughest opponents out there. Facing them alone can be a daunting task. The good news is that you don't have to. It all starts with finding a trusted partner and advisor to help protect your business. Take inventory of your top security challenges and requirements, and start your search for partners that meet your needs. If you have questions or need help on your search, feel free to reach out! Teaming up with businesses like yours to protect environments, users, and devices is what we do.



**45 North Networks**

(612) 429-5665

info@45northnet.com

45 NORTH NETWORKS

*Our products proudly feature WatchGuard Technology. WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, identity security, and secure Wi-Fi.*

WatchGuard

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2024 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo and Unified Security Platform are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67786_091824