

Why partner with a Managed Service Provider?



The New Reality for Enterprise CISOs

Can your cybersecurity strategy keep up?

Increasing Cyber Risk

70% of organizations believe their cyber skills shortage creates additional cyber risk ([WEF](#))

72% of organizations report an increase in cyber risk since 2024 ([WEF](#))

Cybersecurity Talent Crisis

4.8 million Unfilled cybersecurity jobs globally in 2025 ([IPSR](#))

514,000+ Open cybersecurity roles in the U.S. as of June 2025 ([CyberSeek](#))

Rising Costs and Tighter Budgets

4.4 million Global average cost of a data breach in the U.S. in 2025 ([IBM](#))

53% of organizations believe that their cybersecurity budget is underfunded ([ISACA](#))

Business and Financial Risk

41% of organizations hit by ransomware reported a threat to their brand reputation ([IBM](#))

67% of corporate boards find their current cyber risk oversight inadequate ([Gartner](#))

Managing Cybersecurity Complexity

67% of organizations report a moderate-to-critical cybersecurity skills gap in 2025 ([WEF](#))

63% of cybersecurity professionals cite the complex threat landscape as their top stressor ([ISACA](#))

Overstretched IT Security Teams

48% of cyber professionals feel exhausted from trying to stay current on latest cybersecurity threats and emerging technologies, and **47%** said they often feel overwhelmed by the workload they’re expected to bear ([ISC2](#))

Top Reasons for Using an MSP

Many organizations don’t have the in-house expertise to keep up with today’s cybersecurity demands. Even those investing in security often lack the specialized skills needed to handle complex threats at scale.

What is your primary reason for using an MSP for cybersecurity?

- 47%** lack of in-house expertise
- 46%** access to specialized skills or expertise
- 44%** enhanced incident response capabilities
- 43%** proactive threat detection and response
- 42%** 24/7 monitoring and support
- 40%** scalability and flexibility
- 39%** accelerated deployments
- 37%** improved compliance and regulations
- 34%** cost savings



[Hughes State of Secure Network Access Report](#)

Benefits of Working with a Managed Service Provider

An MSP enables organizations to strengthen security, reduce complexity, and maximize the value of technology investments while increasing the efficiency of in-house teams.

Access to In-Depth Expertise

- ✓ Close expertise gaps with expert cybersecurity advisory, consulting, engineering, and design
- ✓ Strategic planning, roadmap, and business strategy alignment
- ✓ Security Operations Center (SOC) fully staffed to provide 24/7 support

Lower Costs and Improve ROI

- ✓ Reduce total cost of ownership (TCO) and eliminate overspending
- ✓ Consolidate vendors, tools, and operational overhead
- ✓ Achieve faster time-to-value with quicker deployments

Minimize Disruption and Downtime

- ✓ Rapid incident response and network optimization
- ✓ Manage routine updates, patches, and maintenance
- ✓ Ongoing policy adjustments and consistent security posture

Strengthen Security Posture and Reduce Risk

- ✓ Foster a security culture and enhance workforce productivity using Zero Trust principles and best practices
- ✓ Protect sensitive data by implementing strong data loss prevention practices
- ✓ Implement responsible GenAI governance

Enable Digital Transformation

- ✓ Drive innovation and ensure technology investments remain financially sound
- ✓ Support long term growth and deliver measurable outcomes aligned with business goals
- ✓ Strengthen customer trust, brand reputation, and competitive advantage

Improve IT Security Staff Efficiency

- ✓ Enable internal teams to focus on strategic business initiatives
- ✓ Reduce operational strain and workload by outsourcing day-to-day management
- ✓ Manage, integrate, and transition legacy and next-generation technologies

Gartner and Magic Quadrant are trademarks of Gartner, Inc. and/or its affiliates. Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner’s business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose.