ARCTIC WOLF

WELCOME

MANAGED SERVICES PARTNERS LLC.

it • communications • hardware • software • internet

END CYBER RISK

PROUD PARTNER OF
MEYER SHANK RACING
MSR

Arctic Wolf and Meyer Shank Racing

Bringing world-class security operations to the racetrack and beyond.

End Cyber Risk

Protect Your Business from Evolving Cyber Threats

AGENDA

01 Cybersecurity Threat Landscape

02 Reducing Risk & Impact

03 Safeguard your Organization

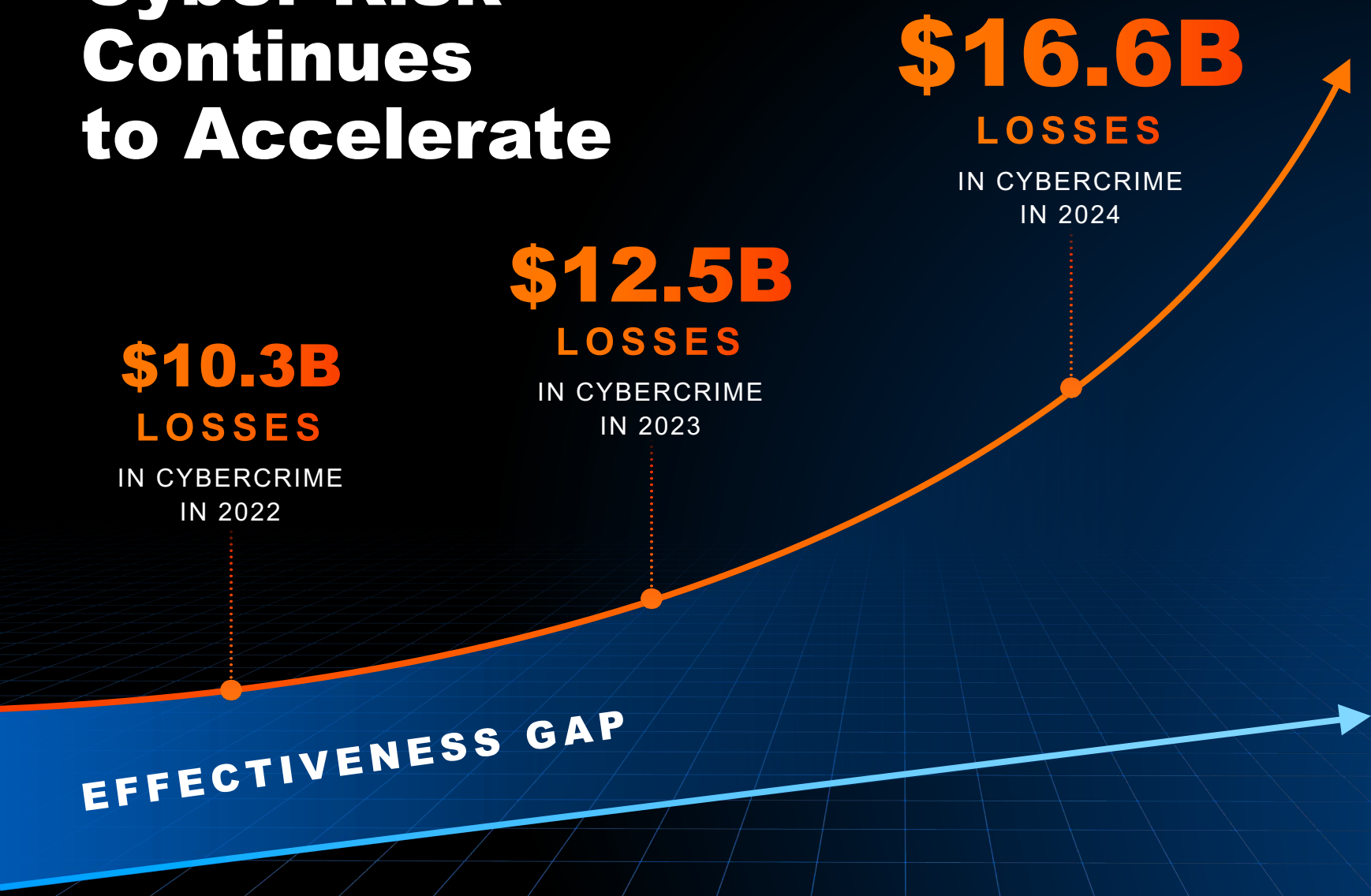
04 Cyber Insurance Benefits

05 MSP Cybersecurity Framework Overview

06 Windows 10 End of Service

07 Q&A

Cyber Risk Continues to Accelerate



2022 → 2023
+21%

2023 → 2024
+33%

TOTAL SECURITY COMPANIES IN 2024:
4,000+

TOTAL SECURITY SPEND:
183B

YOY SPEND INCREASE:
13%

Sources: IC3, Gartner, It-Harvest

Security Operations

Where companies want to be

Arctic Wolf Security Operations

GAP

Where most companies are today

Basic

Passwords / AD

Patch Management

Backups

Perimeter

Firewalls

SPAM / Web Filters

WAF / Proxy

Defense-in-Depth

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

ARCTIC WOLF

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Business Resilience

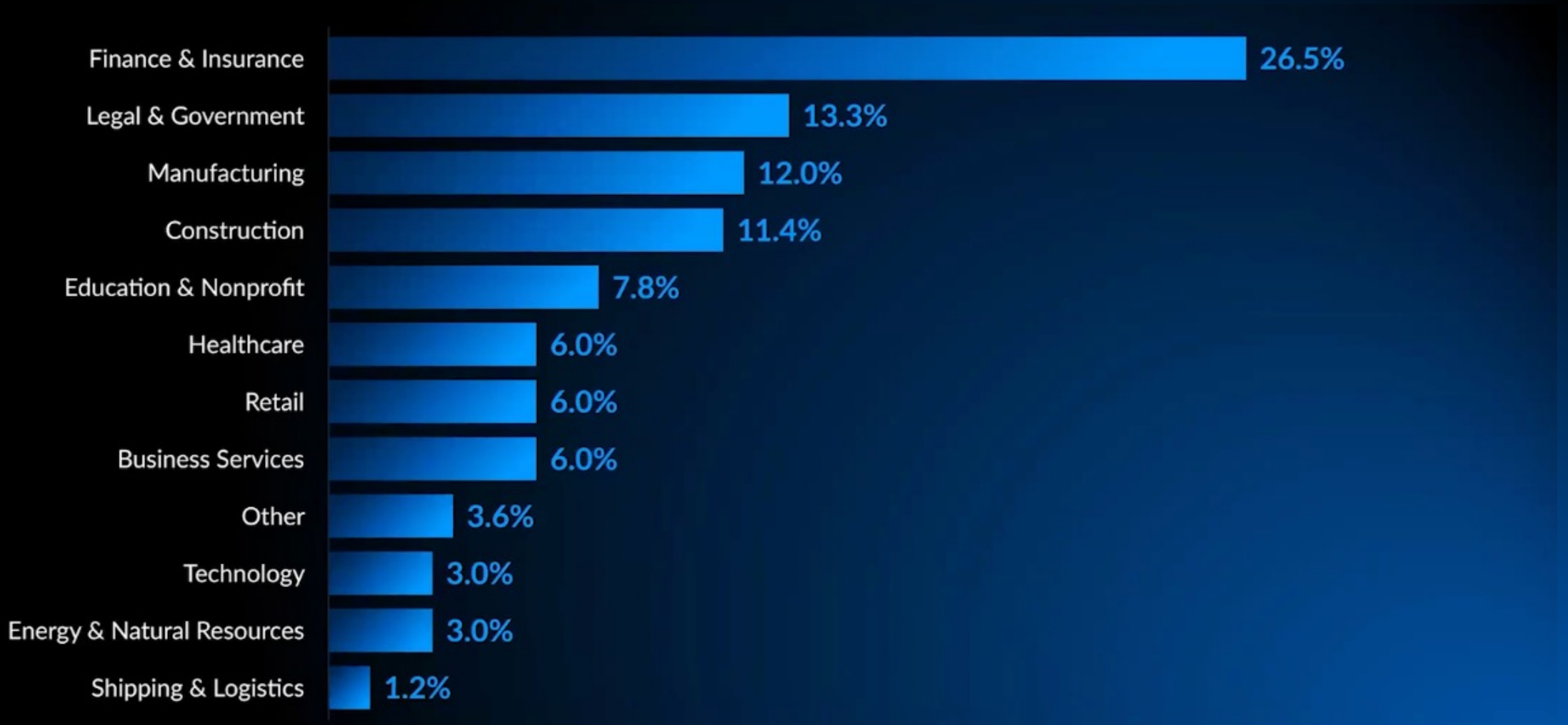
Proactive

Confident

Compliant

Insurable

BEC Incidents by Industry



Business Email Compromise

Arctic Wolf Platform | Arctic Wolf Triage Team | Adversary

12:57 pm

Attacker obtains stolen credentials from the dark web

User accepts MFA request initiated by attacker

The Arctic Wolf Platform logs MFA successful

12:57 pm

1:16 pm

Attacker adds forward and delete rules to user's inbox

Rule creations triggers investigation

1:16 pm

1:18 pm

Arctic Wolf begins investigation into activity

Attackers upload weaponized pdf to OneDrive

1:22 pm

1:25 pm

Investigation results in disabling user account and beginning of remediation

Safeguard your Organization

Develop an incident response plan to minimize the impact of an attack. Consider retaining professionals for help

Ensure you have broad visibility into your environment, assets, and attack surface; create a baseline of normal behavior

Enforce strong identify controls

Establish and continually foster a culture of security

We Are Arctic Wolf

OUR MISSION: END CYBER RISK

10,000+
Customers

1,000+
Security Engineers

8+
Trillion Events per Week

1,000+
IR Engagements per Year

100+
Countries

2,250+
Partners Globally

TRIED, TESTED, & PROVEN

IDC
2X LEADER
MDR MarketScape

Gartner Peer Insights™
MOST RECOMMENDED
MDR, Vulnerability Assessment, and Security Awareness

CNBC DISRUPTOR 50
3X WINNER
Only Cybersecurity Company Ever

bsi ISO/IEC 27001 Information Security Management CERTIFIED
AICPA SOC
CERTIFIED
Ongoing Validation

The Arctic Wolf Security Operations Cloud

MISSION:

End Cyber Risk


Cyber Resilience Assessment


Endpoint Security


Managed Detection and Response


Managed Risk


Security Journey


Managed Security Awareness


Incident Response


Concierge Delivery Model

PURPOSE BUILT

Technology

EXTRAORDINARY

Talent

INCREASED

Insurability

AI POWERED

RISK ASSESSMENT

RISK MITIGATION

RISK TRANSFER

TOTAL RISK

Partnering with Arctic Wolf

DRIVING SECURITY OPERATIONS

Addressing Risk – Assess, manage and mitigate your cyber risk while improving your cyber insurability and overall security posture

Value – Implement a true security operations approach while leveraging the best endpoint performance-to-price ratio in the market.

Open – Arctic Wolf Aurora Platform provides a true XDR product solution enabling our partners to choose the right technology to support their customers' Security Operations

Security Journey– Effectively operationalize continuous security posture improvement and demonstrate improved resilience

The Aurora Platform

Cyber Insurance Benefits

How Does Arctic Wolf Help with Insurance?

Get the best cyber insurance terms possible

The majority of IT Executives surveyed, reported insurance premium decreases **between 5% and 25%** after implementing security solutions provided by Arctic Wolf [1]

UP TO

25%

1) Premium savings based on customers who have Managed Detection and Response, Managed Risk, Managed Awareness, and the Incident Response JumpStart Retainer

   I. Survey conducted by CyberRisk Alliance
   II. 500+ respondents
   III. Profile: IT Executives; 100-5,000 employees;

How Arctic Wolf Maps to Insurance

● Solves For ◐ Augments

SECURITY CONTROL	ARCTIC WOLF
Monitoring and Response: SOC or Managed Detection and Response (MDR)	●
Endpoint or Extended Detection and Response (EDR and XDR)	●
Vulnerability Management	●
Employee Security Awareness Training	●
Privileged Account Management	●
Incident Response: Readiness Planning and Reactive Capabilities	●
Multi-Factor Authentication (MFA)	◐
Closed Remote Access Ports, Including Remote Desktop Protocol (RDP)	◐
Patch Management Programs and Practices	◐
Secure and Tested Data Backups	◐
Email and Web Filtering	◐

ARCTIC WOLF

Thank You!

END CYBER RISK

MANAGED SERVICES PARTNERS LLC.
it • communications • hardware • software • internet

Cybersecurity Framework Overview

THE MORE YOU LAYER, THE BETTER

THINK DRESSING FOR WINTER

NIST CSF 2.0: Overview

MANAGED SERVICES PARTNERS LLC.
it • communications • hardware • software • internet

Managed Services Partners recommends as a starting point

- Helps to understand, document, and maintain the plan for your business
- A voluntary framework to manage cybersecurity risk
- Designed for organizations of all sizes and sectors
- Emphasizes outcomes instead of prescriptive controls
- Structured around Functions, Categories, and Subcategories

Checklist Overview

Identify business-critical assets and data

- Collaboration between business and Managed Services Partners LLC
- Computers, servers, websites, applications, phone services, data (real time and historical), proprietary methods
- Physical offices, inventory, logistics

Checklist Overview

Develop and implement access control policies

- Referred to often as ”IDENTITY” in industry language
- Collaboration between business and Managed Services Partners LLC
- Full administrative access needs to be closely guarded and minimized
- Understand the minimum access third parties need (software vendors, HVAC or utilities vendors, contractors, etc.)

Checklist Overview

Develop and implement access control policies

- Monitor changes to administrative access in order to stop unwanted elevations (part of the Arctic Wolf solution)
- Monitor anomalies and unexpected changes to user accounts (part of the Arctic Wolf solution)
- 24x7x365 monitoring is critical
- Minimize physical access to important data and systems

Checklist Overview

Develop and implement access control policies

Common terms for tools used in this category include:

- Security as a Service
- Multi Factor Authentication (MFA or 2FA)
- Zero Trust Access (ZTA)
- Detection and Response (EDR, XDR)
- Managed Detection and Response
- Office 365 Business Premium

Checklist Overview

Train employees on security best practices

- Security awareness program via Arctic Wolf
- Program managed by Arctic Wolf and results available in reporting
- Combination of email phish simulations and supporting educational videos

Checklist Overview

MANAGED SERVICES PARTNERS LLC.
it • communications • hardware • software • internet

Regularly back up data (onsite and offsite/cloud)

- Collaboration between business and Managed Services Partners
- Onsite backup tools provide fast backups and recovery
- Cloud backups provide disaster recovery options as well as “air gapped” backups away from premise and network
- Computers, servers, email, OneDrive, and SharePoint are all “sources” that can be included

Checklist Overview

Establish a disaster recovery and continuity plan

- Collaboration between business and Managed Services Partners LLC
- How to “re-activate” critical items identified in previous sections
- Identify how staff will work if office space is not available
- Identify how customers/vendors can be notified of any critical process changes

Checklist Overview

Review and update the plan quarterly/periodically

- Identify responsible personnel to maintain and own the business' roles in cybersecurity
- "Implementing" this checklist will answer the vast majority of questions that you may receive from insurance carriers or other organizations that want to assure your attention to security
- Human engagement and awareness is an important key to remaining secure
- Review reports from security tools and adjust protection based on results

MANAGED SERVICES
PARTNERS LLC.
it • communications • hardware • software • internet

Windows 10 End of Service

OCTOBER 14, 2025

PREPARE NOW!

Windows 10 End of Service

MANAGED SERVICES PARTNERS LLC.
it • communications • hardware • software • internet

As of October 14, 2025, PCs running Windows 10 will still function, but Microsoft will no longer provide the following:

- Technical support
- Feature updates
- Security updates or fixes

While your Windows 10 PC will continue to function, it will be at greater risk for viruses and malware when Windows 10 reaches end of support. We recommend and can help you transition to a version of Windows that is still supported.

MANAGED SERVICES
PARTNERS LLC.
it • communications • hardware • software • internet

Questions?

ARCTIC WOLF

Thank You!

MANAGED SERVICES PARTNERS LLC.

it • communications • hardware • software • internet

END CYBER RISK