DATASHEET

# Arctic Wolf® Managed Risk

## Reduce Risk, Increase Resilience

Organizations everywhere struggle with the complexity of identifying and managing security risks within their environment. Often, even fundamental information like what assets exist, which systems have vulnerabilities, and which systems are misconfigured is difficult to obtain. Even when this information is available it usually overwhelms the security team because their existing tools generate too many alerts and lack context. As security teams struggle with what to do next and how to prioritize, these risks pile up and leave organizations vulnerable to threats and damaging data breaches.

> ***"By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach."***
>
> — *Jeremy D'Hoinne, Implement a Continuous Threat Exposure Management (CTEM) Program - Published 21 July 2022 - ID: G00763954*

Built on the industry's only cloud-native platform to deliver security operations as a concierge service, Arctic Wolf Managed Risk enables you to define and contextualize your attack surface coverage across your networks, endpoints, and cloud environments; provides you with the risk priorities in your environment; and advises you on your remediation actions to ensure that you benchmark against configuration best practices and continually harden your security posture.

### *Discover*

The ability to discover and gain visibility into your current attack surface.

- Attack surface coverage
- Dynamic asset discovery
- Account takeover risk detection

### *Prioritize*

Determine your cyber risk in the context of your business.

- Classification and contextualization
- Risk scoring
- Concierge-led prioritization

### *Harden*

Expertise to guide your strategy and help you harden your environment.

- Configuration benchmarking
- On-demand reporting
- Guided remediation

## Concierge Security® Team

The Concierge Security Team (CST) is your single point of contact for your Arctic Wolf Managed Risk solution. Your CST intimately learns your environment and then develops a Security Journey based on your security objectives, hardening your security posture and helping to tune your environment.

### *24x7 Monitoring*

Around-the-clock monitoring for vulnerabilities, system misconfigurations, and account takeover exposure across your endpoints, networks, and cloud environments. Deliver timely critical outcomes with the deep scan tools.

### *Unified Visibility*

Gain greater insight into your security posture and broader visibility into your attack surface by pairing the detection and response of MDR with the risk-based vulnerability management provided through Managed Risk for proactive improvements as well as faster remediation.

### *Strategic Recommendations*

Your named security operations expert becomes your trusted security advisor, working with you to make recommendations that harden your security posture over time.

### *Personalized Engagement*

Regular meetings with your named security operations expert let you review your overall security posture and find areas of improvement that are optimized for your environment.

- Scans your environment for digital risks
- Performs regular risk posture reviews
- Provides actionable remediation guidance
- Works with you to build risk management plans
- Delivers a customized risk management plan to prioritize remediation and measure progress
- Provides comprehensive visibility into your risk posture

## Arctic Wolf Managed Risk Capabilities

### *External Vulnerability Assessment*

Scans internet-facing assets to understand your company's digital footprint and quantify your business's risk exposure. Key features include:

- Scanning of external-facing assets
- Cloud Security Posture Management (CSPM)
- Account takeover risk detection
- OWASP Top 10 scanning
- Automated sub-domain detection

### *Internal Vulnerability Assessment*

Continuously scans all your internal IP-connected devices while cataloging your core infrastructure, equipment/peripherals, workstations, Internet of things (IoT) devices, and personal (e.g., tablets, cell phones) devices. Key features include:

- Continuous scanning of internal assets
- Proactive risk monitoring
- Stateless scanning and secure transfers

### *Host-Based Vulnerability Assessment*

This capability extends visibility inside devices through continuous host-based monitoring to identify and categorize assets, as well as reveal system misconfigurations, user behaviors, and vulnerabilities that put your organization at risk. Key features include:

- Endpoint agents for Windows Server/workstation, MacOS, and Linux distributions
- Proactive endpoint risk monitoring
- Audit reporting
- Security controls benchmarking

### *Quantify Your Cyber Risk Posture*

A cloud-based portal provides visibility into continuous cyber risk assessment by incorporating all meaningful cyber risk indicators from your business. It identifies the highest-priority issues and alerts you to emerging risks before they escalate into real problems. It empowers you to take meaningful, efficient action to mitigate risk using these key features:

- Comprehensive risk profiling
- Informative user interface
- Proactive notifications and alerts
- Actionable reporting
- API integrations

### *Security Risk Scoring*

For effective risk management, you need to know if your security posture improves or declines over time. Benchmarking against other organizations in similar industries helps you understand where you stand and how to improve.

### *Configuration Benchmarking*

To help you prioritize your risk mitigation, configuration benchmarking is a risk score based on criteria such as the attack vector accessibility, attack complexity, and the impact of accessed data. These benchmarks provide context so you can address the most critical misconfigurations first.

**"Having a team to assess and manage vulnerabilities while monitoring our environment really helps us reduce our threat surface. We've made considerable progress in rebuilding integrity and trust in our IT systems, but risk never goes away — and if we aren't aware of it, we can't work to mitigate it."**

*— Dr. Jason A. Thomas, Chief Operating Officer and Chief Information Officer, Jackson Parish Hospital*



JACKSON PARISH HOSPITAL

## Arctic Wolf Managed Risk Capabilities (continued)

### *Account Takeover Risk Detection*

By continuously scanning the dark and gray web for corporate credentials harvested in data breaches, account takeover detection enables you to quickly take action to secure compromised accounts. Typically, your solution partner provides details such as the source, description of the data breach involved, and the exposed emails.

### *Cloud Security Posture Management (CSPM) Add-On*

A solution that protects against misconfigurations, mismanagement, and other mistakes occurring in cloud infrastructure, CSPM includes prevention, detection, and response capabilities based on criteria such as security frameworks, IT policies, and regulatory compliance.

### *Asset Inventory*

Your attack surface constantly changes as you add more users and hosts. To build and maintain a comprehensive inventory of assets, dynamic asset identification profiles and classifies your IT assets automatically and continuously so that no new asset falls through the cracks.

### *Asset Tagging*

Managed risk allows you to gain additional asset context of your risk prioritization efforts, assisting with asset classification and asset organization efforts. You can use asset tags to pivot and review assets as well as your risks during your risk management and hardening efforts. It makes the automation of managing assets possible, makes reports more meaningful for the business, and improves risk prioritization efforts.

### *Asset Criticality*

Assigning an asset a level of criticality as an attribute for risk prioritization provides a standardized critical labeling system with a clear definition of the asset's importance. The level of asset criticality can be critical, high, medium, low, or unassigned.

### *Risk Remediation Steps*

Managed Risk allows you to export a report with remediation resources against your risk, vulnerabilities, and assets. By including the remediation steps alongside the vulnerabilities, you can efficiently — and consistently — remediate known risks.

## About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform. The Arctic Wolf Aurora Platform ingests and analyzes more than eight trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

ARCTIC WOLF



SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE