Arctic Wolf Managed Risk Solution

Continuous Risk Management Delivered by the Concierge Security Team

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 not configured properly is too hard to get. And when this information is available it usually overwhelms the security team because existing tools generate too many alerts and lack context. As they struggle with what to do next and how to prioritize, these risks pile up and leave the organization vulnerable to threats and damaging data breaches.

> "By 2022, organizations that use the risk-based vulnerability management processes will have 80% fewer breaches."
>
> **— Dale Gardner,** Forecast Analysis: Risk-Based Vulnerability Management, Worldwide | Published: 14 June 2019 ID: G00384640

Built on the industry's only cloud-native platform to deliver security operations as a concierge service—Arctic Wolf® Managed Risk enables you to continuously scan your networks, endpoints, and cloud environments to quantify digital risks. Your security operations expert from the Concierge Security® Team works directly with you to discover risks beyond simple vulnerabilities, benchmark the current state of your environment, and implement risk management processes that harden your security posture over time.

Discover

Identify and categorize risky software, assets, and accounts

- Risk visibility
- Dynamic asset discovery
- 24x7 risk monitoring

Benchmark

Quantify your digital risk exposure and identify gaps

- Security Controls Benchmarking
- Risk scoring
- Actionable reporting

Harden

Know where you're exposed and prioritize security posture improvements

- Guided remediation
- Risk management plans
- Strategic recommendations

Concierge Security Team

The Concierge Security Team (CST) is your single point of contact for your Arctic Wolf Managed Risk solution. Your CST serves as your trusted security advisors and an extension of your internal team, and:

- Customizes service to your needs
- Continuously scans your environment for digital risks
- Performs monthly 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

Comprehensive Visibility Into Your Risk Posture

See the big picture

Assess risks associated with your internal and external networks, devices, cloud environments, system configurations, and more to understand how your critical resources could be impacted.

Discover risks that others miss

With Arctic Wolf® you get continuous discovery of digital risks beyond simple vulnerabilities, which traditional tools cannot identify.

Prioritize what matters

Quantify digital risk using data enriched by the Arctic Wolf® Platform, meaningful numerical risk scores, and risk management workflows so you can filter out the noise and focus on what's important.

Arctic Wolf Managed Risk Capabilities

External Vulnerability Assessment

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

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

Quantify Your Cyber Risk Posture

A cloud-based dashboard 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

Figure 1: Actionable insights from the Managed Risk Dashboard

Internal Vulnerability Assessment

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

- Continuous scanning of internal assets
- Proactive risk monitoring
- Dynamic asset identification and classification
- 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 and 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

> "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

AUTHORIZED PARTNER | TECH HEADS