Arctic Wolf Managed Risk Solution

DATASHEET

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 misconfigured is difficult to obtain. Even when this information is available it usually overwhelms the security team because its 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 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 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 to your current attack surface

- Attack Surface Coverage
- Dynamic Asset Discovery
- Account Takeover Risk Detection

Assess

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 serves as your trusted security advisors and an extension of your internal team, customizing services to your needs.

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.

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.

- Continuously 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

Managed Risk Process

Deployment Phase

Our team will work with you to deploy the Arctic Wolf® Platform, install the Arctic Wolf® Agent, integrate critical data points, configure Cloud Security Posture Management, and build an understanding of your network through internal, external, and host-based vulnerability assessments.

Configuration Phase

We provide clear understanding and full visibility into your attack surface through the following steps:

Active Vulnerability Management Cycle

This cyclical 4-step process ensures proper coverage, provides prioritization of risks, allows for consultation, and ensures mitigation efforts succeed.

Deployment

INSTALLATION AND INTEGRATION STAGE

Install and integrate scanners; configure the Cloud Security Posture Management

Configuration Review

CORE STAGE

Concierge Kick-Off

Walk-through of the Managed Risk Process, Q&A about your environment, goal defining, expectation setting

FUNDAMENTALS STAGE

Identity and Coverage Resolution

Insight on device coverage, network coverage, and identity issues; verification of total attack surface coverage

FUNDAMENTALS STAGE

Define and Configure Asset Context

Review of initial critical asset list, identification of gaps, recommendations for asset criticalities, workflow, and organization tagging

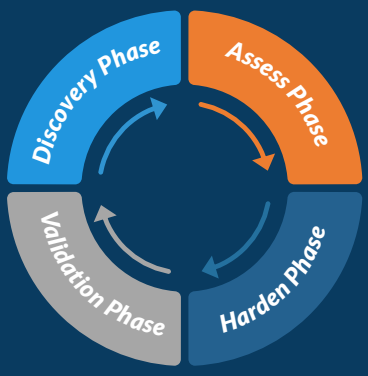
OPTIMIZED STAGE

Threat Landscape and Prioritization Review

Tailored risk prioritization according to asset and risk context on your overall attack surface; remediation recommendations

Active Vulnerability Management Cycle

Identify differences between the initial / previous vulnerability and asset baseline to understand attack surface



Set priorities for mitigation and remediation through risk metrics and prioritized risk links

Rescan risks to ensure that mitigation efforts were successful

Resolution of priority risks with CST, discussions to reduce overall risk

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

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
- 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, 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 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

> "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)

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.

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)

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.

ARCTIC WOLF