The Arctic Wolf Difference

Concierge Security Team™

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

- Conducts daily triage and forensics
- Customizes service to your needs
- Provides actionable remediation recommendations

Customized Rule Engine (CRulE)

CRulE provides unlimited flexibility to tailor our services to the specific needs of every customer. It allows the Concierge Security Team to apply your exact security and operational policies and update them as needed to align expeditiously with your changing business needs, including:

- Unlimited security policy customization
- Unlimited rules granularity or generalization
- Unlimited situational rules customization

Hybrid AI

Hybrid AI demonstrably identifies attacks, reduces false positives, and speeds up the time between detection and response. It augments a security team's expertise with the efficiency and productivity of artificial intelligence.

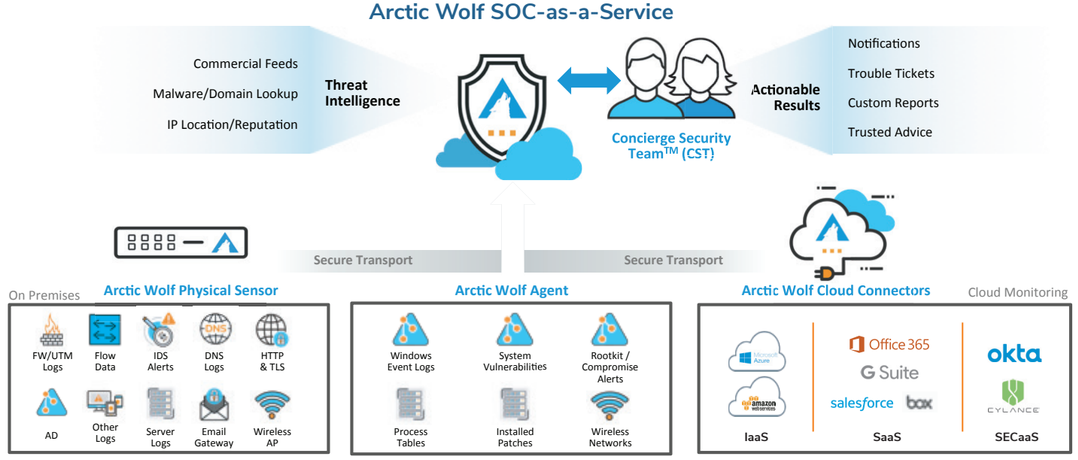
- 10X better threat detection
- Human intelligence and intuition
- Machine scale and efficiency

Security Optimized Data Architecture (SODA)

SODA unifies the ingestion, parsing, and analysis of network traffic and log data. It provides the foundation for the security analytics that give our security engineers deep pervasive visibility into your security posture.

- On-demand access to the relevant security data for incident investigation
- Instrumented for cybersecurity data science
- Immediately operational with zero setup time

Arctic Wolf SOC-as-a-Service



HAVE QUESTIONS OR WANT TO FIND OUT MORE ABOUT HOW ARCTIC WOLF WILL IMPROVE YOUR WORKFLOW AND SECURITY INFRASTRUCTURE?

(866) 777-9920

sales@IT360.biz

MANAGED SECURITY SERVICES

ARCTIC WOLF MANAGED RISK™ SERVICES

Continuous Vulnerability Scanning and Endpoint Analytics Managed by Security Experts

The Managed Risk portfolio of Arctic Wolf's risk assessment services enables you to continuously scan your networks and endpoints, and quantify risk-based vulnerabilities. Unlike alternatives that rely on automated approaches that make assessing vulnerabilities difficult, Arctic Wolf's Concierge Security Team™ provides a quantified, real-time understanding of your cyber risks so you can take prioritized action to improve your cyber risk posture. It complements Arctic Wolf Managed Detection and Response™, which provides the most comprehensive security operations center (SOC)-as-a-service in the industry.

- Continuous Risk Assessment
- Internal Vulnerability Assessment
- External Vulnerability Assessment
- Host-Based Vulnerability Assessment
- Dynamic Asset Identification
- Comprehensive Risk Profiling

Customer Portal – Management and Analytics

The Arctic Wolf Managed Risk dashboard is tailored to your organization's priorities to help you make sense of your network and endpoint vulnerabilities, and help you manage and prioritize patching to reduce cyber risk exposure.

Comprehensive Visibility into Your Risk Posture

Continuous Risk Assessment

- Continuously scans assets to avoid risky delays in security awareness

Internal Vulnerability Assessment

- Identifies exploitable vulnerabilities in systems inside the corporate network

External Vulnerability Assessment

- Discovers exploitable vulnerabilities in internet-facing systems on the corporate network

Host-Based Vulnerability Assessment

- Monitors hardware, software, and registry configurations and changes to reveal risks only detectable by on-device observations

Dynamic Asset Identification

- Profiles and classifies assets on your network to build a comprehensive inventory

Comprehensive Risk Profiling

- Aggregates and quantifies risk indicators from external and internal networks, as well as licensed endpoints.

Arctic Wolf Managed Risk™ Portfolio of Services

Arctic Wolf's Concierge Security Team™ (CST) continuously scans your external/internal networks and endpoints on which Managed Risk agents are installed, looking for vulnerabilities and securely reporting the results in the Managed Risk portal. Your CST also informs you of high-priority vulnerabilities that require immediate attention to reduce your cyber risk/exposure.

Managed Risk: External Vulnerability Assessment

External Vulnerability Assessment continuously scans internet-facing servers to understand your company's digital footprint and quantify risk/exposure to your business. Key features include:

- Continuous scanning of external-facing assets
- Proactive risk monitoring
- Webserver scans
- Automated sub-domain detection

Managed Risk: Internal Vulnerability Assessment

Internal Vulnerability Assessment continuously scans all your internal IP-connected devices, cataloging your core infrastructure, equipment/peripherals, workstations, and Internet of Things (IoT) and personal (i.e., tablets) devices. Key features include:

- Continuous scanning of internal assets
- Proactive risk monitoring
- Dynamic asset identification and classification
- Automatic updates
- Stateless scanning and secure transfers

Managed Risk: Host-Based Vulnerability Assessment

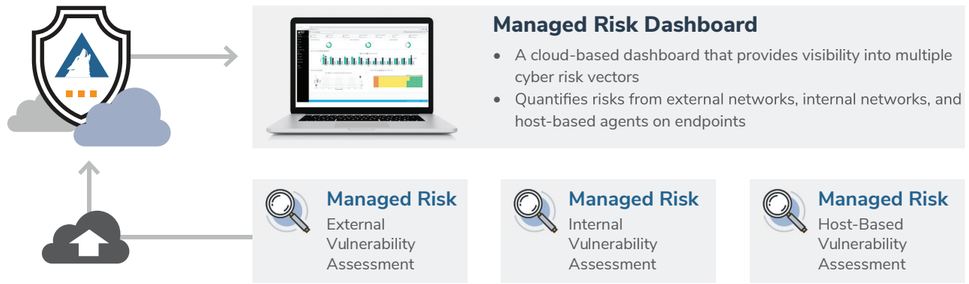
Host-Based Vulnerability Assessment extends visibility inside devices through continuous host-based monitoring to reveal threats and user behavior that put your organization at risk. This service provides actionable insight into exactly what is occurring on your devices. Key features include:

- Risk agents for Windows Server/workstation, macOS®
- Proactive risk monitoring
- Audit reporting

Managed Risk Dashboard: 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
- Advanced threat data analysis
- Actionable reporting
- API integrations



"Arctic Wolf Managed Risk has enabled Guelph Hydro to do two things: one is to quantify where we stand on risk mitigation; the other is to expose where our holes are."

– Dan Amyot, Guelph Hydro

*Windows Server is a registered trademark of Microsoft Corp; **MacOS is a registered trademark of Apple Inc.