Arctic Wolf® Managed Detection and Response

DATASHEET

Threat Detection and Response Delivered by the Concierge Security® Team

Organizations everywhere are struggling with detecting and responding to modern cyber threats efficiently. While many IT departments have deployed security tools in an attempt to address this, the lack of 24x7 monitoring, extensive security operations expertise, and a well-staffed security team means many threats go unnoticed and can linger in the environment for months. Many high-profile data breaches occur not because the security tool failed to raise an alert — they fail because the alert isn't addressed, or is overlooked.

The Arctic Wolf Concierge Security Team has found latent threats lingering in 73% of our customers' environments within the first 90 days of the engagement.

Built on the industry's first cloud-native platform to deliver security operations as a concierge service, the Arctic Wolf Managed Detection and Response (MDR) solution eliminates alert fatigue and false positives to promote a faster response with detection and response capabilities tailored to the specific needs of your organization. Your Arctic Wolf Concierge Security Team (CST) works directly with you to respond to and remediate threats, while also providing ongoing, strategic guidance to harden your security posture and prevent future threats.

Detect

See more with continuous monitoring of your security landscape, managed by our security operations experts.

- Broad visibility
- 24x7 monitoring

Respond

Engage managed investigation and rapid response to quickly contain threats.

- Managed investigations
- Incident response
- Log retention and search

Recover

Learn from incidents and implement custom rules and workflows for proactive protection.

- Guided remediation
- Root cause analysis
- Personalized engagement

Concierge Security Team

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

- 24x7 monitoring
- Alert triage and prioritization
- Custom protection rules
- Guided remediation
- Detailed reporting and audit support
- Ongoing strategic security reviews

Leverage Existing Infrastructure

The Arctic Wolf MDR solution leverages security technologies within your current environment so you can quickly detect, respond, and recover from threats without worrying about vendor lock-in, or replacing your existing systems.

Advanced Threat Detection

Machine learning with adaptive tuning detects advanced threats and provides forensic analysis for greater efficiency and scale.

Managed Containment

Rapidly respond to threats and stop their spread by preventing host devices from communicating externally, as well as with other devices on your network.

IR JumpStart Retainer

Arctic Wolf® IR JumpStart Retainer is the first proactive incident response retainer that combines incident response planning with a 1-hour SLA and no prepaid hours.

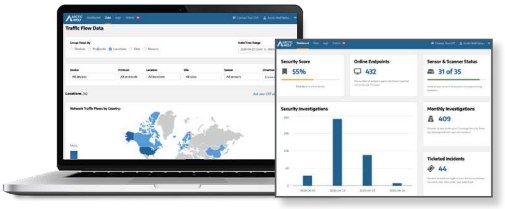
The Arctic Wolf Difference

Broad Visibility

Security telemetry collected from internal and external networks, endpoints, and cloud environments are enriched with threat feeds, OSINT data, CVE information, account takeover data, and more to provide granularity and context to incidents that are investigated and triaged by the Concierge Security Team.

Arctic Wolf Customer Portal – Tactical and Strategic Insights

A purpose-built UI provides visibility into open tickets, lets you interact with your CST, view your security score, and view deployment elements such as the number of Arctic Wolf® Agents currently deployed.



Summary and customized reports to understand your security posture and fulfill compliance needs

The Arctic Wolf Agent

The included Arctic Wolf Agent provides endpoint intelligence and enhanced threat detection and response capabilities that give our security engineers deep, pervasive visibility into your security posture.

- Sysmon event monitoring provides east/west visibility into the lateral movement of threats
- Weekly endpoint reporting
- Managed containment

Unlimited Log Retention and Search

The Arctic Wolf® Platform automatically collects, normalizes, analyzes, and retains log data from existing networks, systems, and applications for a minimum of 90 days and is available on demand to address your reporting and compliance needs.

> **"Technical limitations of previous tools we had was a big factor [in changing vendors]. We've been able to fulfill that and utilize the concierge approach where we have the interaction with people who give us guidance and how best to move forward."**
>
> *— Paul Chapman, IT Operations Manager, JCB Finance*

About Arctic Wolf®

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf Platform® delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

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

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE