Arctic Wolf Managed Detection and Response Solution

Threat Detection and Response Delivered by the Concierge Security Team

Organizations everywhere are struggling with detecting and responding to modern cyberthreats efficiently. While many IT departments have deployed security tools in an attempt to address this, the lack of 24x7 coverage, 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 only 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 perform threat hunting, incident response, and guided remediation, while also providing strategic recommendations uniquely customized for your environment.

Detect

See more with continuous monitoring and threat hunting managed by security operations experts

- Broad visibility
- 24x7 monitoring
- Threat hunting

Respond

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 solution. Your CST serves as your trusted security operations advisor and an extension of your internal team, and provides 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 provides proactive threat hunting and remote 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.

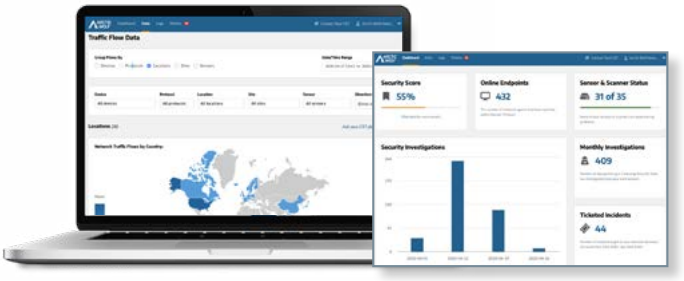
The Arctic Wolf Difference

Broad Visibility

Security telemetry collected from internal and external networks, endpoints, and cloud environments are enriched with threat feeds, OSINT data, CVE information, ATO 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 GUI 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

Endpoint Threat Detection and Response

The included Arctic Wolf Agent provides endpoint intelligence and enhanced threat detection 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

> "The value for me is that Arctic Wolf is an extension of our team. Arctic Wolf has helped enhance our security and improve our compliance reporting posture while enabling the Bay Federal team to focus on projects that add the most value to our business."
>
> **— Richard Roark,** VP and Chief Information Officer (CIO), Bay Federal Credit Union

Bay Federal CREDIT UNION

ARCTIC WOLF

Contact Name
Email Address
Phone Number
Web Address