Arctic Wolf Security Operations Cloud

DATASHEET

Cloud-Native Security Analytics Platform to Simplify Security Operations

To successfully defend against today's threats requires analyzing massive amounts of data. This means gathering telemetry from a number of IT and security products and processing it as quickly as possible. While most organizations have tools that generate this data, they lack the ability to make sense of the data or get value from it.

Our platform is built on an open XDR architecture, solving the biggest challenge organizations face in cybersecurity: collecting and storing security data across attack surfaces in real time; enriching, analyzing, and investigating this data; and using both humans and automation to respond decisively to threats and attacks. The Arctic Wolf Security Operations Cloud has scaled to ingest, parse, enrich, and analyze trillions of security events and petabytes of data each week from over one million licensed users at thousands of global customers. The Arctic Wolf Security Operations Cloud delivers critical outcomes across the whole security operations framework, is delivered as a concierge service, and protects customers to ultimately help end cyber risk.

Collect

Works with your existing technology stack to avoid vendor lock-in and reveal the big picture

- Broad visibility
- Unlimited data
- Generous retention

Enrich

Adds context to collected data to create actionable intelligence

- Threat intel
- Digital risk
- Broad perspective

Analyze

Customized rules, machine learning, and multiple detection engines reduce alert fatigue

- Cloud analytics
- Customized rules
- Alert aggregation

Broad visibility

We eliminate blind spots with complete visibility across endpoints, networks, and cloud.

Extensible

Works with your existing IT and security systems to avoid vendor lock-in, while delivering multiple solutions from a single platform.

Predictable pricing and unmetered data

Arctic Wolf retains log source data for compliance purposes, and provides you with on-demand access to platform data with no limit on event volume and no additional fees.

Core technology already included

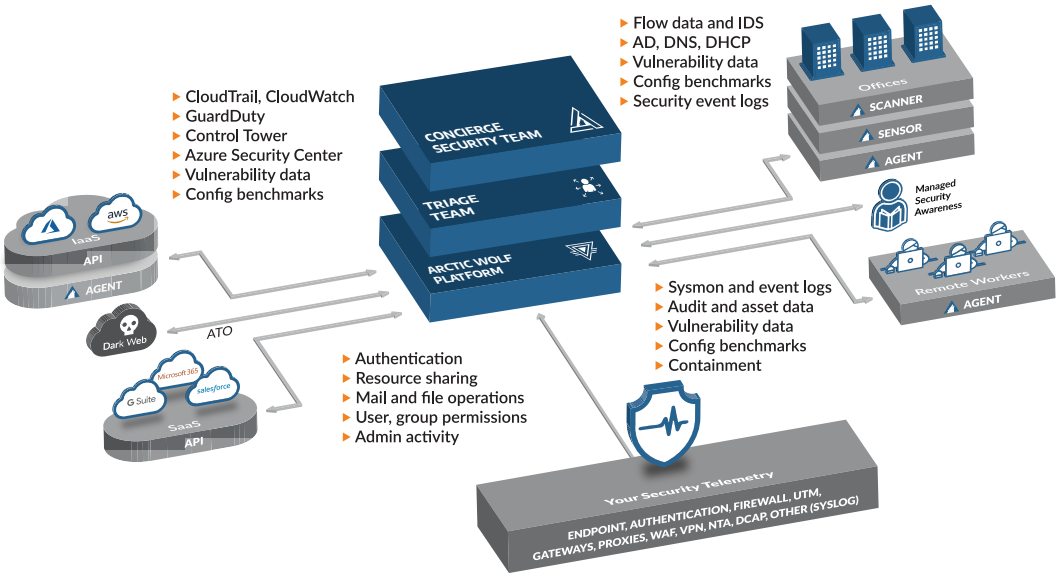
Core technologies like threat intelligence, advanced threat detection, and vulnerability management are included with Arctic Wolf.

Holistic and agnostic data sources

Enriches telemetry collected from your existing systems with data from multiple sources to add context without needing to rip and replace your existing products.

> ***"The top barrier to SOC success, according to 65 percent of respondents, is the lack of visibility into the IT security infrastructure and the top reason for SOC ineffectiveness, according to 69 percent, is lack of visibility into network traffic."***
>
> *— Ponemon Institute Research: Improving the Effectiveness of the SOC*

The Arctic Wolf Difference



> ***"We had never bought a security product we didn't learn to hate. That all changed with Arctic Wolf. We developed confidence in the service pretty quickly."***
>
> *— Steve Roach*
> *Senior VP and Chief Information Officer (CIO), Valley Strong Credit Union*

VALLEY STRONG CREDIT UNION

Concierge Security Team

Unlike SIEMs—which are challenging to implement, complex to master, and impose high maintenance and tuning costs—the Concierge Security® Team (CST) leverages the Arctic Wolf® Platform, which works with your existing security systems and includes foundational technologies to collect multiple sources of telemetry, enrich it with holistic and agnostic data sources, and analyze it with machine learning and custom rules to eliminate alert fatigue. The technical elements of the Arctic Wolf Platform include:

Arctic Wolf Sensor

The Arctic Wolf Sensor is a threat detection network appliance designed to continuously monitor your network for security threats and risks. The sensor collects data and telemetry from multiple sources, and stores it in the cloud for enrichment and analysis. Sources of telemetry include:

- FW/UTM logs
- IDS alerts
- DNS logs
- HTTP & TLS
- Active Directory
- Flow data
- Other logs
- Server logs
- Email gateway
- Wireless AP

Arctic Wolf Agent

Included with all Arctic Wolf deployments, the Arctic Wolf® Agent is lightweight software that installs on endpoints to collect actionable intelligence from your information technology (IT) environment, scans endpoints for vulnerabilities and misconfigurations, and responds to threats when required. It monitors:

- Geo-location of the asset (based on GeoIP)
- Process tables
- Installed software
- SSL certificates
- Wireless networks both available and in-use
- Network configurations
- ARP table information
- Installed patches
- Windows event logs
- System configurations
- Managed containment

Arctic Wolf Cloud Detection and Response

Arctic Wolf Cloud Detection and Response leverages API integrations with third-party data sources, commercial feeds, cloud log sources, and purpose-built cloud technologies to correlate, detect, and respond to threats against IaaS and SaaS platforms and generate meaningful security outcomes. It monitors:

- IaaS: Azure, AWS
- SaaS: Microsoft 365, Salesforce, Box, Gsuite

Managed Risk Scanner

The Managed Risk Scanner is deployed as a virtual or physical appliance that completes scans of internal and external networks and cloud environments against known CVEs and account takeover data. It regularly conducts port scans to identify open services, and attempts access with usernames/passwords to assess their vulnerability or risk level. It scans and monitors the environment for:

- Vulnerability data
- Device inventory
- Nmap data
- DNS
- Account takeover
- Publicly accessible ports/services
- OWASP Top-10
- Automated sub-domain detection