Arctic Wolf® & SentinelOne

DATASHEET

24x7 Threat Detection with Arctic Wolf and SentinelOne

The endpoint continues to be a key access point for malicious actors looking to gain access to your environment. Organizations choose industry-leading endpoint detection and response (EDR) provider SentinelOne because of its robust ability to broaden a customer's endpoint visibility and secure every endpoint. Arctic Wolf ingests telemetry generated by the SentinelOne Singularity Platform (Core, Control and Complete) for advanced investigation into potential threats and correlation with your other security tools, such as cloud, identity, network, and users. Broad visibility and centralized monitoring of your entire attack surface, including endpoint, enhances your ability to detect and respond to suspicious activity.

Together, SentinelOne and Arctic Wolf provide a holistic and efficient approach to advanced threat detection, response, and recovery. Arctic Wolf ingests, analyzes, and alerts on activities and threats such as malware, viruses, ransomware, and remote shell activity.

Integration Features

- 24x7 monitoring, triage, and alerting for SentinelOne EDR
- Expert review of suspicious activities and threats
- Centralized monitoring for all security telemetry, including endpoint
- Host-based containment

SentinelOne Notification and Alert Type Examples

- Malware
- Virus
- Ransomware
- Remote shell activity

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

Broad Visibility with Arctic Wolf Integrations

Organizations achieve the best protection when security data generated across their environment is ingested centrally and analyzed holistically. Arctic Wolf is vendor neutral, meaning that we leverage your existing tools. Your security data is ingested, enriched, and analyzed by the Arctic Wolf® Platform. Arctic Wolf monitors your environment for cyber attacks and alerts you only when incidents are confirmed. Best of all, there is no incremental cost based on the volume of data we collect.

Endpoint

Detect malware, ransomware, and active threats on endpoints

Network

Spot data exfiltration attempts and unauthorized network access

IaaS

Uncover misconfigured IaaS and unsecured data

SaaS

Monitor SaaS applications and usage of shadow IT

Authentication

Identify rogue user activity and authentication issues

Email

Detect phishing, ransomware, and impersonation attempts

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, 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.

ARCTIC WOLF

SOC2 Type II Certified

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE