Security Operations for Zscaler (ZIA)

Arctic Wolf Managed Detection and Response Delivered by the Concierge Security® Team (CST)

Organizations everywhere struggle to detect and respond to modern cyberthreats efficiently. While many IT departments deploy security tools to address this, the lack of 24x7 coverage and well-staffed security teams with security operations expertise means many threats go unnoticed and can linger in the environment for months. Many high-profile data breaches occur not because the security tool fails to raise an alert—they fail because the alert isn't addressed, or is overlooked.

Zscaler Monitoring

Arctic Wolf triages and investigates alerts generated by your ZScaler Internet Access (ZIA) deployment. Integration of ZScaler and Arctic Wolf enables security and incident response teams to leverage DNS security to improve threat detection, protection and response. This integration provides protection for DNS, firewall, and weblogs. Arctic Wolf ensures you only receive the true positives from your ZScaler Internet Access deployment, saving time, reducing alert fatigue, and ultimately preventing breaches.

Alerts for Zscaler

The data ingested from ZScaler provides your Concierge Security Team (CST) with better visibility and context into your environment for security investigations. IT and security teams don't need to monitor these alerts separately; they are triaged and escalated based on established playbooks with customers. Below is a list of ZScaler alert types that Arctic Wolf monitors to keep customers safe.

Notification and Alert Types

- DNS Security - identify and route suspicious command-and-control connections to Zscaler threat detection engines for full content inspection.
- Cloud Firewall - full DPI and access controls across all ports and protocols. App and user aware.
- Cloud Browser Isolation - eliminate exposure to risky web content and data exfiltration by separating browsing activity from the end user device.

Required Products: Zscaler ZIA with Nanolog Steaming Service (NSS)

Integration Features

- Expert review of suspicious events
- Centralized telemetry for all data
- Event correlation of Zscaler with other sources
- 24x7 monitoring, triage, and alerting
- Consistent alerting with context and remediation steps

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

"Getting clear visibility across our infrastructure was a worrisome issue until we engaged Arctic Wolf. Collaborating with Arctic Wolf's Concierge Security Team lets us maintain visibility and meet compliance obligations."

— Dr. Jason A. Thomas, COO and CIO, Jackson Parish Hospital

Arctic Wolf— Zscaler ZIA Integration

zscaler™

NSS Service

Zscaler logs are ingested via the Arctic Wolf Log Collector

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 cyberattacks 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 market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com