

# Never Trust, Always Verify: Managed Zero Trust Security Operations

DATASHEET

## Securing the Hybrid Workforce with Arctic Wolf and Zscaler

The world of hybrid work is here to stay. So, too, are the security challenges this new world has created.

As organizations adjust to this permanent shift in the way they work, they must provide access to the systems, tools, and data employees need to do their jobs without increasing cyber risk. Already taxed security teams are struggling to keep security and productivity in balance as they manage the day-to-day complexity of evolving security threats alongside the expanding attack surfaces created by the world of hybrid work.

IT and security teams are being asked to:

- Provide users safe and reliable remote access to let them do their jobs from anywhere
- Reduce security incidents without compromising collaboration or user experience
- Eliminate tech debt, tool sprawl, and time-intensive management of disparate solutions

It's a monumental task. And one that most organizations aren't equipped to tackle alone.

## Zero Trust + Industry-leading Security Operations with Arctic Wolf and Zscaler

To help organizations overcome these challenges and progress on their security journey to end cyber risk, Arctic Wolf and Zscaler work together to deliver simplified managed security operations with zero trust connectivity designed to help growing businesses get back to focusing on what matters.

Together, Arctic Wolf and Zscaler help you establish security operations with:

- **Zero trust connectivity** that provides secure remote access, streamlining the user experience and reducing security risk to ensure your business can focus on what's important
- **Cloud security architecture** to secure users working from anywhere, delivering the ultimate gains in protection and productivity
- **24x7 security operations** customized to your environment with the expertise required to stop advanced threats and improve security maturity

## 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, providing you with:

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

“As soon as we make an acquisition, it's easy to plug in an Arctic Wolf sensor [...] and connect Zscaler. It gives us comfort knowing we can focus on growing and building our core business without security risks holding us back.”

— John Seaver, Director of Information Technology, DLZ



### Integration Features

Through a seamless integration, Arctic Wolf ingests, analyzes, and alerts on components such as DNS, firewall and weblogs generated by Zscaler. This integration also allows Arctic Wolf to correlate events sent by Zscaler with other telemetry sources including endpoints, network, and users for full visibility into your security landscape.

- 24x7 monitoring, triage, and alerting
- Expert review of suspicious events
- Event correlation of Zscaler ZIA telemetry with other security tools
- Consistent alerting with context and remediation steps

### You Can't Protect What You Can't See

Organizations achieve the best protection from central ingestion and total analyzation of security data. 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. We monitor your environment for cyberattacks and alert 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 a global leader in security operations, delivering a premier cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes more than 1.9 trillion security events a week across the globe, enabling critical outcomes for security use cases and optimizing customers' disparate security solutions.

## About Zscaler

Zscaler accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

