Solution Brief

Netskope and Arctic Wolf

As the move to cloud and hybrid work models continues, organizations' security complexity increases. To address this, a collaboration between Arctic Wolf and Netskope combines cloud-delivered SSE protection with 24×7 SOC monitoring and expert investigation. This improves visibility and accelerates response without overwhelming internal security teams.

At a glance

- **Maximize security ROI** with 24×7 SOC monitoring to eliminate the cost and complexity of internal operations.
- **Strengthen cyber resilience** through continuous correlation of Netskope cloud telemetry with existing identity and network data sources.
- **Accelerate incident containment** with structured escalation workflows that ensure high-priority cloud threats receive immediate expert investigation.
- **Reduce digital risk** by gaining unified visibility across web, cloud, and hybrid environments to protect critical assets.
- **Optimize team productivity** by offloading managed parsing and detection logic, allowing internal staff to focus on strategy.

The challenge

Organizations have access to rich telemetry generated by distributed cloud environments, but struggle to put it to use. Internal teams often lack the bandwidth to continuously monitor alerts, validate configurations, or investigate complex incidents in their ever-expanding cloud and hybrid estates. This operational gap creates siloed visibility, where critical cloud events are disconnected from endpoint, network, and identity data. Without constant expert oversight, response times lag and security risks escalate. By using Netskope's robust SSE capabilities with Arctic Wolf's proactive SOC monitoring, businesses bridge this divide. This combined approach ensures seamless data correlation and structured escalation, turning raw telemetry into usable information, helping teams maintain a resilient, proactive security posture.

The solution: Integrated Security Monitoring

Together, Arctic Wolf and Netskope deliver 24×7 monitoring across secure web gateway (SWG), cloud access security broker (CASB), cloud firewall, and remote browser isolation (RBI) telemetry. By matching Netskope's cloud insights with endpoint and identity data, Arctic Wolf triages malware and configuration threats through structured workflows. Its Concierge Security Team provides investigation and guidance, maximizing visibility and resilience. This approach ensures comprehensive protection across cloud and hybrid environments without overloading internal teams.

netskope + ARCTIC WOLF

Strengthen cyber resilience

With Arctic Wolf and Netskope working together, organizations can transform fragmented cloud telemetry into a unified, resilient defense. By fusing Netskope's industry-leading Security Service Edge (SSE) with Arctic Wolf's 24×7 Security Operations Center (SOC), businesses benefit from improved monitoring and expert investigation without having to hire and train more staff.

This integration provides granular visibility across SWG, CASB, cloud firewall (CFW), and RBI. Critical events and alerts such as malware, unauthorized configuration changes, and suspicious administrative activity are automatically triaged through structured escalation workflows.

Key capabilities include:

- **Multi-source correlation:** integrates endpoint, network, identity, and cloud data for contextualized alerts and reduced false positives
- **API integration and managed parsing:** telemetry ingestion, cursor-based polling, and detection rule management to streamline operations
- **Concierge security team support:** provides actionable guidance, investigation insights, and remediation recommendations for escalated alerts.

By bridging the gap between proactive protection and continuous operations, this combined approach allows executives to maximize their SSE investment. The result is a hardened security posture, faster incident response, and resource efficiency that keeps pace with the speed of modern cloud business.

> Maximize SSE visibility and accelerate threat response with Arctic Wolf's 24x7 SOC, multi-source correlation, and expert investigative guidance without increasing internal workload.

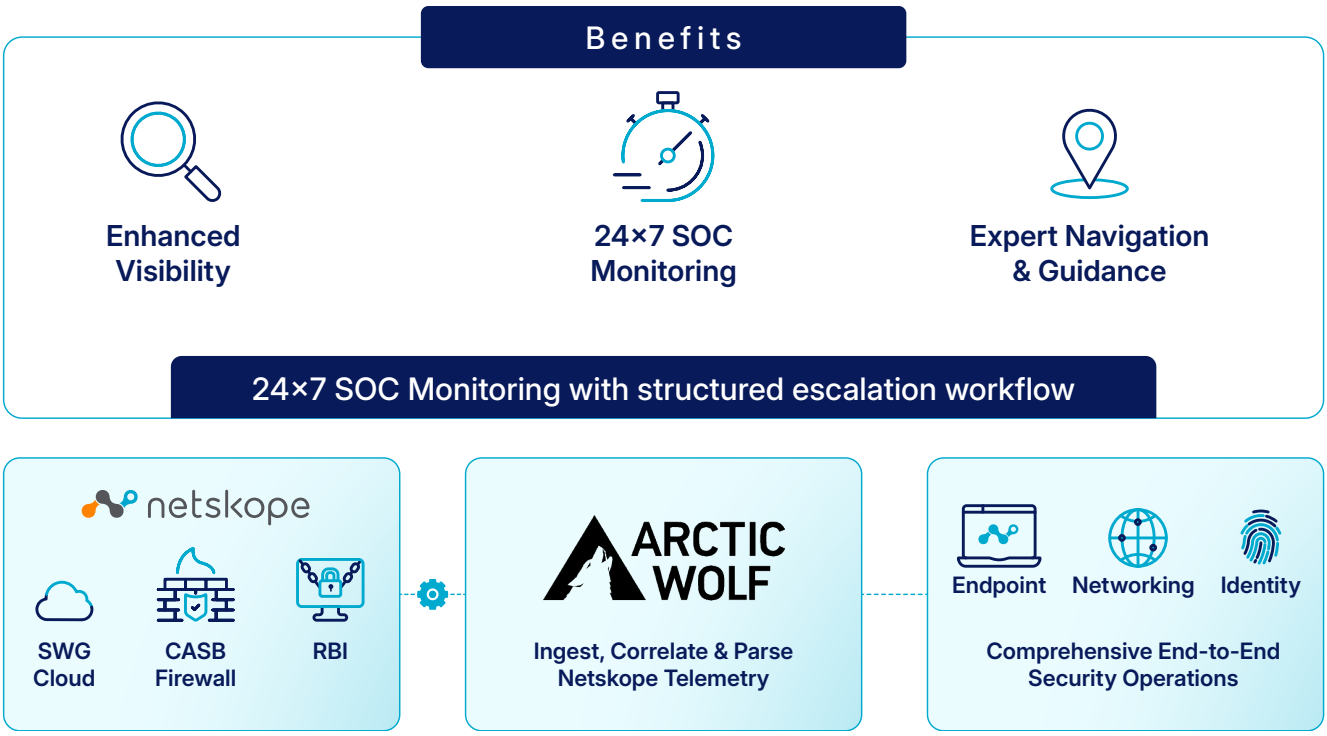
Reduce digital risk with operational and investigative support

Beyond comprehensive monitoring, this integration delivers sophisticated operational capabilities that sharpen decision-making and enhance defensive agility. By unifying Netskope's deep cloud insights with Arctic Wolf's operational abilities, organizations move from reactive alerting to proactive risk management.

Strategic Operational Pillars:

- **Contextual threat intelligence:** multi-source correlation enriches Netskope alerts with endpoint and identity data, providing the full narrative behind every cloud threat to reduce guesswork
- **Structured escalation and prioritization:** ensures high-risk events are routed to the appropriate SOC tier (L1, L2, L3) for timely and effective action
- **Guided remediation and investigation:** Arctic Wolf's Concierge Security Team acts as a force multiplier, delivering specific remediation roadmaps that reduce mean-time-to-resolution (MTTR) and harden the environment against future attacks
- **Turnkey governance:** managed API integration, parsing, and detection rules streamline telemetry ingestion while maintaining compliance and control
- **Elastic scalability:** organizations can confidently expand their digital footprint, knowing their SOC capabilities scale automatically alongside their cloud adoption

The partnership between Netskope and Arctic Wolf ensures that telemetry is never a burden, and instead is a strategic asset. By removing the complexities of data parsing and investigation, it allows security leaders to focus on high-level strategy while keeping a robust, proactive posture across all web and cloud environments.



Arctic Wolf & Netskope: Integrated Security Monitoring

Cost efficiency and operational optimization

The Arctic Wolf and Netskope partnership introduces efficiencies by transforming sophisticated security into a streamlined, predictable operational model. With the help of this partnership, organizations can achieve enterprise-grade resilience without the cost of building and maintaining a 24×7 in-house security operations center.

Organizations also remove the hidden cost of alert fatigue by integrating Netskope's SSE telemetry with Arctic Wolf's managed detection and response. Managed API ingestion, automated parsing, and expert-led triage ensure that internal teams stop chasing false positives and start focusing on high-value strategic initiatives. This combined approach optimizes existing security investments, ensuring every cloud event is actionable and contextually enriched.

Financial and Operational Impact:

- Predictable scaling: expand your cloud footprint without a proportional increase in headcount or licensing complexity
- Reduced incident impact: faster detection and Concierge-guided remediation significantly lower the risk of costly downtime, data breaches, and regulatory penalties
- Resource optimization: offload detection engineering and 24×7 monitoring to specialized experts, maximizing the productivity of your current staff

This integration bridges the gap between comprehensive protection and fiscal responsibility. By combining advanced multi-source correlation with structured escalation, organizations can confidently secure their hybrid workforce while reducing the total cost of ownership (TCO) for their entire security stack.

BENEFITS	DESCRIPTION
24×7 Continuous SOC Monitoring	Provides nonstop security monitoring of cloud and web telemetry, reducing detection gaps and risks.
Multi-source Data Correlation	Deliver secure, least-privilege access to private apps with granular policies that route traffic intelligently through cloud or local brokers. End users get a smooth, reliable experience on any device or location, while built-in Digital Experience Management (DEM) provides visibility and monitoring to simplify operations and reduce troubleshooting.
Expert Guided Remediation	Arctic Wolf's Concierge Security Team offers actionable, timely advice to speed incident resolution and reduce impact.
Automated API Integration	Streamlines telemetry ingestion, parsing, and detection workflows, lowering manual effort and errors.
Operational Efficiency Gains	Reduce internal workload and support compliance through managed security operations and governance.
Scalable Security Operations	Extend SOC capabilities as organizations grow without requiring extra staffing or resources.

About Arctic Wolf

Arctic Wolf envisions a future without cyber risk. With its comprehensive suite of security operations solutions that span the entire security operations framework, the Aurora Superintelligence Platform now ingests and analyzes the more than 10 trillion security events each week. As the backbone of the largest commercial agentic security operations centers (SOCs) in the world, the Aurora Superintelligence Platform, powered by Aurora AI, delivers game-changing noise reduction that transforms thousands of daily alerts into a single actionable ticket for most customers.

05/26 SB-994-1