Solution Brief

# Netskope and Tines

Netskope and Tines transform deep security service edge (SSE) intelligence into immediate, automated action. By unifying real-time visibility with smart orchestration, teams can proactively reduce their attack surface and enforce adaptive policies at scale. This integration eliminates the visibility-to-action gap, enabling speedy remediation and hardened security posture without operational friction.

### At a glance

- Automate response to SaaS and insider threats
- Accelerate operational resilience with smart orchestration
- Dynamically enforce adaptive zero trust policies
- Transform manual triage into automated remediation
- Strengthen security posture and compliance visibility

> By automating workflows with Tines, Netskope's own internal SOC tripled its operational efficiency and reduced response times by 25%.
>
> - Netskope

## The challenge

Modern cloud environments generate a constant, often overwhelming stream of high-fidelity signals, ranging from sensitive data exfiltration to the proliferation of shadow AI. While modern SSE platforms surface these critical insights, the subsequent response is often mired in disconnected tools and manual ticketing systems. These fragmented handoffs introduce dangerous latency and inconsistency, allowing threats to persist. As cloud adoption scales, the widening gap between signal volume and team capacity creates a primary point of failure: zero trust strategies that stall at detection. Without continuous, automated enforcement, zero trust strategies stall at detection, leaving organizations exposed to escalating threats, extended dwell times, and an expanding attack surface.

## The joint solution

Netskope and Tines transform real-time intelligence into decisive action, replacing fragmented processes with governed, automated execution. While Netskope provides deep, inline visibility into data movement and user risk, Tines orchestrates that context into structured response pathways across your entire stack. Together, we bridge the visibility-to-action gap, equipping organizations to scale remediation, harden their security posture, and enforce adaptive zero trust policies at machine speed, while reducing operational friction and ensuring every action is defensible.

netskope + tines

## Automate response and govern execution

Modern enterprise security demands more than just visibility; it requires the ability to neutralize threats the moment they emerge. Cloud and SaaS environments generate a relentless stream of telemetry, from unintentional data exfiltration to the unsanctioned use of genAI and other shadow applications. Identifying these risks is a foundational requirement, but relying on manual triage creates a "protection gap" that allows threats to escalate. Together, Netskope and Tines close this gap by transforming real-time SSE intelligence into immediate, automated remediation.

Netskope detects risky user behavior and sensitive data movement in real time, applying inline policy controls directly at the point of activity. When an anomaly occurs, Tines acts as the orchestration engine, triggering precise response workflows across your entire security ecosystem. Instead of a threat persisting while an analyst manually triages a ticket, containment, such as revoking access or isolating files, can take place at machine speed.

This automation is built on a foundation of governed execution. Organizations retain granular control over every pathway, with the ability to seamlessly integrate human-in-the-loop approvals for high-impact actions while allowing routine remediations to run autonomously. By turning deep cloud insights into structured action, Netskope and Tines help organizations shrink the attack surface, drastically reduce mean time to respond (MTTR), and ensure consistent, defensible enforcement across all applications. This approach protects critical data, eliminates operational friction, and hardens your security posture against the evolving insider threat landscape.

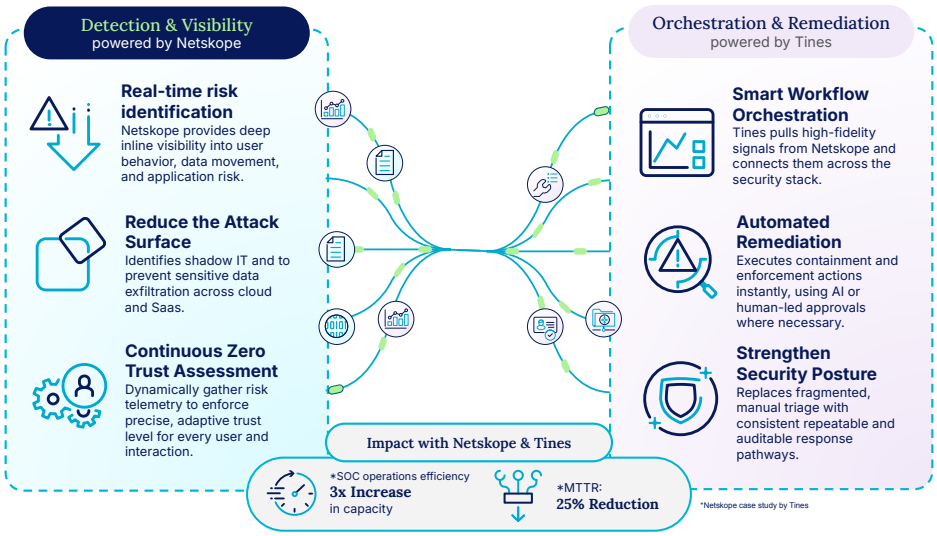
> Stop threats instantly with automated response the moment risk appears, eliminating the tickets and delays that slow containment and widen the blast radius.

## Accelerate operational resilience with smart orchestration

Security teams are overwhelmed by low-level jobs that are often repetitive and mundane. Gathering context, coordinating actions across disconnected tools, and managing ticket workflows leaves little time for high-value investigation. The more cloud services an organization adopts, the higher the volume of security signals. But this increase is rarely matched by team capacity. Ignoring this operational drag accelerates analyst burnout and weakens overall security posture, exhausted employees leave, taking their knowledge and experience with them.

Netskope and Tines help regain control. Netskope continuously surfaces high-fidelity, context-rich signals across users, data, and applications, cutting out the background noise that often hampers security operations. Tines removes operational friction by automating repetitive response steps, creating standardized guardrails and workflows across your tools and teams.
Removing manual execution and ticket-chasing from analysts' to-do lists frees analysts to focus on decision-making and strategic improvements. Automated workflows handle the coordination, updating URL lists, creating Jira issues for large downloads, and routing alerts to Slack for visibility. This streamlined approach ensures your security operations scale sustainably without increasing team fatigue. The result? Lower operational costs, improved job satisfaction, and a more resilient organization that responds to threats with speed and accuracy, regardless of cloud footprint growth.

> Reduce time to contain risk by turning real-time cloud intelligence into governed, automated action.




Netskope identifies risks and enforces adaptive zero trust policies in real time to shrink the attack surface. Tines orchestrates those signals to transform manual triage into automated remediation workflows

## Enforce adaptive zero trust policies dynamically

Many organizations define zero trust as a strategic goal, but struggle to truly achieve it. Without continuous, automated enforcement, trust decisions are applied inconsistently, and often too late. The principle of least privilege access begins to erode over time, leaving the organization exposed to insider risks, SaaS misuse, and data leakage.

To make zero trust an effective reality, it is necessary to enforce policy continuously — not just when something goes wrong. Netskope helps by evaluating trust dynamically, using real-time context around user behavior, data sensitivity, and application risk. In turn, Tines puts these crucial trust decisions into practice by automating enforcement actions across the entire security ecosystem.

This powerful integration ensures security policies are applied uniformly, delivering predictable, repeatable outcomes across all identities and endpoints. Outcomes no longer depend on who is on shift, or which tool generated an alert.

By applying adaptive zero trust enforcement, we empower you to:

- Automatically restrict access or isolate risky users the moment anomalous behavior is detected
- Transform zero trust from an abstract strategy into a robust operating reality

## Automate shadow IT and application governance

Widespread adoption of unmanaged applications introduces significant new risks. The rapid proliferation of generative AI tools, as well as other forms of shadow IT, creates vulnerabilities that are difficult to track and control by hand.

Netskope and Tines automate shadow IT governance, systematically eliminating these blind spots. Netskope provides unrivaled visibility into application usage across your environment, easily identifying third-party or AI applications that have been marked for removal in Netskope SaaS Security Posture Management (SSPM). Tines takes this intelligence and executes the necessary remediation steps.

Through intelligent workflows, Tines can automatically disable access, remove unapproved applications, or directly notify application owners via Slack, all without requiring manual intervention from your security team. We ensure that governance policies are enforced consistently, maintaining compliance and drastically reducing your attack surface. In automating application governance, you eliminate the delays associated with manual audits and ticket creation, ensuring that your environment remains secure, compliant, and optimized for business performance.

| BENEFITS | DESCRIPTION |
|---|---|
| **Accelerate threat response** | Reduce time to contain risk by turning intelligence into governed, automated action. Netskope identifies risky behavior, and Tines instantly executes a structured response. |
| **Scale security operations efficiently** | Handle growing cloud and SaaS risk without adding complexity. We automate repetitive tasks and standardize response, freeing analysts for high-value decision-making. |
| **Deliver consistent zero trust** | Apply security policy uniformly across cloud, data, and identity. Policy decisions translate into predictable outcomes every time, with repeatable response actions. |
| **Automate shadow IT governance** | Identify and remove unmanaged applications and update URL blocklists in real time to reduce your attack surface and minimize data exposure. |
| **Ensure defensible security outcomes** | Replace ad hoc decisions with predictable execution. Every automated action is documented, explained, and aligned to business policy, improving compliance and executive assurance. |
| **Prevent insider data loss** | Automate data loss prevention (DLP) and threat investigations. Dynamically enforce policies based on risky user behavior to close the gap between detection and remediation. |

## About Tines

Tines is the intelligent workflow platform trusted by the world's most advanced organizations to power their most important workflows. With Tines, they've built a secure, flexible foundation to operationalize AI agents and intelligent workflows, unlocking productivity, moving faster, and future-proofing how work gets done.



06/26 SB-995-1