netskope + aws

eBook +

6 Zero Trust Use Cases for Netskope One, and AWS

6 Zero Trust Use Cases for Netskope One, and AWS

Introduction

Many networking and security teams today are tasked with supporting a hybrid work environment using collections of mostly legacy defenses. They are in an unenviable position, because when resources migrate to the cloud and employees to remote-work environments — as has happened at rapid scale since 2020, the onset of the COVID-19 pandemic — on-premises perimeter security and hardware-centric network segmentation are no longer effective.

As a set of principles, zero trust is a better approach for securing the assets of a modern organization. In the zero trust security model, users and devices must be authenticated for each new session, and they are granted access to only the resources they need. This least-privilege approach is supported by comprehensive security monitoring, through which user and asset activities, behaviors, and trends are *continuously* watched and analyzed.

Essential Elements of a Zero Trust Strategy

Zero trust security is not a product companies can buy. It is an essential business strategy aligned with controls tailored for today's workplace. Several technologies working interoperably support a zero trust security model, including:

- ***User and identity management:*** Identity and access management (IAM) or privilege access management, role-based access controls, and user and entity behavior analytics (UEBA)
- ***Device management:*** Device health checks and confidence ratings
- ***Application and workload management:*** Secure web gateways (SWGs) and security service edge (SSE) solutions with cloud access security broker (CASB) functionality
- ***Network security devices:*** Next-generation firewalls (NGFWs), secure email gateways, and SSE solutions with SWG, CASB, and zero trust network access (ZTNA) functionality

Figure 1: Zero trust security model

Where To Start — or Go Next — with Zero Trust

An effective zero trust security model delivers a great user experience, making security transparent and creating little to no friction across the company's workloads. That means companies need to consider people and processes first. An organization moving to zero trust should start by mapping out its business use cases and processes.

Once their attention turns to technology, many companies focus on securing remote workers' access to resources, in the cloud and in the data center. The legacy approach of placing hardware security devices in employees' homes is expensive and difficult to scale, while backhauling remote employees' traffic to corporate firewalls creates bottlenecks. The easier solution is to install a software client on employee devices that connects to cloud-edge security services — in other words, an SSE cloud security platform that integrates CASB, SWG, and ZTNA.

Another popular starting point for the zero trust technology journey is prioritizing and securing business application traffic. Software-as-a-Service (SaaS)-based applications, such as Slack and Salesforce, need direct-to-internet connections for remote workers and all offices. Introducing an SSE solution enables inspection of web, SaaS, and Infrastructure-as-a-Service (IaaS) user traffic across every user, device, and location, providing visibility and control across the business's entire digital ecosystem.

An effective zero trust security model delivers a great user experience. That means an organization moving to zero trust should start by mapping out its business use cases and processes.

How Netskope and AWS Support Your Zero Trust Journey

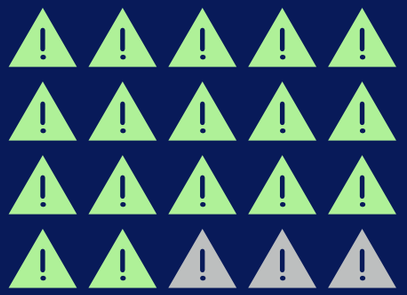
In today's evolving security landscape, traditional perimeter security with binary allow-or-block policy controls for ports, protocols, domains, URLs, and applications is no longer sufficient. Netskope, in partnership with AWS, provides a more advanced approach to securing modern cloud environments through the adoption of Zero Trust principles..

At the core of the Netskope platform is the Intelligent SSE powered by the Zero Trust Engine, which assesses transactional risks for each session, ensuring no network, device, or user is implicitly trusted. By integrating seamlessly with AWS Verified Access and other AWS security services, Netskope helps organizations secure access to cloud workloads with precision and confidence.

Netskope Intelligent SSE also supports application risk profiles, user risk profiles, and device security-posture checks, exchanging these risk profiles with third-party security solutions, including AWS-native services. For instance, AWS Verified Access can enhance identity services and multi-factor authentication (MFA) controls, allowing Netskope's Zero Trust Engine to request step-up authentication based on session risk, further strengthening Zero Trust access.

Netskope and AWS together enable businesses to securely scale their cloud environments while adhering to Zero Trust principles. Below are six key use cases that demonstrate the strength of this partnership in supporting Zero Trust security for cloud workloads.

Together, Netskope and AWS provide adaptive, context-driven access controls that dynamically respond to the risk profiles of users and devices. For example, if a user's session on an AWS-hosted application shows increased risk, Netskope's granular activity controls can limit what the user is allowed to do within the application, rather than completely blocking access.



85%

Risk reduction from use of security service edge, while increasing business agility.

Source: Enterprise Strategy Group

Zero Trust Use Case 1

Increasing SaaS Visibility

Netskope research has found that employees of the average midsize company use more than 800 applications, while employees of larger enterprises may use 2,400 or more. Many of these are cloud-based SaaS applications, and 97% are adopted by business units or individual users without the oversight of the IT team.

The idea of employees moving corporate data into unmanaged SaaS applications is unnerving. That is why Netskope Intelligent SSE comes with CASB inline inspection for thousands of applications. Just as firewalls inspect packets across ports and protocols, SSE solutions with CASB capabilities decode applications inline to understand the context and content of each transaction. This enables access control policies to be adaptive and to be based on zero trust principles.

Netskope Intelligent SSE also references risk profiles for more than 80,000 applications via the Cloud Confidence Index in developing a cloud app risk rating for all the applications in use within the organization.

These capabilities dramatically improve a security team's ability to understand employees' usage of cloud apps — whether company-sponsored or personal, and whether managed or unmanaged. The security group can better understand employees' risky behaviors in the cloud and can limit the exposure of company assets to high-risk SaaS solutions.

97% of applications in use within enterprises are not managed by IT, but are adopted independently by business units or end-users.

800 apps used by average midsize company

to 2,400+ apps used by larger enterprises

Zero Trust Use Case 2

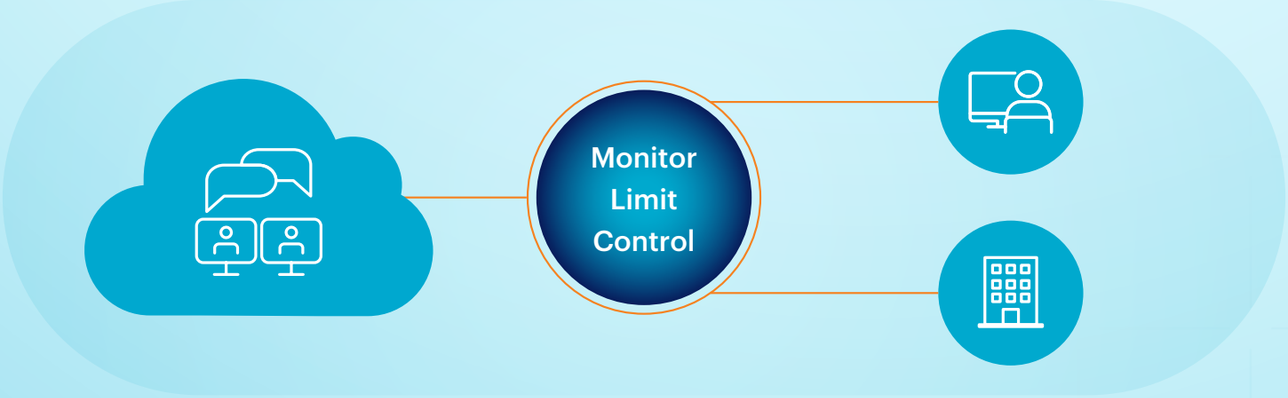
Protecting Cloud Collaboration

In companies that rely heavily on remote work, cloud collaboration platforms are business-critical. Employees use them to share information, to meet with customers and vendors, and to accomplish everything that used to take place in conference rooms or around the water cooler.

Cloud collaboration solutions pose a unique level of security risk because they are used so often, for such a wide range of business activities, but are typically unmanaged by corporate IT. Security staff need the ability to control how employees are using these solutions and the information shared within them.

The adaptive access controls within Netskope Intelligent SSE are an excellent solution to this challenge. The Netskope platform includes activity controls for common cloud collaboration solutions. Slack, for example, has 15 activity controls described within Netskope Intelligent SSE, and Zoom has 10. That means security teams can use Netskope Intelligent SSE to restrict users' behaviors around any of those activities without cutting off the users' access to Slack or Zoom. So, users may be allowed to create and attend Zoom meetings as often as they like, but image and data sharing are limited, restricted, or otherwise controlled.

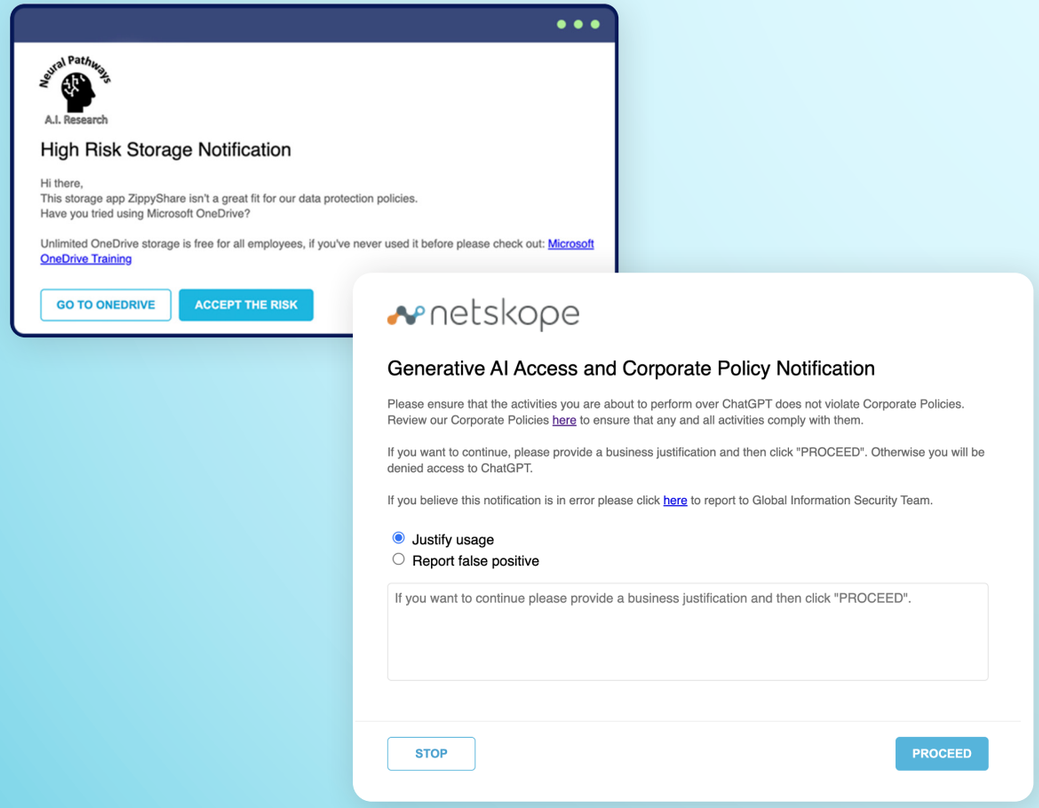
Security teams historically have been seen as the purveyors of "no." The ability to control individuals' actions within an unmanaged application, which Netskope Intelligent SSE makes possible, helps security to become, instead, the function of "How can we make these capabilities available — safely?"



Zero Trust Use Case 3

Active User Coaching

When users attempt to take a risky action, Netskope Intelligent SSE can either block that activity outright or provide advice. For example, if a user attempts to open a risky application or transfer sensitive data to a personal instance of a company-approved application, Netskope Intelligent SSE can coach them in real time to select a safer option. For example:



Alternatively, Netskope Intelligent SSE can ask the user to justify the higher-risk choice. Or it can be set to simply alert users to any risky transaction they attempt and give them the option to cancel the decision. When advised that their intended data activity is risky, more than 95% of users will cancel the transaction. For the remaining 5%, the security team can collect their justifications and use those to refine security policies for the corresponding use cases, if appropriate.

Leveraging rich context and content alongside a transactional risk assessment, Netskope Intelligent SSE supports users in making the right decisions. It educates them rather than impeding their ability to access applications they need. This gentler approach helps create good digital citizens who work hard to uphold corporate security policies.

> *"Humans are not the weakest link in our security posture, they are our last line of defense, so it's important that we recognize that and train them."*
>
> *— Dane Blackmore, Netskope*

Zero Trust Use Case 4

Secure Access to Internal Apps Hosted on AWS

Although corporate data is increasingly moving to SaaS applications, many organizations continue to operate internally developed apps hosted on AWS. These internal applications also benefit from a Zero Trust security approach, ensuring users access them through the company's ZTNA (Zero Trust Network Access) solution. By leveraging Netskope and AWS, organizations can ensure that users access only the specific internal resources they need, without unnecessary lateral movement through the network. This approach secures internal AWS-hosted applications, reducing the risk of unauthorized access and improving overall cloud security.

Another benefit of taking a ZTNA approach with application development is that it can bring security teams into development and operations (DevOps) processes. Too often, software development teams ignore security until far too late, then expect the security group to bolt on controls after a solution is designed. Instead, security teams should be involved in DevOps from start to finish.

The zero trust security model can make that happen. By making security a business enabler, the zero trust approach encourages development teams to involve security staff earlier in their pipeline, deploying security checks during development.
In some cases, this closer cooperation between teams leads to an integrated DevSecOps group.

Such a partnership among corporate functions sets up the entire organization for success. It can reduce vulnerabilities in internally developed software, eliminate software supply-chain issues, and minimize security weaknesses in web applications.

Zero Trust Use Case 5

Unapproved Data Movement

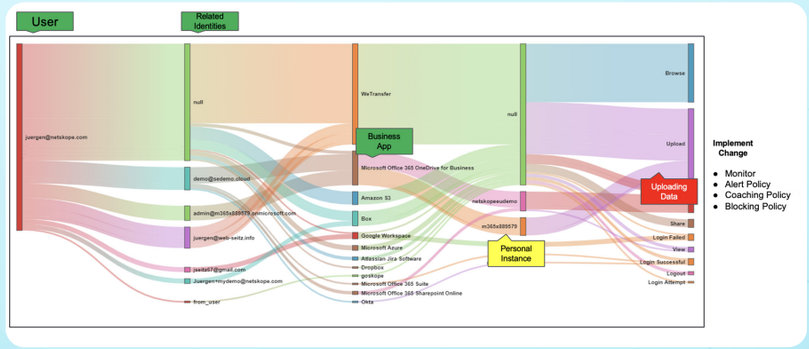
Data security has always been fundamental to corporate risk management. Today, however, the corporate network perimeter cannot prevent data from transferring offsite, so traditional approaches to data security fall flat.

By contrast, Netskope Intelligent SSE helps security professionals understand how their organization collects, transmits, stores, and shares data across SaaS, IaaS, and internally developed applications. They can answer questions such as: Where is our data flowing, and within which apps? What are the risk profiles of users attempting to move data? What devices are they using, and on what networks? When an employee departs, the security team can assess that individual's data movement and application usage over the prior few months. And when SaaS applications are updated, security can see whether those changes resulted in any new data paths or transactions.

Netskope Intelligent SSE provides instance awareness for more than 450 applications, allowing the security team to distinguish whether data resides in a corporate instance or a personal instance of the same application. This capability is critical for preventing unauthorized data movement, particularly when it comes to sensitive information stored in corporate AWS S3 buckets.

For example, without proper controls, a user might attempt to move sensitive data, such as intellectual property, financial records, or customer information, from the company's AWS S3 bucket to their personal AWS account. Such an action can expose the company to significant risks, including data breaches, loss of proprietary information, or violations of data privacy regulations. Legacy security controls might miss this nuance, but Netskope Intelligent SSE recognizes the difference between corporate and personal instances in real time.

By leveraging this instance awareness, Netskope Intelligent SSE can prevent unauthorized data exfiltration before it happens. The platform can either block the transfer outright or use real-time coaching to alert the user of potential risks, reducing the likelihood of accidental or malicious data movement. This level of visibility and control over sensitive data is vital for protecting against data loss and maintaining compliance with regulatory standards.



Netskope Advanced Analytics providing visibility of unknown data exfiltration to personal storage

Zero Trust Use Case 6

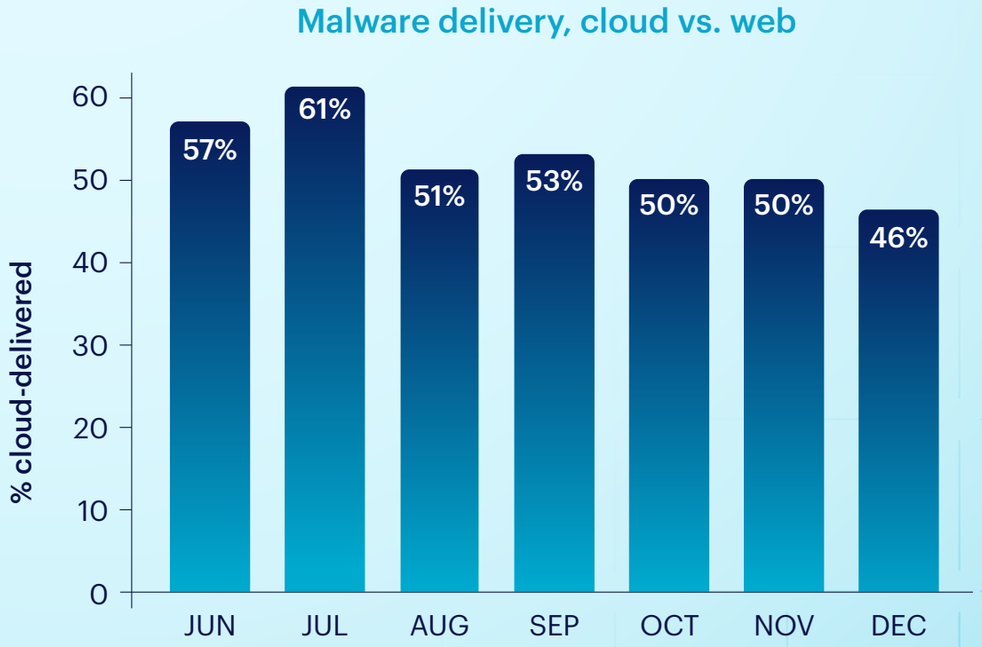
Cloud Misconfigurations

The vast majority of cloud security failures result from configuration mistakes. Properly implementing Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) solutions is essential for ensuring that employees use cloud services safely and securely. These systems help organizations understand the security posture of workloads deployed in public IaaS clouds like AWS or SaaS applications. They assess configurations, compliance, and overall security posture, then compare the findings against best practices and standards from experts like the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA).

Netskope Intelligent SSE, integrated with AWS Security Hub, provides real-time insights and continuous auditing of security configurations for AWS services and popular SaaS applications, such as Salesforce and other business-critical tools. The platform uses APIs to investigate configurations without causing production downtime or requiring lengthy integration processes. Netskope offers hundreds of out-of-the-box rules that continuously monitor security settings across AWS, ensuring that any misconfigurations are detected before they can lead to security incidents.

For example, if a misconfiguration is found in a corporate AWS S3 bucket that could expose sensitive data, Netskope Intelligent SSE flags the issue and provides remediation steps, allowing teams to fix the problem swiftly. This continuous auditing reduces the likelihood of a cloud misconfiguration turning into a security crisis and enhances overall cloud security posture.

46% **of malware downloads originate from popular cloud apps.***



Source: Netskope Cloud and Threat Report 2024.

Behind the Scenes Power: Netskope Zero Trust Engine

As noted in our introduction, all of these capabilities are made possible by the Netskope Zero Trust Engine at the heart of Netskope Intelligent SSE. The Zero Trust Engine is the technology that assesses the myriad variables at the time of a business transaction, provides real-time coaching to users, collects justifications, and logs events with rich details for continuous monitoring. Figure 2 describes how the Zero Trust Engine supports the six key use cases we've described.

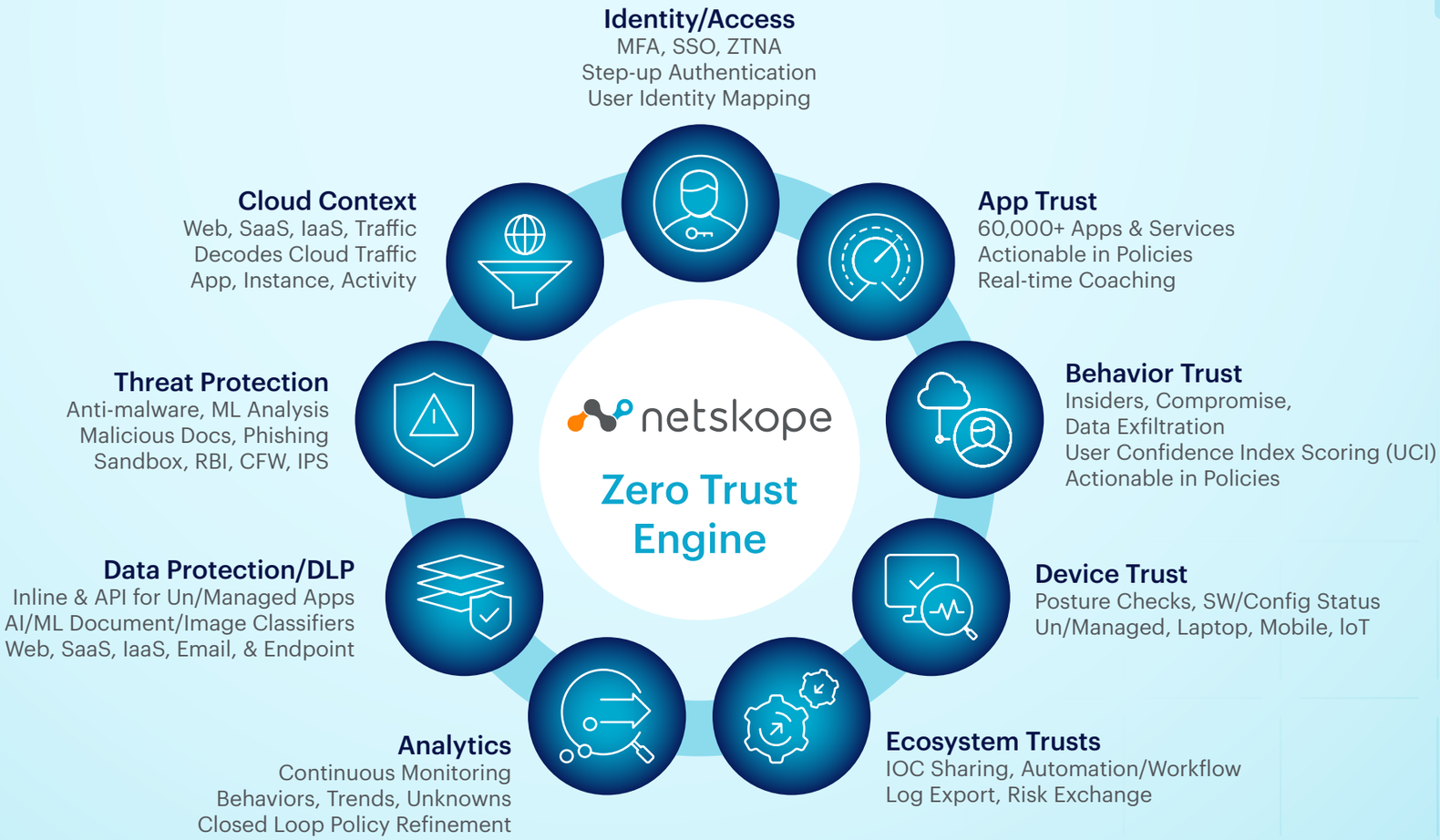


Figure 2: Netskope Zero Trust Engine provides risk-based context in support of zero trust policies

The Netskope Zero Trust Engine's tight integration of all the critical zero trust technologies makes it a powerful force in driving deployment of a zero trust security model companywide. Surveys of hundreds of Netskope customers have revealed three key outcomes from adopting an SSE solution:

85% Reduction in security risk through critical asset protection, stability, resiliency, and making users better digital citizens

51% Reduction in total cost of operations by retiring appliances, freeing up staff time, reducing dedicated network links, and optimizing cloud spend

19% Improvement in business agility because adopting zero trust principles moves defenses closer to users, accelerating speed to market and data-driven decisions

To learn more, visit 2024 Magic Quadrant for Security Service Edge.

Together with Netskope and AWS, we can help you start or enhance your zero trust journey.

Netskope, a leader in Secure Access Service Edge (SASE), is redefining cloud, data, and network security by enabling organizations to apply Zero Trust principles across their environments. The Netskope Intelligent Security Service Edge (SSE) platform, integrated with AWS services, delivers fast, seamless protection for people, devices, and data—whether hosted in AWS or elsewhere.

By combining Netskope's visibility and adaptive security with AWS's robust infrastructure and security tools, organizations can significantly reduce risk, enhance their security posture, and implement Zero Trust across both internal and cloud-hosted applications.

Thousands of customers, including over 25 of the Fortune 100, rely on Netskope's advanced capabilities to secure their AWS workloads and beyond, mitigating threats and addressing ever-evolving security challenges. Together, Netskope and AWS provide the foundation you need to securely scale and protect your organization in the cloud era.

netskope + aws

©2024 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Discovery, Cloud Confidence Index, Netskope Cloud XD, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 03/24 EB-722-1-PV