netskope

eBook

# Beyond the Perimeter:

## 6 Key Use Cases for Advancing Federal Cybersecurity with Zero Trust

# Beyond the Perimeter: 6 Key Use Cases for Advancing Federal Cybersecurity with Zero Trust

## Introduction

Federal agencies migrating legacy systems to the cloud to gain operational efficiency, data-driven insights, and improve scalability, agility, and collaboration has spurred the need to acknowledge the cyber threat landscape and its sprawling complexity.

To this order, the federal government continues to make progress toward zero trust adoption. On May 12, 2021, President Biden signed Executive Order 14028 to improve the nation's cybersecurity and protect federal government networks, and on January 26, 2022, the Office of Management and Budget (OMB) released a federal strategy to move the U.S. government toward a zero trust approach to cybersecurity.

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

**As mandated  by the OMB, all federal agencies must meet zero trust goals set by 2024, building on earlier federal cybersecurity initiatives.** An effective zero trust security model for federal agencies should deliver a great user experience, making security transparent and creating little to no friction across the organization's workloads.

Furthermore, the National Cybersecurity Strategy takes a "better together" approach that calls for the public and private sectors to work together to drive better integration of security tools to give unparalleled context and visibility across the enterprise. It also gives agencies the control to build cybersecurity strategies around risk.

That means federal agencies and associated organizations 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 organizations 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 Microsoft 365 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 GovCloud Supports the Zero Trust Journey

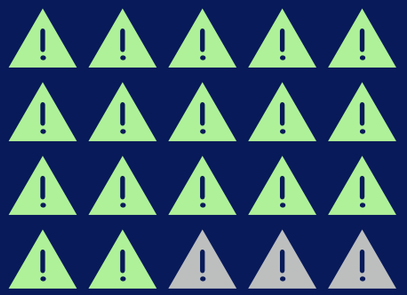
Rather than traditional perimeter security's binary allow-or-block policy controls for ports, protocols, domains, URLs, and applications, Netskope GovCloud assesses transactional risks for each session. No networks, devices, or users are trusted implicitly. Netskope GovCloud is the government authorized instance of the Netskope Intelligent SSE platform and powered by the NewEdge network, used by thousands of commercial organizations around the world. Moreover, Netskope GovCloud is a FedRAMP High authorized platform for cloud-delivered cybersecurity services.

The heart of the Netskope One platform and the Intelligent SSE component is powered by the Netskope **Zero Trust Engine**, which supports application risk profiles, user risk profiles, and device security-posture checks, and can exchange these risk profiles with third-party security solutions. It integrates with leading IAM solutions for identity services and multi-factor authentication (MFA) and can request step-up authentication depending on the transactional risk of the session.

Finally, comprehensive security monitoring within Netskope GovCloud uses business intelligence analytics and data visualizations to support refinement of an organization's zero trust least-privilege policies. Dashboards and charts identify any noteworthy user risks, data movement between application instances, application risk profiles and trends, and concerning user behaviors. The same rich context that enables adaptive least-privilege access controls is available across a 3-, 6-, or 13-month time horizon.

Netskope GovCloud and the Zero Trust Engine offer significant benefits for any business with workloads in the cloud. Following are six key use cases that highlight its value.

Netskope GovCloud leveraging Intelligent SSE makes access decisions using adaptive controls based on rich context and user input, enhanced by more than 100 unique detailed activities for thousands of applications. For example, if Netskope GovCloud has a dozen activity controls for a given application and detects risk based on user and session context, it can appropriately limit the user's behaviors within the application rather than simply blocking access to the software.



**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

**As federal agencies continue to rapidly adopt cloud-based IT services, implementing a comprehensive security strategy that delivers complete visibility and control across these applications has to become a priority.**

The idea of employees moving corporate data into unmanaged SaaS applications is unnerving. That is why Netskope GovCloud 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 GovCloud also references risk profiles for more than 75,000 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 organization-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 organization 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

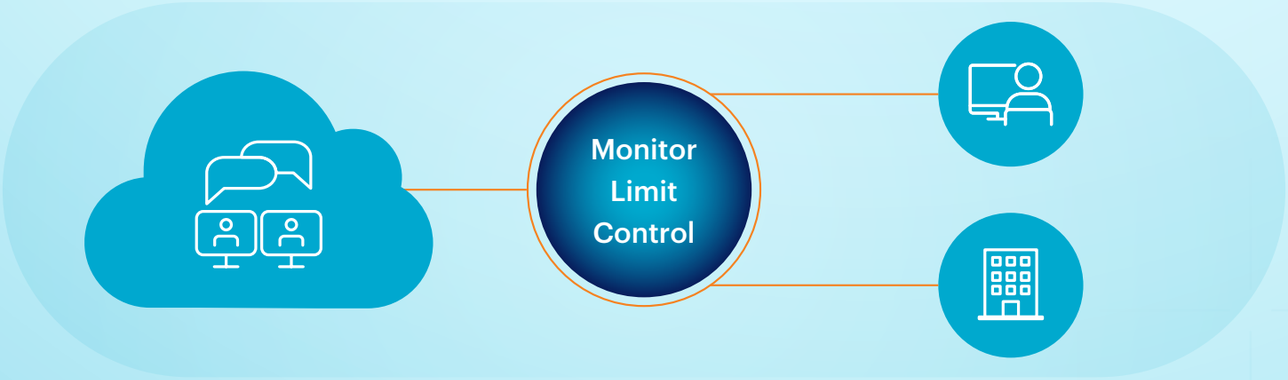
## Protecting Cloud Collaboration

**The U.S. federal government leverages a vast number of IT applications to handle huge volumes of confidential and private data. The government employs an ecosystem of partners and entities that rely heavily on remote work and business-critical, cloud collaboration platforms.** Employees use these platforms 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 GovCloud 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 GovCloud, and Zoom has 10. That means security teams can use Netskope GovCloud 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.

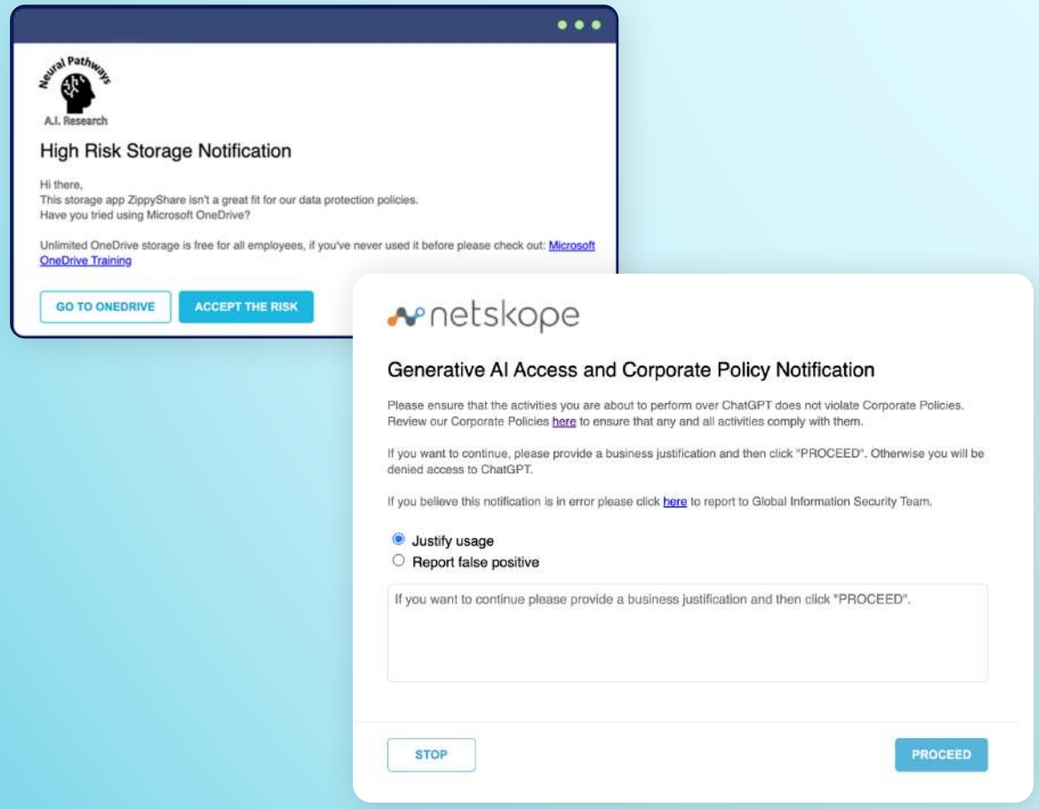
Security teams historically have been seen as the purveyors of "no." The ability to control individuals' actions within an unmanaged application, which Netskope GovCloud makes possible, helps security to become, instead, the function of "How can we make these capabilities available — safely?"



Zero Trust Use Case 3

## Active User Coaching

When users attempt to take a risky action, Netskope GovCloud 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 GovCloud can coach them in real time to select a safer option:




Alternatively, Netskope GovCloud 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 GovCloud 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

**Federal zero trust guidelines developed following the cyber EO further stress moving beyond access control and isolation to enforce continuous zero trust security policies, including real-time access and policy controls that adapt on an ongoing basis based on users, devices, apps, threats, and data context.**

Although corporate data is increasingly moving to SaaS applications, many organizations continue to operate internally developed apps. These, too, are best locked down with zero trust security, so that users access the internal application through the company's ZTNA software. This approach ensures that users are accessing only what they need and not unnecessarily moving laterally through the company's network.


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. **As highlighted in the Federal data security strategy, developing a comprehensive, accurate approach to categorizing and tagging data will be challenging for many agencies.**

By contrast, Netskope GovCloud 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 GovCloud provides instance awareness for more than 450 applications, which enables the security team to understand whether data resides in a company instance of an application or a personal instance of the same application. This gives Netskope GovCloud insight into any user attempts to exfiltrate data. For example, while

legacy controls might allow users to move sensitive data from the organization's Google Workspace into their own personal Workspace environment, Netskope GovCloud understands the difference and can provide real-time coaching or simply prevent the exfiltration.

For applications that do not support instance awareness, identity mapping in Netskope GovCloud can map company and personal logins to distinguish which application tenant a user is working in.

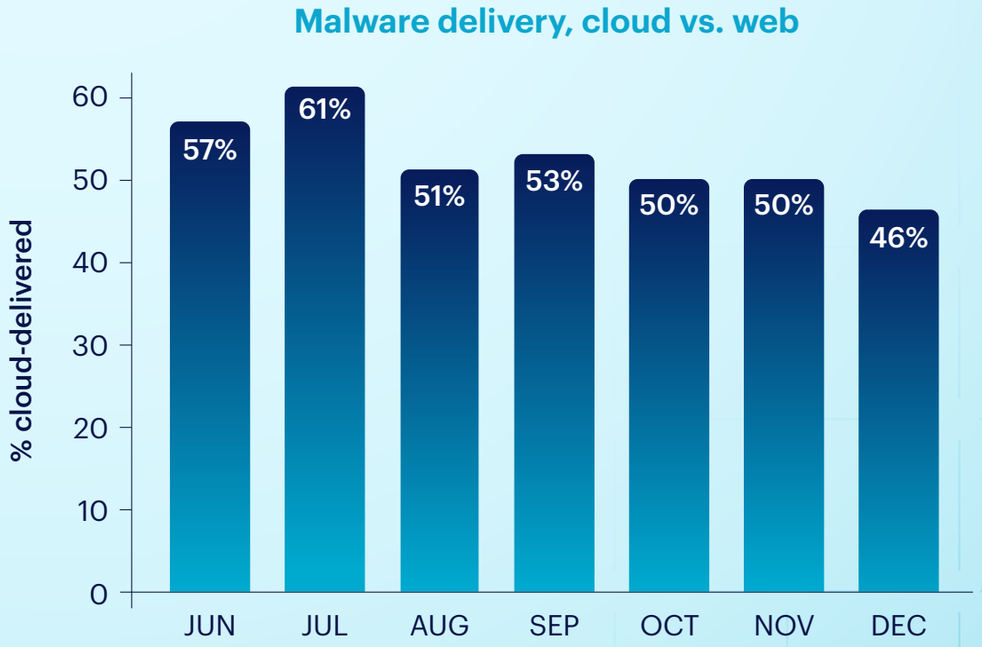
## Cloud Misconfigurations

The vast majority of cloud security failures stem from configuration mistakes. Properly implementing cloud security posture management (CSPM) and SaaS security posture management (SSPM) solutions is the best way for an organization to ensure that employees are using the cloud safely and securely.

These systems help federal organizations understand the security posture of the workloads they have deployed in a public IaaS cloud or SaaS applications, respectively. They evaluate the configurations, compliance, and overall posture of a company's cloud platforms or apps, then compare these results against security control recommendations from third-party experts such as the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA). And because CSPM and SSPM systems use APIs to investigate the cloud configurations, they require no production downtime or lengthy integration.

Netskope GovCloud includes hundreds of out-of-the-box rules for popular SaaS applications, including Salesforce, Microsoft Exchange, and SharePoint, and for IaaS platforms including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. Across all these solutions, Netskope GovCloud can continuously audit security configurations, and when it finds a problem, it can offer steps to guide remediation — reducing the chance that a misconfiguration in a cloud system will result in a security crisis for the organization.

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




*Source: Netskope Cloud and Threat Report 2024.*

# Conclusion

A cyberattack can have a cascading and long-lasting impact not only on the government entity but also its constituents and its customers. As a result, implementing strong cybersecurity measures has become a prime responsibility of government agencies.

Although the federal government is prioritizing  building cyber resilience into these increasingly complex cloud environments to effectively defend against ever-evolving threats, security still remains one of the greatest obstacles to any network, cloud, or data transformation project.

Many networking and security teams today are tasked with supporting a hybrid work environment using collections of mostly legacy defenses. Netskope helps federal agencies overcome the obstacles created by legacy infrastructure by both delivering the security that meets today's requirements and tackling future needs from the same platform. Netskope GovCloud has been purpose built to address modern security challenges of a modern digital-first world.

As a leader in the **Gartner SSE MQ**, we can help you build out a performant, collaborative, adaptive risk solution.

**Request a meeting/demo**

Additional

**Netskope Federal Solutions information**

# About Netskope

Netskope is a leader in Secure Access Service Edge, redefining cloud, data, and network security and helping organizations apply zero trust principles. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and protects people, devices, and data no matter where they are. Netskope helps organizations reduce risk, increase effectiveness, and gain unparalleled visibility into all cloud, web, and personal application activity.

Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to mitigate threats and address technological, organizational, network, and regulatory changes.

netskope