Ebook

The Top SSE Data Protection Use Cases

How to stop data breaches in the modern business world with Zscaler SSE

Contents

The rise of SSE

Organizations' users and apps were all once on-premises, giving rise to castle-and-moat security via costly appliances that made network perimeters to protect data therein.

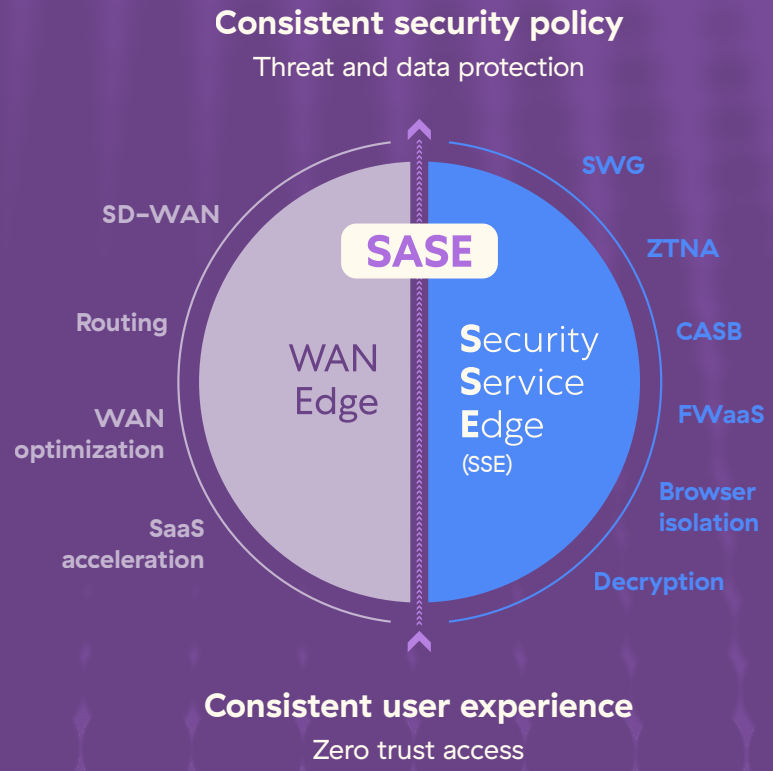
With cloud, the web, and remote work, the castle has vanished—but many still rely on castle-and-moat architectures. Unfortunately, complex stacks of appliances can't address modern data protection needs, and backhauling traffic breeds poor performance, limits scalability, and hinders user productivity.

Many modern data protection tools also fall short—specifically, when they focus on insider threats and neglect external threats to data. In other words, proper data protection must be complete with strong security.

Security service edge (SSE) is the solution to these challenges. It refers to complete platforms that reduce complexity and fill modern data protection gaps by integrating CASB, SWG, ZTNA, and more. Through cloud-delivered security at the edge, SSE offers maximum performance, scalability, and user experience.

The **Zscaler Zero Trust Exchange™** is the world's largest security cloud and was designed to secure any transaction long before the inception of SSE. It stops all insider and outsider risks to data.

Read on to learn the data protection use cases that customers leverage our SSE to address.



Achieving zero trust security

Legacy security tools extend unfettered access to the network as a whole (and all of the data and apps inside). But this allows lateral threat movement between resources that can balloon the effects of data breaches. It violates the zero trust principle of least privilege, whereby authorized users only receive access to the resource they need—at the moment they need it.

The Zero Trust Exchange

The Zero Trust Exchange takes a fundamentally different approach and delivers modern, zero trust data protection. By serving as an intelligent switchboard between users, SaaS apps, private apps, IoT/OT, and more, Zscaler extends secure access only to individual resources as appropriate—all while enforcing data loss prevention (DLP) measures for additional granularity.

The Zscaler advantage

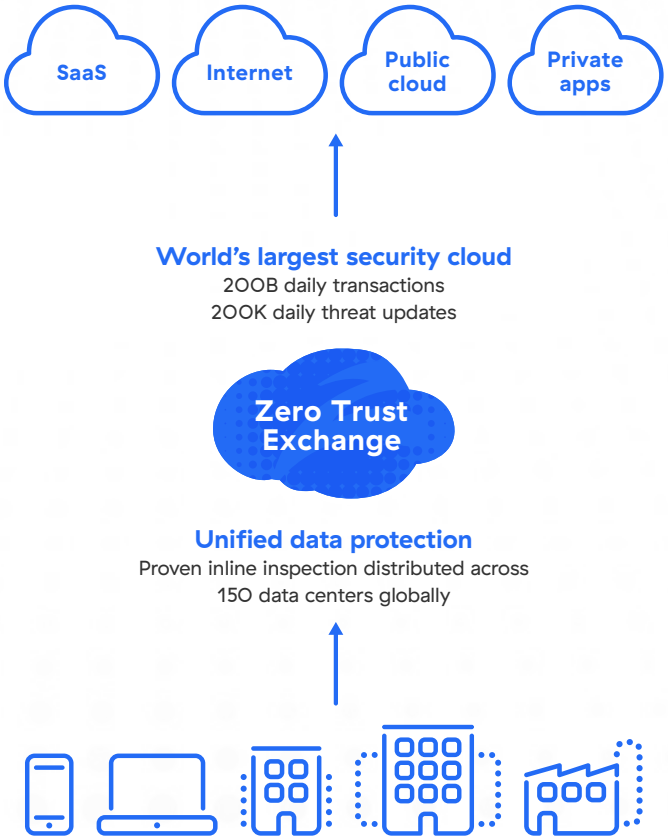
- Hide all IT resources behind the Zero Trust Exchange to eliminate the attack surface
- Prevent lateral threat movement by connecting users directly to apps, not the network
- Stop compromise by securing all user-to-app, app-to-app, and machine-to-machine transactions

Preventing data loss via encrypted traffic

Legacy security appliances (whether hardware or virtual) are often used to inspect web traffic for data loss. But appliances have fixed capacities to service users, cannot handle encrypted traffic at scale, and, as a result, provide little to no SSL inspection. With more than 95% of web traffic now encrypted, this is a dangerous weakness.

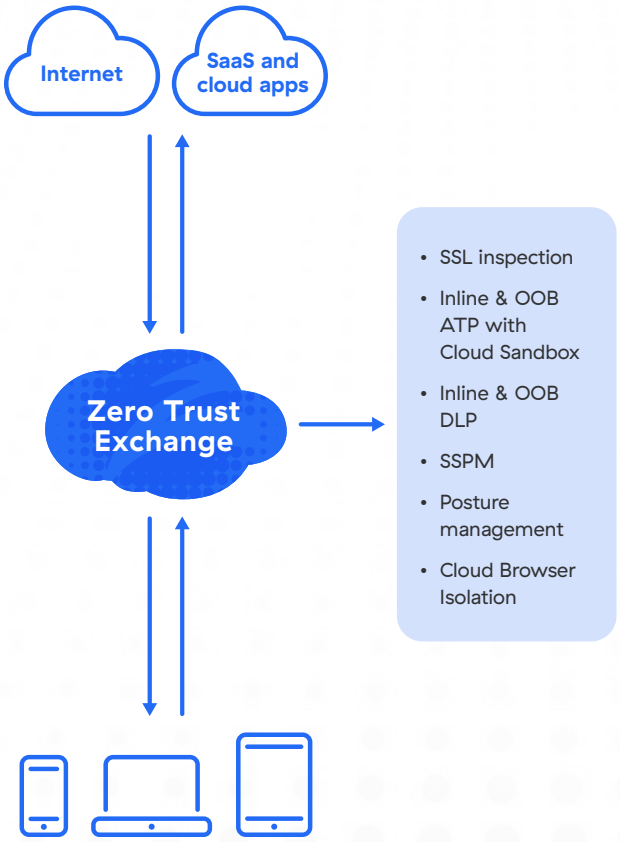
A true cloud architecture

Built upon the world's largest security cloud, the Zscaler security service edge boasts the performance necessary to inspect encrypted traffic at scale for global corporations with hundreds of thousands of users. This ensures that any potential data loss hidden via SSL is successfully detected and remediated in real time.



The Zscaler advantage

- A security service edge with unrivaled scalability and performance that processes over 200 billion transactions daily
- A platform built on a proven inline architecture used by over 25% of Forbes Global 2000 companies
- A global footprint of over 150 data centers that deliver security at the edge for maximum user experience



Stopping double-extortion ransomware

On top of device encryption, double-extortion ransomware steals data and threatens leakage if a ransom is not paid. These threats use soft targets (like unsecured data at rest and misconfigured apps) to proliferate and exfiltrate data. Unfortunately, legacy security appliances can't prevent this in our cloud-first world.

Complete threat and data protection

Zscaler provides complete threat protection to stop ransomware at upload and at rest across the IT ecosystem. Additionally, DLP and CASB scrutinize all cloud data channels to stop exfiltration while posture management and SSPM uncover cloud app misconfigurations that expose data.

The Zscaler advantage

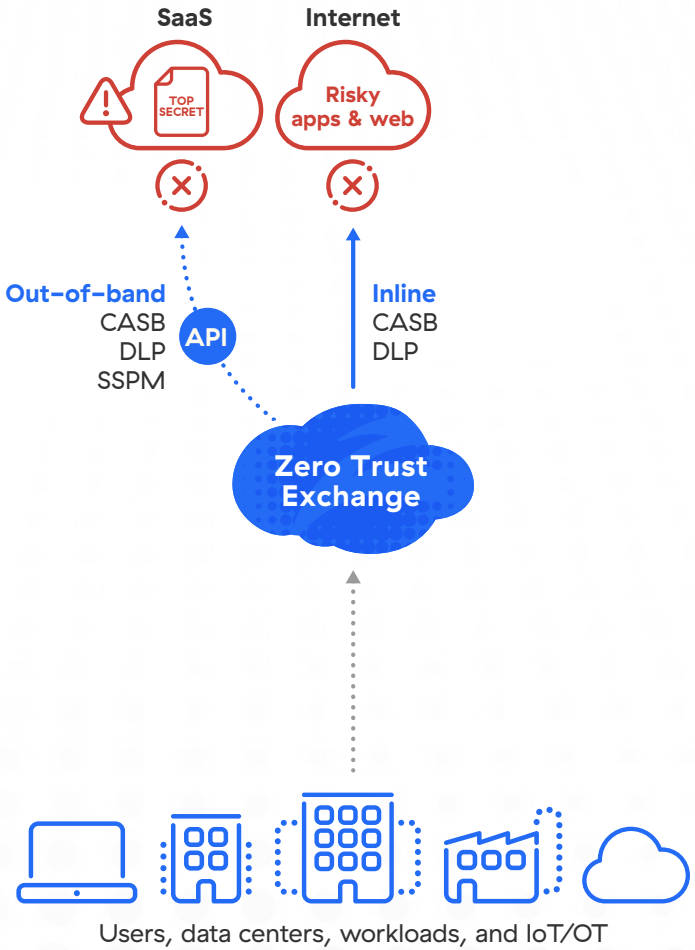
- Full, scalable SSL inspection for real-time identification of data exfiltration and ransomware in transit
- Cloud sandboxing technology for stopping zero-day ransomware both inline and out of band
- The power of the world's largest security cloud—threats found anywhere are blocked everywhere

Securing SaaS applications

SaaS apps deliver unprecedented productivity and flexibility, but they can easily lead to data loss if not properly secured. This is because users regularly upload data to unsanctioned apps, files at rest can easily be shared with unauthorized parties, and misconfigurations can compromise app security posture and expose data.

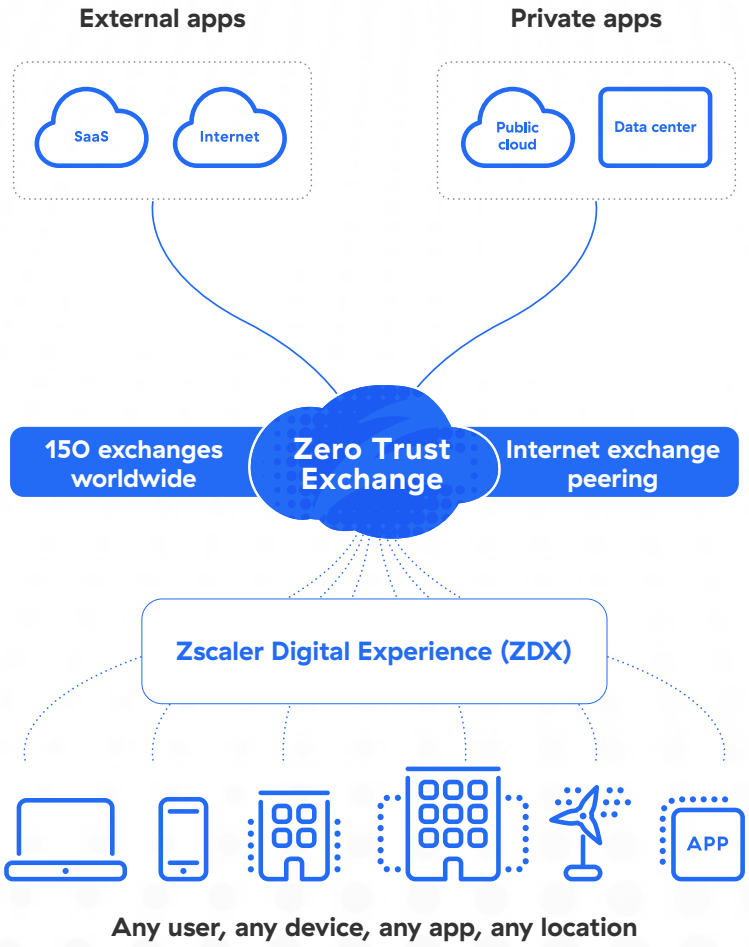
CASB with DLP

Zscaler secures the use of SaaS apps by automatically discovering shadow IT, controlling data uploads to unsanctioned cloud apps, and securing data at rest in sanctioned cloud apps. Additionally, SaaS security posture management scans apps for misconfigurations that could expose data or compromise compliance.



The Zscaler advantage

- Unified data protection that consistently secures all SaaS and cloud data channels with a single policy
- High-performance CASB functionality as part of the most proven and integrated security service edge
- Cloud DLP complete with advanced capabilities like EDM and OCR for protecting specific values and image data



Defending data for remote users

Remote work is here to stay, but legacy security wasn't designed for this new style of business. Leveraging VPN and backhauling user traffic to security appliances yields insufficient scalability, harms user productivity, and fails to address the modern data protection use cases that cloud-first companies need to solve.

Cloud-delivered security at the edge

With the world's largest, most proven security cloud, Zscaler boasts the scale and expertise necessary to defend data while enabling remote work around the world. Zscaler is able to secure the use of SaaS, IaaS, PaaS, the web, and private apps without backhauling traffic to an appliance, ensuring global data protection with maximum performance.

The Zscaler advantage

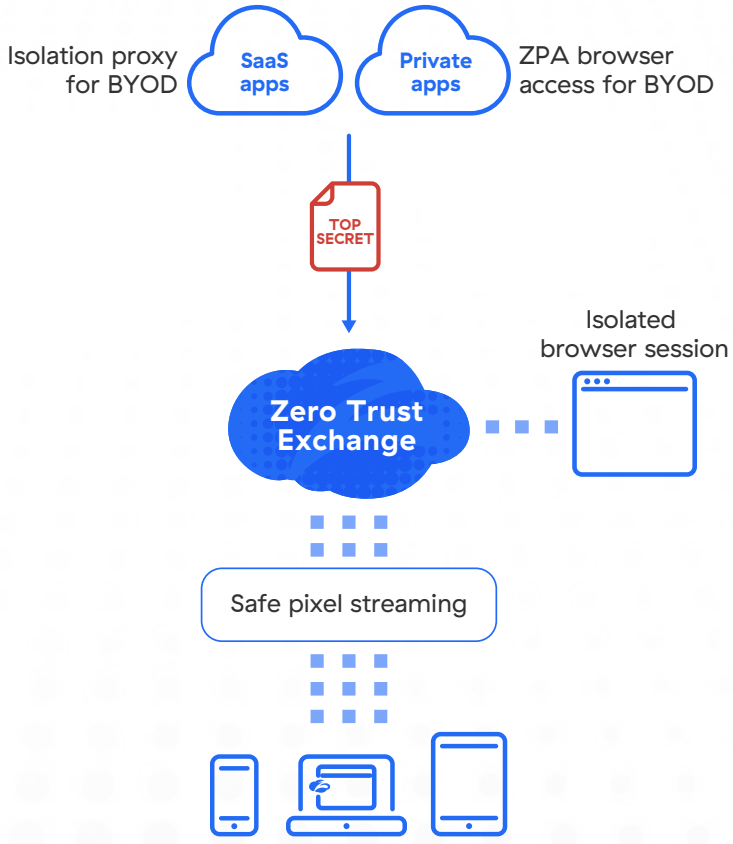
- A global security cloud with over 150 data centers provides high-performance data security at the edge
- A security-as-a-service offering eliminates the need for backhauling to hardware and virtual appliances
- A single-pass architecture with CASB, SWG, ZTNA, and more offers efficient, complete protection—everywhere

Securing BYOD and other unmanaged devices

Non-corporate or unmanaged endpoints like BYOD and B2B devices often have valid reasons to access corporate apps—but IT loses control once they download data. Unfortunately, blocking these devices disrupts productivity, software agent installations are typically infeasible, and reverse proxies frequently break. So what is IT to do?

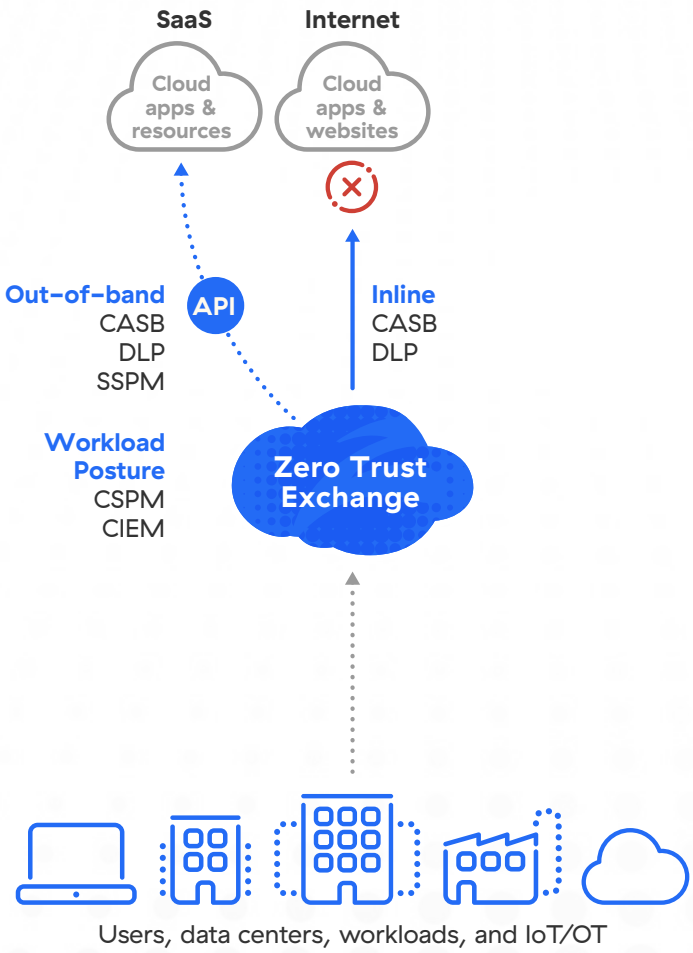
Cloud Browser Isolation

With agentless browser isolation, Zscaler virtualizes a user's app session in an isolated environment and streams only pixels to the endpoint, preventing download, copy, paste, and print. This means that IT can enable unmanaged device access while keeping data safe and circumventing the challenges of agents and reverse proxies. It also prevents infected file uploads from risky endpoints.



The Zscaler advantage

- Cloud Browser Isolation built upon the world's largest, highest performance security cloud
- Isolation Proxy for agentless security on any device accessing any SaaS application
- ZPA Browser Access for secure private app access without client-side software installations



Reaching regulatory compliance

Data regulated under GDPR, HIPAA, and more is moving off-premises with the rest of the enterprise's sensitive information—but legacy tools are incapable of protecting it and maintaining compliance in the cloud. This is critically important, as failing to adhere to privacy laws like CCPA and frameworks like PCI DSS can lead to fines, a loss of consumer trust, and reduced revenue.

Airtight compliance assurance

We built the Zscaler security service edge with regulatory compliance in mind. The solution delivers complete visibility and control across the IT ecosystem to ensure that regulated data stays safe, applications don't contain any compliance-hindering vulnerabilities, and the principles of zero trust are enforced everywhere.

The Zscaler advantage

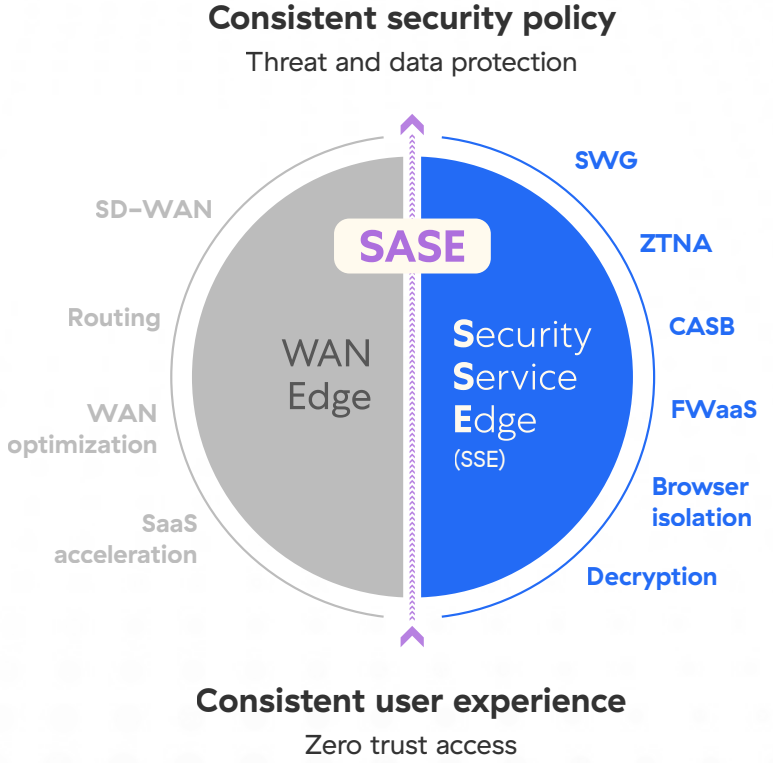
- Cloud DLP with multimode CASB functionality that secures regulated data in motion and at rest
- Compliance preserved—Zscaler doesn't download data for inspection, even for measures like exact data match
- Zscaler SSPM and posture management to find and fix misconfigurations and entitlements that lead to noncompliance

Gaining consistent, manageable data protection

Relying upon a patchwork of disjointed point products with disparate capabilities creates a number of challenges. In particular, it breeds inconsistent data protection across an increasingly complex IT ecosystem. Additionally, admins overseeing myriad siloed solutions face a hefty management burden.

An all-in-one platform

Zscaler SSE integrates leading technologies that can secure any transaction and defend data wherever it goes—consistently and completely. Through a comprehensive cloud offering with a single-pass architecture, the enterprise can also reduce IT complexity while easing the management burden for administrators.



The Zscaler advantage

- Consistent data protections for all SaaS, cloud, web, and private applications
- Simplification of architecture that cuts down on point products and appliances
- Consolidated ease of management that forgoes duplicating policies and saves admins time

Cloud and mobility offer innumerable productivity and flexibility benefits, but to take advantage of them without compromising the safety of data, you need to embrace a new approach to cybersecurity. The Zscaler security service edge empowers your enterprise to embrace digital transformation while protecting data, wherever it goes.

- **Learn what customers have to say about Zscaler SSE**
- **Read the Magic Quadrant for Security Service Edge**

zscaler™ | **Experience your world, secured.™**

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com