Secure Web Gateway (SWG) Buyer's Guide: Key Use Cases and Evaluation Criteria

A cloud-native Secure Web Gateway (SWG) is a modern, SaaS-based security architecture specifically designed to meet the unique challenges of hybrid and cloud-first environments.

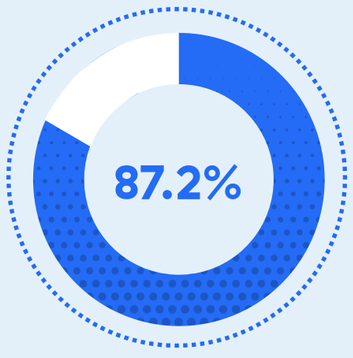
Think of a cloud-native SWG as a security service engineered from day one for elastic scale and universal reach. Delivered from the cloud, it applies uniform policy and full SSL/TLS inspection whether your users sit in a campus office, a hybrid branch or a fully remote workforce.

By contrast, appliance-based and even "virtualized" SWGs are effective only for legacy environments. They pose multiple challenges due to their capacity limitation, policy-management gaps, high costs and encrypted-traffic blind spots.

Why cloud-native SWGs are critical for modern enterprises

The modern enterprise faces a perfect storm of challenges that demand a new approach to security. Increased adoption of cloud applications, the rise of remote work and the growing sophistication of cyberthreats are rendering traditional security solutions obsolete.

One of the most pressing challenges is the proliferation of encrypted traffic, which has reached more than **90% of web traffic**[1]. Hiding in the layers of your encrypted internet traffic are malware payloads, phishing scams and sensitive data leaks.



In fact, a staggering **87.2% of total threats are now delivered over encrypted channels**[2], underscoring the urgent need for a full inspection of all internet and SaaS traffic.

Traditional security solutions, like appliance-based and virtualized SWGs, struggle to inspect encrypted traffic at scale, leaving organizations vulnerable to malware and data exfiltration. Because legacy systems lack the necessary power to handle the massive volume of encrypted traffic, they create security gaps that cybercriminals readily exploit.

Relying on antiquated appliance-based SWGs is a choice between the agonizing latency of backhauling traffic through your central data center for security inspection—slowing down access and creating a frustrating user experience—or grappling with a costly and complex hybrid SWG deployment that ends up creating management headaches with disparate interfaces and policies.

And while virtualized SWGs offer a seemingly more flexible, service-based approach, they often inherit the same underlying software limitations as their hardware counterparts. As you scale your cloud adoption and the number of remote users grows, you might face unexpectedly high costs and performance bottlenecks. This is because they often still rely on centralized control points within the cloud, leading to inefficient routing of traffic and diminishing performance precisely when you need it most.

Organizations today require security solutions that can keep pace with the evolving threat landscape and the complexities of cloud applications and remote work. Cloud-native SWGs are purpose-built to meet these needs by offering unmatched scalability, comprehensive threat protection and seamless SSL/TLS inspection—all without performance trade-offs.

---

[1] New ThreatLabz Report Reveals Over 85% of Attacks are Encrypted

[2] ThreatLabz 2024 Encrypted Attacks Report

This guide covers six use cases to help organizations evaluate cloud-native SWG solutions with specific scenarios and critical features to consider.

We'll look at why and how practitioners commonly apply cloud-native SWGs in their organizations and address and provide insight into how to implement features that improve security and user experience.

01 Inspect 100% of traffic to block encrypted threats

02 Protect against advanced threats and malware

03 Monitor and control access to websites through URL filtering

04 Enforce policy on usage of cloud applications and services

05 Prevent bandwidth overuse for non-critical apps

06 Neutralize online threats with secure, isolated browsing

Six key use cases for a cloud-native SWG

01 Use case #1: Inspect 100% of traffic to block encrypted threats

The majority of web traffic today is encrypted, marking significant progress for data privacy. However, this same encryption is often leveraged by attackers to carry out threats, creating a substantial advantage for them. Encrypted traffic can hide malware, creating a blind spot for traditional security measures. With a substantial 87% of total threats now delivered over encrypted channels[3], SSL/TLS inspection plays a critical role in defending against modern threats. It's critical to fully inspect all internet and SaaS traffic. However, inspecting encrypted traffic is resource-intensive and can adversely slow down network performance of legacy security devices.

A cloud-native architecture allows you to decrypt, detect and prevent threats in all encrypted traffic at scale without any performance trade-offs. By inspecting 100% of SSL/TLS traffic, organizations can prevent data breaches caused by hidden malware while meeting regulatory requirements.

A cloud-native SWG will:

- Provide visibility into traffic that is not scannable by dedicated engines
- Enable full SSL/TLS inspection without performance degradation
- Meet regulatory compliance requirements by ensuring employees aren't putting confidential data at risk
- Prevent data breaches by finding hidden malware and stop hackers from sneaking past defenses
- Perform SSL/TLS inspection without latency impact
- Inspect all encrypted content across cloud, web and apps

[3] ThreatLabz 2024 Encrypted Attacks Report

Deployment requirements

- Inspect 100% of SSL/TLS traffic without backhauling and without impacting user performance
- Inspect traffic for all users across all locations and devices without the need to backhaul web traffic or use VPNs

How to test

- Enable SSL inspection policies and measure performance
- Verify blocking of malicious encrypted content

Key benefits

- Seamless inline inspection of encrypted traffic
- Prevent system compromise by finding hidden malware in encrypted traffic
- Reduce risk with control and visibility over Internet usage based on business policies

Zscaler capabilities: SSL/TLS inspection

- Inspects 100% of SSL/TLS inspection with no impact on performance
- Cloud-native, proxy-based architecture to decrypt, detect and prevent threats in all encrypted traffic at scale without any adverse performance impact

Pro Tip: To learn more, check out SSL Inspection Deployment and Operations Guide

02 Protect against advanced threats and malware

To effectively detect and block increasingly sophisticated attacks requires a layered security approach. A comprehensive strategy should include real-time monitoring, advanced AI-driven analysis and the ability to adapt defenses dynamically.

A robust security posture involves inspecting all traffic, including encrypted channels, to uncover hidden malware and prevent data exfiltration. It also requires leveraging threat data from extensive security clouds to gain real-time threat intelligence and proactively block suspicious content.

By adopting this layered approach, organizations can enhance their ability to detect anomalies, quarantine threats and secure users both on and off the network, ensuring comprehensive protection against cyber risks.

A cloud-native SWG will:

- Improve security posture by protecting against ransomware, zero-day threats and unknown malware
- Analyze internet and SaaS traffic to monitor for security and operational anomalies
- Leverage threat data and cloud-based threat intelligence in real time

Deployment requirements

- Configure ATP and Malware Protection policies to deploy cloud-native inline threat prevention across all office locations and for remote users
- Inspect 100% of encrypted SSL/TLS traffic at scale with a zero trust, cloud-proxy architecture

How to test

- Simulate malware attacks to validate detection and prevention

Key benefits

- Effective advanced threat protection monitors all your traffic, all the time
- As soon as a solution stops a new threat anywhere, it can stop it everywhere
- Reactive, real-time, predictive security measures powered by advanced AI give security teams the full picture, resulting in faster threat detection, prevention and remediation

Zscaler capabilities: Advanced threat and malware protection

- Stops threats before they have the chance to sneak past defenses
- Automatically detect and quarantine unknown threats and suspicious files, preventing compromise, lateral movement and data loss
- Secure users on- and off-premises and from wherever they work
- Unmatched, real-time global threat protection built on data from the world's largest security cloud

Pro Tip: To learn more, check out Threat Protection Deployment and Operations Guide

03 Monitor and control access to websites through URL filtering

Preventing access to certain web content by restricting certain URLs and URL categories is crucial to improving the security posture of your organization. By setting up URL filtering, you're essentially restricting access to non-work-related sites, which helps everyone focus better. With a clearly defined web governance policy you can guarantee that your employees navigate the web safely.

From a compliance perspective, you can also categorize websites associated with embargoed countries or those containing restricted content, ensuring you stay on the right side of trade regulations. Financial institutions, for example, can use URL classification to block access to gambling websites to comply with industry regulations. Plus, you can generate reports on web usage, blocked sites and compliance violations—a must-have for regulatory reporting.

A cloud-native SWG will:

- Limit exposure to certain types of web content
- Control access privileges for users
- Define access to custom allow and deny lists
- AI/ML-powered URL categorization

Deployment requirements

- Easily configure URL filtering policies
- Scale effortlessly without impacting user performance to inspect SSL/TLS encrypted traffic
- Get inline visibility into web traffic, applications and cloud services

How to test

- Deploy URL filtering policies across selected offices/users.
- Verify access restrictions, real-time blocking and reporting.

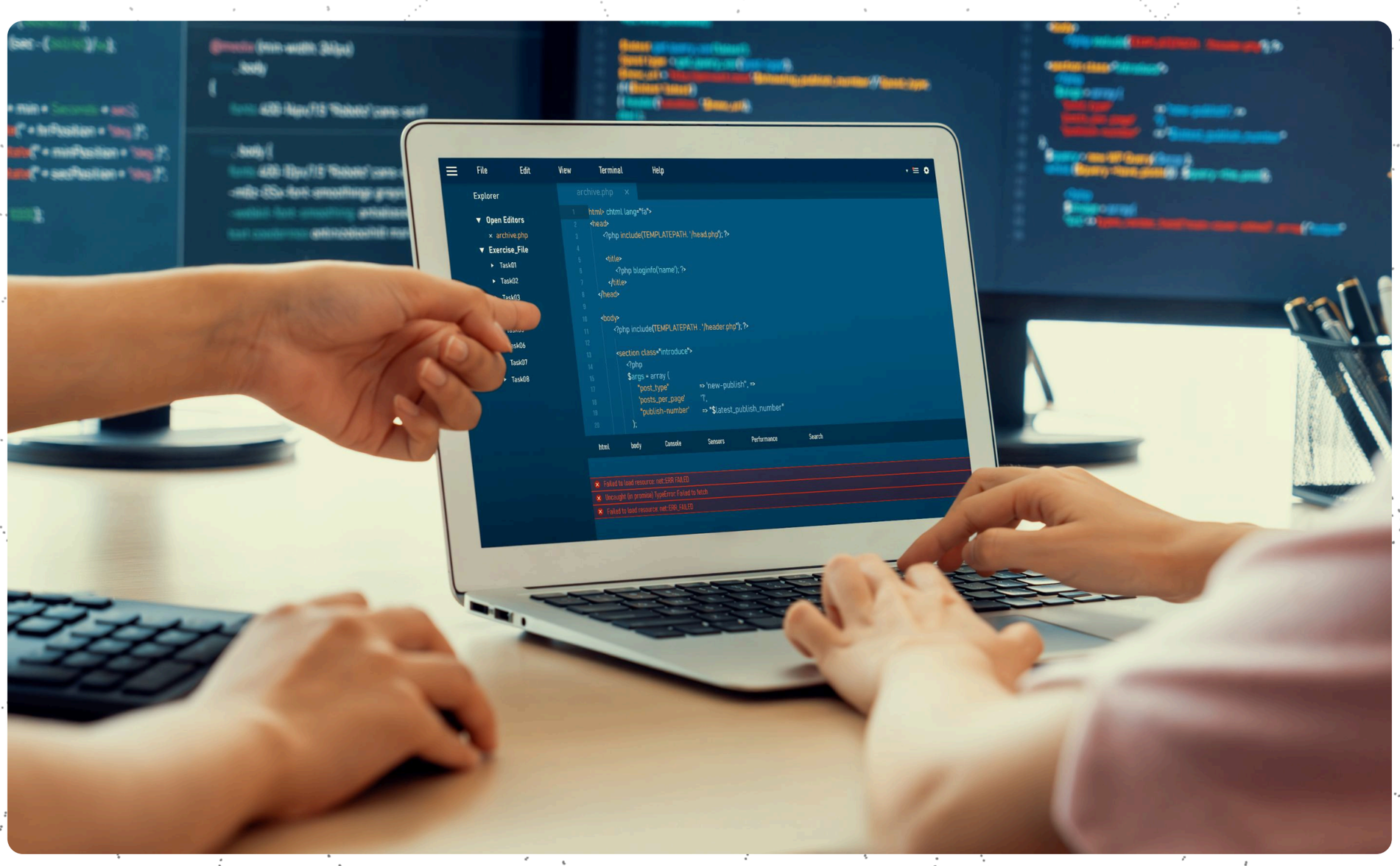
Key benefits

- Block malicious or inappropriate sites in real time
- Improve productivity by restricting access to non-work-related content
- Maintain compliance and adhere to industry regulations

Zscaler capabilities: URL filtering

- Categorizes billions of URLs into 100-plus categories
- Real-time updates powered by threat intelligence
- Inline deployment ensures seamless enforcement across users
- Straightforward, easy deployment

Pro tip: To learn more, check out URL Filtering Deployment and Operations Guide



04 Enforce policy on usage of cloud applications and services

One of IT's biggest challenges is figuring out how to safely enable access to cloud applications without disrupting user productivity. Balancing security and usability is no easy task. That's the job Cloud Access Security Broker (CASB) controls were invented to solve. And any cloud-native SWG worth its salt needs to offer inline security for cloud data in motion. (And a pro tip is to ensure that the CASB has extensibility to provide out-of-band security for data at rest as well.)

Implementing strict security measures can lead to a frustrating user experience, with slow access times and cumbersome authentication processes. This not only reduces productivity but can also lead to employees circumventing security protocols in favor of convenience.

CASB integrated with a cloud-native SWG uses granular security and access policies to provide secure internet and SaaS app access for all users, on any device, from any location, without slowing performance. This approach allows organizations to safely grant access to cloud applications, maintain high productivity and reduce the risk of data leakage and unauthorized app usage.

A cloud-native SWG will:

- Control user access to cloud applications at a granular level based on users, tenants, domains and activities
- Easy deployment using a pre-defined set of cloud application policy rules
- Define daily access limits via criteria such as bandwidth or time
- Perform app scoring to assess application risk and enforce policy-based access controls
- Create a cloud application risk profile based on application status (sanctioned or unsanctioned), risk index, certifications supported, etc., and associate the profile with Cloud App Control policy rules

Deployment requirements

- Scale effortlessly without impacting user performance
- Configure cloud app control policies with ease
- Understand application risk
- Enable app scoring to dynamically classify applications based on risk and enforce security policies accordingly

How to test

- Apply access policies
- Assess app scoring effectiveness by verifying risk categorization and policy enforcement
- Monitor cloud app usage
- Verify visibility into app-specific user behaviors

Key benefits

- Safely enable access to cloud applications without affecting user productivity
- Easily create fine-grained, activity-based controls for applications
- Eliminate unauthorized cloud app usage
- Restrict and control access to prevent data leakage

Zscaler capabilities: Cloud application control

- Identifies sanctioned and unsanctioned cloud app usage
- Applies granular, activity-based access and data control policies
- Provides app risk scoring to inform decision-making

Pro Tip: To learn more, check out Cloud App Control Deployment and Operations Guide

05 Prevent bandwidth overuse for non-critical apps

It's a common scenario: A mission-critical business system—like your customer relationship management (CRM) platform, which tracks sales, manages customer data and supports marketing and service workflows—starts lagging, and operations slow to a halt. What's going on? The culprit could be unmanaged bandwidth, where non-critical applications hog the resources needed for high-priority business tools like your CRM. Ensuring these core applications function optimally requires effective bandwidth management. When apps consume too much bandwidth, it can lead to sluggish performance and reduced productivity across your organization.

Bandwidth control technologies address this problem by prioritizing business-critical apps. They can also identify bandwidth constraints before they negatively impact user experience. That way, essential apps always have the resources they need, keeping productivity high and frustration low.

A cloud-native SWG will:

- Limit the impact of streaming media, file sharing and social media on business apps
- Identify internet bandwidth constraints before they impede user experience
- Align policies for all users to business needs with granular rules spanning application class, location and time

Deployment requirements

- Enable Bandwidth Control on the location and sub-location to prevent bandwidth overuse for non-critical apps, delivered as a cloud service
- Create a seamless user experience with advanced bandwidth control technology

How to test

- Monitor and restrict bandwidth consumption for selected apps/sites

Key benefits

- Ensure high performance for business-critical applications
- Reduce network congestion caused by streaming or downloads
- Improve user productivity

Zscaler capabilities: Bandwidth management

- Enforce bandwidth policies without the need to deploy or manage hardware or software
- Create granular policies based on multiple parameters, including traffic type, location, time of day, file size, minimum and maximum bandwidth and more
- Provide a superior user experience with bandwidth control technologies, including TCP window shaping and bandwidth throttling

Pro Tip: To learn more, check out Bandwidth Control Deployment and Operations Guide

06 Neutralize online threats with secure, isolated browsing

How do you let users access the web freely without exposing your organization to threats, such as malicious scripts, drive-by downloads and other hidden dangers in web pages? The answer is a cloud browser (still widely known as *remote browser isolation*, or RBI). Leading vendors—including Zscaler with its *Zero Trust Browser*—ensure this feature is tightly integrated with cloud-native SWG, so you gain an extra safety layer without deploying a separate product.

With cloud browsers, users can safely access web content. Even if a webpage contains malware or exploits, the user's device remains protected, mitigating the risk of data loss and potential system compromise. This approach allows for more open internet policies, giving users more leeway when browsing the web while minimizing policy complexity and reducing overall risk.

A cloud-native SWG will:

- Host browsing sessions on a remote server
- Prevent downloads or execution of malicious scripts

Deployment requirements

- Determine how the user interacts with isolated web pages, where the isolation containers are spun up and what the isolation experience looks like to the user
- Identify criteria for enabling Isolation (based on risk or specific use case)
- Create URL filtering rules for respective destinations with web traffic action “Isolate”

How to test

- Browse high-risk sites and verify isolation

Key benefits

- Enables secure access to risky web content without requiring an endpoint agent on every device
- Protects sensitive data from targeted attacks hidden in web pages, downloadable web content and vulnerable plugins
- Removes the threat of data exfiltration even if the browser contains vulnerabilities or has unsafe plugins installed
- Minimize policy complexity, reduce risk and give web users more freedom

Zscaler capabilities: Remote browser isolation

- Protects users from web threats with AI–based isolation of suspicious internet content and high–risk users
- Enables full productivity with no risk
- Allows users to temporarily store documents in the cloud browser, upload files to another sanctioned corporate app, or download secure flattened PDFs using Content Disarm and Reconstruction (CDR)
- Protect data, even on BYOD endpoints, with controls that block data leakage, stop risky actions and even watermark data
- Extend agentless access to web–based and SaaS applications via the cloud browser with data security controls for employees or contractors on unmanaged or BYOD endpoints

Pro Tip: To learn more, refer to Isolation Deployment and Operations Guide

SWG evaluation checklist and scorecard

Securing your digital world can feel like navigating a labyrinth. To simplify the journey, here's a checklist and scorecard to verify which security partner meets your organization's critical requirements. This scorecard will help you assess what solutions provide the features and capabilities needed to secure your cloud journey.

Use case	Evaluation criteria	zscaler™	Vendor A	Vendor B
URL filtering	Block malicious and innapropriate sites in real time	☐	☐	☐
Cloud App control	Identifies and controls unsactioned cloud applications	☐	☐	☐
SSL/TLS inspection	Inspects 100% of encrypted traffic at scale	☐	☐	☐
Advanced threat protection	Detects zero-day malware with sandboxing and AI	☐	☐	☐
Bandwidth controls	Applies granular policies to throttle non-critical traffic	☐	☐	☐
Remote browser isolation	Provides isolation for risky web browsing sessions	☐	☐	☐

To help organizations evaluate their options, our understanding of, Gartner® Magic Quadrant™ for Security Service Edge™ suggests that robust Security Service Edge (SSE) solutions typically meet a set of mandatory requirements and offer common features that ensure comprehensive protection. Since SSE solutions encompass SWG, Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA), these criteria serve as a benchmark for evaluating modern security platforms.

Below is a breakdown of the Gartner recommended SSE capabilities, categorized into mandatory requirements (must-have functionalities) and common features (capabilities that enhance security, visibility and integration across the enterprise)[4]:

The must-have capabilities of this market include:

- [ ] Cloud-delivered management and data planes
- [ ] Identity-aware forward proxy (including encrypted traffic visibility and control, malware protection, threat prevention and URL filtering)
- [ ] Both inline (via identity-aware proxy supporting managed and unmanaged devices) and out-of-band (via API) protection of in-use SaaS apps including adaptive access, encrypted traffic visibility and control, data loss prevention (DLP), malware protection and threat prevention
- [ ] Adaptive and granular access (controlled by identity and context) to private and SaaS applications by both agent and agentless methods, and from managed and unmanaged devices
- [ ] Integration with identity providers for identity context and validation

---

[4] Gartner. "Gartner® Magic Quadrant™ for Security Service Edge", Charlie Winckless, Thomas Lintemuth, Dale Koeppen, Charanpal Bhogal, 20 May, 2025.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The standard capabilities of this market include:

- [ ] Ability to apply controls consistently across multiple network and application destinations
- [ ] Support for managing and securing traffic from common endpoints (such as Windows, macOS, iOS and Android devices)
- [ ] Integration with key enterprise technologies such as security information and event management (SIEM), extended detection and response (XDR), SD-WAN and other adjacent technologies
- [ ] Support for published and documented APIs that are accessible to the customer and that allow automation of common tasks and integration with other security platforms
- [ ] Control of traffic on all ports and protocols
- [ ] Remote browser isolation (RBI) to enhance security across all network destinations and channels
- [ ] SaaS security posture management for visibility and remediation of SaaS configurations and visibility into SaaS plug-in applications
- [ ] Continuous adaptive access controls across all channels based on initial connection status and any change in state during connection
- [ ] Read, write and act upon labels from common data classification platforms
- [ ] Embedded user entity behavior analytics (UEBA) to provide automated detection and response for anomalous and risky device and user behaviors
- [ ] Advanced data protection capabilities such as redaction, tombstoning and on-the-fly encryption (both in-line and out-of-band) and advanced data detection capabilities such as exact data matching (EDM), optical character recognition (OCR) and machine learning (ML) classifiers
- [ ] Support for controlled access from managed and unmanaged devices

Why Zscaler Internet Access?

Zscaler's cloud-native SWG overcomes the shortcomings of traditional approaches by providing a scalable, flexible and effective solution designed for modern cloud environments in three key areas:

01. Zero trust architecture

- **Built on a zero trust:** Verify every connection and grant access based on identity, context and business policies. This approach significantly reduces the attack surface and prevents lateral movement of threats.

- **Full TLS/SSL inspection:** Perform 100% TLS/SSL inspection at scale without impacting user experience.

- **AI and ML powered:** Use AI and machine learning to analyze uncategorized URLs in real time. By dynamically analyzing content, it assigns appropriate categories and enforces policies consistently, expanding URL categorization coverage and accuracy.

02. Secure access

- **Advanced threat protection:** Features like AI-Powered Phishing Detection, AI-Powered C2 Detection and a cloud sandbox stop advanced threats such as ransomware, zero-day exploits and malware. These features go beyond the capabilities of traditional SWGs, providing layered, inline security controls.

- **Dynamic and granular policies:** Create granular policies, blocking, allowing, or monitoring access to specific categories. You can also create custom categories based on URLs, IP addresses, keywords and IP ranges, or top-level domains. This level of customization helps to align security policies with specific business needs.

- **No backhauling:** Eliminate the need to route traffic back to a central location for inspection, securing all web traffic via the cloud infrastructure, which is essential for remote and hybrid workforces.

03. Operational simplicity

- **Scalability and performance:** Scale dynamically, ensuring consistent performance without the bottlenecks associated with legacy systems.

- **Simplified management:** A single, unified platform for web security reduces complexity, costs and overhead, allowing organizations to focus on their core business rather than managing security infrastructure.

- **No manual updates:** Always stays fully up to date to ensure protection against the latest threats without the need for manual updates or patches.

Secure your cloud journey

The modern enterprise needs a web security solution that can keep pace with the speed and complexity of today's cyber landscape. Cloud-native SWGs are no longer just an option; they are a necessity for organizations seeking to maintain a robust security posture in an increasingly connected world.

Zscaler Internet Access is a comprehensive solution that addresses the shortcomings of traditional approaches by providing scalability, superior threat protection, simplified management and a seamless user experience.

With 100% SSL/TLS inspection, cloud-native performance and unmatched visibility, Zscaler gives organizations the confidence to navigate the complexities of cloud security, ensuring their data, users and applications remain protected.

Experience AI-powered advanced threat protection with through our **Zscaler Internet Access Product Tours.**

Don't wait to help your business achieve its cloud security goals. To get started, **schedule a demo** and validate these use cases in your environment.

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. To learn more, visit www.zscaler.com.

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

zscaler.com