The 7 Critical Questions Agencies Should Ask Security Providers

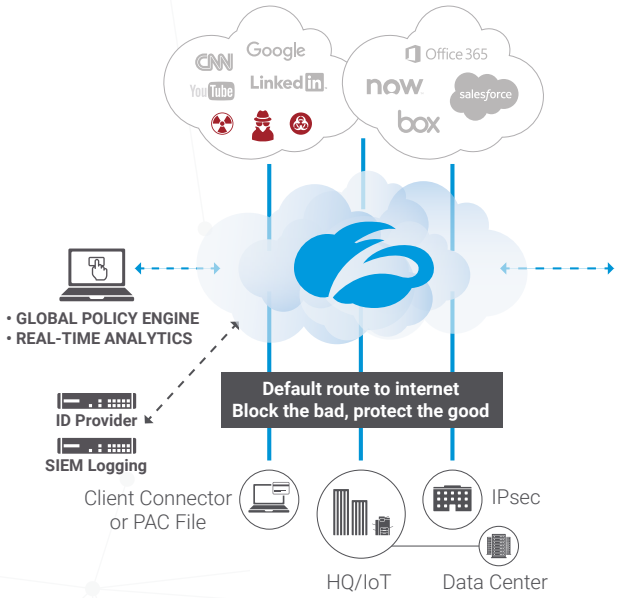
zscaler™

Introduction

With the acceleration in the adoption of Public Cloud, Government departments and agencies are looking to leverage Cloud Security. One would expect choosing a cybersecurity solution would be easy—just find the tools and systems that integrate with what the agency is using.

If only it really were that simple. In the ever-changing security landscape, finding a solution that works right now isn't good enough—it also has to work in the future, without adding unanticipated costs.

To help government choose a service that works for them, Zscaler compiled a list of the seven critical questions to ask security providers about their solutions. With this information in hand, agency IT decision-makers can choose the service that best fits with their agency missions and priorities.



Secure internet and web gateway as a service

Zscaler Internet Access delivers a completely integrated gateway that inspects all ports and protocols, even across SSL.

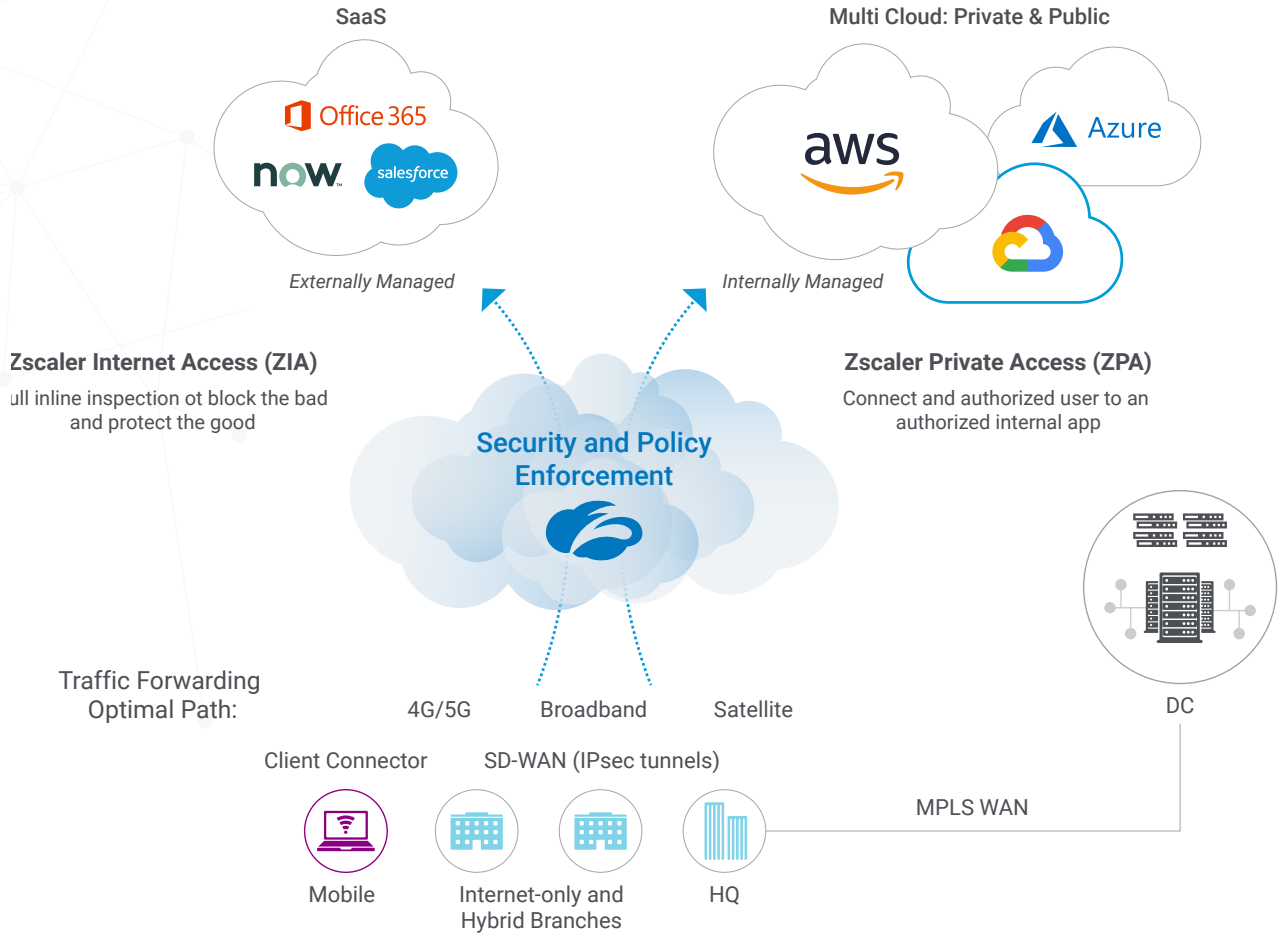
ACCESS CONTROL	THREAT PREVENTION	DATA PROTECTION
Cloud Firewall	IPS/Adv. Protection	Data Loss Prevention
URL Filtering	Cloud Sandbox	Cloud Apps (CASB)
Bandwidth Control	Antivirus	File Type Control
DNS Filtering	DNS Security	

Just point your traffic to the Zscaler cloud. For offices, you can set up a tunnel from your edge router. For mobile, you can use our Client Connector or a PAC file.

1 Has the Cloud Security platform been IRAP assessed?

Why this matters: It's one thing for a vendor to say their services are secure enough for sensitive agency data. It's another to have third-party verification that solutions and services comply with within a consistent framework of standards.

For government it is imperative that the Cloud Security platform has been independently validated as being compliant in support of Australian Government security policy. The IRAP assessment validates the organisation to best support the Australian government as it strengthens public sector cloud security posture to protect employees and citizens.



2 Does the service scale, and does scaling in any way cause outages?

Why this matters: Cloud-native and resilient services mean fewer interruptions to the mission, plain and simple. Therefore, you need to first know if the service scales. Then you need to know if scaling will cause outages. For example, if you change the service from 100 megabit, provisioning to 150, you may have to schedule an outage. It takes time and effort to implement the updates. Often, updates to the legacy infrastructure require an outage window, which is downtime for your users. That can quickly become untenable as you work among different sites.

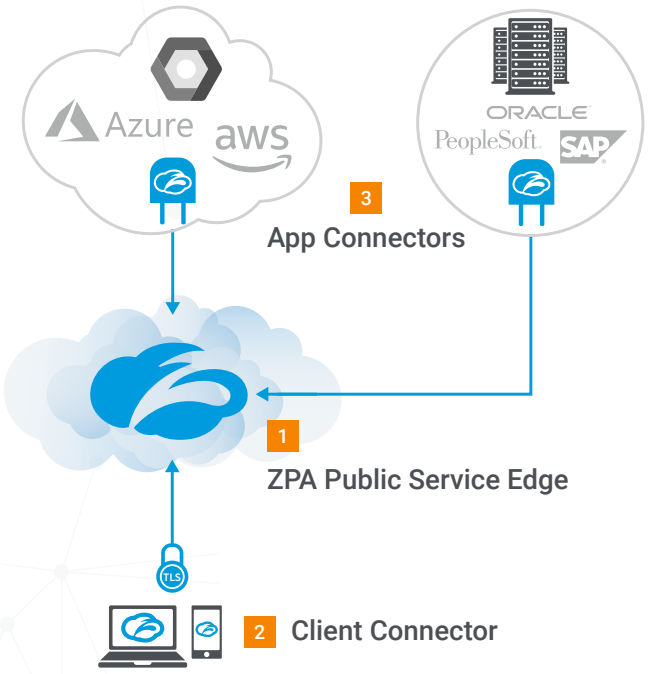
A true multi tenant platform that scales reduces outages. The upgrades happen automatically on behalf of the customer. No time or effort is spent on the update process and no downtime occurs as a result of the continuous updates. This is why choosing a cloud-native service is important.

3 Is the service zero trust by default?

Why this matters: Zero trust security by default means the system is designed from the start with zero trust principles. Identity verification is required from everyone trying to gain access to the system and each user, per application, is specifically granted access via policy. All other connections are denied by default. This added layer of security prevents data breaches and secures agency data.

A service that does not provide zero trust as the default will require additional configuration, architecture, and design—which can significantly increase costs due to complexity.

If you are looking at a legacy system that does not do zero trust by default, find out how many professional services hours per user and location it will cost.



Zero Trust Architecture

1 ZPA Public Service Edge
- Brokers a secure connection between Client Connector and an App Connector
- Hosted in cloud
- Used for authentication
- Customizable by admins

2 Client Connector
- Mobile client installed on devices
- Requests access to an app

3 App Connector
- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections

4 How does the solution peer with SaaS providers?

Why this matters: Knowing how your data moves improves performance. Cost and performance are impacted by several factors, including the number of peering locations, the number of peering content providers, and whether the service provider has peering with SaaS providers (like Microsoft and Salesforce).

A service hosted in a single cloud provider will have all traffic hair-pinning through that provider, regardless of where the application is hosted. Look for a service that is hosted in major internet exchange colocation data centers that provide direct peering to Google, AWS, Azure, and Tier 1 ISPs. Look for support for efficient traffic (peering) routing per application to the closest cloud data center based on the application accessed, including Office 365.

5 How long does it take/how much does it cost to set up a proof of concept?

Why this matters: If the company says they can set up proof of concept/value quickly, that speaks to the tool being cloud-native and resilient. If the company says it's going to take eight weeks to investigate and there will be an additional cost, then the service is likely not easy to scale.

Look for these warning signs that a system will be difficult to manage, configure, and scale:

- Logs are sent uncompressed, with duplicate fields, and force you to pay for log transfer and bandwidth.
- Pilots/test drives are time-consuming and last up to eight weeks. It should be easy, like the ability to stand up a pilot by a single systems engineer in a couple of days.
- Cloud SLAs include a clause for "unplanned maintenance," which indicates the service will periodically be unavailable.

6 How does it interact with Office 365? Is it easy to configure? How does it perform?

Why this matters: NNearly every federal agency uses Office 365 to some extent, meaning hundreds of thousands of users rely on it for everything from creating documents to hosting team meetings. Any security-as-a-service solution must interact well with Office 365. It must be easy to configure and it must perform. If configuration isn't seamless, you will again be looking at pro service hours to get it working.

It is important to ask what the standard latency to Office 365 is, and if it is enabled by default to whitelist Office 365 from SSL inspection, to auto-whitelist communication with Office 365 service IPs using MSFT API, and to auto-enable optimization for TCP optimizations. Ask also if the provider is peered with Microsoft..

7 What is the experience like for mobile users?

Why this matters: Mobile devices are ubiquitous within the government, and they need to perform as well as desktop devices. Whether a user is deployed in the field or working from home, they need to be able to access video conferencing and other high-bandwidth apps.

Ask about configuring the service for mobile devices: will there be additional costs for decrypting that bandwidth? Does split tunneling make you less secure? Will you be forced to use IPSec tunnels on mobile? Does the VPN client have support for split-tunneling on iOS and Android? If not, you may be forced to pay for video streaming to and from your locations.

Conclusion

Asking these seven questions will help you determine whether your security provider truly has a cloud-native platform that is dynamic, scalable, and resilient. This is essential to your organisation's cloud future, is needed to accelerate your digital transformation, and ensures you meet your agency's long-term needs.

Don't settle for a forklift of old appliances to the cloud. This could impact your operations, scale, and ability to meet agency demands. Knowing what the additional costs are upfront, as well as the cost of implementation and operations, will help you plan for a more secure and truly native cloud environment.

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.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com