tdmgroup
we make IT possible
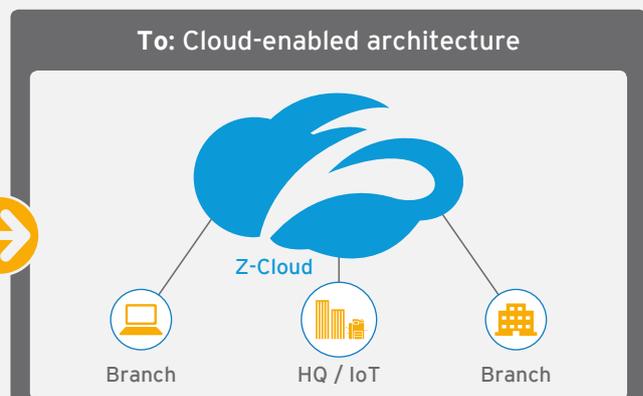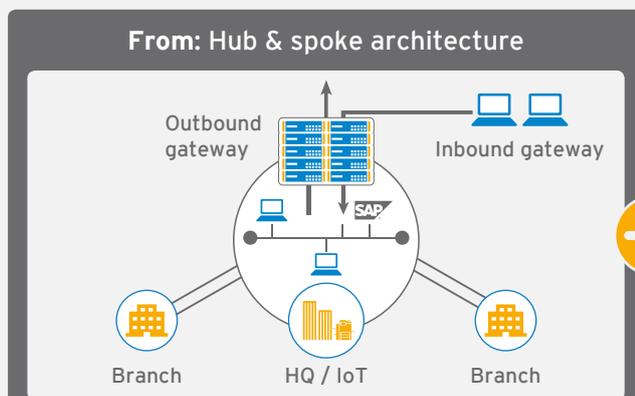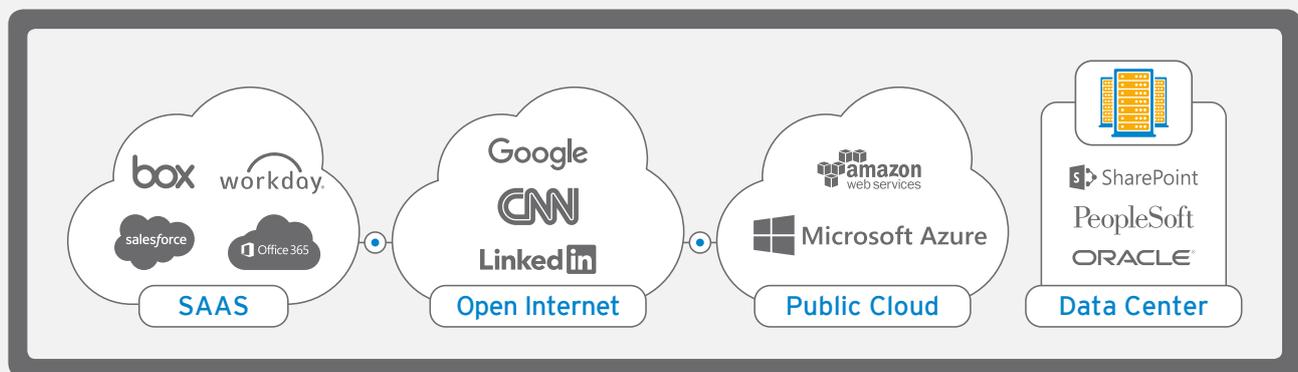
zscaler®
The Cloud Security Company

Zscaler – Enabling your secure transition to the cloud

Your applications are moving to the cloud – Salesforce, Office 365, AWS, and Azure – but your security appliances are still sitting on-premise, protecting your corporate network.

Now there's a cloud-based approach to security as a service, with a Zscaler solution from TDM Group. Through software-defined policies, not networks, Zscaler securely connects the right user to the right app or service. While it's doing so, it delivers automated threat forensics and dynamic malware protection against advanced cyber threats, such as advanced persistent threats and spear phishing.

box, workday, salesforce, Office 365	Google, CNN, LinkedIn	amazon web services, Microsoft Azure	SharePoint, PeopleSoft, ORACLE
SAAS	**Open Internet**	**Public Cloud**	**Data Center**

From: Hub & spoke architecture

Outbound gateway
Inbound gateway
SAP
Branch   HQ / IoT   Branch

To: Cloud-enabled architecture

Z-Cloud
Branch   HQ / IoT   Branch

From	To
Secure the network to protect users and apps	Software-defined policies, not networks, connect users to apps
Internal app access requires network access	Access policies determine which apps are visible/hidden
All users must be on the network for protection	On-net or off-net, the protection is identical
Internet traffic must be backhauled (i.e. sent to the network backbone) for protection	Secure local Internet breakouts

Global 24/7 IT Outsourcing

Managed Cloud Services

Security Services

Communication and Networking

Professional Services

Why are so many enterprises making the switch to Zscaler?

Protecting users with a consistent and enforceable policy requires much more than simple URL or web filtering. Thousands of companies have already switched their IT security from appliances to the Zscaler Security Cloud, the largest security cloud in the industry. They are now experiencing benefits such as:

- A simplified approach to IT
- Optimum total cost of ownership
- Protection for mobile device users
- Unified security, not just point solutions
- Protection for employees out on the road
- Protection for the distributed enterprise
- Interactive, consolidated reporting in real-time
- Integration and consolidation of point products
- Improved user experience, with reduced network latency

Key benefits

Universally accessible:

The Zscaler cloud is always reachable from anywhere, at any time, from any device.

Scalable:

Efficiently add new features and scale to thousands of users.

Integrated:

Security and other services talk to each other, giving you the complete picture.

Comprehensive:

The Zscaler cloud scans every byte coming and going, including SSL and CDN traffic.

Intelligent:

The Zscaler cloud learns from every user and connection; a threat to one is blocked for all.

Global visibility:

See what's happening in near real-time with all your users, locations, services and applications, as well as threats blocked and attempted communications from botnet-infected machines.

Security for everyone on the network

Zscaler cloud security delivers all the services you need – antivirus, firewalls, sandboxes, URL filters, SSL inspection, and the rest – in a unified platform service from the cloud. It's airtight security without the cost and complexity of stacks of appliances.

Zscaler enables modern working practices while protecting your business. As the Zscaler security cloud is everywhere, positioned between every user and the Internet, it closes security gaps created by mobility and BYOD (bring your own device).

By virtue of its global scale, the Zscaler cloud can inspect every byte of traffic, coming and going, even if it's encrypted, to make sure nothing bad comes in and nothing good leaves. It delivers consistent inline protection, whether users connect from an office, coffee shop or airport, at home or abroad.

Zscaler Cloud Firewall –
Full next-gen firewall capabilities without the cost and complexity of appliances

Securely embracing the cloud and delivering a fast user experience requires local Internet breakouts, where Internet traffic leaves the corporate network at the remote site, via a locally connected Internet service provider. However, securing Internet traffic with traditional unified threat management and next-generation firewall appliances requires deploying stacks of security appliances in all locations. This approach is cost-prohibitive and extremely difficult to manage.

Zscaler Cloud Firewall enables fast and secure local Internet breakouts for all ports and protocols, without appliances. It scales elastically to handle all your cloud application traffic, and is an integral part of the Zscaler Cloud Security Platform, which brings the entire security stack closer to the user to ensure identical protection no matter where they connect.

Award-winning:
Zscaler named a leader for the 7th consecutive year on Gartner Magic Quadrant.

The Zscaler Cloud Firewall difference:

- Enables secure local Internet breakouts for all ports and all protocols without any appliances to deploy or manage.

- Reduces Multiprotocol Label Switching (MPLS) backhauling costs and eliminates the need for costly and time-consuming patch management, coordination of outage windows, and policy management.

- Provides security and access controls for Internet traffic on all ports to prevent advanced threats.

- Scales services elastically to handle SSL inspection and cloud application traffic requiring long-lived connections for a fast user experience.

- Logs every session and delivers near-real-time visibility and immediate policy enforcement across all users, all locations, all applications, all ports and all protocols from a single console.
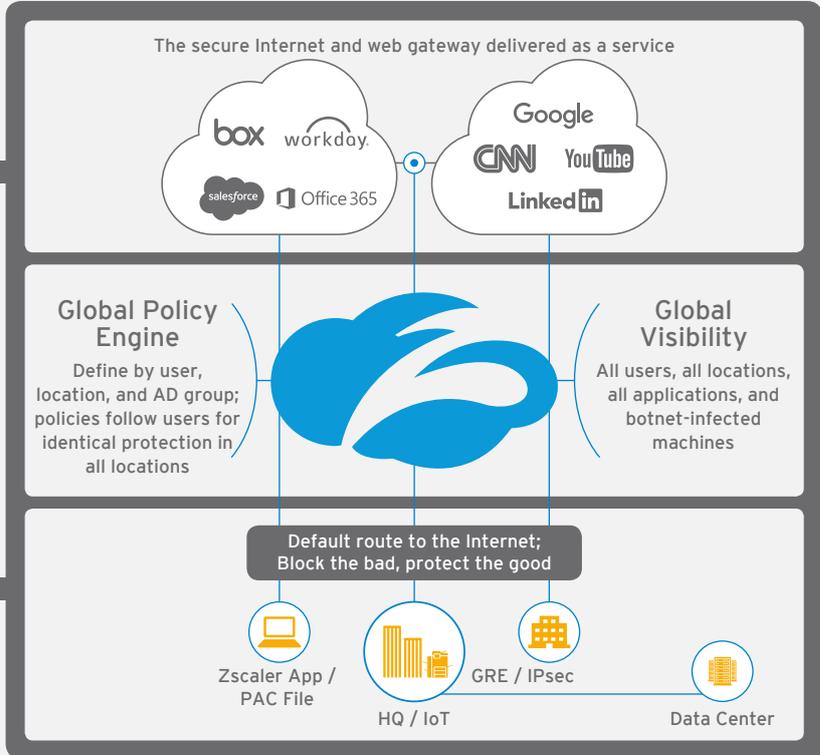
Application access and security –
Fast, secure policy-based access that connects the right user to the right service or application

The Zscaler platform is designed to replace your appliances at the inbound and outbound gateways.

Zscaler Internet Access

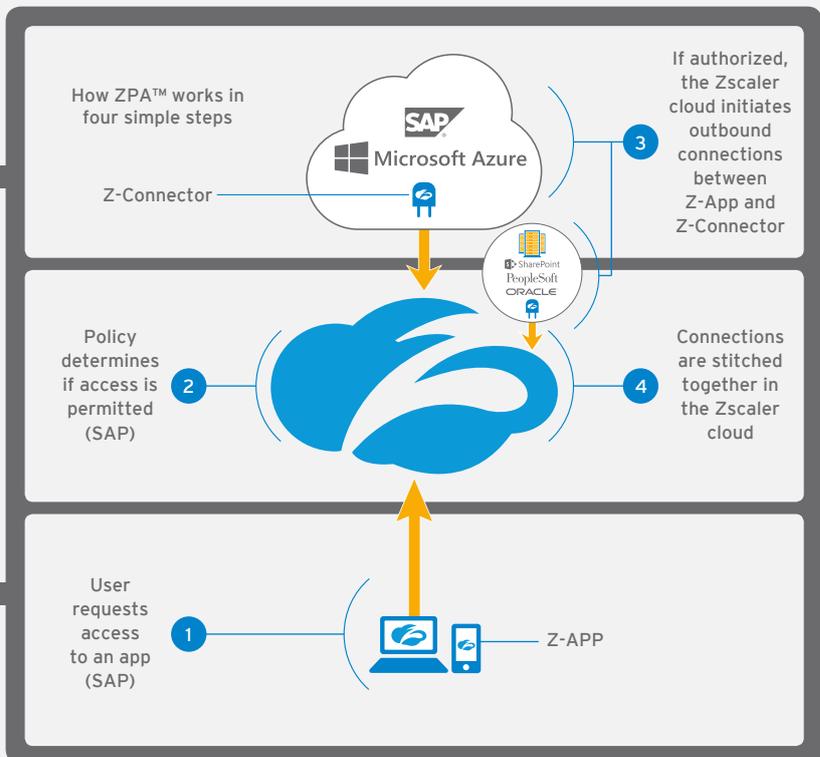**for fast, secure access to the Internet and SaaS apps**

Zscaler Internet Access provides secure access to the open Internet and SaaS apps, no matter where users connect. It provides inline inspection of all traffic to protect from threats and to secure corporate data assets.

The secure Internet and web gateway delivered as a service

box · workday · salesforce · Office 365

Google · CNN · YouTube · Linked in

Global Policy Engine
Define by user, location, and AD group; policies follow users for identical protection in all locations

Global Visibility
All users, all locations, all applications, and botnet-infected machines

Default route to the Internet;
Block the bad, protect the good

Zscaler App / PAC File

HQ / IoT

GRE / IPsec

Data Center

Zscaler Private Access

for fast, secure access to internal apps

Zscaler Private Access delivers a completely new way of providing access to internal applications, whether they reside in the data centre or in the cloud, without a virtual private network. It enables secure application access without network access, and without exposing apps to the Internet.

How ZPA™ works in four simple steps

SAP
Microsoft Azure
Z-Connector

3 If authorized, the Zscaler cloud initiates outbound connections between Z-App and Z-Connector

SharePoint · PeopleSoft · ORACLE

2 Policy determines if access is permitted (SAP)

4 Connections are stitched together in the Zscaler cloud

1 User requests access to an app (SAP)

Z-APP