Rethinking Security in a Cloud and Mobile World and Path to a Zero Attack Surface

Steve House, Sr. Vice President, Product Management, Zscaler
Steve Grossenbacher, Head of Product Marketing (ZIA), Zscaler
Leading experts agree

Zscaler named a **LEADER** in the **Gartner SWG MQ**

We do a lot more than SWG
(SWG is only 10% of use cases)

**Gartner**

“Legacy perimeter security simply won’t work and won’t scale for the requirements of digital business and digital government.”

---

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

1 Gartner, “Zero Trust Is an Initial Step on the Roadmap to CARTA,” Nov. 2018
Leading experts agree

Zscaler named a **LEADER** in the **Gartner SWG MQ**

Gartner **Secure Access Service Edge (SASE)**
**Market Guide**

“The enterprise perimeter is no longer a location; it is a set of dynamic edge capabilities delivered when needed as a service from the cloud”

Read at [zscaler.com/sase](http://zscaler.com/sase)
A proven and trusted partner of global brands

Zscaler = Zenith of scalability

Protection across countries

<table>
<thead>
<tr>
<th>Company</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siemens</td>
<td>185</td>
</tr>
<tr>
<td>A-B-In-Bev</td>
<td>150</td>
</tr>
<tr>
<td>Airfrance</td>
<td>113</td>
</tr>
<tr>
<td>ENGIE</td>
<td>70</td>
</tr>
</tbody>
</table>

Locations protected

<table>
<thead>
<tr>
<th>Location</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Church of Jesus Christ of Latter Day Saints</td>
<td>30,000</td>
</tr>
<tr>
<td>Kering</td>
<td>6,000</td>
</tr>
<tr>
<td>Petsmart</td>
<td>1,800</td>
</tr>
<tr>
<td>Kelly Services</td>
<td>900</td>
</tr>
</tbody>
</table>

Users protected

<table>
<thead>
<tr>
<th>User Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365</td>
<td>1.3M</td>
</tr>
<tr>
<td>MCNC</td>
<td>400K</td>
</tr>
<tr>
<td>Nestle</td>
<td>200K</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>120k</td>
</tr>
</tbody>
</table>

Office 365 monthly traffic

<table>
<thead>
<tr>
<th>Traffic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omnicom</td>
<td>78 TB</td>
</tr>
<tr>
<td>L'oreal</td>
<td>77 TB</td>
</tr>
<tr>
<td>Alstom</td>
<td>75 TB</td>
</tr>
<tr>
<td>Koch</td>
<td>60 TB</td>
</tr>
</tbody>
</table>

All Traffic – All Users – All Locations

<table>
<thead>
<tr>
<th>Sector</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conglomerates</td>
<td>2 of the top 3</td>
</tr>
<tr>
<td>Oil &amp; Gas Operations</td>
<td>4 of the top 8</td>
</tr>
<tr>
<td>Beverages</td>
<td>5 of the top 7</td>
</tr>
<tr>
<td>Apparel &amp; Accessories</td>
<td>3 of the top 4</td>
</tr>
<tr>
<td>Food Retail</td>
<td>6 of the top 12</td>
</tr>
</tbody>
</table>
Cloud and mobility: enablers, but disrupt networking and security

Old world

It started with cloud app adoption...

And that drives network transformation...

Which disrupts network security

Hub-and-spoke to DC

Network security

New world

Cloud + DC

Direct-to-cloud

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
Legacy data center

The **data center was the center of gravity**

Legacy network

Internal networks were built and optimized to connect users to apps in the data center

- **MPLS connects 100s of offices worldwide**
- **3–6 DCs with a few internet gateways**
- **VPN to connect mobile workforce (50%)**
Legacy castle-and-moat network security

Network security = secures the network to protect users and apps

Perimeter (moat) of appliances protects the network

And serves as gateways (drawbridges) to go in and out

You controlled: network, apps/data, users
Cloud breaks legacy networks and security

The cloud is the new data center

Backhaul traffic
Branch: MPLS / Mobile: VPN

Natural path
Direct-to-cloud

But, security is still sitting in the DC

Poor user experience

MPLS backhaul costs

Security risk

NotPetya
Can you do network security in the world of cloud?

How do you secure a network you don’t control?

Can’t build a “moat” around it with firewalls and proxies

How do you protect your users and apps?

A new approach to security is needed

Agnostic
Cloud
Network
Device
Zscaler: Securely transforms IT for a world of cloud
Fast, secure, and reliable access to your apps – to any cloud, over any network, on any device

**Legacy network**
- Hub-and-spoke – private

**Legacy security**
- Secure the network

**Security and Policy Enforcement**
- Zscaler Internet Access (ZIA)
  - Full inline inspection to block the bad and protect the good
- Zscaler Private Access (ZPA)
  - Connect an authorized user to an authorized internal app

**Traffic Forwarding**
- Optimal Path:
  - 4G/5G
  - Zscaler App
  - SD-WAN (GRE/IPsec tunnels)
  - Mobile
  - Internet-only and hybrid branches
  - MPLS WAN

**New network**
- Direct-to-cloud over any network

**New Security**
- Secure the Network
- Business policies securely connect users to apps
It’s a rare occasion in history where it got more secure, better, and cheaper all at once.

There is no more remote, on-network or off-network. You’re just a secure GE employee.

Chris Drumgoole
Chief Technology Officer, GE
ZIA: Fast, secure, and reliable access to the internet and SaaS
The best approach for secure SD-WAN and Office 365

Platform Services

Access Control
- Cloud Firewall
- URL Filtering
- Bandwidth Control
- DNS Resolution

Threat Prevention
- Cloud Sandbox
- DNS Security
- Proxy (Native SSL)
- Advanced Threat Protection

Data Protection
- Cloud DLP
- Exact Data Match
- CASB
- File Type Controls

Unprecedented visibility

Logs only written in memory and forwarded to a logging cluster in a geography of your choice

Log streaming to your SIEM / SOC

Security and Policy Enforcement

3rd party auth

4G/5G
Broadband
Satellite

MPLS WAN

Mobile
Internet-only and hybrid branches
HQ

New York
London
Sydney

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
ZPA: A modern adaptation of an age-old process

Anyone can call … and they do

Only those authorized are connected

Policies securely connect an authorized user to an authorized app

A modern approach

Remote users never brought on the corporate network:
- App access without network access

Apps are invisible:
- not exposed to the internet

Native app segmentation:
- microtunnels connect an authenticated user to an authorized app

Use cases:
- VPN replacement
- Multi-cloud access
- Third-party access
- M&A / Divestitures
ZPA: Fast and secure access to private apps
Best approach for web and non-web apps in multi-cloud environments

How it works:
1. A user requests access to an app
2. Policies determine if the user has access to the app
3. If allowed, the cloud establishes inside-out connections to a ZEN

A modern approach:
- Remote users never brought on the corporate network
- App access without network access
- Apps are invisible not exposed to the internet
- Native app segmentation microtunnels connect an authenticated user to a named app
What we eliminate

DC / Regional hubs

ZIA eliminates outbound gateways
ZPA eliminates VPN gateways

OUTBOUND SWG (protect users)

INBOUND VPN Server protection

What we enable

Secure local internet breakouts for every office and every mobile user

Remote access (VPN)

Global Network

Branch regional office

AutoNation

Avoided deploying firewalls in 300+ branches
Proprietary architecture built for unmatched protection and performance

Multi-Tenant Cloud Security Architecture

Control Plane
Policy Definition and Administration

Enforcement Plane
100+ Data Centers
6 Continents
Policy Follows the User

Logging Plane
USA
EU
Private
Nanolog
Streaming
SIEM

Policies follow the user for identical protection everywhere

Enforcement at the edge in 100 data centers to maximize performance

Scales elastically to handle spikes in traffic (company webcasts / sporting events)

Backed by over 100 patents
Modern partner ecosystem for cloud and mobility
Representative partners

Cloud Providers
- SaaS
- Internet Apps
- Multi-Cloud
- Data Center

Identity and Authentication
- Microsoft
- Okta
- Ping Identity
- OneLogin

Device Management | Protection
- Microsoft
- AirWatch
- VMware
- MobileIron

Security and Policy Enforcement
- New York
- London
- Sydney

Better value: Easy deployment & operations

Security Operations
- Splunk
- Sumologic

Branch (SD-WAN)
- Cisco
- VMware
- Silverpeak
A three-step journey to secure IT transformation

SECURE
Up-level security
Make Zscaler the next hop to the internet – no infrastructure change

SIMPLIFY
Remove multiple point products
Phase out gateway appliances, reduce cost and complexity

TRANSFORM
Direct-to-cloud architecture
Enable local internet breakouts (SD-WAN), better user experience, network savings

MARS
100,000 users / 85 countries

UNITED
80,000 users / 48 countries
Global data center footprint brings security close to the user

150
Data centers on six continents

70B+
Requests processed/day

100M+
Threats blocked/day

120K+
Unique security updates/day

Nestle, Siemens, and GE users are all secured by Zscaler DCs

Peering: https://www.peeringdb.com


Requests processed/day: 70B+
Threats blocked/day: 100M+
Unique security updates/day: 120K+
How customers use Zscaler

**Reduce business risk**
- Proxy replacement
- Mobile protection
- Zero-day protection (SSL/sandbox)
- Data protection (DLP-EDM)

**Local internet breakouts**
- Secure SD-WAN
- Office 365
- Faster user experience

**Private app access**
- VPN replacement
- Multi-cloud access
- Secure partner access
- Zero trust / segmentation
- M&A / Divestiture

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com
Thank You