Enabling Enterprise to Digitally Transform

Alex Simons
Corporate Vice President
Microsoft
Digital Transformation
Digital Transformation is an economic imperative
Digital Transformation
Wave of technology disruption

Four secular technology trends
Four secular technology trends

- Cloud: Many applications and services
- Devices: Many devices and applications
- IoT: Billions of devices and things
- Social: Many corporate & personal personas
CLOUD APPS AND SAAS SERVICES
MOBILE AND PERSONAL DEVICES
INTERNET OF THINGS (IOT) DEVICES

On-premises & web apps
On-premises & web apps
Intelligent Identity Control Plane

On-premises & web apps

Microsoft Azure AD
Digitally transforming the employee experience
Mary joins the team
Onboarding Information Workers
Mary joins the team

Information Worker Experience
Callie joins the team

Front Line Worker Manager’s Experience

My Staff
Managers of Front Line Workers can provision and configure users.

Provision and configure FLWs
Managers manage access, reset passwords, and add phone numbers.

Azure AD
DEMO
Select a location

Greeley Store 203

Dinelo Store 124
Digitally transforming the employee experience
Zscaler + Azure AD Integration

Secure your users and apps with Conditional Access and Identity Protection

- Azure AD
- ADFS
- MSA
- Google ID
- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP
- Corporate Network
- Geo-location
- Browser apps
- Client apps
- Client apps & Auth Method
- Physical & Virtual Location
- Trusted & Compliant Devices
- Employee & Partner Users and Roles
- Machine learning
- Real time Evaluation Engine
- Session Risk
- Policies
- Effective policy
- Controls
- Allow/block access
- Limited access
- Require MFA
- Force password reset
- Block legacy authentication
- Cloud SaaS apps
- On-premises & web apps
Microsoft Intune and Zscaler

Device compliance policy via Microsoft Conditional Access
Microsoft Cloud App Security and Zscaler
Complete Visibility and Control with In-band and Out-of-band CASB

Sanctioned Apps

Out-of-band App Intelligence

Unsanctioned Apps

In-band CASB
Access Control for out-of-band CASB

Microsoft Cloud App Security
Microsoft Azure Sentinel and Zscaler Integration*
The enterprise connectivity challenge

Enterprise last mile

ISP

 cabeza Office

On premises network

Hotel

Coffee shop

Home Office

Corporate MPLS WAN / Network perimeter

MPLS

Cloud Access Security Broker

Firewall / NGFW

Intrusion Prevention System

Data Loss Prevention

Secure Web Gateway

WAN Accelerator

Proxy Server

VPN

On premises network

Home Office

Hotel

Coffee shop

Enterprise last mile

Enterprise first mile

Microsoft global network

Network first mile

Other Cloud Services

Windows/Office Updates

Office 365
Office 365 connectivity principles

- Differentiate traffic
- Egress connections locally
- Optimize route length
- Assess network security

Microsoft Office 365 Network Partner Program (NPP) – Works with Office 365

Certified solutions follow these connectivity principles
Customer case study

- Egressing traffic from APAC clients in EMEA, via an inspecting, on-premises proxy stack & seeing very poor performance
- Egress changed to local breakout so local front doors can be used
- Tested using multiple sized file upload/download from/to OneDrive for Business hosted in an EMEA tenant

Download Times from Sydney (EMEA Tenant)

- 30MB Download Time (sec) via EMEA Proxy: 140 sec
- 12MB Download Time (sec) via AU Local Breakout: 40 sec
- 3MB Download Time (sec) (via EMEA Proxy)
Microsoft + Zscaler Demonstration

Patrick Foxhoven
CIO and VP, Emerging Technologies
Internet Destinations

Private Apps

Better value: Easy deployment & operations

CASB (out of band)
CLOUD APP SECURITY

Device Management | Protection

Security Operations
AZURE SENTINEL

Identity and Authentication
AZURE ACTIVE DIRECTORY

Microsoft + Zscaler

Office 365
A day in the life of a user of Microsoft and Zscaler…
Better value: Easy deployment & operations
Base VPN

* Connection type
  - Zscaler

Base VPN
3 of 6 settings configured

Automatic VPN
1 setting available
Microsoft Azure

Home > Microsoft > Enterprise applications > All applications > Categories > Add an application > Zscaler Internet Access Administrator

Categories
- Data services (151)
- Developer services (112)
- E-commerce (75)
- Education (150)
- ERP (93)
- Finance (262)
- Health (64)
- Human resources (297)
- IT infrastructure (198)
- Mail (35)
- Management (1)
- Marketing (214)
- Media (73)
- Productivity (282)
- Project management (84)
- Security (149)
- Social (109)
- Supply management (33)
- Telecommunications (96)
- Tools (82)
- Travel (84)
- Web design & hosting (54)

Add an application

Add your own app
- Application you're developing: Register an app you're working on to integrate it with Azure AD
- On-premises application: Configure Azure AD Application Proxy to enable secure remote access
- Non-gallery application: Integrate any other application that you don't find in the gallery

Add from the gallery

1 applications matched "Zscaler Internet Access (ZIA)"

NAME: Zscaler Internet Access (ZIA)
CATEGORY: Security

Zscaler Inc.

Use Azure AD to manage user access and enable single sign-on for Administrators to Zscaler Admin Portal. Requires an existing Zscaler Cloud subscription.

Use Microsoft Azure AD to enable user access to Zscaler Internet Access Administrator.

Requires an existing Zscaler Internet Access Administrator subscription.

Name:
Zscaler Internet Access (ZIA)

Publisher:
Zscaler Inc.

Single Sign-On Mode:
SAML-based Sign-on

URL:
https://www.zscaler.com/products/zscaler-internet-access

Logo:

Read our step-by-step Zscaler Internet Access Administrator Integration tutorial

Add
Add from the gallery

<table>
<thead>
<tr>
<th>NAME</th>
<th>CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zscaler Internet Access (ZIA)</td>
<td>Security</td>
</tr>
</tbody>
</table>

1 applications matched "Zscaler Internet".
Single Sign-On Mode

SAML-based Sign-on

URL
https://www.zscaler.com/products/zscaler-internet-access

Logo

Read our step-by-step Zscaler Internet Access Administrator integration tutorial

Add
Better value: Easy deployment & operations
Zscaler Private Access Connector enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. One half of Zscaler's Cloud platform, Zscaler Private Access (ZPA) provides secure, software-defined access to internal applications running on public cloud and within hybrid environments without the need for VPN. ZPA decouples application access from network access and delivers comprehensive visibility into user activity, enabling enterprises to embrace a zero trust strategy. ZPA automatically selects the fastest connection route for users, resulting in better performance when accessing Azure production environments. The Zscaler Connector is a lightweight VM that deploys within your Azure cloud instance or datacenter. The application connector front-ends your internal applications and sends an inside-out TLS-based connection to the Zscaler Cloud where the authorized user to internal app connection is stitched together based on customizable zero trust policies. The connector acts as a load balancer and can also help discover previously unknown applications.

Useful Links
Zscaler Private Access
Zscaler (NASDAQ: ZS) enables the world’s leading organizations to securely transform their networks and applications. Zscaler Internet Access™ and Zscaler Private Access™ create fast, secure connections between users and applications. These services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that your business needs. Zscaler's Cloud platform, Zscaler Private Access (ZPA) provides secure, software-defined access to internal application environments without the need for VPN. ZPA decouples application access from network access, and delivers complete control and automation capabilities to embrace a zero-trust strategy. ZPA automatically selects the fastest connection route for users, resulting in better application performance. The Zscaler Connector is a lightweight VM that deploys within your Azure cloud instance or datacenter. The connector acts as a load balancer and can send an inside-out TLS-based connection to the Zscaler Cloud where the authorized user is validated to ensure secure and customizable zero-trust policies.
Better value: Easy deployment & operations
PTD Request

Jay Claudin

Hi dear,

I hope this email finds you during business hours. Without further ado, you are hereby approved for this PTD request. 

Sincerely,

Jay Claudin
Doa, Chairman and Founder
Docado, The Leader in Cloud Security
PTO Request

- Jay Chaudhry <jay@zscaler.com>

Thursday, September 12, 2019 at 4:05 PM

- patrick

Show Details

Patrick,

This may surprise you but today I approved your first ever PTO request. Enjoy!

Jay Chaudhry
CEO, Chairman and Founder
Zscaler, The Leader in Cloud Security
Identity and Authentication

Device Management | Protection

Internet Destinations | Private Apps

CASB (out of band)

Cloud App Security

Microsoft + Zscaler

Office 365

Security Operations

Azure Sentinel

Identity and Authentication

Azure Active Directory

Better value: Easy deployment & operations
# Cloud Applications

## Cloud Application Trend

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Risk Level</th>
<th>Threat Index</th>
<th>Risk Index</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflix</td>
<td>Streaming Media</td>
<td>2</td>
<td>5.0</td>
<td>No Data</td>
<td>21.2</td>
</tr>
<tr>
<td>YouTube</td>
<td>Streaming Media</td>
<td>2</td>
<td>10.2</td>
<td>No Data</td>
<td>15.1</td>
</tr>
<tr>
<td>Facebook</td>
<td>Social Networking</td>
<td>5</td>
<td>9.4</td>
<td>No Data</td>
<td>6.4</td>
</tr>
<tr>
<td>iCloud</td>
<td>File Sharing</td>
<td>2</td>
<td>5.8</td>
<td>No Data</td>
<td>3.0</td>
</tr>
<tr>
<td>Gmail</td>
<td>Web Mail</td>
<td>35</td>
<td>3.7</td>
<td>No Data</td>
<td>3.8</td>
</tr>
<tr>
<td>Outlook</td>
<td>Web Mail</td>
<td>17</td>
<td>2.9</td>
<td>No Data</td>
<td>2.9</td>
</tr>
<tr>
<td>Slack</td>
<td>Collaboration and Online Meetings</td>
<td>4</td>
<td>3.8</td>
<td>No Data</td>
<td>2.94</td>
</tr>
<tr>
<td>Common Office 365 Applications</td>
<td>Productivity and CRM Tools</td>
<td>5</td>
<td>2.6</td>
<td>No Data</td>
<td>2.66</td>
</tr>
<tr>
<td>Google Search</td>
<td>Web Search</td>
<td>35</td>
<td>2.8</td>
<td>No Data</td>
<td>2.8</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Social Networking</td>
<td>2</td>
<td>2.5</td>
<td>No Data</td>
<td>2.7</td>
</tr>
<tr>
<td>Hulu</td>
<td>Streaming Media</td>
<td>1</td>
<td>2.1</td>
<td>No Data</td>
<td>2.1</td>
</tr>
<tr>
<td>Spotify</td>
<td>Streaming Media</td>
<td>11</td>
<td>1.8</td>
<td>No Data</td>
<td>1.8</td>
</tr>
<tr>
<td>SharePoint Online</td>
<td>Collaboration and Online Meetings</td>
<td>17</td>
<td>1.5</td>
<td>No Data</td>
<td>1.47</td>
</tr>
<tr>
<td>Amazon</td>
<td>Consumer</td>
<td>53</td>
<td>2.1</td>
<td>No Data</td>
<td>2.1</td>
</tr>
<tr>
<td>Box</td>
<td>File Sharing</td>
<td>11</td>
<td>1.8</td>
<td>No Data</td>
<td>1.8</td>
</tr>
<tr>
<td>GDrive</td>
<td>File Sharing</td>
<td>17</td>
<td>1.5</td>
<td>No Data</td>
<td>1.5</td>
</tr>
<tr>
<td>Yahoo Search</td>
<td>Web Search</td>
<td>35</td>
<td>1.4</td>
<td>No Data</td>
<td>1.4</td>
</tr>
<tr>
<td>Instagram</td>
<td>Social Networking</td>
<td>2</td>
<td>1.3</td>
<td>No Data</td>
<td>1.3</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>Hosting Providers</td>
<td>53</td>
<td>1.3</td>
<td>No Data</td>
<td>1.3</td>
</tr>
<tr>
<td>Salesforce</td>
<td>Productivity and CRM Tools</td>
<td>4</td>
<td>0.9</td>
<td>No Data</td>
<td>0.91</td>
</tr>
<tr>
<td>Twitter</td>
<td>Social Networking</td>
<td>2</td>
<td>0.8</td>
<td>No Data</td>
<td>0.8</td>
</tr>
<tr>
<td>Reddit</td>
<td>Social Networking</td>
<td>7</td>
<td>0.7</td>
<td>No Data</td>
<td>0.7</td>
</tr>
<tr>
<td>Dropbox</td>
<td>File Sharing</td>
<td>43</td>
<td>0.4</td>
<td>No Data</td>
<td>0.4</td>
</tr>
<tr>
<td>Zoom</td>
<td>Collaboration and Online Meetings</td>
<td>43</td>
<td>0.4</td>
<td>No Data</td>
<td>0.48</td>
</tr>
<tr>
<td>Hotstar</td>
<td>Streaming Media</td>
<td>43</td>
<td>0.3</td>
<td>No Data</td>
<td>0.3</td>
</tr>
</tbody>
</table>

## Social Networking Applications

### Microsoft Cloud App Security

- **Risk Level:** Medium
- **Risk Score:** 7
- **Data at Rest Security:** Not Supported
- **Admin Audit Trail:** HTTP Security Headers: content
- **Data Audit Trail:** Multi-Factor Auth:
- **HQ Location:** USA
- **Compliance Certifications:** Privacy Shield
- **PCI DSS**

## Streaming Applications

<table>
<thead>
<tr>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Hours</td>
</tr>
</tbody>
</table>

## Social Networking Users

### Transactions

<table>
<thead>
<tr>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Hours</td>
</tr>
</tbody>
</table>

## Streaming Users

<table>
<thead>
<tr>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Hours</td>
</tr>
</tbody>
</table>
Zscaler Corporate

Sorry, you don't have permission to visit this site.

Website blocked
Not allowed to browse MCAS Unapproved Apps category.
You tried to visit: https://firstrop.com

See our internet use policy.

Next steps: Contact your support team at mca@firstrop.com, https://firstrop.com
Sorry, you don't have permission to visit this site.

Website blocked

Not allowed to browse MCAS Unsactioned Apps category.

You tried to visit: https://filedropper.com

See our internet use policy.

Need help? Contact our support team at +1 (408) 890-2212, helpdesk@zscaler.com
• User moved from US to South Africa
• User accessing data exfiltration sites
Identity and Authentication

Device Management | Protection

Internet Destinations

Private Apps

CASB (out of band)

CLOUD APP SECURITY

Office 365

Security Operations

AZURE SENTINEL

Identity and Authentication

AZURE ACTIVE DIRECTORY

Better value: Easy deployment & operations
# Zscaler Threats Overview

### TimeRange: Last 7 days

<table>
<thead>
<tr>
<th>Threat name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML.Phish.Gen.KP</td>
<td>22011</td>
</tr>
<tr>
<td>HTML.Phish.Gen.HO</td>
<td>13023</td>
</tr>
<tr>
<td>HTML.Phish.Gen.NR</td>
<td>6668</td>
</tr>
<tr>
<td>HTML.Phish.Paypal.NR</td>
<td>3322</td>
</tr>
<tr>
<td>RETAIN_THREATNAME</td>
<td>2670</td>
</tr>
<tr>
<td>Win32.Trojan.ZBOT</td>
<td>1610</td>
</tr>
<tr>
<td>HTML.Malurl.Gen.XO</td>
<td>1614</td>
</tr>
<tr>
<td>Win32.PUA.Qiwormonk</td>
<td>1594</td>
</tr>
<tr>
<td>Win32.Trojan.Zbot.TZ</td>
<td>1155</td>
</tr>
<tr>
<td>HTML.Phish.Bankofamerica.NR</td>
<td>993</td>
</tr>
</tbody>
</table>

Results were limited to the first 250 rows.

### Blocked threats over time

![Blocked threats over time chart](chart.png)
## Zscaler Threats Overview

**Time Range:** Last 7 days

### Blocked Threats

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML.Phish.Gen.KP</td>
<td>22011</td>
</tr>
<tr>
<td>HTML.Phish.Gen.HO</td>
<td>13023</td>
</tr>
<tr>
<td>HTML.Phish.Gen.NR</td>
<td>6666</td>
</tr>
<tr>
<td>HTML.Phish.Paypal.NR</td>
<td>3322</td>
</tr>
<tr>
<td>RETAIN_THREATNAME</td>
<td>2670</td>
</tr>
<tr>
<td>Win32.Trojan.ZBOT</td>
<td>1610</td>
</tr>
<tr>
<td>HTML.Malurl.Gen.XO</td>
<td>1614</td>
</tr>
<tr>
<td>Win32.PUA.Qiwmonk</td>
<td>1594</td>
</tr>
<tr>
<td>Win32.Trojan.Zbot.TZ</td>
<td>1156</td>
</tr>
<tr>
<td>HTML.Phish.Bankofamerica.NR</td>
<td>993</td>
</tr>
</tbody>
</table>

Results were limited to the first 250 rows.

### Blocked Threats Over Time

- HTML.Phish.Gen.KP (Sun): 22k
- HTML.Phish.Gen.HO (Sun): 13k
- HTML.Phish.Gen.NR (Sun): 6.6k
Better value: Easy deployment & operations

Internet Destinations

Private Apps

Office 365

CLOUD APP SECURITY

CASB (out of band)

Device Management | Protection

Security Operations

AZURE SENTINEL

Identity and Authentication

AZURE ACTIVE DIRECTORY

Plus Conditional Access & SCIM
Use Azure AD to manage the creation and synchronization of user accounts in SCIM Demo based on user and group assignment.

- **Admin Credentials**

- **Mappings**
  - **Mappings allow you to define how data should flow between Azure Active Directory and customapp**
  - **Synchronize Azure Active Directory Groups to customapp**
    - Yes
  - **Synchronize Azure Active Directory Users to customapp**
    - Yes
  - **Remove default mappings**

**Settings**
Start and stop provisioning to SCIM Demo, and view provisioning status.

- **Provisioning Status**
- **Scope**
  - Sync only assigned users and groups

- **Current Status**
  - Incremental cycle completed
  - Click refresh to get the latest status
  - **[3]**

- **Statistics to date**
  - [3]
  - [1]
  - View provisioning details
  - View technical information

**View Audit Log**
Settings
Start and stop provisioning to SCIM Demo, and view provisioning status.

Provisioning Status: On/Off

Scope: Sync only assigned users and groups

Clear current state and restart synchronization

Current Status
Incremental cycle completed
Click refresh to get the latest status

100% complete

Statistics to date
Users: 3
Groups: 1

View provisioning details
View technical information

View Audit Logs
<table>
<thead>
<tr>
<th>ZPA Internal Group ID</th>
<th>SCIM Group Name</th>
<th>SCIM Group ID</th>
<th>Last Updated On</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Global Roaming Users - Relaxed Security</td>
<td></td>
<td>Sep 9th, 12:17 (PDT)</td>
</tr>
<tr>
<td>ZPA Internal Group ID</td>
<td>SCIM Group Name</td>
<td>SCIM Group ID</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Global Roaming Users - Relaxed Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Internet Destinations

Private Apps

CASB (out of band)

Secure App Access

Cloud App Security

Device Management | Protection

Office 365

Identity and Authentication

AZURE ACTIVE DIRECTORY

Better value: Easy deployment & operations

Security Operations

AZURE SENTINEL
Digital Transformation
Wave of technology disruption
Four secular technology trends
Thank You