Under the Hood of the Largest Security Cloud

Misha Kuperman, SVP Cloud Operations
Security platform – Born in the cloud, for the cloud

Zscaler Internet Access
Externally Managed Apps

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

Threat Prevention
- Advanced Protection
- Cloud Sandbox
- Antivirus
- DNS Security

Data Protection
- Data Loss Protection
- Cloud App Controls
- File Type Controls

Zscaler Private Access
Internally Managed Apps

Secure App Access
- Users never “on-net”
- Context-aware policy
- Dual encryption tunnels

App Segmentation
- User-to-app connection
- Prevent lateral movement
- Internal app visibility

App Protection
- Prevent DDoS
- Invisible apps
- Load balancing

Zscaler multi-tenant cloud security platform

Extensible through API for layering of additional services by Zscaler and partners

Built as proxy-based platform that enables full inspection
Zscaler code base and intellectual property

- **4.2 million** lines of code
- **155 thousand** code revisions
- **130+** issued and pending patents
A day in the life of the largest security cloud

**DAILY TRAFFIC**

- 3,500+ customers
- 1Tbps peak GBPS
- 2.5PB scanned

**DAILY PROTECTION**

- 120K updates/day
- 15 minutes & on-demand
  - 70B transactions
  - 2.4B blocked (4.4%)
  - 2.3B policies (4.2%)
  - 100M threats (0.2%)

**EXTERNAL SECURITY FEEDS**

- CLOUD SANDBOX
- SECURITY RESEARCH
- Google Safe Browsing
- Phishtank
- Snort
- IT ISAC
- Zeus Tracker
How we scale: Two years ago!

Baseline peak (934Gbps peak) - July 2019
Baseline peak (250Gbps peak) - July 2017
No legacy technology: Born and bred in the cloud

Building a cloud with single-tenant appliances

- Control
- Enforce
- Log

Sandbox
- C
- E
- L

DLP
- C
- E
- L

Full AV
- C
- E
- L

SSL Proxy
- C
- E
- L

LB
- C
- E
- L

IPS
- C
- E
- L

NGFW
- C
- E
- L

DNS
- C
- E
- L

X Increased latency

Would you build a power plant with home generators?

Home power generators

Power plant

- Disparate redundant control, logging, and enforcement policies
- Multiple appliances, multiple hops — slow user experience
- Expensive and complex to scale and manage
No legacy technology: Born and bred in the cloud

Building a cloud with single-tenant appliances

- Sandbox
- DLP
- Full AV
- SSL Proxy
- LB
- IPS
- NGFW
- DNS

Zscaler built from scratch a highly scalable and ultra-fast multi-tenant cloud security architecture

- 100+ data centers across 6 continents
- Integrated control, logging, and enforcement
- Single pass architecture — performance SLA and security efficacy
- Infinitely scalable — cost effective

Disparate redundant control, logging, and enforcement policies
- Multiple appliances, multiple hops — slow user experience
- Expensive and complex to scale and manage
Our code, our infrastructure,

No legacy technology: Born and bred in the cloud.

Building a cloud with single-tenant appliances

Zscaler built from ultra-fast multi-region data centers

- Single pass architecture — performance SLA and security efficacy
- Infinity scalable — cost effective
- Integrated control, logging, and enforcement
- Performance SLA and security efficacy
- Slow user experience
- Manage and enforce policies

- Increased latency
- Log
- Enforce
- Control
- Sandbox
- DLP
- Full AV
- LB
- IPS
FY2019 in review

Major adds to the cloud

17 new DCs online
Hong Kong, Sydney, Auckland, Seoul, Tokyo, Johannesburg, Beijing, New York, Atlanta, Stockholm, Los Angeles, London, Lagos, Manchester, Normandy, Vienna, Copenhagen

3,987 ZEN instances added to service

11 petabytes of Nanolog data

2Tbps of peering and 130 transit ports

FedRAMP, SOC2, ISO27001, ISO27018, CSTAR
Availability + Performance + Reliability
At Cloud Scale
Global presence – Local performance

Datacenter Usage - Transactions

Remaining 8.4%
Washington DC 6%
Tokyo 3%
Sydney 3.1%
Singapore 4%
Paris 1.5%
New York 0.1%

Amsterdam 7.4%
Atlanta II 2.4%
Chicago 7.4%
Delhi I 5.0%
Frankfurt IV 5.6%
Hong Kong III 2.2%
London III 7.4%
Mumbai II 2.0%

4.06 billion
5.16 billion
8.40 billion
5.18 billion

Datacenter Usage - Bytes

Remaining 7.7%
Washington DC 4.2%
Sydney 3.3%
Singapore IV 3.7%
San Francisco IV 1.9%
Paris II 4.0%
New York III 3.3%

Amsterdam 7.7%
Atlanta II 4.2%
Chicago 7.7%
Dallas I 7.7%
Frankfurt IV 6.2%
London III 7.7%
Los Angeles 2.6%
Mumbai II 2.4%

214 trillion
272 trillion
378 trillion
277 trillion

<table>
<thead>
<tr>
<th>Datacenter</th>
<th>Transactions</th>
<th>(Rx+Tx) Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Primavera</td>
<td>1.3 billion</td>
<td>0.2 billion</td>
</tr>
<tr>
<td>2 Atlanta II</td>
<td>2.84 billion</td>
<td>0.42 trillion</td>
</tr>
<tr>
<td>3 Auckland</td>
<td>200 million</td>
<td>0.08 billion</td>
</tr>
<tr>
<td>4 Beijing</td>
<td>164 million</td>
<td>0.07 billion</td>
</tr>
<tr>
<td>6 Brussels</td>
<td>738 million</td>
<td>0.57 billion</td>
</tr>
<tr>
<td>7 Copenhagen</td>
<td>135 million</td>
<td>0.08 billion</td>
</tr>
<tr>
<td>8 Chennai</td>
<td>1.77 billion</td>
<td>0.11 billion</td>
</tr>
<tr>
<td>9 Chicago</td>
<td>5.06 billion</td>
<td>0.71 billion</td>
</tr>
<tr>
<td>10 Hong Kong III</td>
<td>591 million</td>
<td>0.76 billion</td>
</tr>
<tr>
<td>11 Johannesburg II</td>
<td>520 million</td>
<td>0.58 billion</td>
</tr>
<tr>
<td>14 Kuala Lumpur</td>
<td>1 million</td>
<td>0.04 billion</td>
</tr>
<tr>
<td>15 London III</td>
<td>51.8 million</td>
<td>2.54 billion</td>
</tr>
<tr>
<td>16 Los Angeles</td>
<td>1.46 billion</td>
<td>0.13 billion</td>
</tr>
<tr>
<td>19 Madrid</td>
<td>465 million</td>
<td>0.29 billion</td>
</tr>
<tr>
<td>20 Milan</td>
<td>577 million</td>
<td>0.31 billion</td>
</tr>
<tr>
<td>22 Mexico III</td>
<td>1.16 billion</td>
<td>0.62 billion</td>
</tr>
<tr>
<td>23 Milan II</td>
<td>634 million</td>
<td>0.44 billion</td>
</tr>
<tr>
<td>24 Moscow II</td>
<td>430 million</td>
<td>0.36 billion</td>
</tr>
<tr>
<td>25 Miami</td>
<td>1.73 billion</td>
<td>0.57 billion</td>
</tr>
<tr>
<td>26 New York II</td>
<td>605 million</td>
<td>0.24 billion</td>
</tr>
<tr>
<td>27 New York III</td>
<td>4.24 billion</td>
<td>1.61 billion</td>
</tr>
<tr>
<td>28 Osaka</td>
<td>267 million</td>
<td>0.22 billion</td>
</tr>
<tr>
<td>29 Paris II</td>
<td>3.15 billion</td>
<td>1.85 billion</td>
</tr>
</tbody>
</table>
Inside Zscaler’s DC 4.0

- Massive terabit core network
- Standardized building blocks
- Support a minimum of 200Gbps of service
- Supports minimum 8 clusters of 25Gbps
- Order, deploy, provision
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

Peer with content and service providers

Office 365 DC peering

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

   Peering: https://www.peeringdb.com
Designed for high availability at every layer

### Cloud level
100+ data centers

- Intelligent failover and automatic fault management across DCs

### Data center level
- Clustering
  - N+1 redundancy within data center
  - N+2 redundancy for policy & logging – real-time replication

### Component level
- System resiliency
  - Integrated load balancers
  - Redundant routers and switches
  - RAID storage, multiple power supplies
Service performance

Traditional service chaining

- Different vendors
- Different UIs and policies
- Looking for different things

Zscaler Enforcement Node

- One vendor
- One UI
- One action
- ZERO copies
Ensuring performance and security – Our network

Zscaler customers

Customer transit providers

orange

BT

verizon

Zscaler transit providers

CenturyLink™

NTT

T

TELSTRA
gtt

Zayo

Internet exchange

Cloud services

Google

aws

Office 365

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
Helping our customers stay compliant
Our code, our infrastructure, our network

- Critical part of customer environment
- Partner to support customer business need
- Simplify compliance and audit

Compliance/Certification is a business enabler!
Zscaler growth over time

Annual YoY growth
56% transaction increase
68% traffic bytes increase

Zscaler cloud 1H FY18 summary
- Processed: 5.4 trillion transactions
- Stopped: 13.5 billion threats (0.25%)
- Enforced: 145 billion policies (3.2%)

Zscaler cloud 1H FY19 summary
- Processed: 8.1 trillion transactions
- Stopped: 10 billion threats (0.12%)
- Enforced: 380 billion policies (4.75%)
Measuring success – Transaction-to-ticket trends

**Monthly transaction volume**

**Tickets/billion transactions**

[Bar charts showing Zscaler Quarterly Transactions and Support Tickets Per Billion Transactions over Q2'15 to Q4'19]
Cloud Built for Applications and Performance
Defense in depth – Full inline scanning

Full SSL inspection

Destination-based blocking
Intrusive content control
Complete packet ByteScan
Browser control
Risk-based scoring
Sandboxing

Malicious hosts, sites, botnets phishing, GEO, protocol & ACLs
File, user, group and QoS control, signature-based AV and IPS
Web content scanning, risk-based analysis, app control
Dynamic & behavioral analysis of user content

DNS security

Botnet and callback detection

DLP security

Command & control (C2)
Remote control, additional malware downloads

Action on objectives
Lateral movement, data exfiltration, disruption, etc.

Delivery
Via trusted/untrusted sites and web content

Exploitation
Payload exploits unpatched vulnerability

Installation
Installing malware onto asset

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
Key Takeaways
Born in the cloud, full ownership of the cloud
Not cloud-washed

Control our application

Control our infrastructure

Control our network

End-to-end control of all aspects!
ENGAGE  |  In an open forum with Zscaler employees, partners, and customers

SHARE  |  Your knowledge and learn from experts in cloud security

JOIN  |  The conversation at community.zscaler.com
Thank you