What’s New in ZIA!
Zscaler Cloud Scales: >1.6 Trillion Transactions per month!

~ 5X Growth over 4 years!!

Billions of Transactions

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
World’s Largest Security Cloud

100 data centers across 6 continents

70B+ Requests processed/day
100M+ Threats blocked/day
120K+ Unique security updates/day

Internet Peering across 150 Vendors

Secure
Ongoing third-party testing

Reliable
Redundancy within and failover across DCs

Transparent
Trust portal for service availability monitoring

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

★ Recently Added
Analytics & Configuration
New Reports and Insights
New Reports and Insights

Cloud Sandbox
7,650 files sent to Sandbox for analysis by Acme Inc. Your subscription does not allow protection of all file types

- 70 B Total Transactions
- 52.72 B Transactions with Files
- 12.6K Unwanted Files FOUND
- 7.65 K Malicious Files Blocked
- 151 Malicious Files Blocked

Malicious Files Blocked By Files:
- ZIP: 40%
- EXE: 21%
- DLL: 35%
- DLLBin: 3%
- EXE64: 18%

Zscaler
Executive Insights

- Insights into critical usage for Acme Corporation.
- Over 99% of all transactions processed by Zscaler for Acme Corporation were blocked due to threats and policy violations.
- 4.11% of the traffic was blocked.
- The locations to bandwidth ratio is 1:1.

Threats Stacked and Policy Violations

- The overall traffic for Acme Corporation has decreased by 0.3% in the last year.
- Policy violations have decreased by 3.3% in the last year.
Executive Insights App

- Exec summary
- Significant changes
- Share widgets
- Notifications
- Curated content and news for Execs
Web Insights Improvements

- Improved UX
- Client-side filter & search
- Sort by most recent
Top Level Domain Control

- Custom Top Level Domain categories
Top Level Domain Control

- Custom Top Level Domain categories
- URL filtering rules to whitelist or blacklist TLDs
Core Platform Enhancements
ZIA Integrations
Strengthen Security and Lower TCO with Automation and Simplification

<table>
<thead>
<tr>
<th>SOAR</th>
<th>Threat Intel</th>
<th>CASB</th>
<th>IDAM</th>
<th>SD-WAN</th>
<th>Firewall Mgmt</th>
<th>Endpoint (EPP, UEM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>splunk &gt; phantom&lt;br&gt;LogicHub&lt;br&gt;exabeam&lt;br&gt;DEMIStO&lt;br&gt;SWIMLANE</td>
<td>bitglass&lt;br&gt;ANOMALI&lt;br&gt;INTSIGHTS</td>
<td>Microsoft&lt;br&gt;okta&lt;br&gt;Ping&lt;br&gt;skyhigh</td>
<td>Microsoft&lt;br&gt;CITRIX&lt;br&gt;aruba&lt;br&gt;onelogin</td>
<td>silver peak&lt;br&gt;CloudGenix&lt;br&gt;riverbed</td>
<td>CROWDSTRIKE&lt;br&gt;SKYBOX SECURITY&lt;br&gt;CARBON BLACK&lt;br&gt;SentinelOne</td>
<td></td>
</tr>
</tbody>
</table>
Cloud IPS

• 15,000+ IPS signatures for web and non-web traffic
• Security for all users on all ports & protocols with Ztunnel 2.0
Cloud IPS

- 15,000+ IPS signatures for web and non-web traffic
- Security for all users on all ports & protocols with Ztunnel 2.0
Cloud IPS

- 15,000+ IPS signatures for web and non-web traffic
- Security for all users on all ports & protocols with Ztunnel 2.0
- Real-time, granular control and visibility
DLP Policy Enhancements

- Extended support for content extraction
- New preconfigured dictionaries
DLP Policy Enhancements

- Extended support for content extraction
- New preconfigured dictionaries
- Schedule EDM data refresh
DLP Incident Reporting Enhancements

Incident Tracking ID, DLP content MD5 in Web Insights, NSS logs, Auditor Notification, ICAP
DLP Incident Reporting Enhancements

Incident Tracking ID, DLP content MD5 in Web Insights, NSS logs, Auditor Notification, ICAP
DLP Incident Reporting Enhancements

Incident Tracking ID, DLP content MD5 in Web Insights, NSS logs, Auditor Notification, ICAP
Match count in Web Insights, NSS logs, Auditor Notification
Access to our threat research
Searchable threat database
Detailed threat descriptions
Threat severity & score
Threat Library

Access to our threat research
Searchable threat database
Detailed threat descriptions
Threat severity & score

Threat Severity

- All
- Critical (90-100)
- High (60-89)
- Medium (30-59)
- Low (0-29)

VBS.Downloader.Agent
VBS.Downloader.Agent is a Downloader that targets the VBS platform. It is designed to download additional malicious payloads.

Agent refers to a group of generic Trojans that maintain persistent system. Agents leverage system resources to download additional stolen sensitive information to a third party attacker.

Category: Botnet Callback
Direction: Outbound
Engine: IPS (web)

Threat Score: 78
Severity: High
Signature ID: 54460
Threat Protection Improvements

- Add ML Findings to Sandbox Detail Report
- OS chaining – detonate on multiple VMs
- Windows 10 support
- Granular policy support of new archive types
- Expanded NRD metadata
- Blocking HTTP RFC non-compliant traffic
- New Ransomware category
IoT

Build fingerprinting engine and classification DB

Publish ThreatLabZ IoT reports

Global Cloud IoT insights on Zscaler.com
In an open forum with Zscaler employees, partners, & customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com
Thank You