Advanced DLP that Works in a Mobile-First World

Moinul Khan, Sr. Director Product Management, Zscaler
The traditional approach to data loss prevention (DLP)

Classification on endpoints
- Requires immense compute power

Classification by end users
- Not reliable, either mark everything or nothing sensitive

Classification on network
- Too noisy with many false positives and requires backhauling

Sensitive data is now everywhere in the cloud
Our mobile-first world has changed the rules of the game
Users connect directly to apps in the cloud

83% of enterprise workloads will be in the cloud by 2020¹

73% of enterprises will run almost entirely on SaaS by 2020, report says²

70% of professionals do some work remotely and connect directly to the cloud³

70% of web traffic is encrypted⁴

Your data protection strategy requires transformation

1. Purpose-built architecture for scale and performance
2. Context- and content-aware inspection engine for visibility and enforcement
3. Protection across all cloud channels
Zscaler Data Protection Architecture
Global footprint brings data protection close to the user

150 DCs  Unified policy  Always on  Data residency

- Global footprint brings data protection close to the user
- Peering with content and service providers
- 150 DCs
- Unified policy
- Always on
- Data residency

Peering: https://www.peeringdb.com
Zscaler’s Data Protection Engine in the Cloud
Visibility with full context and content inspection

SSL decryption
- Power Point
  - file type
- prodmgmt
  - group
- shouse
  - user

SSL protocol
- upload
  - app function

HTTPS protocol
- "Confidential"
  - content
- jumpshare
  - application
- file sharing
  - URL category

Firewall or Proxy
- 172.16.1.12
  - source IP
- TCP/443
  - destination port
- 64.81.2.24
  - destination IP

57 MB
Zscaler data protection

1. Context driven
   - File type control
2. Cloud app control
   - Content driven
3. Data loss prevention

Granular policy control & reporting in ZIA Platform
Best Practices for Leveraging Zscaler Data Protection
Leverage file type controls

- Basic data protection
- True file type detection
- Control over outbound and inbound traffic
- Allow, block or provide caution
- Multicriteria framework
Use cloud application control

- Design sanctioned and unsanctioned data flows
- Restrict specific action
# Leverage content inspection dictionaries

<table>
<thead>
<tr>
<th>Content Inspection Technology</th>
<th>Content Inspection Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regex</td>
<td></td>
</tr>
<tr>
<td>Preconfigured Data Patterns</td>
<td>Described content</td>
</tr>
<tr>
<td>Single multiword keywords with proximity</td>
<td></td>
</tr>
<tr>
<td>Pre-trained engines</td>
<td>Trained data sets</td>
</tr>
<tr>
<td>Structured fingerprints (EDM)</td>
<td>Fingerprinting</td>
</tr>
</tbody>
</table>

## DLP Dictionary

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Dictionary Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ABA Bank Routing Numbers</td>
<td>Names (US)</td>
</tr>
<tr>
<td>2</td>
<td>Adult Content</td>
<td>National Health Service Number (UK)</td>
</tr>
<tr>
<td>3</td>
<td>Citizen Service Numbers (Netherlands)</td>
<td>National Insurance Numbers (UK)</td>
</tr>
<tr>
<td>4</td>
<td>Credit Cards</td>
<td>NRIC Numbers (Singapore)</td>
</tr>
<tr>
<td>5</td>
<td>Financial Statements</td>
<td>Salesforce.com Data</td>
</tr>
<tr>
<td>6</td>
<td>Gambling</td>
<td>Social Insurance Numbers (Canada)</td>
</tr>
<tr>
<td>7</td>
<td>Illegal Drugs</td>
<td>Social Security Numbers (US)</td>
</tr>
<tr>
<td>8</td>
<td>Individual Taxpayer Registry ID (Brazil)</td>
<td>Source Code</td>
</tr>
<tr>
<td>9</td>
<td>Medical Information</td>
<td>Standardized Bank Code (Mexico)</td>
</tr>
<tr>
<td>10</td>
<td>Medicare Numbers (Australia)</td>
<td>Tax File Numbers (Australia)</td>
</tr>
<tr>
<td>11</td>
<td>Names (US)</td>
<td>Weapons</td>
</tr>
</tbody>
</table>
Precise detection with Exact Data Match

Content inspection using data fingerprints

- Fingerprint tabular data

- Zscaler enforces policy inline globally using data hash

- Works on all web-bound traffic

SSN  First Name  Last Name  ZIP Code
736565416  Johnny  Cage  90007

PC

SSN  First Name  Last Name  ZIP Code
4716653795988590  Johnny  Cage  90007

Rewards/ Membership Info

Last Name  Email  Rewards ID
Lee  L_lee@gamil.com  8315EGJ51

Product/ Inventory Codes

Design  Prod-Code
Lifestyle  NK-LF-009

Hash cells on-premise

Only hashes, never plain text

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
Precise detection with Exact Data Match

Mobile user sharing customer credit card info via HTTPS

1. SSL intercepted, content available for inspection
2. DLP policy applied
3. EDM rule triggered based on matching hash
4. Content blocked
5. Incident remediated via integration with GRC
Enforce Policies in all Cloud Channels
Inline enforcement

Block all other users from transferring credit card numbers to any cloud application.

Allow finance to transfer credit card numbers to Salesforce.

Block internal Word, Excel, PowerPoint and PDF documents.
Why Zscaler?
Slowly migrate from your existing to your new world.

Single data protection & threat prevention engine for all cloud channels.

Single pane of glass for visibility, monitoring and reporting.

Unified policies are enforced across all cloud channels.

Best end-user experience with traffic optimization and local breakouts.
Getting started with simple three use cases

Password protected files

Tagged information

Sensitive information

https://zscaler.wistia.com/medias/m9hl5u72o3

https://zscaler.wistia.com/medias/tv2a8jo3b6

https://zscaler.wistia.com/medias/wmshnwqi9v
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