Taking Security to the Next Level with Browser Isolation

Dhawal Sharma, Sr. Director PM, Zscaler
Understanding Browser Isolation

Key capabilities

“Air Gap” between the user and the actual web site

Physically isolates the user’s browser, machine and the network from the app

The web app is accessed and loaded on the remote browser and only the rendering of the webpage is served

Use cases

• Protects user’s devices from harmful content
• Sensitive data protection
• Malware and phishing threats are reduced
• VDI Replacement
“By 2022, **25%** of enterprises will adopt browser isolation techniques for some high-risk users and use cases.”

*Gartner*
# Top browser isolation use cases

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risky Internet content access</td>
<td>It is not always easy to decide whether to block or allow traffic to certain internet destinations.</td>
</tr>
<tr>
<td>Weaponized Documents</td>
<td>No more patient zero, all weaponized documents rendered remotely.</td>
</tr>
<tr>
<td>Phishing Protection</td>
<td>Phishing and Spear Phishing attacks could lead to loss of sensitive data if unidentified.</td>
</tr>
<tr>
<td>3rd Party Access</td>
<td>3rd party contractors and select outside users need access to critical internal applications of an organization.</td>
</tr>
<tr>
<td>Sensitive Internet App Access</td>
<td>Sensitive Internet apps hosting IP is always best kept behind lock and key.</td>
</tr>
</tbody>
</table>
• May 30th 2019  Zscaler announced acquisition of Appsulate

• Integration underway with Zscaler platform, available with ZIA as well as ZPA services.

• Fully agentless solution.

• Pixel streaming based technology.
The Zscaler Browser Isolation Architecture
Browser Isolation + Zscaler Internet Access
ZIA Integration Flow (Exec User/Unknown Web Page/Phishing Links)

1. User tries to access an uncategorized webpage via the ZIA-ZEN.

2. The ZEN evaluates the request against the defined policies, upon a match, redirects the request to the isolation platform with the original URL appended as a query string.

3. The browser follows the redirect and makes the connection to the Browser isolation endpoint in Zscaler cloud.

4. Zscaler Isolation Platform spins up a isolated browser in a container and makes a connection to the originally requested webpage.

5. Isolation browser loads the content after the same being inspected by the ZIA platform (optional).

6. The loaded web content is streamed to the end user’s native browser as pixels as HTML5 stream.
1. User Makes a request to download a document (PDF/WORD/Excel/PPT) from the internet via ZIA.

2. The ZEN Downloads the requested file from the internet destination.

3. The ZEN Identifies the file as "unknown" and forwards the same file to Zscaler Sandbox for further analysis.

4. The ZEN redirects the user to the isolation platform.

5. The isolation platform loads the potentially malicious file on the Isolated Browser.

6. The end-user sees the rendering of the original file on the native browser without having to download the same.
ZIA Integration policies

Example policies

Dedicated port-based location
ZIA Integration policies

Example policies

Dedicated port-based location

PAC file with dedicated proxy port
ZIA Integration policies

Available with Early Access

Example policies

Dedicated port-based location

PAC file with dedicated proxy port

Block and redirect policies
ZIA Integration policies

Available with Early Access

Example policies

- Dedicated port-based location
- PAC file with dedicated proxy port
- Block and redirect policies

Available with General Availability
Browser Isolation + Zscaler Private Access
1. BYOD/Contractor makes a request to an internal application, DNS cname of which points to the ZPA exporter.

2. The ZPA cloud redirects the user to the Isolation browser.

3. The user makes a connection to the isolation browser following the redirect.

4. The isolation browser establishes a connection to the internal application via the ZPA cloud and the App Connector and fetches the webpage.

5. Rendering of the webpage is served to the 3rd party contractor who needs access to the webpage.
Data Exfiltration Protection

1. User needs to access certain applications that host sensitive corporate data (e.g., financial data or has source code).

2. User’s request is redirected by the ZPA cloud to the Isolation platform.

3. The application loads in the Isolation browser for the user in a view only mode.

4. Any attempts to download files from the isolation platform or copy/paste of code or any other text from the isolation platform to user’s computer is blocked.
VDI Replacement

- Can function as VDI replacement for workflows that primarily rely on browser-based activity.
VDI Replacement

- Can function as VDI replacement for workflows that primarily rely on browser-based activity.
VDI Replacement

- Can function as VDI replacement for workflows that primarily rely on browser-based activity.
## Popular Features and Capabilities

<table>
<thead>
<tr>
<th>Security Controls</th>
<th>Usability</th>
<th>Media Support</th>
<th>Platform Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disable copy-paste to clipboard - Both Directions.</td>
<td>• Better UX- No double auth or inconsistent UX</td>
<td>• Support for Video streaming</td>
<td>• Wider Browser versions Supported – Isolation support for any desktop browser supporting HTML5.</td>
</tr>
<tr>
<td>• Disable download and upload of files to and from isolation browser.</td>
<td>• Agent or Plugin less isolation-client less traffic redirection</td>
<td>• Audio streaming.</td>
<td>• Pixel Rendering instead of DOM object rendering - Secure.</td>
</tr>
<tr>
<td>• ZIA Policy enforcement for isolated traffic</td>
<td>• Global Isolation platform - Isolation platform available spread across the globe.</td>
<td>• Rendering of PDF files in isolation before download.</td>
<td></td>
</tr>
<tr>
<td>• Trusted Application Isolation – Ability to force isolation on corporate SAAS applications.</td>
<td>• Session persistence- Personalized UX on the isolation browser.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Roadmap:

<table>
<thead>
<tr>
<th>Security Controls</th>
<th>Usability</th>
<th>Media Support</th>
<th>Platform Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Read only Access to webpages.</td>
<td>• Persist Bookmarks and favorites across isolation sessions.</td>
<td>• Rendering Microsoft Office Files on isolation browser.</td>
<td>• Support for Mobile Browsers – Display of webpages in mobile form factor and on-screen keyboard.</td>
</tr>
<tr>
<td>• Integration with sandbox - Rendering of Office and PDF files while in quarantine.</td>
<td>• Matching time zones between isolation platform and native machines.</td>
<td>• Convert webpages and documents to PDF for download.</td>
<td>• Ability to mirror user-agent based on the native browser.</td>
</tr>
<tr>
<td>• Ability to switch to incognito/anonymous mode.</td>
<td></td>
<td>• Ability to print documents from isolation browser.</td>
<td></td>
</tr>
</tbody>
</table>
Recommended Next Steps

• Visit ‘Browser Isolation’ demo pod on show floor.
• Sign up for early access for Browser Isolation
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