DATA SHEET

Zscaler™ Cloud Browser Isolation

Bringing your internet security to the next level

Zscaler Cloud Browser Isolation reduces web-based threats and protects executives and users with access to sensitive data from the risks of data exfiltration.

The challenge of unknown and risky web content

According to Gartner estimates, 98 percent of external attacks are carried out over the public internet and, of those attacks, 80 percent are targeted directly at end users through their browsers, making browsers the largest surface area for threats.

Executives, finance teams, and other high-risk functions are prime targets for hackers. They have access to the most sensitive information in an organization. Browser-based attacks hidden in webpages, vulnerable browsers, and malicious plugins provide a convenient means to deliver ransomware, phishing attacks, and other advanced threats, as well as to extract sensitive data. Many organizations struggle to give users access to the webpages they need to successfully run their business while still protecting them and reducing the potential for data exfiltration and damage to the organization.

But, blocking all potentially risky websites is not a practical approach to protecting users from web-based attacks as this approach can impede business productivity and negatively impact the user experience. It isn't always easy to determine which sites pose a threat and which do not. A fundamentally different approach to browser security is needed to give users the ability to browse and give you the confidence that your users are protected.

Eliminate web-based threats and protect sensitive data

Enabling business while still protecting users, networks, and data from risky or malicious web content is critical.

Zscaler Cloud Browser Isolation creates an isolated browsing session that enables users to access any webpage on the internet without having to download any of the web content served by the webpage onto the local device or the corporate network. With Zscaler Cloud Browser Isolation, users are not directly accessing active web content; instead, only a safe rendering of pixels is delivered to the user so malicious code that may be hidden is kept at bay. And since Cloud Browser Isolation is a 100-percent cloud-delivered service, you have no hardware or endpoint agents to deploy or manage.

Simply route internet-bound traffic for your high-risk employees to Zscaler Cloud Browser Isolation and it immediately creates an airgap between these users and the internet— establishing browser isolation sessions for questionable websites to protect your users against web-based threats and data exfiltration.

As an integrated component of Zscaler Internet Access™, the same level of security is applied across all traffic, irrespective of whether it originates in the native browser or browser isolation platform. All traffic is inspected by Zscaler Internet Access and defined corporate policies are applied, including data loss prevention and file-type policies. Combined, Zscaler Internet Access and Zscaler Cloud Browser Isolation take your security to the highest level.

Zscaler Cloud Browser Isolation benefits

With Zscaler Cloud Browser Isolation, your users can securely browse the internet without the hassle of managing additional endpoint agents or plugins on every device. Cloud Browser Isolation delivers a 100-percent cloud-based solution that eliminates the need to deploy custom hardware or software components within the customer environment. This approach fundamentally changes the way enterprises protect users, data, and critical business systems from web-based threats.
Zscaler Cloud Browser Isolation:

Eliminates web-based threats

- Protects executives and users who handle sensitive data from phishing attacks, ransomware, and other advanced threats
- Eliminates the threat of active content on your device
- Stops zero-day attacks and other web-based threats from ever accessing endpoint devices or the network
- Limits the ability of an attacker to move laterally and cause damage

Prevents data exfiltration

- Prevents users from activating targeted data theft attacks hidden in web pages, downloadable web content, and browser plug-ins
- Eliminates the threat of data exfiltration from phishing and spear phishing attacks
- Prevents outdated and vulnerable browsers, or even questionable and unsafe plug-ins from being leveraged to compromise the user's device or exfiltrate data
- Prevents users from exfiltrating sensitive data from business-critical applications

Integrates with Zscaler Internet Access

- Deploys in minutes, not months – simply by checking a box in configuration
- Eliminates the need for architectural changes and point product maintenance by delivering security as a cloud service
- Reduces operational cost and complexity
- Provides a uniform framework for policy definition, enforcement, and authentication

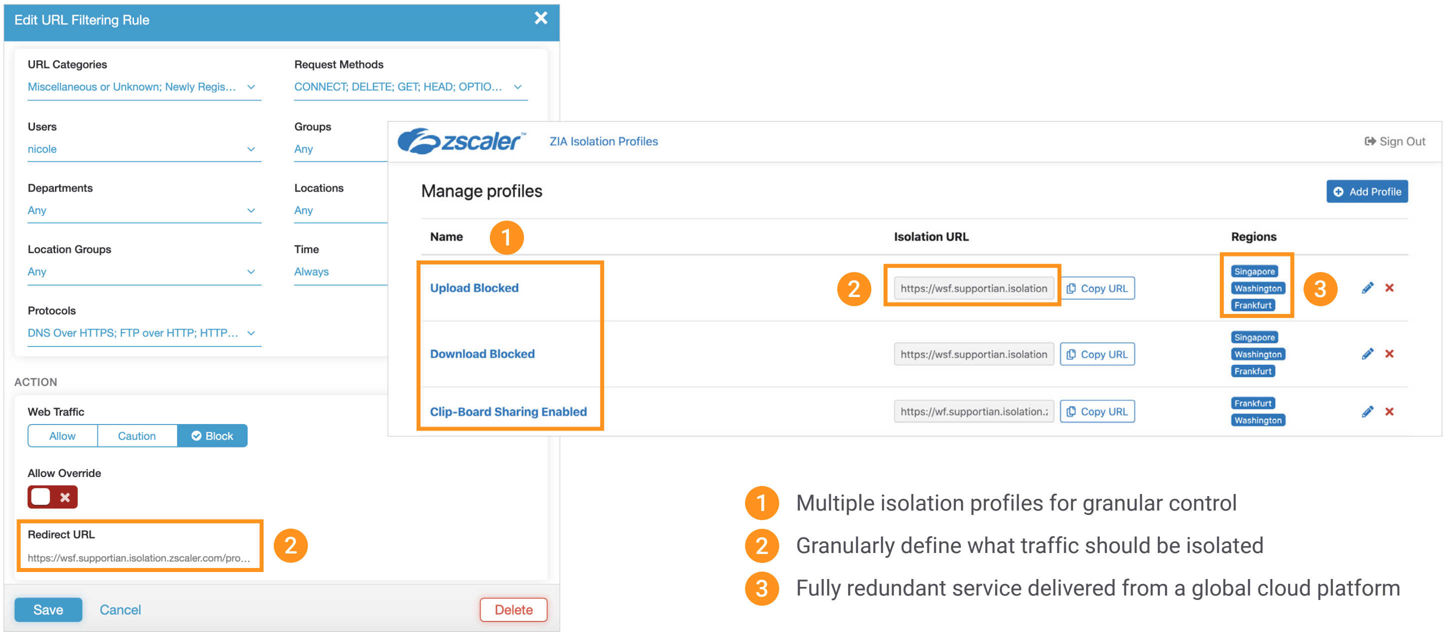
Enables a secure internet browsing experience

- Enables more open internet policies by delivering a safe rendering of web content in a remote browser
- Provides safe access to uncategorized URLs, newly registered domains, and other active web content, without having to download the actual files
- Increases user productivity by making more content/data available with reduced associated risk

FEATURES

- **Agentless solution** – Provide secure access to web content without physical hardware or an endpoint agent on every device
- **Integrated with Zscaler Internet Access** – All traffic destined to the isolation environment and traffic from the isolation environment to the internet is governed by the policies (URL, cloud app, DLP, etc.) defined in ZIA
- **Pixel streaming-based technology** – Securely stream content to the end user's native browser as pixels over an HTML5 canvas to protect users against connecting to active content
- **Centralized granular policy management** – Define all web-security policies, including isolation policies, on a centralized granular policy framework without having to replicate policies on multiple platforms
- **Data exfiltration controls** – Define the level of interaction the user's local computer can have in the isolation environment, including upload/download control and clipboard sharing between isolation and the local computer
- **Secure file rendering** – Render PDF files, text files, etc., in the isolation environment to protect against weaponized documents

Cloud Browser Isolation capabilities



Edit URL Filtering Rule

URL Categories: Miscellaneous or Unknown; Newly Regis...

Request Methods: CONNECT; DELETE; GET; HEAD; OPTIO...

Users: nicole

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Protocols: DNS Over HTTPS; FTP over HTTP; HTTP...

ACTION

Web Traffic: Allow | Caution | Block (selected)

Allow Override: off

Redirect URL: https://wsf.supportian.isolation.zscaler.com/pro...

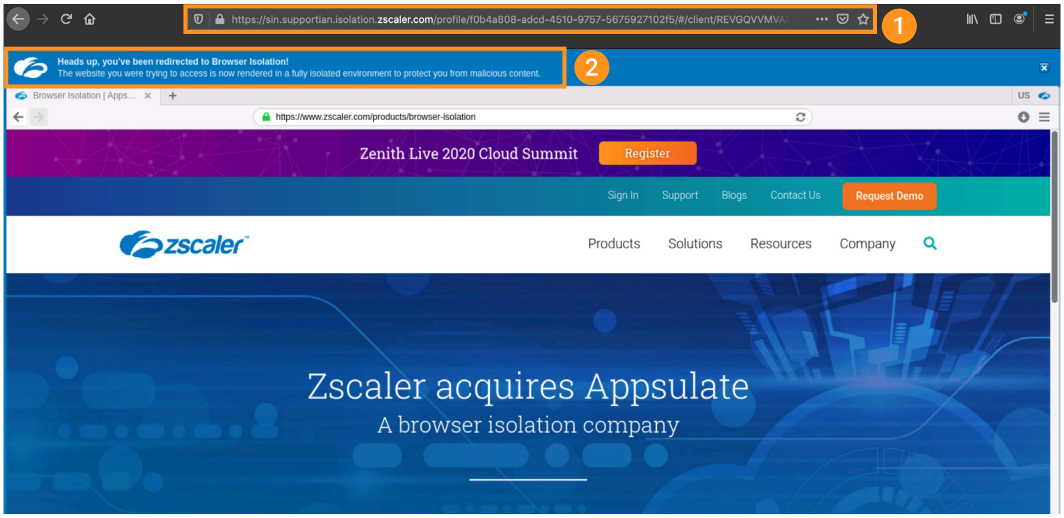
Manage profiles

Name	Isolation URL		Regions
Upload Blocked	https://wsf.supportian.isolation	Copy URL	Singapore Washington Frankfurt
Download Blocked	https://wsf.supportian.isolation	Copy URL	Singapore Washington Frankfurt
Clip-Board Sharing Enabled	https://wf.supportian.isolation.:	Copy URL	Frankfurt Washington

1. Multiple isolation profiles for granular control
2. Granularly define what traffic should be isolated
3. Fully redundant service delivered from a global cloud platform

Cloud delivery and reduced management burden

Agentless cloud delivery lets you use Zscaler Cloud Browser Isolation without requiring hardware appliances or installing and maintaining remote browser isolation endpoint agents on every device. Web requests are evaluated according to defined policies and, when needed, Cloud Browser Isolation establishes a remote browser session.



https://sin.supportian.isolation.zscaler.com/profile/f0b4a808-adcd-4510-9757-5675927102f5/#/client/REVGQVVMVA

Heads up, you've been redirected to Browser Isolation!
The website you were trying to access is now rendered in a fully isolated environment to protect you from malicious content.

https://www.zscaler.com/products/browser-isolation

1
2
Browser Isolation | Apps...
US
Zenith Live 2020 Cloud Summit
Register
Sign In
Support
Blogs
Contact Us
Request Demo
zscaler
Products
Solutions
Resources
Company
Zscaler acquires Appsulate
A browser isolation company

1. Native browser invoking the remote isolation environment
2. Webpage is loaded in the isolation browser and streamed to the native browser as a pixel stream and images

Increase security with pixel streaming

Maximize your security by enabling safe access to unknown web content without downloading actual files. By using pixel streaming-based technology, Zscaler Cloud Browser Isolation delivers only secure renderings of web content via an HTML5 canvas, ensuring your users never come in contact with active web content. This technique eliminates the risks associated with Content Disarm and Reconstruction (CDR) approaches, and improves your security and the ability to support more open internet access policies.

Why Zscaler Cloud Browser Isolation

Reduce web-based threats

Eliminate the risk of ransomware, zero day threats hiding in internet web pages and documents

Prevent data exfiltration

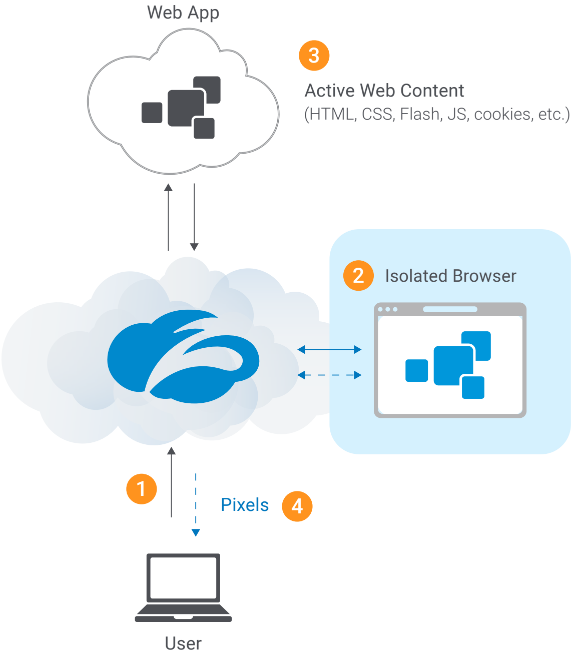
Protect executives and users who handle sensitive data from becoming victims of phishing, spear phishing, and other targeted attacks

Integrated platform

Deliver the entire security stack as a cloud service and provide a unified framework for policy definition, enforcement, and authentication

Secure internet browsing experience

Provide safe access to web content and web data, including uncategorized URLs and newly registered domains



How it works

1. User tries to access a potentially malicious webpage
2. Request is evaluated against defined policies, and if there is a match, creates an isolated browser session
3. Zscaler connects to the webpage and loads the content onto the isolated browser
4. Web content is streamed to the end user's native browser as pixels over a HTML5 canvas

Raise your internet security to the next level

As part of the integrated Zscaler Cloud Security Platform, you can easily activate Cloud Browser Isolation to eliminate web-based threats and protect sensitive data

Request a Demo

About Zscaler

Zscaler 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% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com