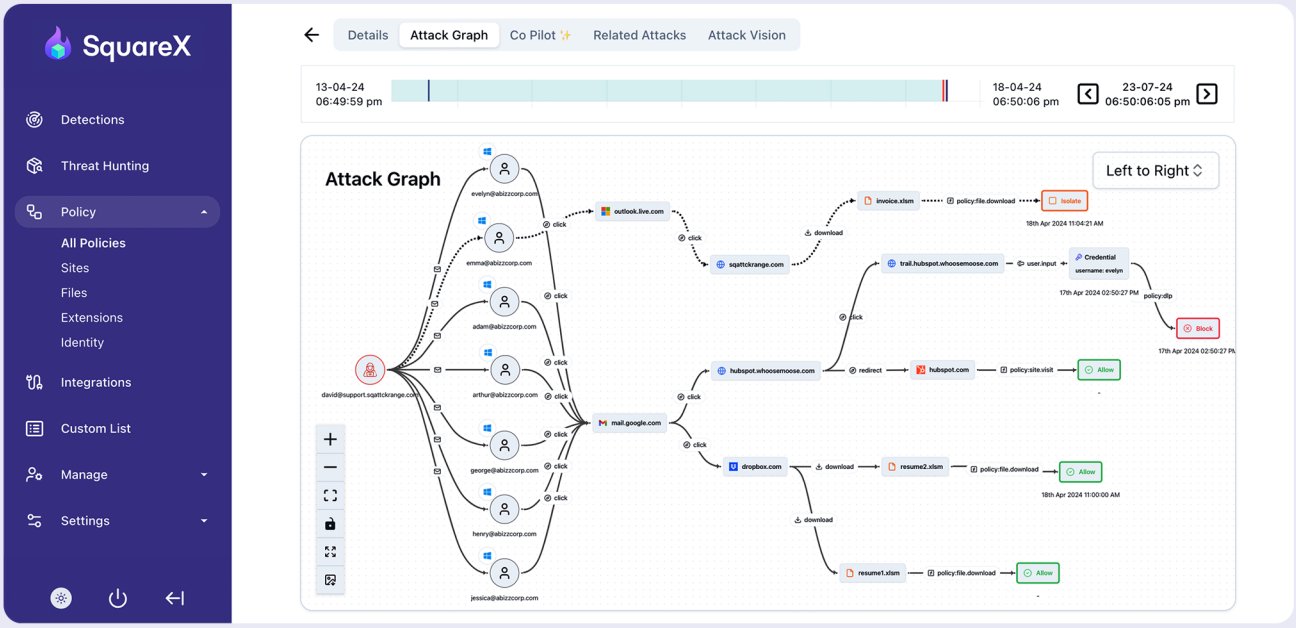
SquareX

DETECT | MITIGATE | THREAT HUNT
PROTECT ENTERPRISE USERS FROM WEB ATTACKS



SquareX helps organizations detect, mitigate, and threat hunt web attacks happening against their users in real-time. With our innovative browser-native security product, SquareX safeguards enterprise users from a spectrum of web-based threats, encompassing malicious files, websites, scripts, and compromised networks.

Web Attacks on your employees, a Blind Spot?

The web browser is the most used application within the enterprise but also the least protected. Bad actors are now increasingly targeting the weakest link: employees and consultants. Unfortunately, most of these attacks happen online when the employee or consultant is going about his daily work. Existing security solutions like Secure Web Gateways as part of SASE/SSE solutions are unable to protect users against modern web threats that happen on the client-side, and endpoint security solutions have no visibility into what happens in the browser during an attack. This makes it currently impossible for enterprise security teams to detect, mitigate and threat hunt these attacks.

SquareX's Technology Advantage

SquareX combines rules-based methods, heuristic analysis, and machine learning algorithms that run in the browser to continuously monitor page DOM changes, user interactions, and web traffic patterns to identify and block potential threats in real-time. Our technology can be deployed on any browser and does not need to inconvenience enterprises with a custom browser which additionally opens them up to other threats.

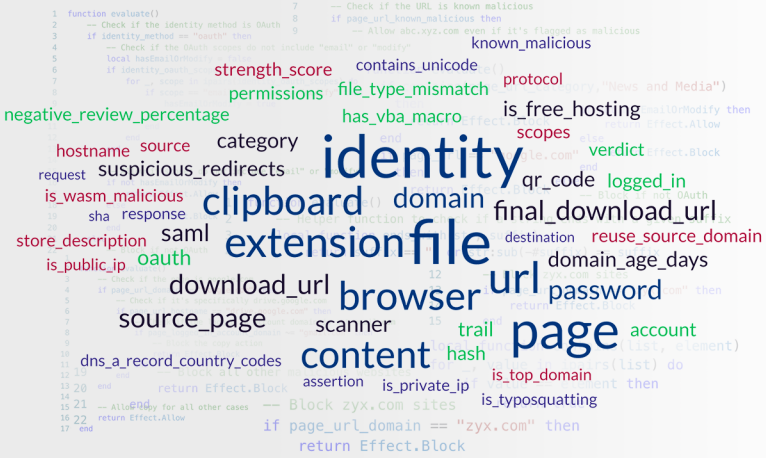
Why is SquareX's In-Browser Solution Superior?

- WebApp Context Aware
- Upstream Threat Prevention
- Multi-layer Attack Detection
- User Interaction Aware
- Zero-lag Attack Mitigation
- Web Attack Threat Hunting

Eliminating Browser Security Risks, One Use Case at a Time

SquareX

- Granular Access Control
- Malicious Websites
- Malicious Files
- Risky SaaS Applications
- Content Disarm & Reconstruction
- Page Content Analysis
- Browser Isolation
- File Isolation: Cloud-based
- File Isolation: Office 365-based
- Malicious Browser Extensions
- Identity Attacks
- Web, File & Clipboard DLP
- Gen AI DLP
- Web-VPN
- Web-AV
- Malicious QR Code
- Email Security
- MitM Attacks
- Insider Attacks
- Monitor Visit Path
- Malware Sandbox
- URL Analysis Engine
- SaaS-native Integrations
- Device Posture
- Wifi Security

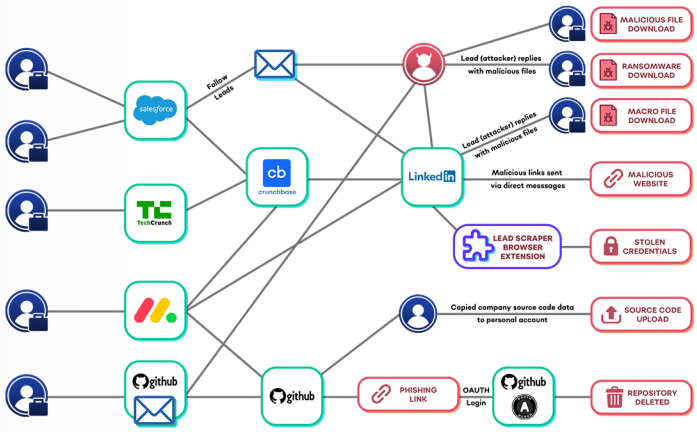


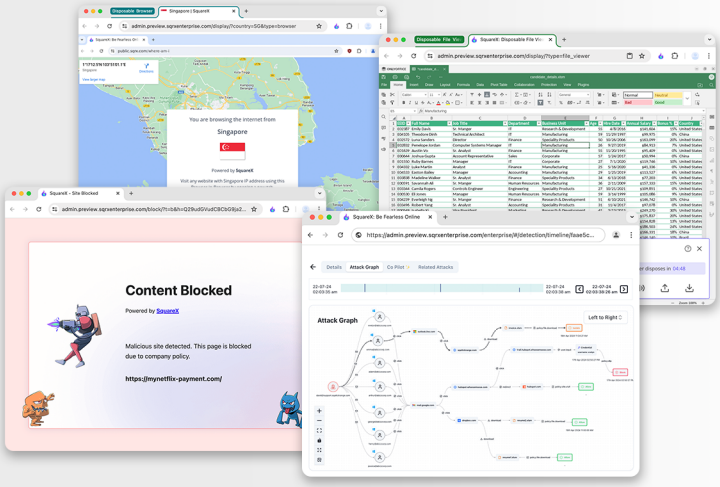
Build Granular Policies

- AI-powered Policy Engine helps you build complex policies with 100s of rule-based parameters. A custom scripting engine is also available at your disposal.
- Create policies encompassing site visits, site content, clipboard copy & paste, user input, file downloads & uploads, browser extensions and even identity, access, and SaaS app permissions.
- Our policy manager runs entirely in the browser, making it fast, inline and effective to stop client-side attacks in real time.

Monitor Any Web Workflow

- SquareX allows you to inspect and monitor arbitrary web workflows with ease.
- Monitor user actions in real time as they traverse across multiple websites, interact with various web page components, download files and so on.
- Configure additional checks to prevent users from interacting with phishing login pages or giving risky permissions to third-party SaaS applications.





Block, Isolate and Threat Hunt

- SquareX's cloud-based browser & file isolation creates a secure environment for browsing and file viewing. Enterprises can seamlessly build policies to isolate any file type or links from any source.
- Office 365-based isolation and Content Disarm & Reconstruction options are available for Office Documents.
- With the aid of Attack Graphs, AI Copilot, Attack Correlation and Attack Vision, admins can accurately visualize attacks as they happen and threat hunt for similar attacks enterprise wide.

Why choose SquareX over SASE Solutions?

SquareX

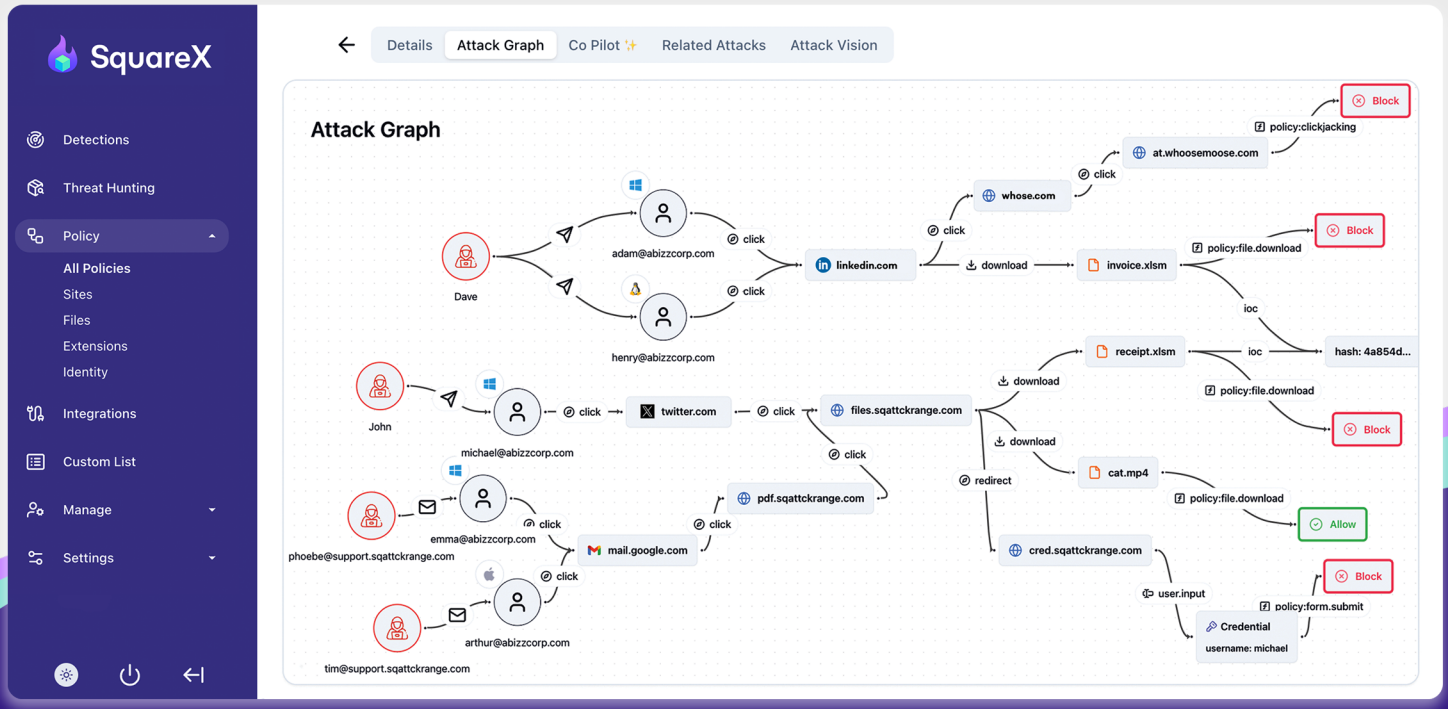
	SASE/SSE Solutions	SquareX
Deployment	• Requires agent and certificate installation, making deployment complex and time-consuming • All user traffic is routed through Secure Web Gateways (SWGs) which can create traffic bottlenecks and inefficiencies	• Agentless, deploys as a browser extension within minutes via a group policy or managed workspace • Analysis happens in-browser so there is no need to proxy traffic, creating a seamless user experience
Visibility	• Tries to detect application layer attacks on the browser using network traffic, making it easy for attackers to bypass using Last Mile Reassembly Attacks* • Unable to inspect protocols like websocket, WebRTC, gRPC, webtorrent and so on, allowing attackers to smuggle malicious files and websites through them	• Has access to rich browser metrics such as clipboard access, site permissions, DOM changes and extensions, as well as context and user identity awareness across websites, making it possible to detect complex attacks on the client-side • As an in-browser solution, SquareX has visibility into all data going in/out of the browser regardless of the network layer protocol
Access Controls via Policies	• Primarily URL-based, with limited parameters for building policies: URL categories, file types, etc	• Advanced policy engine provides the ability to monitor/block/isolate arbitrary web workflows in the browser • Hundreds of parameters including Lua-based rule
Web Threat Detections	• Can only detect file-based attacks when the entire file is available for scanning. SWGs get bypassed when Last Mile Reassembly Attacks* are applied to the same file • Primarily can only block resources based on URLs and associated parameters	• Can detect and block all file download/ upload-based attacks as it is an in-browser solution • Ability to block advanced attacks such as malicious QR codes, identity attacks, AiTM, BiTM and many more
Web DLP	• Doesn't provide a robust web DLP solution due to limited visibility • Easily bypassed by Insider Attacks where Last Mile Reassembly* techniques are used	• Provides enhanced DLP protection by monitoring clipboard access, form submissions, and file download/upload events across websites while maintaining user identity context
Live Analysis	• Incapable of performing live analysis of web content and relies entirely on network traffic to emulate what might be happening on the user's browser	• As an in-browser solution, SquareX is capable of advanced runtime analysis by monitoring browser events, DOM changes, user interaction and network changes

Why choose SquareX over Enterprise Browsers?

	Enterprise Browsers	SquareX
Deployment	• A new browser needs to be deployed on all endpoints, and all other browsers need to be blocked	• Deploys as a browser extension and supports all existing browsers, making it easy to deploy via a Group Policy or managed workspaces
Adoption	• Major change in user's workflow and experience, which requires internal awareness and training	• Fits seamlessly into the user's workflow as the extension runs on their existing browser, eliminating the need for adjustments and maintaining productivity
Security Patch	• Custom fork of Chromium that always needs to be kept in sync with the main Chromium branch to ensure compatibility with web protocols and experience • Always lags in security patches, making it vulnerable to all Chromium-based zero-day attacks	• Works with all existing browsers which automatically update new security patches, ensures timely updates and enhanced protection
Isolation	• Local/Process-based isolation is not sufficient and can still put users at risk	• Supports both file and browser isolation in the cloud, making it impossible for attackers to execute local exploits

*To read more about Last Mile Reassembly Attacks visit sqrx.com/lastmilereassemblyattacks

Case Study: Multi-channel Ransomware Attack



***Attack Description*:**
An adversary is targeting multiple users of an organization with the same ransomware, packaged as a malicious Excel document, and sent over multiple channels including Linkedin, Twitter and Email.

SquareX Detect-Mitigate-Threat Hunt

***Detect*:** SquareX's browser extension continuously monitors user interactions with websites, including file downloads. In this scenario, when the enterprise user downloads a file, the in-browser malicious file detector activates, detecting that the Excel file contains malicious macro-based ransomware.

***Mitigate*:** Once the malicious file is detected, SquareX checks if the enterprise policy is set to 'Block' or 'Isolate.' In this case, the policy is set to 'Block' all malicious files, so the download is blocked, and a warning message is shown to the user. SquareX immediately sends the file hash and the file to the cloud, where automatic remediation policies are deployed to block the same file across all enterprise user browsers.

***Threat Hunt*:** The enterprise admin receives an alert, and in the SquareX enterprise portal, a full description of the attack, the attack graph, and the details of the malicious file are made available. The admin can also see all related attacks with a single click using our automated threat hunting feature. Our AI Copilot presents a full timeline analysis of the attack and proposes remedial measures. Using our generalized threat hunting interface, the admin can further investigate similar threats and apply policies and other remedial actions.

Contact Us

Get your free trial set up!

Email us at **founder@sqrx.com**

sqrx.com labs.sqrx.com