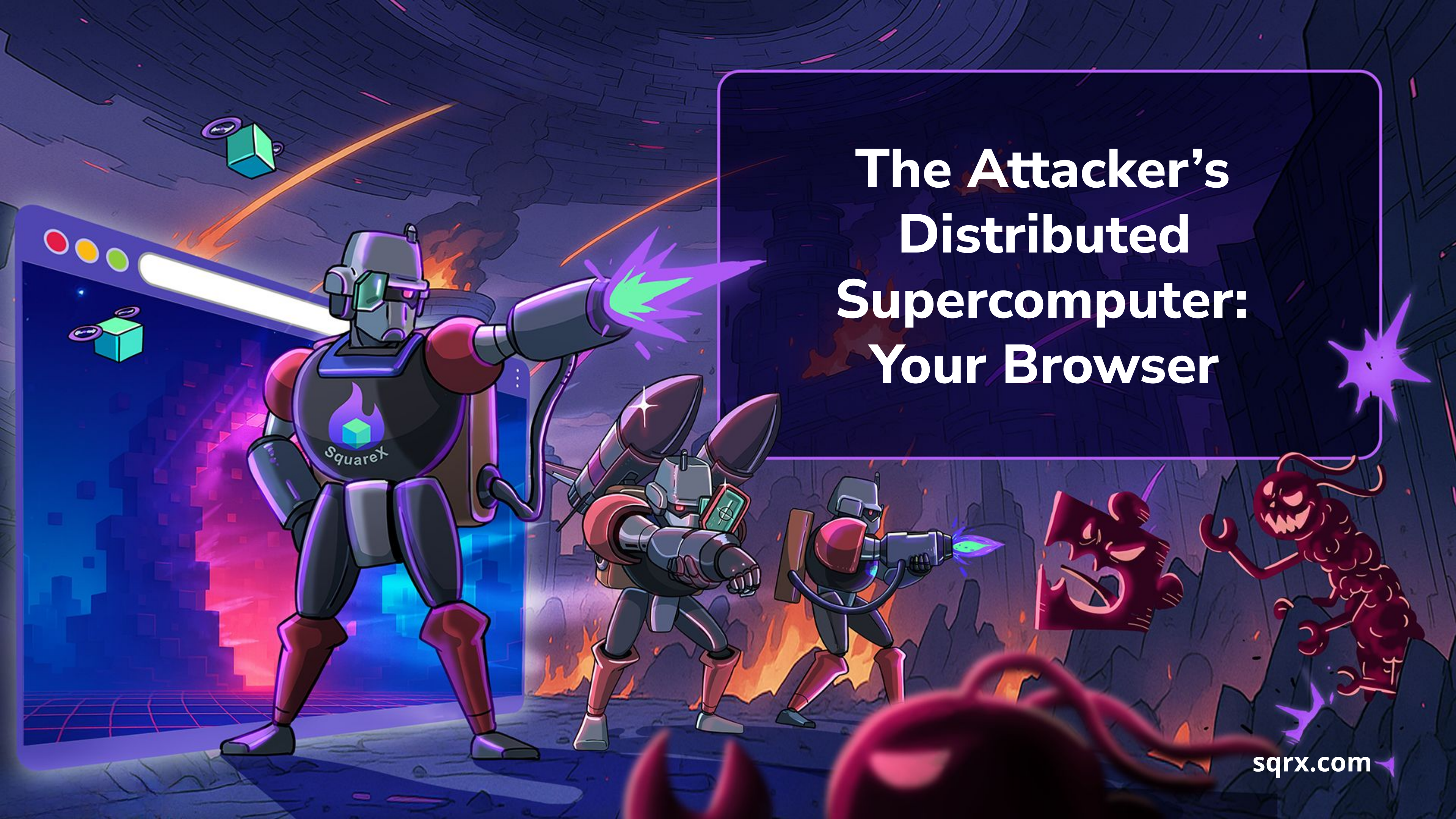


The Attacker's Distributed Supercomputer: Your Browser

sqrx.com

About me

SquareX

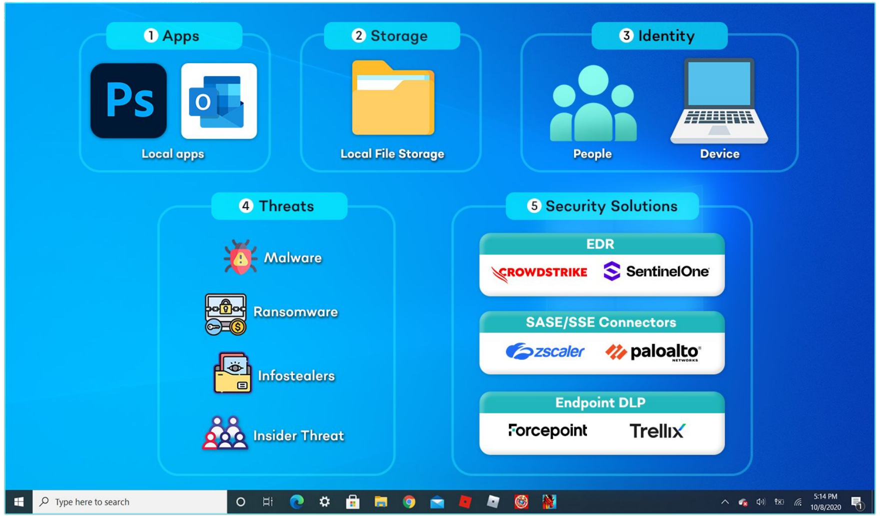
Shourya Pratap Singh

- Building Browser Security Extension
- Browser Security Research
- Main Stage Talks at DEF CON
- Workshop on Browser Extensions at Texas Cyber Summit
- Black Hat Europe Arsenal

The Browser is the New Endpoint

SquareX

ENDPOINT



1 Apps
- Local apps

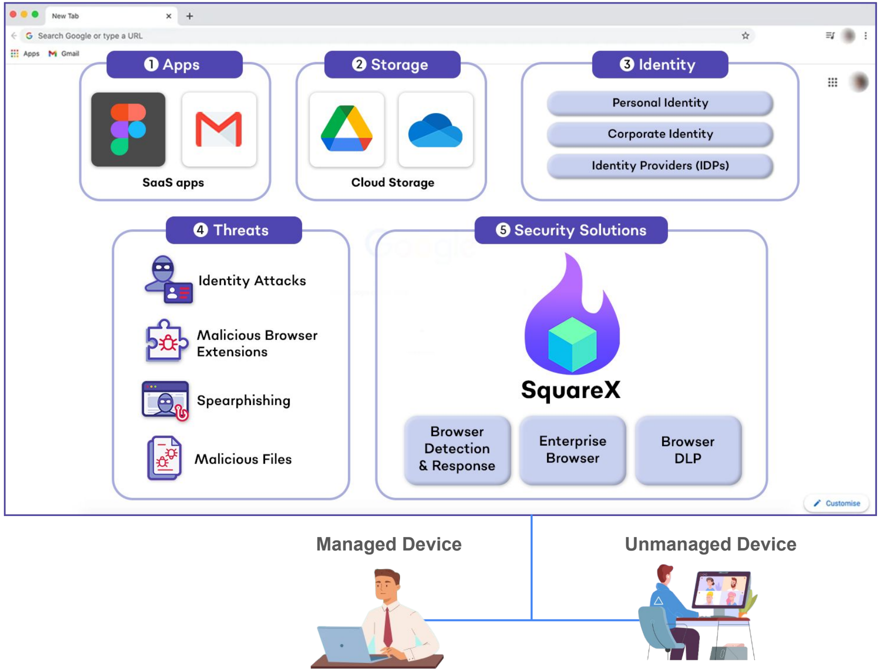
2 Storage
- Local File Storage

3 Identity
- People
- Device

4 Threats
- Malware
- Ransomware
- Infostealers
- Insider Threat

5 Security Solutions
- EDR: CROWDSTRIKE, SentinelOne
- SASE/SSE Connectors: zscaler, paloalto
- Endpoint DLP: Forcepoint, Trellix

BROWSER



1 Apps
- SaaS apps

2 Storage
- Cloud Storage

3 Identity
- Personal Identity
- Corporate Identity
- Identity Providers (IDPs)

4 Threats
- Identity Attacks
- Malicious Browser Extensions
- Spearphishing
- Malicious Files

5 Security Solutions
- SquareX
- Browser Detection & Response
- Enterprise Browser
- Browser DLP

Managed Device

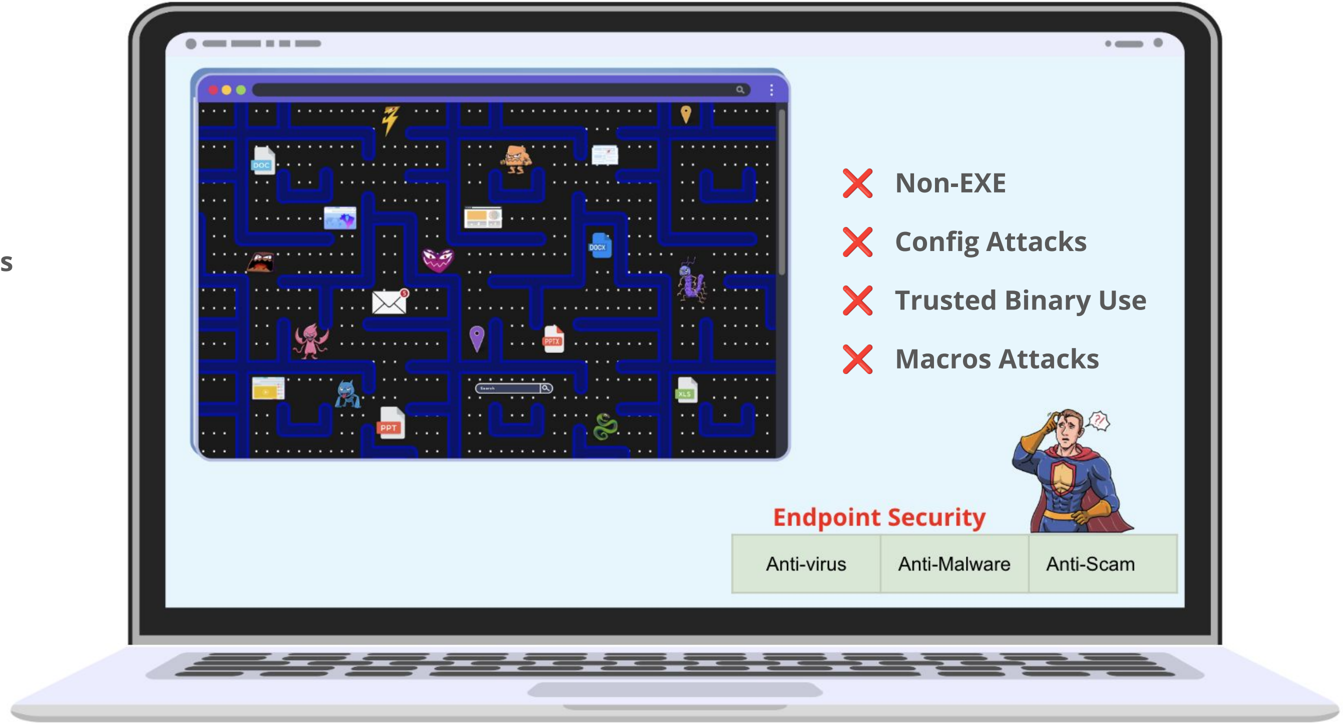
Unmanaged Device

Consumer & AI browsers

sqrx.com

EDRs have no visibility into the browser

- ❌ In-Browser Identity Attacks
- ❌ WASM monitoring
- ❌ Browser Extension
- ❌ Browser Ransomware



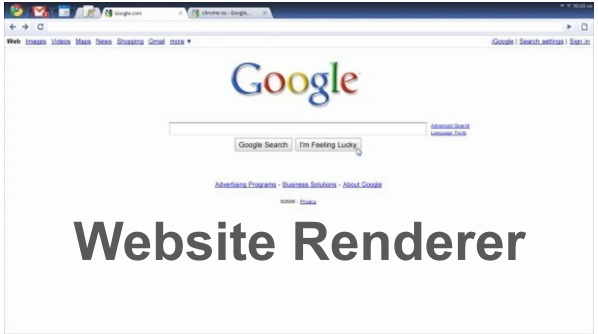
- ❌ Non-EXE
- ❌ Config Attacks
- ❌ Trusted Binary Use
- ❌ Macros Attacks

Endpoint Security

Anti-virus	Anti-Malware	Anti-Scam

Why? The Browser is now an Application Platform

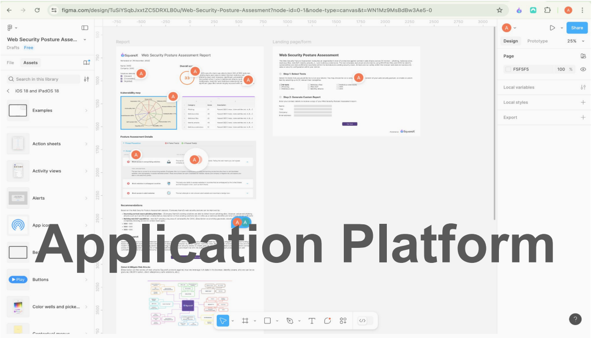
Early 2010s


Web Images Videos Maps News Shopping Gmail more ▾
iGoogle | Search settings | Sign in
Google
Advanced Search
Language Tools
Google Search
I'm Feeling Lucky
Advertising Programs - Business Solutions - About Google
©2009 - Privacy

Website Renderer

Network Data → Attack Detection

Today


figma.com/design/TuSiYSqbJxxt2C5DRXLB0u/Web-Security-Posture-Assesment?node-id=0-1&node-type=canvas&t=WN1Mz9MsBdBw3Ae5-0
Web Security Posture Asse...
Assets
Examples
Action sheets
Activity views
Alerts
Buttons
Color wells and picke...
Share
Design
Prototype
Page
Local variables
Local styles
Export

Application Platform

Network Data —✗→ ~~Attack Detection~~

- ✓ Complex DOM
- ✓ WASM
- ✓ WebRTC, gRPC, SSE, WebTorrent etc.
- ✓ Complex UI Frameworks
- ✓ Identity vaults

Browser Attack Surface: 100+ Unique Attack Vectors

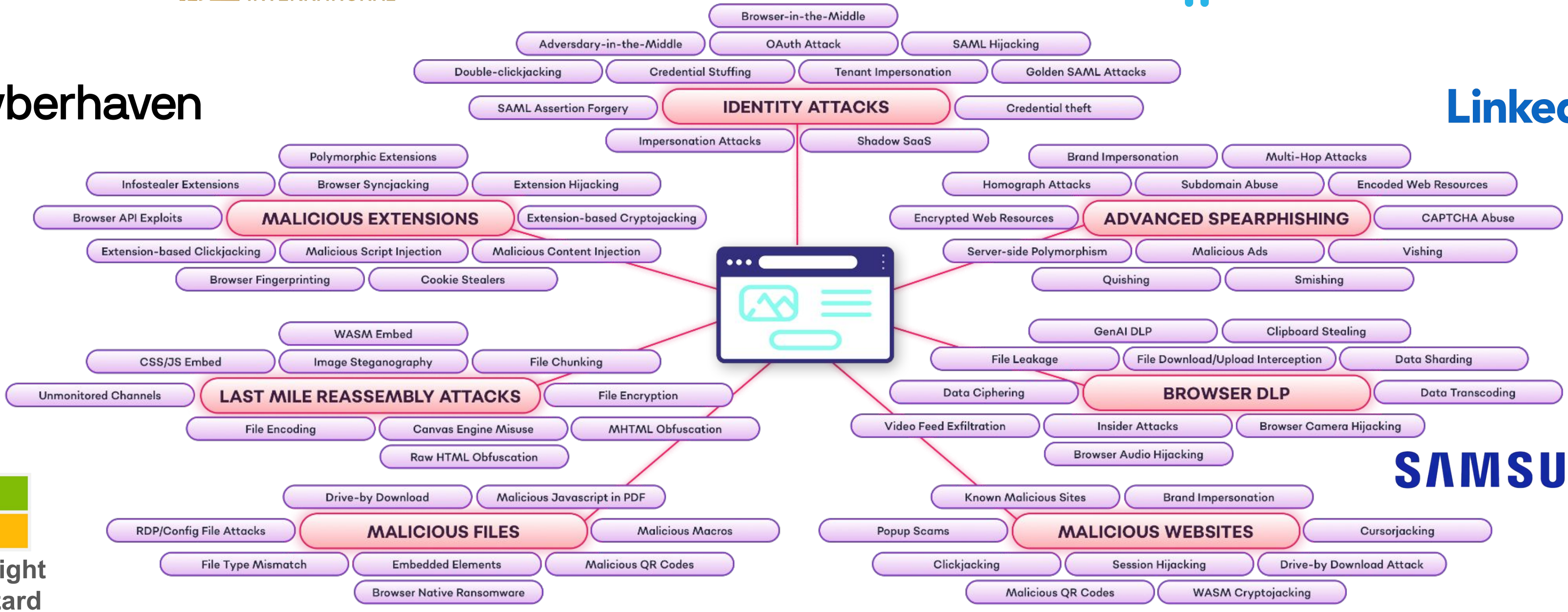
MGM RESORTS INTERNATIONAL™

coinbase

snowflake

cyberhaven

LinkedIn



IDENTITY ATTACKS
- Browser-in-the-Middle
- Adversdary-in-the-Middle
- OAuth Attack
- SAML Hijacking
- Double-clickjacking
- Credential Stuffing
- Tenant Impersonation
- Golden SAML Attacks
- SAML Assertion Forgery
- Credential theft
- Impersonation Attacks
- Shadow SaaS

MALICIOUS EXTENSIONS
- Polymorphic Extensions
- Infostealer Extensions
- Browser Syncjacking
- Extension Hijacking
- Browser API Exploits
- Extension-based Cryptojacking
- Extension-based Clickjacking
- Malicious Script Injection
- Malicious Content Injection
- Browser Fingerprinting
- Cookie Stealers

ADVANCED SPEARPHISHING
- Brand Impersonation
- Multi-Hop Attacks
- Homograph Attacks
- Subdomain Abuse
- Encoded Web Resources
- Encrypted Web Resources
- CAPTCHA Abuse
- Server-side Polymorphism
- Malicious Ads
- Vishing
- Quishing
- Smishing

LAST MILE REASSEMBLY ATTACKS
- WASM Embed
- CSS/JS Embed
- Image Steganography
- File Chunking
- Unmonitored Channels
- File Encryption
- File Encoding
- Canvas Engine Misuse
- MHTML Obfuscation
- Raw HTML Obfuscation

BROWSER DLP
- GenAI DLP
- Clipboard Stealing
- File Leakage
- File Download/Upload Interception
- Data Sharding
- Data Ciphering
- Data Transcoding
- Video Feed Exfiltration
- Insider Attacks
- Browser Camera Hijacking
- Browser Audio Hijacking

MALICIOUS FILES
- Drive-by Download
- Malicious Javascript in PDF
- RDP/Config File Attacks
- Malicious Macros
- File Type Mismatch
- Embedded Elements
- Malicious QR Codes
- Browser Native Ransomware

MALICIOUS WEBSITES
- Known Malicious Sites
- Brand Impersonation
- Popup Scams
- Cursorjacking
- Clickjacking
- Session Hijacking
- Drive-by Download Attack
- Malicious QR Codes
- WASM Cryptojacking

SAMSUNG

Midnight Blizzard

okta

sqrx.com

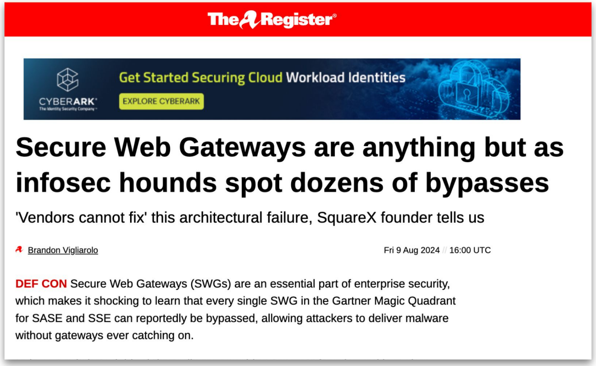
Salesforce OAuth Attack

[Demo]

Browser Attacks | Can SASE/SSE solve this?

SquareX

- ❌ WebApp context unaware
- ❌ User Interaction unaware
- ❌ No concept of windows-tabs
- ❌ Site permissions unaware
- ❌ No access to rich metrics
- ❌ Extensions unaware



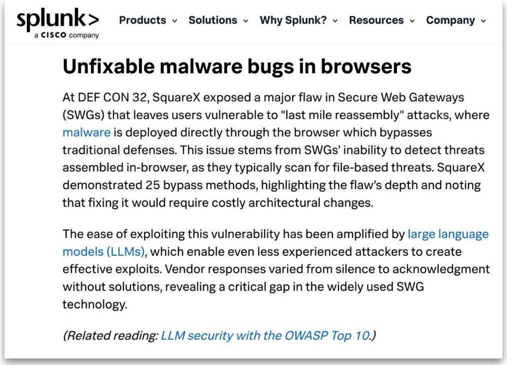
The Register®

Secure Web Gateways are anything but as infosec hounds spot dozens of bypasses

'Vendors cannot fix' this architectural failure, SquareX founder tells us

Brandon Vigliarolo   Fri 9 Aug 2024 // 16:00 UTC

DEF CON Secure Web Gateways (SWGs) are an essential part of enterprise security, which makes it shocking to learn that every single SWG in the Gartner Magic Quadrant for SASE and SSE can reportedly be bypassed, allowing attackers to deliver malware without gateways ever catching on.

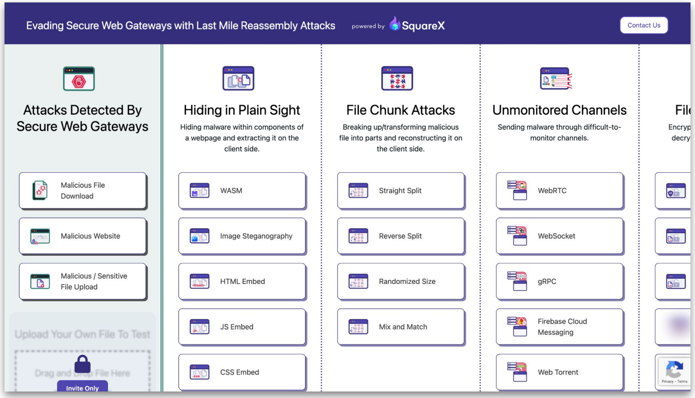


Unfixable malware bugs in browsers

At DEF CON 32, SquareX exposed a major flaw in Secure Web Gateways (SWGs) that leaves users vulnerable to "last mile reassembly" attacks, where malware is deployed directly through the browser which bypasses traditional defenses. This issue stems from SWGs' inability to detect threats assembled in-browser, as they typically scan for file-based threats. SquareX demonstrated 25 bypass methods, highlighting the flaw's depth and noting that fixing it would require costly architectural changes.

The ease of exploiting this vulnerability has been amplified by large language models (LLMs), which enable even less experienced attackers to create effective exploits. Vendor responses varied from silence to acknowledgment without solutions, revealing a critical gap in the widely used SWG technology.

(Related reading: LLM security with the OWASP Top 10.)



Evading Secure Web Gateways with Last Mile Reassembly Attacks   powered by SquareX

Attacks Detected By Secure Web Gateways

- Malicious File Download
- Malicious Website
- Malicious / Sensitive File Upload

Upload Your Own File To Test

Drag and Drop File Here

Hiding in Plain Sight

Hiding malware within components of a webpage and extracting it on the client side.

- WASM
- Image Steganography
- HTML Embed
- JS Embed
- CSS Embed

File Chunk Attacks

Breaking up/transforming malicious file into parts and reconstructing it on the client side.

- Straight Split
- Reverse Split
- Randomized Size
- Mix and Match

Unmonitored Channels

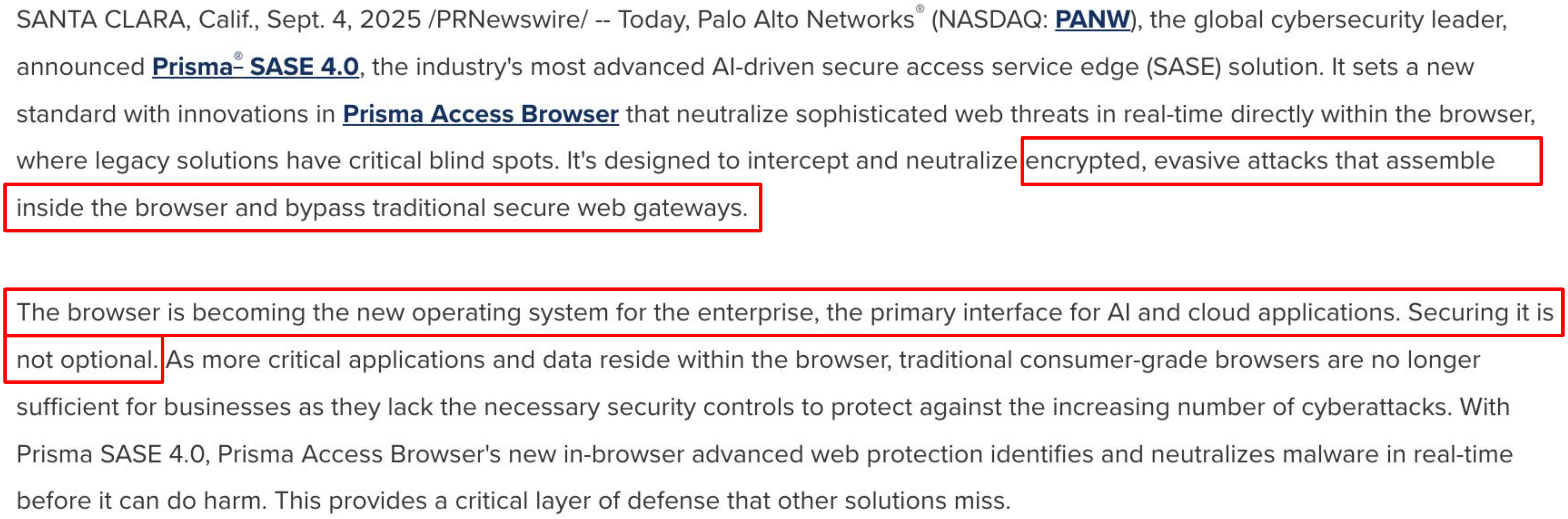
Sending malware through difficult-to-monitor channels.

- WebRTC
- WebSocket
- gRPC
- Firebase Cloud Messaging
- Web Torrent

File

Encryp
decry

Palo Alto Networks admits the importance of browser security

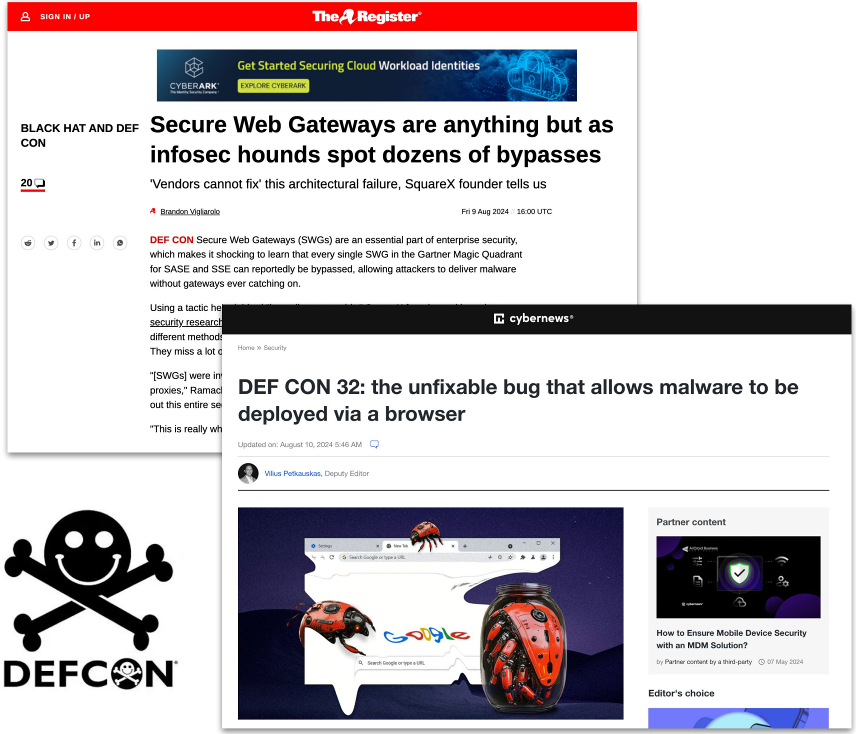


SANTA CLARA, Calif., Sept. 4, 2025 /PRNewswire/ -- Today, Palo Alto Networks® (NASDAQ: **PANW**), the global cybersecurity leader, announced **Prisma® SASE 4.0**, the industry's most advanced AI-driven secure access service edge (SASE) solution. It sets a new standard with innovations in **Prisma Access Browser** that neutralize sophisticated web threats in real-time directly within the browser, where legacy solutions have critical blind spots. It's designed to intercept and neutralize encrypted, evasive attacks that assemble inside the browser and bypass traditional secure web gateways.

The browser is becoming the new operating system for the enterprise, the primary interface for AI and cloud applications. Securing it is not optional. As more critical applications and data reside within the browser, traditional consumer-grade browsers are no longer sufficient for businesses as they lack the necessary security controls to protect against the increasing number of cyberattacks. With Prisma SASE 4.0, Prisma Access Browser's new in-browser advanced web protection identifies and neutralizes malware in real-time before it can do harm. This provides a critical layer of defense that other solutions miss.

SquareX disclosed Last Mile Reassembly attacks at DEFCON last year

SquareX



SIGN IN / UP

The Register®

BLACK HAT AND DEF CON

20

Secure Web Gateways are anything but as infosec hounds spot dozens of bypasses

'Vendors cannot fix' this architectural failure, SquareX founder tells us

Brandon Vigliarolo

Fri 9 Aug 2024 // 16:00 UTC

DEF CON Secure Web Gateways (SWGs) are an essential part of enterprise security, which makes it shocking to learn that every single SWG in the Gartner Magic Quadrant for SASE and SSE can reportedly be bypassed, allowing attackers to deliver malware without gateways ever catching on.

Using a tactic he
security research
different method
They miss a lot c

"[SWGs] were in
proxies," Ramac
out this entire se

"This is really wh

cybernews®

Home » Security

DEF CON 32: the unfixable bug that allows malware to be deployed via a browser

Updated on: August 10, 2024 5:46 AM

Vilius Petkauskas, Deputy Editor

Partner content

How to Ensure Mobile Device Security with an MDM Solution?

by Partner content by a third-party 07 May 2024

Editor's choice

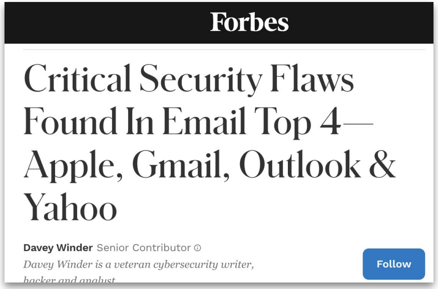
DEFCON®

Hiding in Plain Sight

[Demo]

SquareX is ahead of Attackers: Bleeding edge threat research

Webmail Link-File Scanners

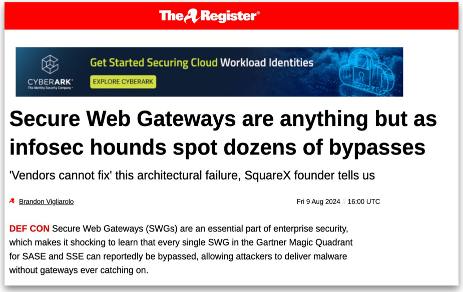


Critical Security Flaws Found In Email Top 4—Apple, Gmail, Outlook & Yahoo

Davey Winder Senior Contributor

Davey Winder is a veteran cybersecurity writer, hacker and analyst

SWGs are Broken


The Register
CYBERARK The Identity Security Company
Get Started Securing Cloud Workload Identities
EXPLORE CYBERARK

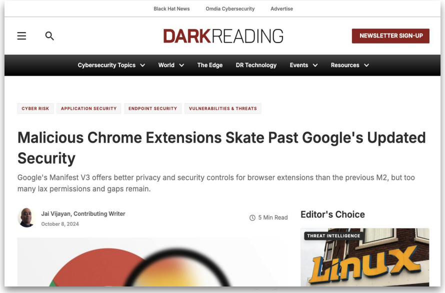
Secure Web Gateways are anything but as infosec hounds spot dozens of bypasses

'Vendors cannot fix' this architectural failure, SquareX founder tells us

Brandon Vigliarolo Fri 9 Aug 2024 // 16:00 UTC

DEF CON Secure Web Gateways (SWGs) are an essential part of enterprise security, which makes it shocking to learn that every single SWG in the Gartner Magic Quadrant for SASE and SSE can reportedly be bypassed, allowing attackers to deliver malware without gateways ever catching on.

Google MV3 Vulnerabilities



Malicious Chrome Extensions Skate Past Google's Updated Security

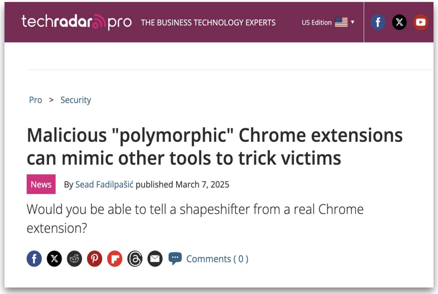
Google's Manifest V3 offers better privacy and security controls for browser extensions than the previous M2, but too many lax permissions and gaps remain.

Jai Vijayan, Contributing Writer
October 8, 2024

5 Min Read

Editor's Choice

Polymorphic Extensions

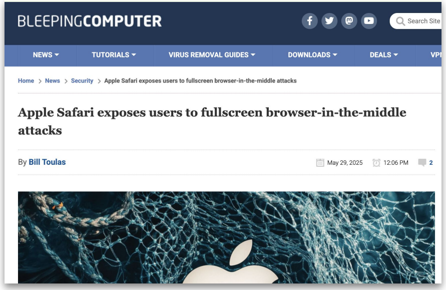


Malicious "polymorphic" Chrome extensions can mimic other tools to trick victims

By Sead Fadilpašić published March 7, 2025

Would you be able to tell a shapeshifter from a real Chrome extension?

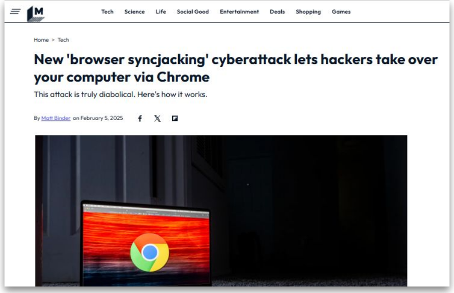
Fullscreen BitM


BLEEPINGCOMPUTER
Search Site
NEWS
TUTORIALS
VIRUS REMOVAL GUIDES
DOWNLOADS
DEALS
VPN
Home > News > Security > Apple Safari exposes users to fullscreen browser-in-the-middle attacks

Apple Safari exposes users to fullscreen browser-in-the-middle attacks

By Bill Toulas May 29, 2025 12:06 PM 2

Browser & Device Takeover via Extension

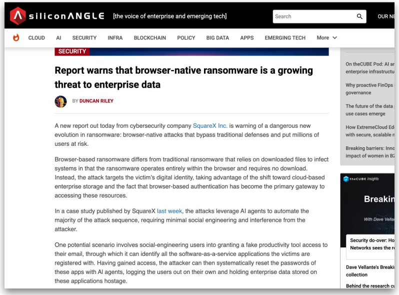


New 'browser syncjacking' cyberattack lets hackers take over your computer via Chrome

This attack is truly diabolical. Here's how it works.

By Matt Binder on February 5, 2025

Browser-native Ransomware


siliconANGLE [the voice of enterprise and emerging tech]
Search
OUR NE
CLOUD
AI
SECURITY
INFRA
BLOCKCHAIN
POLICY
BIG DATA
APPS
EMERGING TECH
More
SECURITY
On theCUBE Pod: AI ar enterprise infrastructu
Why proactive FinOps governance
The future of the data use cases emerge
How ExtremeCloud Ed with secure, scalable n
Breaking barriers: Inno impact of women in B2
theCUBE insights
Breakin
With Dave Vella
Security do-over: Ho Networks sees the r
Dave Vellante's Breaki collection
Behind the research cu

Report warns that browser-native ransomware is a growing threat to enterprise data

BY DUNCAN RILEY

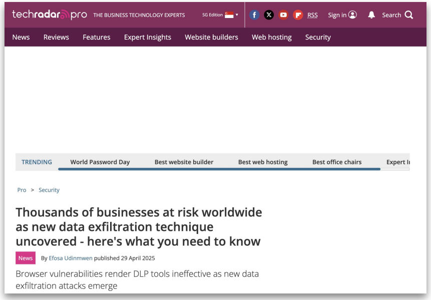
A new report out today from cybersecurity company SquareX Inc. is warning of a dangerous new evolution in ransomware: browser-native attacks that bypass traditional defenses and put millions of users at risk.

Browser-based ransomware differs from traditional ransomware that relies on downloaded files to infect systems in that the ransomware operates entirely within the browser and requires no download. Instead, the attack targets the victim's digital identity, taking advantage of the shift toward cloud-based enterprise storage and the fact that browser-based authentication has become the primary gateway to accessing these resources.

In a case study published by SquareX last week, the attacks leverage AI agents to automate the majority of the attack sequence, requiring minimal social engineering and interference from the attacker.

One potential scenario involves social-engineering users into granting a fake productivity tool access to their email, through which it can identify all the software-as-a-service applications the victims are registered with. Having gained access, the attacker can then systematically reset the passwords of these apps with AI agents, logging the users out on their own and holding enterprise data stored on these applications hostage.

Cloud SASE/SSE & Endpoint DLP Bypass



Thousands of businesses at risk worldwide as new data exfiltration technique uncovered - here's what you need to know

By Efosa Udinmwen published 29 April 2025

Browser vulnerabilities render DLP tools ineffective as new data exfiltration attacks emerge

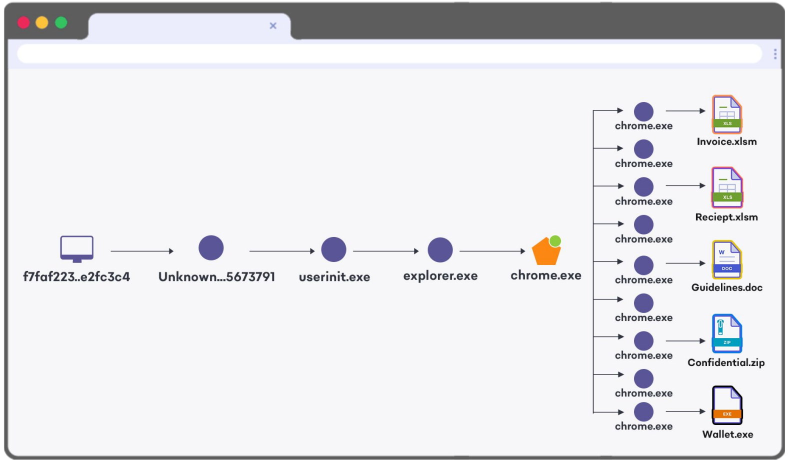
Passkey Proxy Attack

[Demo]

EDR + Browser Security = Full Endpoint Attack Attribution

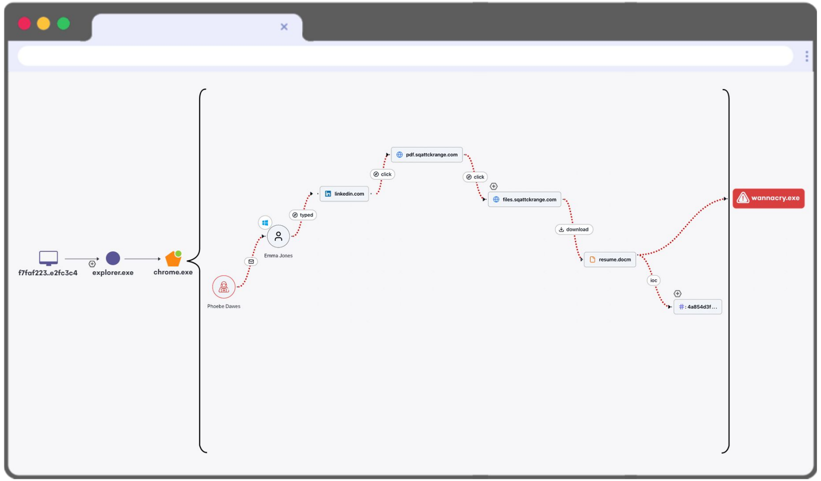
SquareX

EDRs Today



EDRs currently can only tell that the malware was downloaded via the Chrome Browser as it has zero browser visibility

EDR + Browser Security

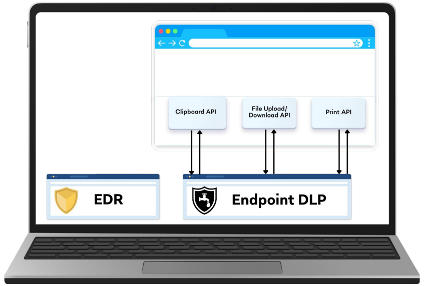


With Browser Security, EDRs can enrich it's attack graphs with full web attack chain visibility

sqrx.com

DLP | Can Endpoint or Cloud SASE/SSE DLP solve this?

Endpoint DLP



Rely on browser APIs for browser DLP

- ❌ Lack of identity context
- ❌ Credential leakage (operations without clipboard)
- ❌ Lack of browser extension awareness
- ❌ Lack of page content context
- ❌ Lack of visibility into network requests and it’s origin

SASE/SSE Cloud DLP

Proxy
SASE/SSE

- ❌ No direct web app context
- ❌ Blind to user interaction with site/web application
- ❌ File limits: size, type, zip recursions, client-side encrypted files
- ❌ Inability to take into account **multiple identities** in the browser
- ❌ Binary channels - e.g. gRPC channels
- ❌ Inability to correlate traffic with browser tabs-windows
- ❌ No access to DOM changes

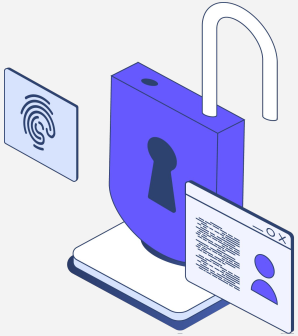
File Chunking Upload

[Demo]

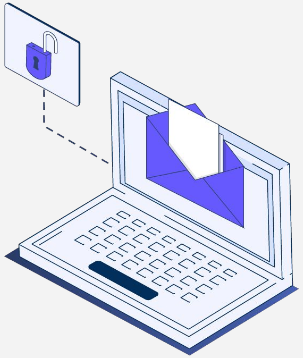
The Browser Data Loss Threatscape

Complexity

Low → High



Employee Negligence



Insider Threat

Data Exfiltration Attacks

Examples

Employee Negligence:

- *Uploading PII/ source code to Chat GPT*
- *Uploading company files to personal accounts*

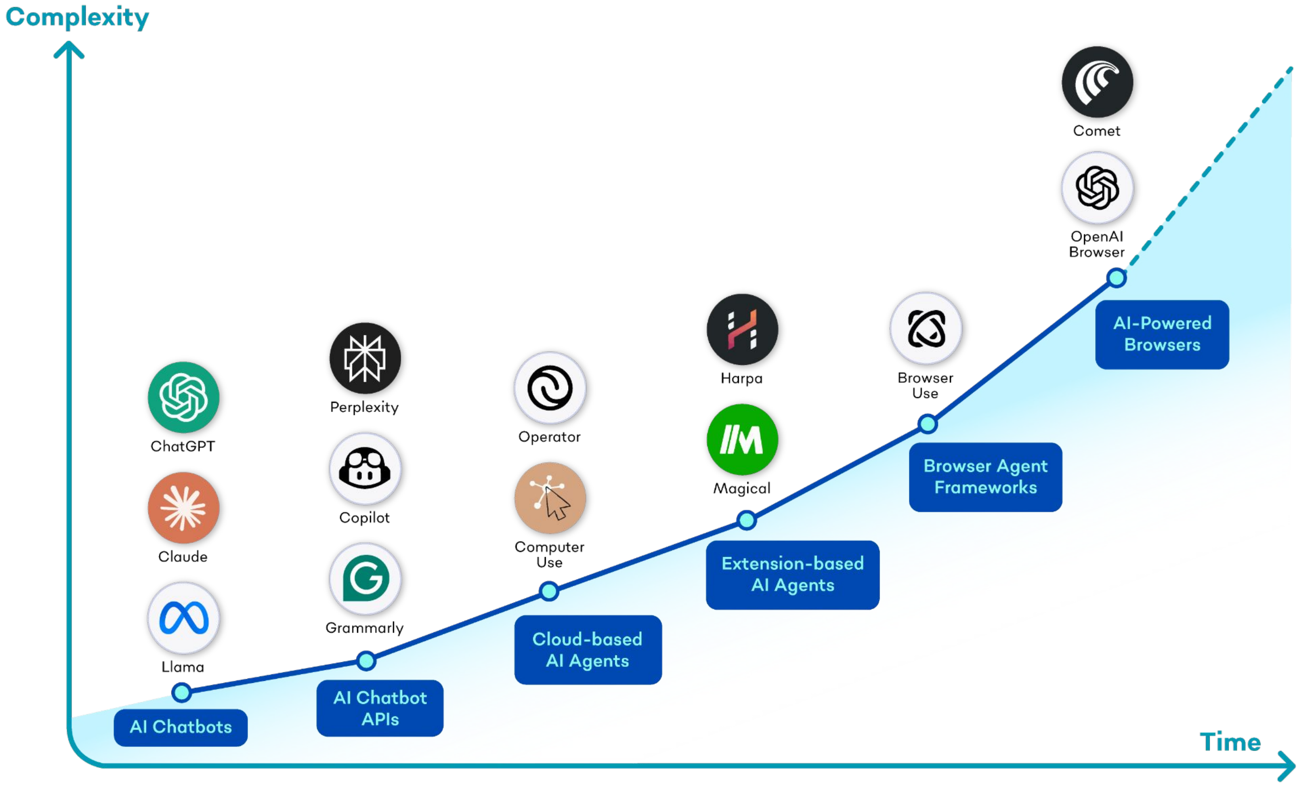
Insider Threat:

- *Emailing customer data to competitors*
- *Printing/screenshotting intellectual property*

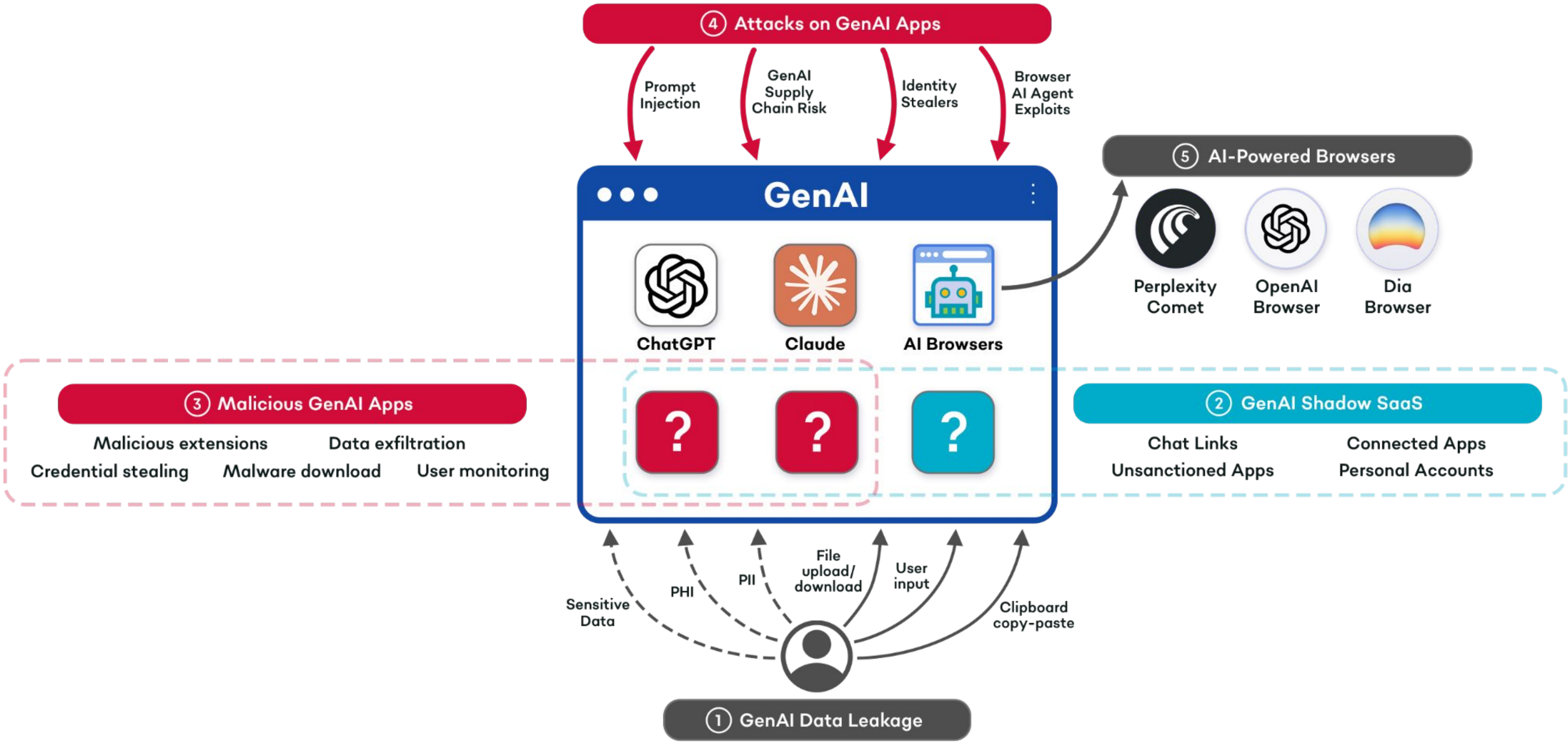
Data Exfiltration Attacks:

- *Identity Attacks*
- *Extension Infostealers*
- *Data Splicing Attacks*
- *Browser AI Agent Exploits*

GenAI: a new threatscape

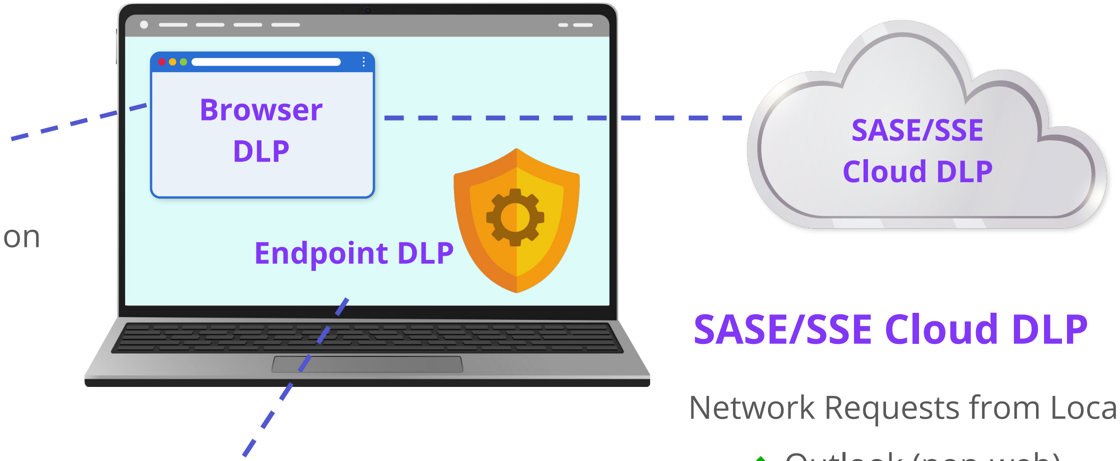


AI Applications Break Traditional DLP + Web Security



Full DLP | Browser + Endpoint + SASE/SSE Cloud DLP

SquareX



Browser DLP

- ✓ Granular User DLP on SaaS
- ✓ Advanced Insider Threat Detection
- ✓ Rogue Browser AI Agents
- ✓ Data Exfiltration Attacks

SASE/SSE Cloud DLP

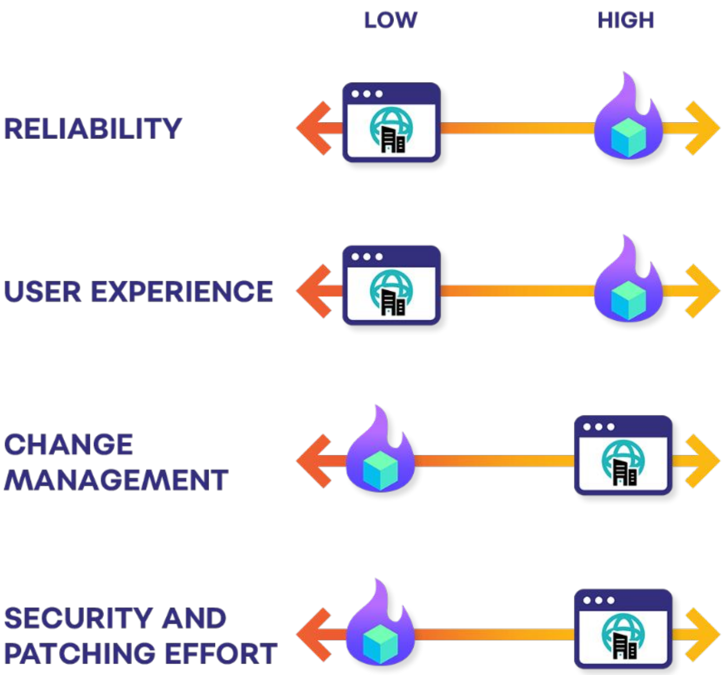
Network Requests from Local Apps

- ✓ Outlook (non-web)
- ✓ Slack (non-web)
- ✓ Zoom (non-web)

Endpoint DLP

- ✓ USB/Removable Storage
- ✓ Bluetooth
- ✓ Local Printing
- ✓ Virtual Desktop

Browser Extensions vs. Enterprise Browsers



LOW

HIGH

RELIABILITY

USER EXPERIENCE

CHANGE MANAGEMENT

SECURITY AND PATCHING EFFORT

Dedicated Enterprise Browsers	Browser Extension
Single point of failure "Crowdstrike Outage Moment"	Cannot bring down the Browser
Major change in user behavior	Invisible to the User
Only one browser Have to remove all other browsers	Bring Your Own Browser Any Browser, any Device
Based on Chromium Update and patching hell?	Fully automatic updates No need for IT to deploy patches

Act early and create a Browser Security Plan

sqrx.com