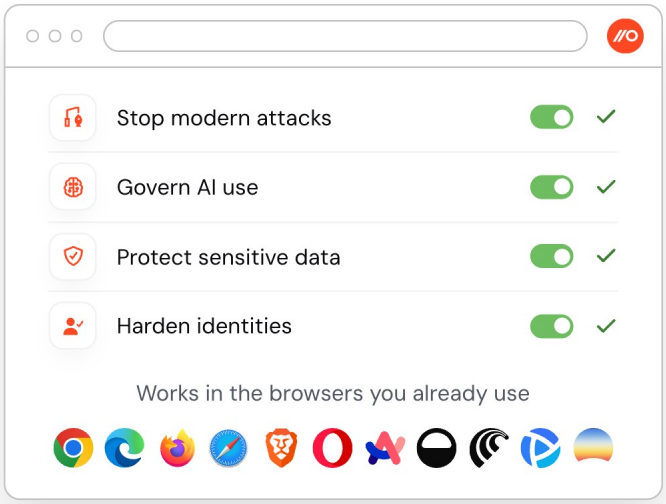
Push Security

Security belongs in the browser.

Push sits closer to your users than any other security tool, so it can stop modern attacks, govern AI use, protect sensitive data and harden identities, right where users work.



Attacks come in. Data goes out.

Attackers use the browser to reach your workforce with fake login pages and downloads. Company data leaves through it too, into AI tools and personal accounts.

190
public breaches since August 2023 were linked to browser-based attacks

1 in 2
payloads Push intercepts arrive outside email, where email security can't see

67%
of employees using AI at work log in with non-corporate accounts (Verizon DBIR 2026)

2 in 5
logins Push observes have no MFA

Your other tools only see pieces. Push sees the page.

Misses the delivery	Where it happens		Misses the aftermath	
Email security Sees the lure but not the page, misses phishing outside email	**SWG / CASB** Sees the domain, not the page or the account	**Push** Sees the page, the paste, and the login	**EDR** Sees the device, not what happens in the tab	**Identity provider** Sees federated logins, not shadow SaaS

One extension, four use cases.

Stop modern browser-based attacks

Stopped on the page, before an account is compromised

- Behavioral phishing detection
- Malicious copy and paste detection
- Stolen session detection

Govern AI

Every AI tool in use, and the account behind each login

- AI app, extension, and agentic browser discovery
- Company-account enforcement
- Prompt capture to your SIEM

Protect data at the browser layer

Risky pastes and uploads stopped as they happen

- Paste controls with redaction
- Upload and download rules
- App category blocking

Discover shadow IT and harden identities

Every login seen, and weak spots fixed at sign-in

- Shadow SaaS and ghost login discovery
- Breached and reused password detection
- MFA and SSO guardrails

Ordinary moments. Real risks.
Stopped at the point of interaction.

The moment	What your stack sees	What Push does
Attacks Lands on a login page that looks normal	✕ The SWG sees a clean, new domain and lets it through.	✓ Push detects the kit and blocks the password before it's submitted.
AI Pastes a customer list into ChatGPT	✕ The CASB sees an approved AI domain, not the personal account.	✓ Push stops the paste and points the user to the approved tool.
Data Uploads a confidential deck to Drive	✕ The CASB sees an allowed domain, not the personal account.	✓ Push sees the personal account and blocks the upload.
Identity Reuses their SSO password on a new tool	✕ The IdP never sees the signup or the reused password.	✓ Push flags the reuse at login and guides the user to SSO.

See everything, find threats first.

Push builds a live inventory from real browser activity: every AI tool, extension, SaaS app, and login, and the account behind each. The same telemetry powers detection, which is how Push researchers were first to find ConsentFix and the first in-the-wild InstallFix attack.

1 → 2 → 3

Discover: Apps, AI tools, extensions, and logins appear as people work

Detect: AI agents and researchers hunt that activity and ship new detections to everyone

Control: Set policy by user group, and Push blocks, warns, or guides in the moment



Detections	Last 24 hours	
Comet agentic browser First seen on 3 devices		New 8 min ago
ChatGPT, personal account Customer data pasted		Warned 41 min ago
Shadow SaaS login notion[.]so · password, no MFA		Flagged 2 hr ago
AiTM phishing kit login-microsoftonline[.]support		Blocked 3 hr ago

"We see the control point moving to the browser. And that's where Push comes in."

Ash Devata · CEO, GreyNoise

Push works for you.

A browser security program that doesn't add to your workload.

Book a demo »

No migration

Installs into the browsers you already use, via MDM or browser policy

No new infrastructure

No proxy, latency, or middleware to manage, and it runs alongside your stack

Fast

100,000 users deployed in under an hour, with zero downtime

Push puts security where it belongs, in the browser. The Push extension runs inside the browsers you already use, so it sees what you see and acts in the moment: stopping phishing and session hijacking, governing AI use, keeping sensitive data where it belongs, and closing identity gaps. No heavy browser migration, and very little upkeep.