Push Security

Attackers operate in the browser. Now you do, too.

The browser is the new battleground

Modern work has moved into the browser. But for most organizations, security hasn't followed.

The result? Attackers are using a range of techniques to target users in their browsers, without even touching an endpoint or their network.

85% of the average workday is spent in the browser.*

95% of organizations responded to a browser-based attack.*

Browser-based threat detection & response

The browser has become the new endpoint. Push Security is the new EDR.

- Detect and block browser-based attacks in real time.
- Accelerate investigations with fine-grained browser telemetry.
- Contain active compromises to impacted apps, users and accounts.
- Proactively harden browser-based attack paths and automatically fix vulnerabilities.

Push Security is like EDR, but for your browser

Geoff Belknap

Deputy CISO at Microsoft
Former LinkedIn, Slack, Palantir

Push Security

HOW PUSH WORKS

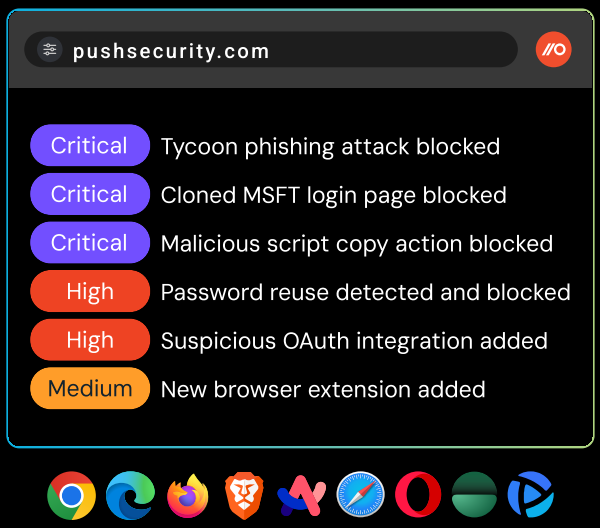
The Push Security browser extension

Push uses a browser extension to make every employee's browser a telemetry source and control point.

The Push extension provides deep visibility of user activity in the browser, enabling attacks to be detected and blocked in real time.

Push is managed via a SaaS platform that can be connected to your SIEM via API or webhooks.

Push supports all major browsers. You can deploy Push within minutes via managed browser config or MDM.



The missing piece in the modern SecOps stack

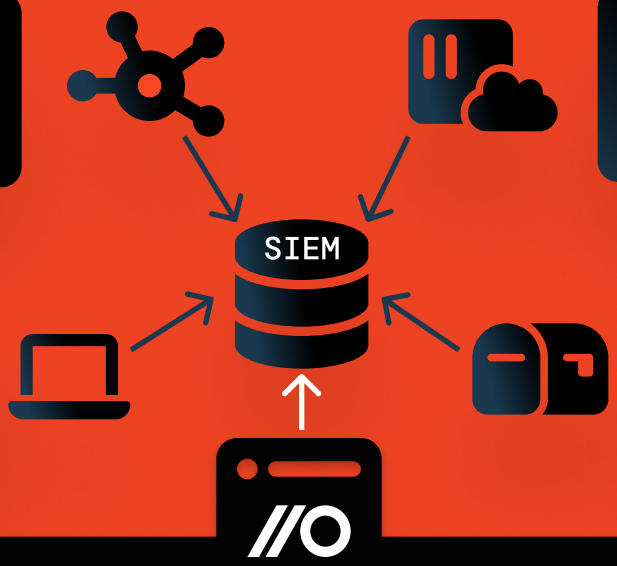
Push Security's telemetry provides blue teams with net-new visibility of browser-based attacks to complement your existing security stack.

Network (e.g. ZScaler)

Monitor internal and web-based traffic for malicious activity

Cloud Services (e.g. Wiz)

Harden and defend enterprise cloud apps and infrastructure



Endpoint (e.g. CrowdStrike)

Detect and block malware on user devices & servers

Email (e.g. Sublime)

Effective at stopping email-based attacks such as BEC

Browser – Push Security

Detect and block web and browser-based attacks that don't touch the network or endpoint and can't be observed by other data sources.

Push Security

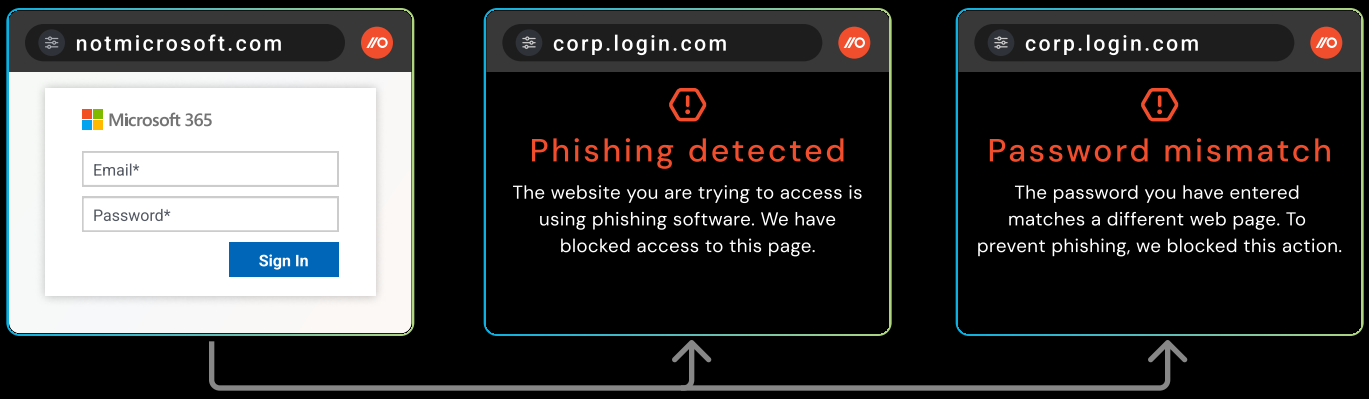
CORE CAPABILITIES

Detect browser-based attacks in real time

Detect & block advanced phishing attacks

Phishing is a bigger challenge than ever for security teams, with MFA-bypassing kits the new normal, non-email delivery vectors catching victims unaware, and the use of layered obfuscation and anti-analysis techniques making phishing harder to detect using email and network controls.

Phishing may no longer stop at the mailbox, but all roads lead to the browser. Push sees the real phishing page that the user sees, as they see it. This enables Push to monitor for malicious properties and content, from cloned login pages to custom attacker tooling, and spot risky user actions — like attempting to enter a password into a page that the credential doesn't belong to. Push detects and blocks this activity in real time as the user loads and interacts with the page.



Intercept browser-based malware delivery

Malware is increasingly delivered to victims via the web browser. In particular, infostealer malware enables attackers to harvest credentials from local applications and the browser.

Attackers are finding success by targeting unmanaged devices lacking security software (e.g. personal or unmanaged BYOD) or by consciously bypassing EDR.

Push monitors common malware delivery mechanisms, such as attacks tricking the victim into running malicious content on their machine (aka ClickFix, FileFix, Fake CAPTCHA).

By preventing malware delivery upstream, Push supports a layered defense against endpoint attacks and prevents stolen credentials and session cookies from being used to take over accounts.

Push Security

CORE CAPABILITIES

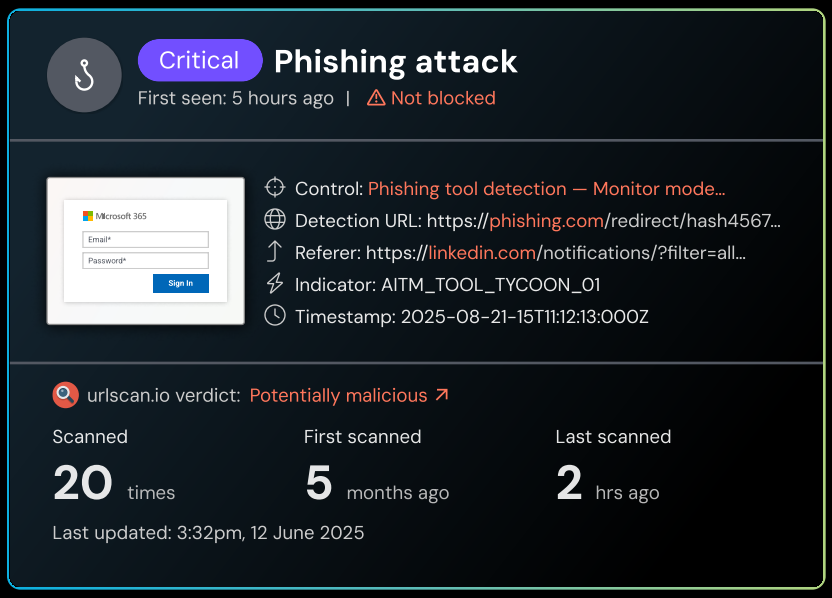
Accelerate investigations & response

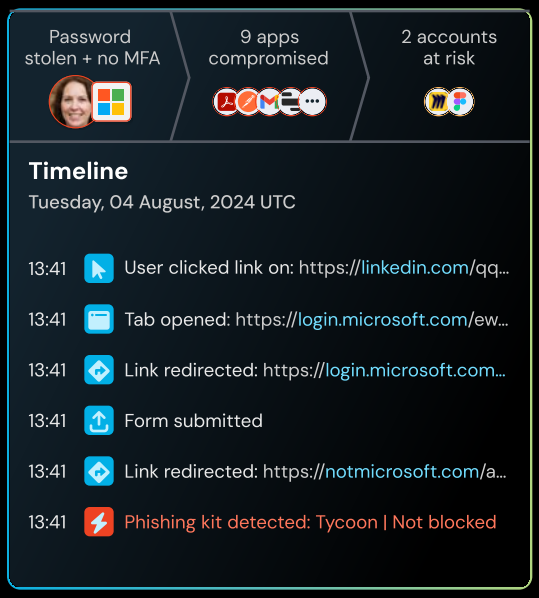
Analyze the context and blast radius of a security incident

Push collects data on key browser actions to provide context to security analysts whenever a security event is generated from a detection.

Push shows you a curated timeline of an incident — such as the links a user clicked, suspicious or malicious page behavior, and user interaction with the page.

You can use this context to investigate the source of a phishing attack, or triage an event if you've set a control to "monitor" rather than "block" mode. If a compromise is confirmed, you can use Push to analyze the blast radius across connected apps and accounts, such as where the same credentials are used, or OAuth integrations are configured.





Build correlated detection and response use cases

You can use Push data along with your existing data sources such as network, EDR, application, and IdP logs to build correlated high-confidence detections. Examples of smart analytics built by Push customers include:

- Matching login events with proxy logs to flag app logins from unapproved locations and devices.
- Automatically resetting accounts using breached credentials via IdP workflows.
- Alerting when an MFA method is enrolled or changed on a high-risk account.
- Reporting on accounts using stolen credentials that have appeared in public data dumps.

Push Security

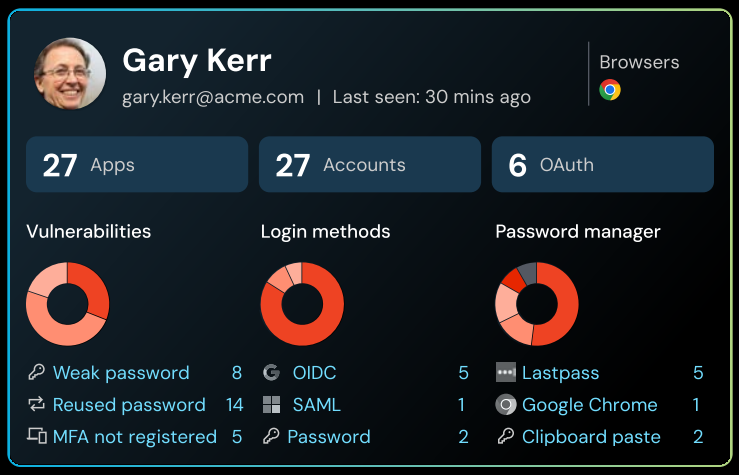
CORE CAPABILITIES

Proactively secure users in the browser

Discover shadow SaaS and fix insecure login methods

Push shows you every app your employees are using (even the unmanaged ones you don't know about), providing detailed information about how users are logging in, and where vulnerabilities exist. This includes accounts missing MFA, where users are logging in with a username and password over SSO, and where a user's password has appeared in a compromised credential feed.

Push also highlights other useful findings, such as where password managers are being used (and which ones) so you can see exactly where credentials are stored, and any OAuth integrations that exist — which could lead to lateral compromises if a specific app or account is breached.

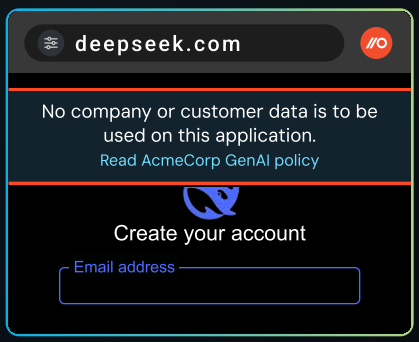


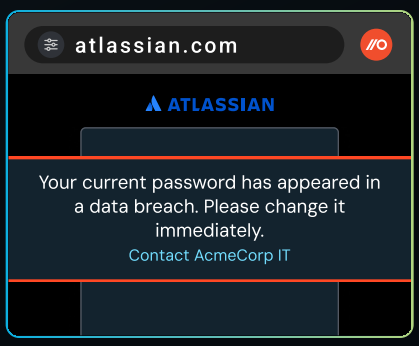
In-browser guidance & enforcement

You can use Push to deliver in-browser guidance to users instructing them to fix the vulnerabilities you identify, or comply with company policy around application use. For example, instructing users to:

- Change breached passwords at the point of login.
- Configure MFA for unprotected accounts at the point of login.
- Adhere to specific guidelines (e.g. no company data in this app).
- Not to use an app (or guide the user to request an exception).

App banners are fully customizable and can be used for just about any point-in-time message you can think of. You can set them to appear on specific page URLs only, or any page on a given web domain. You can also use Push to outright block URLs and URL patterns in the browser.





Push Security

Built by practitioners, powered by research

Push Security was founded by veteran red and blue teamers after we observed attackers shift away from targeting users on their endpoints and instead target them in their browsers.

Realizing security teams lacked the visibility and control to counter this threat, we set our mission: to build **the most advanced security tool in the browser**.

As a research-led organization, our work is driven by real-world attacker behavior and anticipating what comes next. Our researchers continually analyze phishing kits and new browser-based TTPs. Partnering with Push gives you a continuously evolving, threat-informed capability that keeps you two steps ahead of attackers.

Trusted by security teams doing serious work

Josh Lemos
CISO, GitLab

We looked at the enterprise browser approach, but converging on a single platform was tough. Push gave me the security instrumentation and context I needed without onerous headwinds.

Ash Devata
CEO, GreyNoise

No matter the channel for phishing: email; LinkedIn; text; the employee clicks a link that opens a browser session. We see the main control point moving from the endpoint to the browser.

Jason Waits
CISO, Inductive Automation

Security is only as good as its weakest link. From day 1, Push found the gaps that would allow attackers to circumvent our controls. We use Push every day – they're one of my favorite teams to work with.

Myke Lyons
CISO, Cribl

I'm not going to be able to shove a browser on everybody. I need to be able to support them where they are. Push gave us the visibility and control we needed while allowing people to choose their paths.

GitLab · Cribl · upvest · Thinkst Canary · GreyNoise · Risk Ledger · PortSwigger