

BROWSER SECURITY & EXTENSION RISK.



The browser now holds authenticated sessions for email, cloud storage, and every SaaS app an employee uses, all in one place. **A stolen session cookie is functionally a completed login and MFA challenge combined — and an extension with broad permissions can read it directly.**

- SESSION COOKIE THEFT
- EXTENSION PERMISSIONS
- EXTENSION SUPPLY CHAIN
- BROWSER ISOLATION

01 THE MECHANISM



The Browser Holds Every Session, Not Just One

With work concentrated in SaaS and cloud apps, the browser now holds authenticated sessions for email, storage, and financial systems all in one place, **making it a far higher-value target** than any single local app.



Extensions Request Sweeping Permissions

A permission like "read and change all your data on all websites" gives an extension the ability to **see and modify anything happening in the browser**, a scope most users never actually consider.



A Stolen Session Cookie Bypasses MFA

MFA only applies at login. If malware or a malicious extension steals the browser's already-authenticated session token, **the attacker inherits that session without a password or a second factor.**

02 THE FLOW

The Managed Browser Environment

CONTAINED

- Enterprise policy restricts which extensions can be installed to a reviewed allowlist, so a **broad-permission utility never reaches an employee's browser** in the first place.
- Session tokens are bound to the specific device they were issued on, so a **cookie copied off the machine doesn't work anywhere else.**
- High-risk browsing activity runs through an isolated environment, so **even a malicious page can't reach the device** it's rendered on.

The Unmanaged Browser Environment

EXPOSED

- An employee installs a seemingly useful extension with broad host permissions, unaware its **ownership quietly changed hands and an auto-update introduced malicious code.**
- The extension silently reads session cookies for the company's email and cloud accounts and **exfiltrates them to an attacker-controlled server.**
- The attacker loads the stolen cookies into their own browser and **inherits the sessions directly, with no password and no MFA prompt.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Extension Allowlisting & Review	Centrally managed policy restricting which extensions can be installed, with permissions and publisher history reviewed before approval.
Session Token Protection	Binding session tokens to the device they were issued on, so a copied cookie can't simply be replayed from another machine.
Browser Isolation	Executing high-risk browsing activity in an isolated environment rather than directly on the endpoint device.
Extension Supply Chain Monitoring	Ongoing awareness of ownership changes and update behavior for extensions already deployed, not just a one-time approval at install.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Unrestricted Extension Installation From Any Source	No	Any employee can install a broad-permission extension with no review of what it actually requests access to.
MFA Alone, No Session Token Protection	No	MFA secures the login moment, but a stolen, unbound session cookie lets an attacker bypass it by replaying an already-authenticated session.
One-Time Extension Approval, No Ongoing Monitoring	No	An extension approved months ago can change ownership and push a malicious update through the same silent auto-update mechanism.
Treating Browser Security as Solved by Endpoint EDR Alone	No	Traditional endpoint detection focuses on the OS and local processes, not necessarily what an extension does within the browser's own sandbox.
Extension Allowlisting + Device-Bound Sessions + Browser Isolation + Ongoing Monitoring	Yes	Covers what can run in the browser, what a stolen token is worth, and where the riskiest browsing happens.

BROWSER SECURITY & EXTENSION RISK.

ALLOWLIST · ISOLATE · BIND

05 PROGRAM OPERATIONS

A stolen session cookie is functionally as good as a password and a completed MFA challenge combined, since it represents an already-authenticated session an attacker can simply resume.

Extensions auto-update silently in the background, which means an extension trusted months ago can be running different, attacker-controlled code today without anyone re-approving anything.

A broad permission grant is often far more than a utility extension actually needs to function, and is exactly what makes a compromised or malicious extension so valuable to an attacker.

Manifest V3 and similar platform changes exist specifically because extension capabilities had grown broad enough to be routinely abused, not as an arbitrary developer restriction.

06 CONTROL MAPPING

MANIFEST V3

The current browser extension platform standard, restricting some of the broadest and most abusable capabilities extensions previously had by default.

ENTERPRISE BROWSER MANAGEMENT POLICIES

Centrally managed controls that let organizations allowlist or block specific extensions across the workforce.

DEVICE-BOUND SESSION CREDENTIALS

An emerging technique binding a session token cryptographically to the device it was issued on, so a copied cookie doesn't work elsewhere.

OWASP SESSION MANAGEMENT GUIDANCE

General best practices for issuing, protecting, and invalidating session tokens, directly relevant to browser-based session theft.

07 WHAT THIS DOES NOT SOLVE

Phishing and Credential Theft Directly

Browser and extension hardening protects the session layer; it **doesn't stop a user from being phished** into entering credentials on a fake page.

Compromise Outside the Browser

Malware operating at the operating system level can potentially access browser data through other means, **independent of the browser's own protections**.

User-Approved, Overly Broad Permissions

An allowlisted extension can still request more access than it strictly needs; review **reduces but doesn't eliminate** the risk of over-permissioning.

Zero-Day Browser Vulnerabilities

Extension and session controls don't address a **vulnerability in the browser engine itself**, which remains a distinct, ongoing patching responsibility.

08 MYTHS VS. REALITY

MYTH

"MFA makes stolen session cookies irrelevant."

REALITY

MFA only applies at login; a stolen, already-authenticated session cookie lets an attacker **bypass it entirely by resuming the session directly**.

MYTH

"An extension from the official store is automatically safe."

REALITY

Malicious extensions are published directly to official stores, and **legitimate extensions can change ownership** and push malicious updates through the trusted auto-update channel.

MYTH

"Extension permissions don't matter much for simple utilities."

REALITY

A permission like access to all data on all websites gives even a simple-looking tool the ability to **read or modify anything in the browser**, including logged-in sessions.

MYTH

"Traditional endpoint security already covers what happens in the browser."

REALITY

EDR focused on the OS and local processes **doesn't necessarily see what an extension does** within the browser's own sandbox.

MYTH

"If an extension was safe when installed, it's still safe today."

REALITY

Extensions auto-update silently, so an **extension approved months ago can be running different code today** without anyone re-approving it.

09 SPEAK THE PROGRAM — KEY TERMS

SESSION COOKIE / TOKEN

A piece of data proving a user is already authenticated to a service, which an attacker can use to **impersonate that session directly** if stolen.

EXTENSION HOST PERMISSIONS

The scope of websites and data an installed browser extension is granted access to, **often far broader than the extension actually needs**.

MANIFEST V3

The current browser extension platform standard, **restricting some of the broadest capabilities** extensions previously had by default.

BROWSER ISOLATION

Executing risky browsing activity in an isolated remote or sandboxed environment **rather than directly on the local device**.

DEVICE-BOUND SESSION CREDENTIALS

A session token cryptographically tied to the specific device it was issued on, **so it can't simply be replayed from a stolen copy**.

INFOSTEALER MALWARE

Malware specifically designed to **harvest browser data, including stored credentials and session cookies**, for resale or direct account takeover.

SOURCES: MANIFEST V3 · ENTERPRISE BROWSER POLICIES · OWASP SESSION MANAGEMENT · DEVICE-BOUND SESSION CREDENTIALS

BROWSER SECURITY & EXTENSION RISK · FIELD REFERENCE