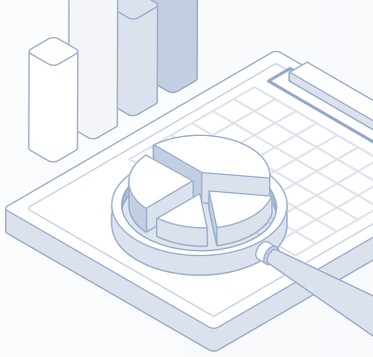
Layer X

Risk Assessment Report: GenAI, Identity, Web, and SaaS Risks



Company Name: [redacted]

Date: November 6, 2024 – November 19, 2024

Users	Identities	Applications	Devices
1,038	**7,113**	**224**	**1,234**

Key Risks ⚠

GenAI Security

23%
Of user pasted data to GenAI applications

67%
Of GenAI tool access is done using non-corporate accounts

Data Leakage Risks

66
SaaS applications had files uploaded to them

1,001
Files uploaded to SaaS applications using non-corporate accounts

SaaS Security

117
SaaS corporate applications that can enforce SSO but currently do not

82
SaaS applications accessed by both corporate and non-corporate accounts

Identity Security

2%
Critical-risk users who use weak passwords, do not apply SSO on all corporate logins and have had a password exposed in a data breach

64%
Of users do not use SSO on all corporate account logins

Browsing Threats

52
Malicious Browsing Events Identified

36
Phishing Attempts Identified

Browser Extensions

12
Risky Extensions Installed

405
Extensions with 'Critical' or 'High' Permission Scope

Actionable Recommendations

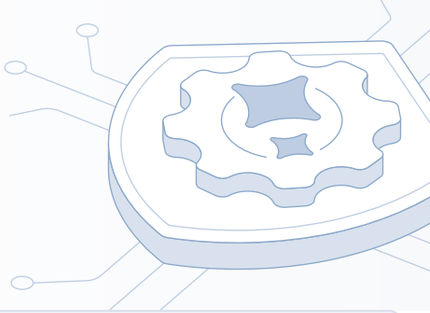
1. Rotate corporate passwords on all weak and medium-strength passwords.
   Action item: Set policy to force rotation of all corporate passwords of medium strength or below
2. Enforce SSO usage on corporate SaaS applications that currently do not require SSO.
   Action item: Set policy to enforce SSO usage on all corporate SaaS applications
3. Prevent password sharing between corporate accounts and non-corporate accounts.
   Action item: Set policy to prevent password sharing between accounts
4. Prevent file upload of files containing PII to SaaS applications using personal accounts.
   Action item: Set policy to block upload of file containing PII to non-corporate accounts
5. Require update of all outdated browsers.
   Action item: Set policy to force version update of all outdated browsers

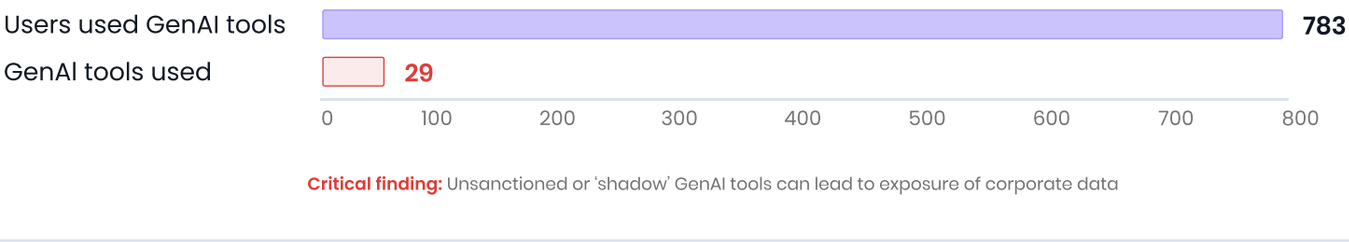
Detailed Analysis:

Click for direct view

GenAI Security

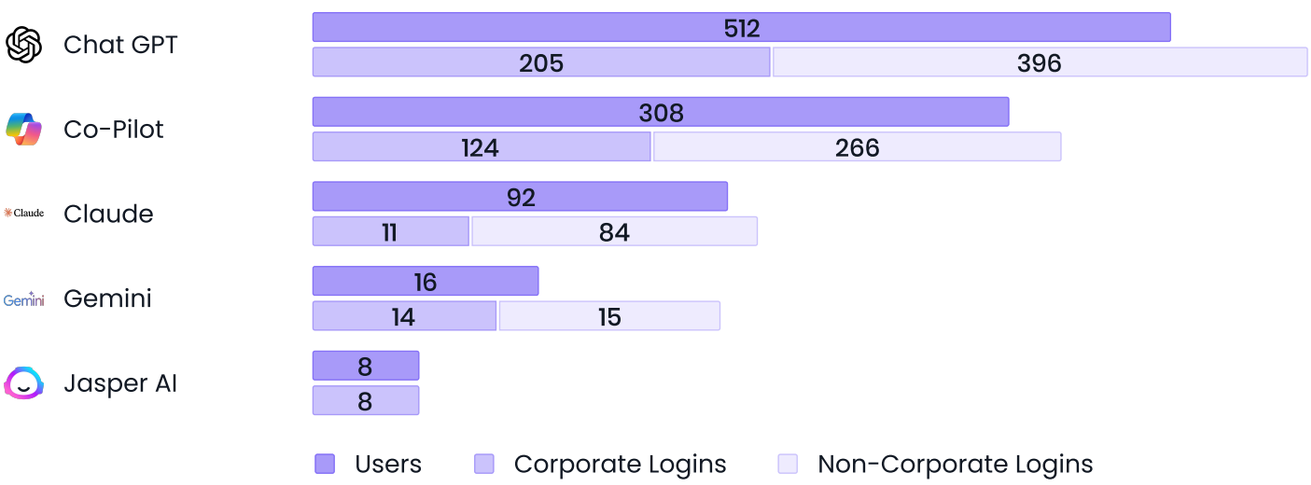
GenAI tools are the new security frontier for many organizations. On the one hand, AI tools have become essential for productivity, while on the other hand, most organizations have little to no oversight on how they are used. This makes auditing GenAI usage and enforcing usage essential for modern organizations.





Critical finding: Unsanctioned or 'shadow' GenAI tools can lead to exposure of corporate data

Top 5 GenAI Tools in the Organization



67%

Of Login events to GenAI tools were with non-corporate accounts

Critical finding: Logging-in to GenAI tools via non-corporate accounts can lead to data exposure and/or corporate data used for LLM training

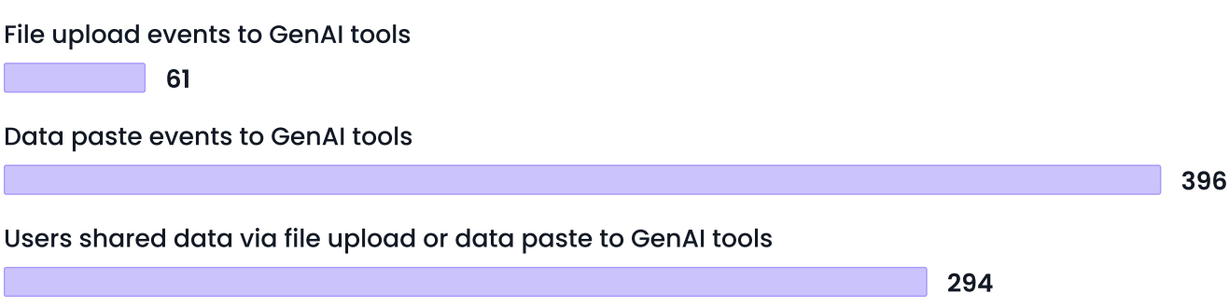
461

Users logged-in to GenAI tools using corporate accounts

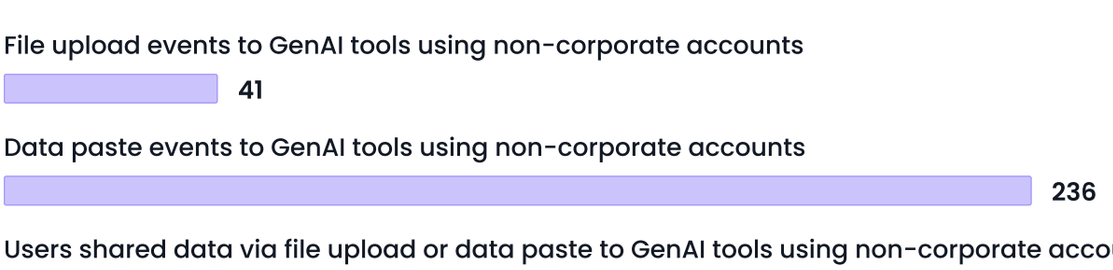
610

Users logged-in to GenAI tools using non-corporate accounts

Information Sharing on GenAI Tools

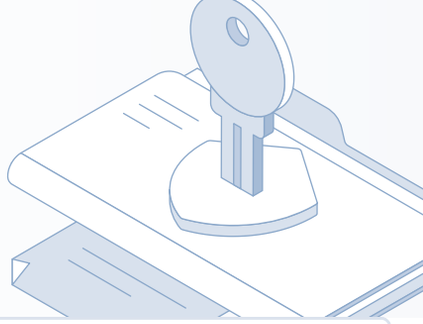


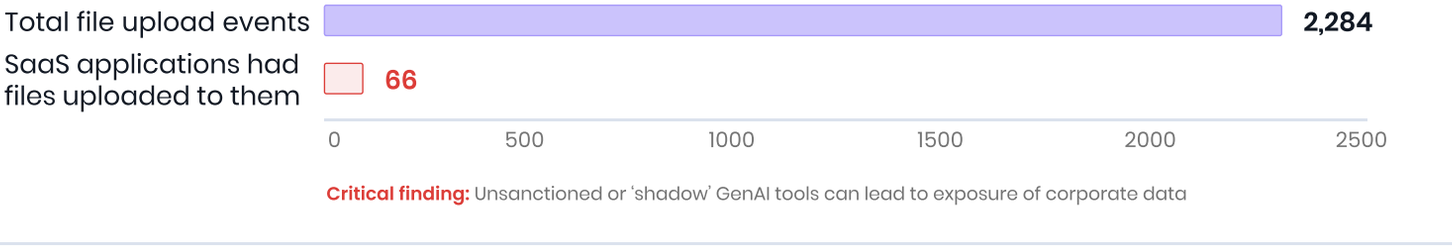
Information Sharing on GenAI Tools Using Non-Corporate Accounts



Data Leakage Prevention

Web-based and SaaS file-sharing applications make it easier than ever to expose corporate data. Whether it is inadvertent exposure by a careless employee or a malicious insider threat, preventing browser-based file-based and file-less data exposure is crucial for maintaining data security.





Critical finding: Unsanctioned or 'shadow' GenAI tools can lead to exposure of corporate data

File Upload by Corporate Accounts	**34** SaaS applications had files uploaded by corporate accounts	**1,283** File upload events using corporate accounts	**568** Users uploaded files using corporate accounts
File Upload by Non-Corporate Accounts	**38** SaaS applications had files uploaded by non-corporate accounts	**1,001** File upload events using non- corporate accounts	**431** Users uploaded files using non-corporate accounts
File Upload by Shared Accounts	**14** SaaS applications had files uploaded by shared accounts	**396** File upload events using shared accounts	**78** Users uploaded files using shared accounts
File-Less Data Exposure	**61** SaaS applications had had data pasted to them	**783** Data pasted events to SaaS applications	**312** Users pasted data to SaaS applications

File Upload by Application Category

Category	File Uploads	Users
File Sharing Sites	82	29
GenAI Tools	61	42
P2P Sites	14	3
SaaS Applications	745	254
Social Media Websites	85	67
Webmail	1,183	508
Others	114	53

SaaS Security

Software-as-a-Service (SaaS) applications have become the beating heart of enterprise work, with most corporate applications now delivered as cloud-based services. However, existing tools are ill-suited to track 'shadow' SaaS applications and usage, leaving organizations exposed to data leakage by unsanctioned applications and/or non-corporate accounts.

Total SaaS applications

224

Critical finding: Unsanctioned or 'shadow' SaaS tools can lead to exposure of corporate data

SaaS applications accessed by both corporate and non-corporate credentials

82

Critical finding: SaaS applications that enable log-in using both corporate and non-corporate accounts can lead to data exposure via account 'crossover'

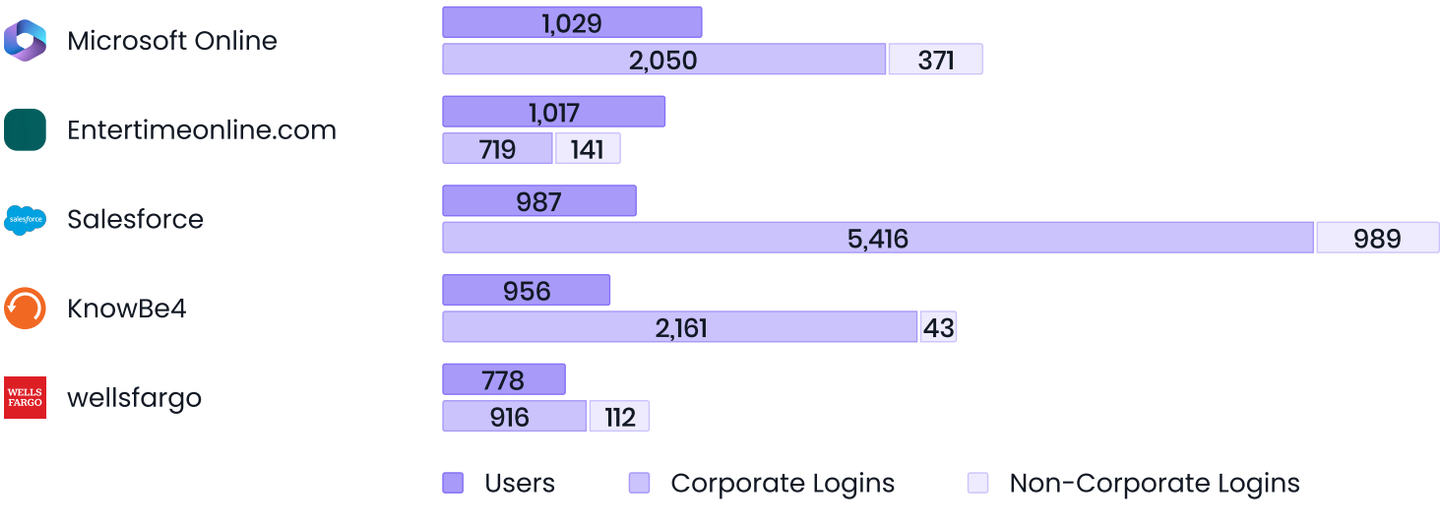
SaaS applications accessed by non-corporate accounts only

94

SaaS applications accessed by corporate accounts only

48

Top 5 SaaS applications



Corporate SaaS Applications

126

SaaS applications accessed by non-SSO corporate accounts

1,026

Users connected to SaaS applications using non-SSO corporate accounts

117

SaaS applications that can enforce SSO, but currently do not

Critical finding: Enforcing SSO/MFA on SaaS applications is an effective method of limiting corporate identity security risks

Multi-Tenant SaaS Applications

983

Users connected to multi-tenant SaaS applications using both corporate and personal accounts, concurrently

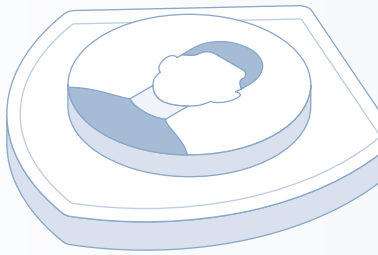
Non-Corporate SaaS Applications

952

Users connected to SaaS applications using non-corporate accounts

Identity Security

Identity is the new perimeter, so securing those identities is critical to safeguarding the organization against outside attacks. Identity security encapsulates multiple layers, including password security, identity governance, external exposure, and more.



User Risk Classification

2%
Critical Risk Users

- Use weak passwords
- Don't use SSO on all accounts
- Exposed in a data breach containing passwords

Critical finding: Weak passwords, exposure on data breaches, and not using SSO are critical identity risks that should be remedied

28%
High Risk Users

- Use weak passwords
- Don't use SSO on all accounts

66%
Medium Risk Users

One or more of:

- Use weak passwords
- Don't use SSO on all accounts
- Re-use passwords across multiple accounts

4%
Low Risk Users

- Use strong passwords
- Use SSO on all accounts
- No shared passwords

Password Security

Of corporate account passwords are medium-strength or below

54%

Of users re-use passwords on corporate accounts

15%

Of users do not use SSO on all corporate accounts SaaS logins

96%

Critical finding: Enforcing SSO/MFA on SaaS applications is an effective method of limiting corporate identity security risks

Corporate Account Exposure in Data Breaches:

Of users appeared in a data breach that included password exposure with their **corporate** account

19%

Of users appeared in a data breach that included password exposure with a **personal** account

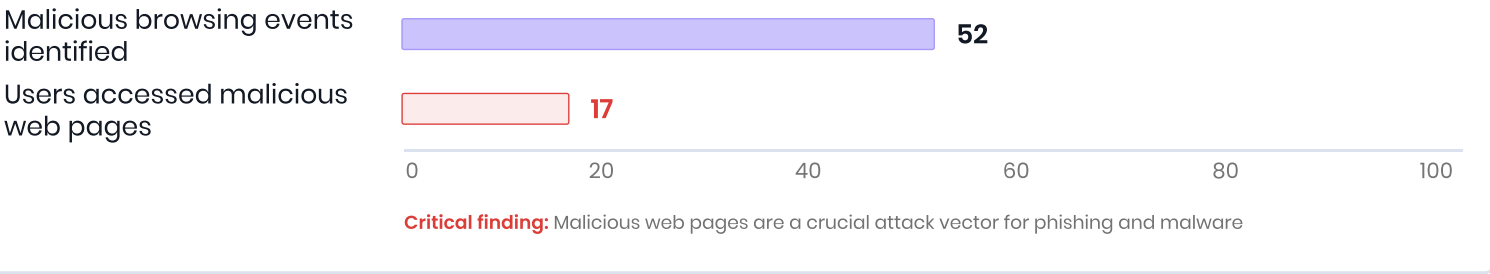
45%

Of users who appeared in a data breach **re-used passwords** between corporate and non-corporate accounts

8%

Secure Browsing

If the browser is the central point of work, that also makes it the central point of risk. Although many organizations deploy multiple layers of web protections, new attack vectors and evasion techniques are challenging traditional protections, meaning that browsing security is a critical vector for organizational data protection.



Critical finding: Malicious web pages are a crucial attack vector for phishing and malware

Phishing Sites

Phishing events identified

36

Users accessed phishing web pages

11

Events of data input to phishing web pages

3

Critical finding: Indicates that no only did the phishing pages bypass existing solutions, but that users interacted with them

Malware

4

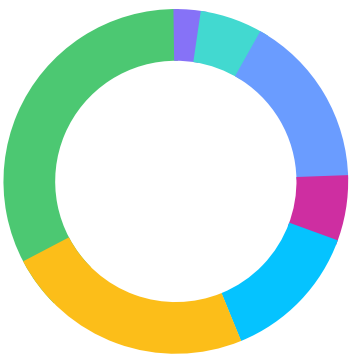
Malware file download events

3

Users attempted to download a file identified as malware

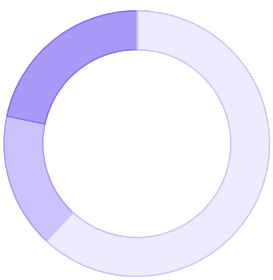
Forbidden Websites

- Adult Sites **1**
- Gambling Sites **3**
- Crypto Sites **15**
- Hacking Sites **3**
- P2P Sites **7**
- Proxy Sites **9**
- VPN Sites **23**



Browser Posture

- Of browsers are fully patched **76%**
- Of browsers are unpatched **10%**
- Of browsers are critically unpatched **14%**

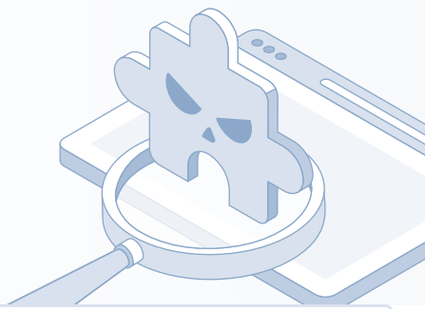


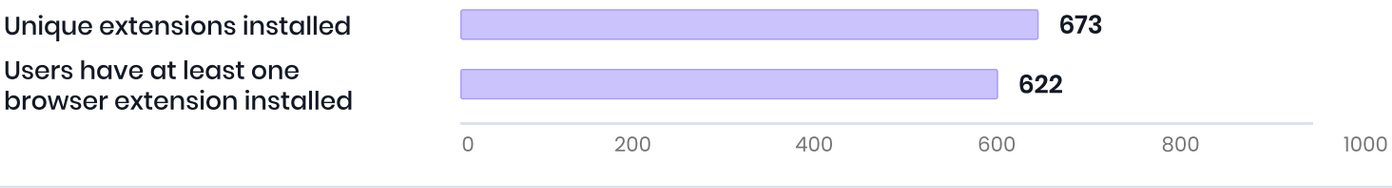
Top 5 Risk Factors

#	Risk Factor	# of Events
1	Hosting on a Legitimate Hosting Service	**26**
2	High Reputation Risk	**18**
3	Homepage Similarity Risk	**15**
4	Phishing Kit Similarity Risk	**12**
5	Download Links Pervasiveness	**8**

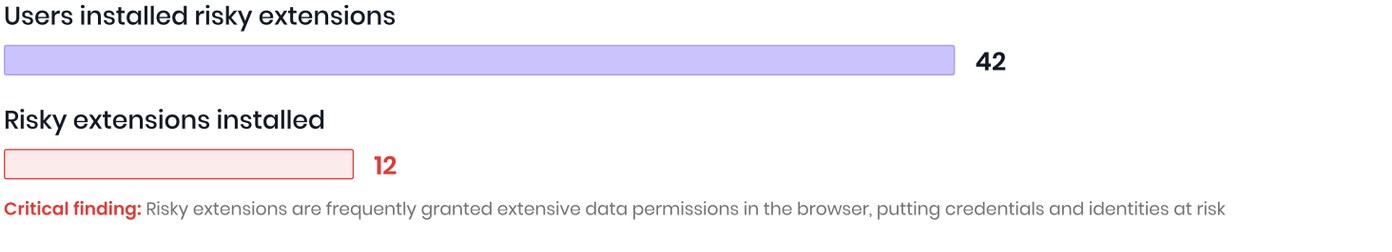
Risky Browser Extensions

Browser extensions are routinely granted extensive permissions to sensitive user data such as browsing data, cookies, password stores, user input, and more. As a result, this makes risky and malicious browser extensions a key emerging attack vector for identity and credential theft attacks.



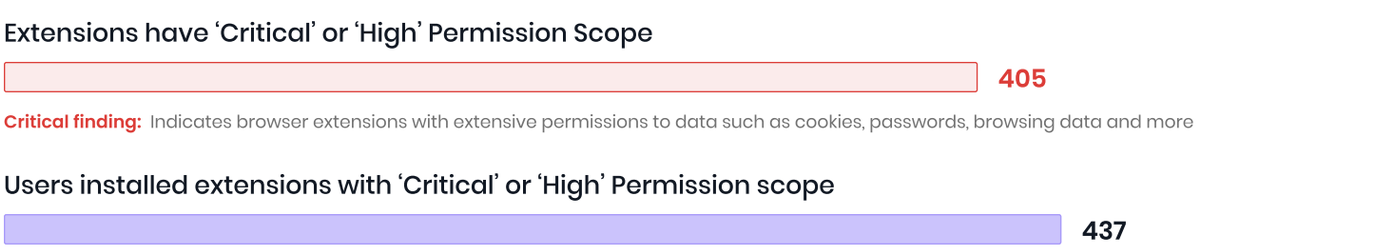


Risky Extensions

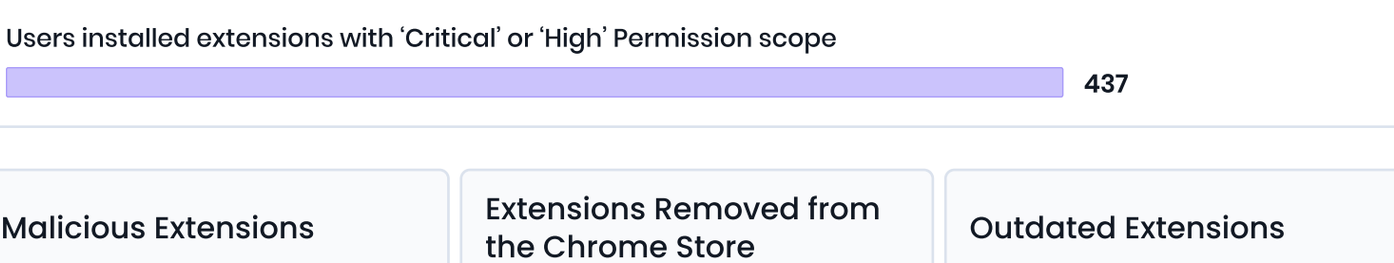


Critical finding: Risky extensions are frequently granted extensive data permissions in the browser, putting credentials and identities at risk

Extensions with Critical or High Permission Scopes



Critical finding: Indicates browser extensions with extensive permissions to data such as cookies, passwords, browsing data and more



Malicious Extensions

4
Known malicious extensions

7
Users installed known malicious extensions

Extensions Removed from the Chrome Store

2
Extensions have been removed from the Chrome store

4
Users installed extensions removed from the Chrome store

Outdated Extensions

412
Extensions have outdated versions of them deployed in the organization

179
Users have installed extensions that are outdated

Obscure Extensions with Fewer Than 10K Downloads

35
Extensions have fewer than 10K downloads on the Chrome store

163
Users installed obscure extensions with fewer than 10K downloads

Extensions by Category:

Category	# of Extensions	# of Users
GenAI Extensions	45	236
VPN Extensions	6	15
Password Managers	11	35