

WHITE PAPER



Browser Extensions

A hidden threat

hello@cytex.io | <https://cytex.io>

© Cytex, Inc. All rights reserved.

Background

Chrome is the most popular browser with a market share of over 65% on the desktop and about 41% on mobile phone. Chrome's over 2.65 billion users worldwide often extend the core browser functionality by choosing from the 188,00+ extensions available in the Chrome store. The most popular categories of extensions are productivity (25%), leisure and fun (24%), photo editing (19%) and developer tools (7%) .¹

Chrome dominates the browser marketplace, and malicious actors have taken notice. In 2022 and 2021, there were 303 and 338 disclosed vulnerabilities that had been exploited. Similarly, bad guys have also weaponized browser extensions to install malware or steal credentials. Recently, a Chrome extension that purported to be an ChatGPT add-on was discovered to be a Trojan horse that hijacked Facebook accounts. Other malicious extensions that claimed to enhance productivity for popular cloud apps such as Google Workspace, Office 365, and Microsoft Azure that use OAuth credentials have been known to access and steal data from these applications.

Understanding the Extension Permissions

Chrome extensions are divided into two main categories².

- **Site permissions:** These are webpages, cookies, or browser tabs that an extension is allowed to access and modify
- **Device permissions:** These are the on-device resources (disk, USB, etc.) that an extension can access on the local device

These permissions are declared in a manifest file that can be reviewed by accessing the permissions section in the installed extension details.

¹ <https://truelist.co/blog/google-chrome-statistics/>

² <https://support.google.com/chrome/a/answer/9897812?hl=en>

For guidance, the following information can be used to evaluate the permissions and align them with the organization's accepted risk profile.

Risk	Permission	Description
Highest	Host permissions	Host permissions allow developers to get access based on a specified list of hosts. Host permissions can be any match pattern [1] - ":///*" means "everything"
High	<all_urls>	The extension wants to interact with the code running on pages which matches any URL that starts with a permitted scheme (http:, https:, file:, ftp:, or chrome-extension). Can be a broad permission with possible risks.
High	app.window.fullscreen.overrideEsc	Can prevent escape button from exiting fullscreen
High	audioCapture	Capture audio from attached mic or webcam
High	browsingData	Clears browsing data which could result in a forensics/logging issues
High	content_security_policy	CSP works as a block/allow listing mechanism for resources loaded or executed by your extensions
High	contentSettings	Could allow plugins to run unsandboxed
High	Copresence	P2P communication
High	debugger	Provides high level super user access
High	declarativeNetRequest	The chrome.declarativeNetRequest API is used to block or redirect network requests by specifying declarative rules
High	declarativeWebRequest	chrome.declarativeWebRequest API to intercept, block, or modify requests in-flight
High	downloads	API to programmatically initiate, monitor, manipulate, and search for downloads. Can be used to download scripts
High	experimental	Access to any of the experimental APIs

Risk	Permission	Description
Highest	hid	Access USB devices
High	history	Full history
High	nativeMessaging	Allows native (Win, Linux, Mac) programs that register with chrome to talk with extensions
High	pageCapture	Gets MHTML (archived Web page) of any page
High	privacy	Can turn off malware protections
High	proxy	Manage Chrome's proxy settings
High	socket	Raw TCP/UDP connection
High	*://*/*	Extension wants to interact with the code running on pages which matches any URL that uses the https: or http: scheme
High	tabCapture	Get picture/video of user's current tab
High	tabs	Can access current URLs and favicons
High	unsafe-eval	Can be used to fetch and execute remote script
High	usb	Interact with any USB device in raw format
High	usbDevices	Used in conjunction with USB permission to specify the types of USB devices the extension wants access to
High	videoCapture	Extension can use webcam, possibly screen contents depending on settings
High	vpnProvider	Extension. can create a VPN tunnel and send/receive packets through it, across sessions
High	web_accessible_resources	This can be used to execute remote scripts.
High	webNavigation	Listen to the websites that a user visits

What should Organizations do?

It is imperative that organizations conduct an inventory of all installed browser extensions and come up with a policy that is consistent with their accepted risk profile.

Cytex EDR users can quickly identify all Chrome extensions and version numbers across all managed devices. Once this inventory is completed, an admin must evaluate the permission model for these extensions using the permission guidance chart.

If you are not a Cytex EDR customer, the Chrome extension permissions can be found through the browser by navigating to the extension and viewing the details. Alternatively, you can review the extension manifest file (manifest.json) that is installed for each directory. The manifest file will contain a permissions entry that can be evaluated to see the extension's entitlement for permissions. The manifest file location is operating system specific. To find out the location for extensions:

- Open a Chrome browser
- In the URL entry, type: chrome://version
- Find the Profile Path

After you have identified the profile path, you will be able to find and review the extension permissions by reviewing the manifest.json file for each installed extension.

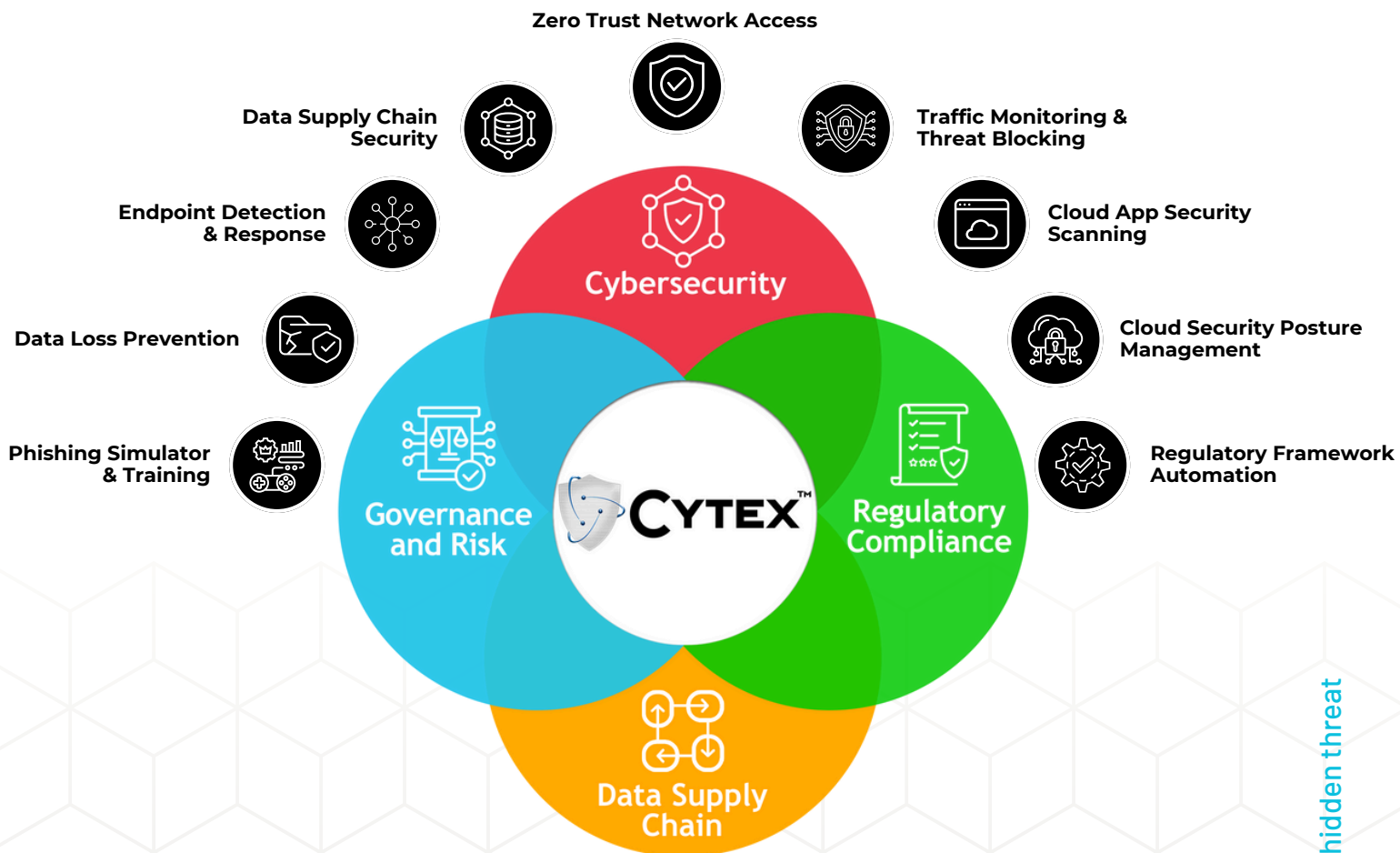


CYTEX™

Unified Resilience Platform

Cytex is a unified resilience platform developed to address the cybersecurity challenges faced by SMBs. Cytex team realizes that SMBs want to grow their business while protecting their valuable data assets against ransomware, cyberattacks, and data breaches. As a unified platform, Cytex provides all the cyber capabilities that enable SMBs to focus on their core business while reducing cost, complexity, and vendor sprawl.

With Cytex, organizations can inventory data exchange partners, conduct CVE indexed vulnerability scans, get cyber threat intelligence, assess cloud and on premise security of applications, perform SOC-2, HIPAA, NIST CSF, PCI, CCPA, GDPR assessments, and manage the security of a hybrid workforce.



<https://cytex.io>



hello@cytex.io



[@cytextsmb](https://twitter.com/cytextsmb)



[@cytexsecure](https://www.youtube.com/c/cytexsecure)