



# Enterprise Browser Battle 1.0

March 2023



Abstract: This document will quantify and compare 47 security features of three Enterprise Browser vendors to find out which one is the most secure.

Author: Patrick Coble – VDISEC @VDIHacker

## Table of Contents

<b>Summary (TLDR)</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Enterprise Browser Use Cases</b> .....	<b>6</b>
<b>Enterprise Browser Vendor Landscape</b> .....	<b>6</b>
Selecting Vendors for this Report .....	6
A Quick Word about the Established Traditional Microsoft and Google Solutions.....	7
<b>Enterprise Browser Vendors Covered in the Report</b> .....	<b>7</b>
Citrix.....	7
Google .....	8
Talon Cyber Security.....	8
<b>Scoring Methodology</b> .....	<b>9</b>
<b>Detailed Analysis and Observations</b> .....	<b>10</b>
<i>1.0 Delivery and Integration</i> .....	<i>10</i>
1.1 Delivery Type.....	10
1.2 Supported Endpoint Operating Systems .....	10
1.3 Enrollment Type .....	11
1.4 VPN-less Access (Internal Apps) .....	11
1.5 Browser Use Enforcement .....	12
1.6 Version Upgrade Control.....	12
1.7 Policy Update Durations.....	13
1.8 Conditional Access Controls .....	13
1.9 Idle Timeout Control .....	14
1.10 Browser Timeout Passcode .....	14
1.11 Endpoint Protection Agent Integration.....	15
1.12 SIEM Integration.....	15
1.13 Chromium Browser Policies .....	16
1.14 Authentication Integration.....	16
<i>2.0 Browsing Controls</i> .....	<i>17</i>
2.1 Website Control.....	17
2.2 Control App Logins .....	17
2.3 Browser Jailbreak Prevention.....	18
<i>3.0 Data Leak Prevention</i> .....	<i>18</i>
3.1 Watermark .....	18
3.2 Screen Capture Protection .....	19
3.3 Keylogger Protection .....	19
3.4 Control File Downloads\Uploads .....	20

3.5 Encrypt Downloads.....	20
3.6 Malicious File Scanning .....	21
3.7 USB Control .....	21
3.8 Clipboard Directional Control.....	22
3.9 Clipboard App Control (Source\Destination) .....	22
3.10 Printing Control .....	23
3.11 Printer List Control .....	23
3.12 Audio and Microphone Control.....	24
3.13 Webcam Control .....	24
<b>4.0 Threat Prevention .....</b>	<b>25</b>
4.1 Malicious URL Protection .....	25
4.2 Read-Only Website Access .....	25
4.3 Leaked Credential Monitoring and Notification .....	26
4.4 Browser Patch Process .....	26
<b>5.0 Endpoint Filters .....</b>	<b>27</b>
5.1 Endpoint Filter — OS Version.....	27
5.2 Endpoint Filter – Disk Encryption .....	27
5.3 Endpoint Filter – Require Screen Lock .....	28
5.4 Endpoint Filter – Require Antivirus .....	28
5.5 Endpoint Filter – Serial Number Filtering.....	29
5.6 Endpoint Filter – Certificates.....	29
<b>6.0 Extension Controls .....</b>	<b>30</b>
6.1 Allow or Block Extension Selection .....	30
6.2 Restrict Extensions Permissions .....	30
6.3 Prevent Apps from communicating with Extensions .....	31
6.4 Force Extension Install.....	31
6.5 Extension Request Workflow .....	32
<b>7.0 Advanced Browser Options.....</b>	<b>32</b>
7.1 Set Custom Header\User-Agent.....	32
<b>7.2 Basic Browser Audit .....</b>	<b>33</b>
Browser Audit Results .....	33
<b>Summary of Results .....</b>	<b>34</b>
Security Feature Rank Overviews.....	34
Security Feature Rank Summary.....	37
Final Score Summary.....	37
<b>Conclusion .....</b>	<b>38</b>
<b>Scoring Appendix .....</b>	<b>39</b>
Other Scoring Summary Matrix .....	42

## Summary (TLDR)

I am pleased to share my first report on a new product category—the Enterprise Browser. An Enterprise Browser is a special web browser for business use. It provides advanced security controls and auditing capabilities not found in popular “consumer” browsers like Chrome, Safari, and Edge.

These days, many businesses rely on SaaS solutions and web apps that run outside the secure confines of the corporate data center. And many people work from home over untrusted networks using unvetted devices that aren’t owned or managed by the company. An Enterprise Browser reduces the security risks posed by SaaS solutions, web applications, and remote workers. It helps protect businesses against data theft, certain types of malware, and other threats by embedding security controls directly into the browser.

For our inaugural investigation, we looked at three Enterprise Browsers: [Citrix Secure Private Access](#) from Tibco Software\Citrix, [Google Chrome Enterprise](#) from Google, and [TalonWork](#) from Talon Cyber Security. Our Google Chrome Enterprise analysis includes BeyondCorp [Enterprise](#), a separately priced product from Google that adds secure enterprise browsing capabilities to Chrome. We compared and graded the solutions by analyzing 47 mutual product features and attributes. All three vendors received high marks, with Talon coming out on top in our ranking.

Browser Security Feature Scores - March 2023			
 VOISEC @VDIHacker	Score	Grade	Rank
Citrix Secure Private Access	79.7	C+	3
Google Chrome Enterprise	82.8	B-	2
Talon Cyber Security	93.0	A	1

This is the first in a series of Enterprise Browser reports I plan to publish. In the coming months, we’ll expand our feature coverage and take a look at other vendors in this space. Of note, Island was invited to participate in this inaugural evaluation but declined to participate at this time.

I hope you find the information interesting and valuable. We had fun investigating the products and kicking the tires.

Please reach out to me on [Twitter](#) or [LinkedIn](#) with questions or feedback. Let us know what other Enterprise Browser features or vendors you’d like us to cover in future reports.

## Introduction

It seems hard to believe, but for over thirty years, businesses have used remote Windows applications and VDI solutions to support offsite workers and centralize IT management. As a VDI security analyst, I've had a front-row seat to the action and have watched the VDI market grow and evolve at an incredible pace. I've always been amazed by how many organizations deploy VDI solutions without fully considering the security implications. Over the years, I've published a series of blogs and research reports to help companies evaluate VDI solutions and compare vendors *purely from a security perspective*.

Now I see a new IT moon rising—the Enterprise Browser. Businesses are using SaaS solutions and web apps to simplify IT operations, speed up software rollouts, and support new hybrid work models. But just like with the VDI market, organizations often fail to fully consider the security implications of using web-based applications and services. Individual business groups often sign up for SaaS solutions independently, without involving or even notifying corporate IT or information security teams.

An Enterprise Browser is a special-purpose browser with enhanced security functionality, designed explicitly with web-based business applications and remote users in mind. It provides enterprise-grade security controls and auditing capabilities that aren't found in consumer-oriented browsers like Chrome, Safari, and Edge.

An Enterprise Browser can help defend against malware, data leakage, and other threats. It can help reduce shadow IT risks. And it is easier and less expensive to deploy and support than a traditional VDI-delivered browser.

Industry analysts like Gartner and IDC are closely monitoring this emerging space. It will be fascinating to watch this new market unfold in 2023. I plan to cover the Enterprise Browser market just like I previously covered the VDI market. Like with my VDI reports, my research will focus exclusively on the security aspects of these products. I won't factor pricing or non-security-related features or attributes into my analysis.

One particular area I plan to pay close attention to in our first report is unmanaged devices. Employees working from home, contractors, and third parties like IT support vendors often access web applications and browser-based administrative consoles using outside devices over which corporate IT and security teams have little visibility and control. Unmanaged devices are a favorite target for threat actors. They are often poorly secured—running outdated or unpatched operating systems, software with known vulnerabilities, and inadequate endpoint security and antivirus solutions. Many Enterprise Browsers support endpoint posture assessment capabilities and other features to reduce the risks posed by unmanaged devices. We take a close look at those features in our first report.

The pandemic forever changed the way many of us work. Many businesses have permanently adopted hybrid work models and allow employees to work from home at least some of the time. Many employees spend most of their working days in the browser accessing Salesforce, Office 365, Google

Workspace, and other SaaS solutions over untrusted networks. The browser is a logical place to implement strong security controls to protect confidential company data and defend against malicious activity.

## Enterprise Browser Use Cases

An Enterprise Browser can benefit any business regardless of size or industry. You can use an Enterprise Browser to provide secure access to any browser-based business application including:

- SaaS solutions
- Internal web apps running on public clouds (AWS, Azure, Google Cloud, etc.)
- Internal web apps running on private clouds

You can also use an Enterprise Browser as a secure, hardened alternative to a consumer-grade browser for employees accessing non-work applications and websites from company-owned and managed devices.

An Enterprise Browser can help reduce your attack surface, protect against ransomware and other types of malware, and defend against data loss. You can use an Enterprise Browser to:

- Defend against insider threats and external threats
- Provide secure web access for managed devices and unmanaged devices
- Improve web security for onsite users and remote users
- Provide secure web access for various users (employees, contractors, freelancers, vendors, business partners, etc.)

## Enterprise Browser Vendor Landscape

The Enterprise Browser market is in the early stages. Several established software vendors and several startups already offer products in this space, including:

- Citrix
- Google
- Microsoft
- Island
- Seraphic
- Talon Cyber Security

### Selecting Vendors for this Report

I contacted several vendors to see if they would be interested in participating in our initial study and would be willing to provide a demo copy of their software. I investigated several established vendors,

including Citrix, Google, Microsoft, and VMware. I was surprised to learn that VMware did not have a product in this space. I skipped over Microsoft because their Edge for Business product is aimed at *managed* devices, and this report spotlights unmanaged devices. Citrix and Google both agreed to participate.

For startups, I contacted Island and Talon Cyber Security, the names that came up most in my research and conversations. Talon accepted, but Island declined to participate.

In future reports, I plan to include other vendors such as Conceal, Epic Browser, Island, Microsoft Edge for Business, Perception Point's Web Security, and Seraphic. If you work at any of these companies and want to participate in this project, don't hesitate to get in touch with me on [Twitter](#) or [LinkedIn](#).

### A Quick Word about the Established Traditional Microsoft and Google Solutions

These two browsers are two of the most deployed worldwide for workforce usage. However, they also have significant disadvantages currently, with their traditional solution typically requiring total device management or user intervention to manage the browser. Google Enterprise gives user-level browser management granularity, which is helpful for unmanaged endpoint scenarios. Microsoft looks like, with the way they can package Edge, they could get into this space for unmanaged devices relatively quickly, but they will make more managing the whole machine and the browser as part of their management suite.

## Enterprise Browser Vendors Covered in the Report

This report compares Enterprise Browser solutions from three vendors: Citrix, Google, and Talon Cyber Security.

### Citrix

Citrix entered this browser space in 2018 when they introduced the bundling of a Chromium browser into their existing Workspace App client used for VDI access. This addition allowed Citrix administrators to publish resources that would be launched locally on the user's endpoint instead of going to a published browser hosted somewhere. Around this time, App Protection was added to the same client that gave the applications the keylogger and screen capture protections which added some protection abilities not yet seen to this point in time. Then in 2021, they released their [Secure Private Access](#) (SPA) and Citrix Enterprise Browser (CEB) solution, a management plane for their Remote Isolation Browser (RBI) solution. This SPA introduced the ability to publish items to the local Workspace App Chromium browser and for specific URLs or conditions to send the users to the hosted Remote Isolation Browser, which was an excellent option for many deployments. They are not doing what many other vendors do, controlling most of the browser settings or all the settings to a managed download or a registration process to an existing browser. The Citrix SPA management console is a purpose-built solution that shows you what you need to control the experience. This complete solution can be purchased outside the typical DaaS, VDI, and NetScaler options many may be familiar with.

## Google

Google created the Chrome browser in 2008, and in 2010, Chrome launched its first enterprise policies for local device management (i.e., via GPO). Then in 2019, they released their Google [Chrome Browser Cloud management](#) offering, leveraging Google Admin Console, allowing administrators to manage browser settings and get reporting for managed Chrome Browsers directly from the Admin Console. Their solution requires IT admins to enroll browsers using a token for device policies or by applying policies at the user level. IT can either manage this download centrally through a software distribution tool or enroll and begin managing existing Chrome installs already in their environment.

Google Chrome is available for free and includes a set of enterprise browser capabilities. Google also offers [BeyondCorp Enterprise](#), a separately priced product that integrates with Chrome and provides additional secure enterprise browsing capabilities. Our Google Chrome Enterprise analysis includes the BeyondCorp Enterprise offering. We parenthetically note when the BeyondCorp Enterprise product fulfills a particular Google capability. Our scoring charts also use color coding to highlight BeyondCorp Enterprise's capabilities.

## Talon Cyber Security

[Talon Cyber Security](#) was founded back in 2021 and set out to make a purpose-built enterprise browser solution. Their solution looked at the most common weaknesses of existing browsers and added some controls and features that didn't exist in standard Chromium-based browsers. Their enrollment model is much simpler than others, with a welcome email to a managed download, install, and log-in, and you are secured and ready to roll. Their policy engine and controls were purpose-built for this solution, resembling familiar firewall or group policy architectures.

The TalonWork browser provides various built-in enterprise security, like data leakage prevention features, threat protection functionality, and Zero Trust capabilities, such as granular authentication and authorization controls. Their solution integrates with popular identity providers to simplify user onboarding and policy enforcement. Talon also offers integrations with external file scanning and threat intelligence services like CrowdStrike Falcon Intelligence to defend against malware and block access to potentially harmful websites.

Talon Cyber Security is well funded (They raised \$100M in 2022). They also have relationships with CrowdStrike and Microsoft. They are a Microsoft for Startups program member, and you can purchase their product on the Azure and AWS Marketplaces.



## Scoring Methodology

To compare the three solutions side-by-side, we identified 47 mutual product features and attributed them to score them. To get our hands around the data and quickly grade and rank the vendors, we organized the features into seven distinct categories:

1. Delivery and Integration
2. Browsing Controls
3. Data Leak Prevention
4. Threat Prevention
5. Endpoint Filters
6. Extension Controls
7. Advanced Browser Options

To simplify the analysis and make the information easier to digest, we consolidated some features we felt were similar. Some of these solutions were surprisingly feature-rich and customizable. We could have easily looked at hundreds of features had we not focused only on capabilities common to all three products. In the future, we may expand our analysis to cover more features.

We used a ranked scoring system to identify the best solution in each feature category. Each vendor started with a perfect 100/A+ score. The best vendor in each category had zero points deducted. We deducted points from the other vendors to reflect feature deficiencies or security gaps compared to the best vendor. (In some cases, two or all three vendors received identical scores). We applied the deductions to create our final grade for each solution.

# Detailed Analysis and Observations

## 1.0 Delivery and Integration

### 1.1 Delivery Type

There are many ways to deliver a browsing experience. The most common is the local installation of the browser, where a package is managed or unmanaged on a system. Another option is a hosted solution where the user connects to something that connects them to a browser. Both options provide isolation and control, but there are cost, performance, and feature tradeoffs to consider.

**Citrix Secure Private Access** — Local Managed (Secure Private Access) and Hosted (Remote Browser Isolation)

Google Chrome Enterprise — Local Managed

TalonWork — Local Managed

**Citrix is more secure** because it supports both delivery types. Talon and Google are tied for second because neither supports a remote browser isolation (RBI) option.

### 1.2 Supported Endpoint Operating Systems

We looked at the number of endpoint operating systems each product supports.

Citrix Secure Private Access — Five operation systems: ChromeOS, iOS, Linux, macOS, and Windows.

Google Chrome Enterprise — Six operating systems: Android, ChromeOS, iOS, Linux, macOS, and Windows

TalonWork — Four operating systems: Android, iOS, macOS, and Windows

**Google scored highest** because they can be used on all six primary operating system types: Android, ChromeOS, iOS, Linux, macOS, and Windows. Citrix is in second place with the ability to support five operating systems with Citrix Secure Private Access and Citrix Remote Browser Isolation with six operating systems based on its HTML 5 browser client. Talon is in third place with four operating systems.

### 1.3 Enrollment Type

There are many ways to distribute browser software and enroll new devices. Each vendor takes a different approach. Since we are focused on unmanaged devices for this first enterprise browser comparison, we are looking for solutions that make it easy and secure for users to download and set up the browser on their own endpoints with little or no corporate IT involvement.

Citrix Secure Private Access — CEB Download Workspace App & Install, RBI Browser Access to an HTML Browser

Google Chrome Enterprise — Download & Install then an Enrollment Token (Script\Reg File) or Google Cloud Identity Managed Profiles

TalonWork — Welcome Email, Download\Install

**Talon has a more secure** enrollment type because users must provision based on their Identity (IdP) Provider. TalonWork users will receive a welcome email prompting them to download the TalonWork browser. Citrix is in second place due to its flexibility of enrollment methods based on your requirements. With Citrix, when a user tries to access the configured resource, the controlled browser appears, whether the local Chromium-based browser or the Remote Isolation Browser, based on the protections required and policies configured. Google Chrome Enterprise is in third place, with its local or cloud-based management of an existing Google Chrome installation on the device.

### 1.4 VPN-less Access (Internal Apps)

This feature allows users to access internal applications from wherever they are without another VPN or VDI solution. A unified solution is more secure than other solutions requiring more servers, components, consoles, and solutions.

Citrix Secure Private Access — Yes, with an integrated gateway solution

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Partial (Integration with leading VPN and ZTNA Solutions)

**Citrix and Google are more secure** because they allow users to access internal applications natively within their solutions. Talon is in third place based on relying on their integration with multiple VPN and ZTNA providers, which is valuable for customers who can leverage their existing investments vs. deploy a new solution.

## 1.5 Browser Use Enforcement

This feature prevents users from accessing specified web applications from a browser other than the Enterprise Browser sanctioned by corporate IT.

**Citrix Secure Private Access** — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Partial (Integrations with IDPs)

**Citrix and Google are tied for first place.** Citrix has the native ability to force the use of its solution based on its control of the network layer paired with its policy controls. TalonWork is in third place, offering multiple ways to enforce access, such as conditional access rules configured with a third-party Identity Provider.

## 1.6 Version Upgrade Control

Browsers are a common target for threat actors. Enterprise Browser vendors regularly release software patches and updates to address vulnerabilities. Version upgrade control features let you track and manage browser releases centrally and force upgrades across your user base outside typical endpoint update channels.

**Citrix Secure Private Access** — Partial (Tied to Workspace App)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Google and Talon are more secure** because they can force specific versions and report on their managed browsers' versions. Citrix is in third place because of its dependency on the Workspace App client being updated to update the Chromium version and requiring Chromium version reporting for each device. Citrix's Remote Browser Isolation hosted solution is automatically patched. Still, the browser version is hidden from the user and administrator, so it is impossible to determine if it is the latest version with either delivery method without testing within the session.

## 1.7 Policy Update Durations

We measured the time it takes to propagate a policy change to an endpoint. Time is of the essence for containing risk and mitigating certain types of threats. An Enterprise Browser must update policies in seconds rather than minutes.

Citrix Secure Private Access — ~20 Seconds

Google Chrome Enterprise — ~20 Seconds

TalonWork — ~10-15 Seconds

**Talon is more secure** because they update most policies within 10-15 seconds after a change has been made. Citrix and Google are in second place, with many setting changes taking effect in less than 20 seconds and others taking effect on the next login. We saw the most variability with Google Chrome Enterprise, which took as short as 10 seconds and as long as 3 minutes to propagate changes.

## 1.8 Conditional Access Controls

This feature lets you control access to applications or websites based on a defined policy. This is a foundational policy expectation on most security-related systems where a baseline configuration can be applied to all devices. Some users, groups, devices, or filters allow them to be more secure or less secure based on their requirements.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes

TalonWork — Yes, with more granular policies

**Talon is more secure** due to its ability to control the security policies based on users, groups, devices, device posture, and policies with more granular control capabilities from its singular policy engine. Citrix and Google are tied for second place for having basic controls, but fewer than Talon, and some policy administration is split between consoles in those solutions. This is a must-have feature for all vendors, and we expect vendors will extend the depth and breadth of these capabilities over time.

## 1.9 Idle Timeout Control

This feature automatically locks the browser session after a configurable period of inactivity. It is particularly useful for unmanaged devices, where users may have disabled native endpoint lock screen or screensaver functions.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — No (Coming Q1-23)

TalonWork — Yes

**Citrix and Talon are more secure** because they detect and control an idle user's session. Google is in second place as they do not support this feature.

## 1.10 Browser Timeout Passcode

This feature is related to the Idle Timeout Control feature. This control allows a passcode to be created that allows the user to reauthenticate to the system beyond any idle endpoint protections. When sensitive data is being accessed, this can be a robust control to help prevent endpoint takeover. If this is a managed device, you will still typically have a password-protected screensaver set to a specific duration based on your compliance requirements.

Citrix Secure Private Access — No

Google Chrome Enterprise — No

TalonWork — Yes

**Talon is more secure** because they detect and control an idle user to lock the browser session. Google and Citrix are tied for second place as they do not support this feature.

## 1.11 Endpoint Protection Agent Integration

Some Enterprise Browsers offer integrations with third-party threat intelligence services and endpoint protection services for advanced file-scanning, URL-scanning, and device posture assessment functions. We expect many Enterprise Browser vendors to expand their integrations' breadth and depth over time.

**Citrix Secure Private Access** — Partial (Coming 2023 CrowdStrike)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Talon and Google are more secure** because they integrate with endpoint protection and threat intelligence vendors. Talon and Google integrate with CrowdStrike Falcon Intelligence for file scanning and URL filtering; and CrowdStrike Falcon Sensor for posture assessment of managed devices. Citrix is in third place as it will integrate into CrowdStrike later this year in 2023. This integration will even the playing field for this feature. We also know that each vendor will continue integrating with more endpoint protection solutions.

## 1.12 SIEM Integration

Most Enterprise Browsers let you forward logs and event messages to an external Security Information and Event Management (SIEM) system. SIEM solutions simplify threat detection and response by gathering, aggregating, and correlating events from various sources.

**Citrix Secure Private Access** — Yes (Analytics) (Splunk, Microsoft Sentinel, Kafka\Logstash Connection)

Google Chrome Enterprise — Yes (Palo Alto, Splunk, Chronicle)

TalonWork — Yes (Splunk, CrowdStrike LogScale, Microsoft Sentinel)

**All three vendors are tied** in this area, so customers are advised to determine which vendor provides the SIEM integration that best meets their needs.

### 1.13 Chromium Browser Policies

This feature lets you control the preferences available to a browser and, in this case, in the Secure Enterprise Browser space. They are all Chromium-based browsers currently. This can allow you to control everything you could typically control when the browser is being managed. This can become an essential filter in high-security industries as your organization may be required to configure specific browser settings to ensure a security baseline is applied.

Citrix Secure Private Access — Partial (4x Policies)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Google and Talon are more secure** due to their ability to control with policies all accessible Chromium-based preferences via approach. Citrix is in third place based on them only having provisions only to configure four policies currently.

### 1.14 Authentication Integration

Most Enterprise Browsers integrate with external IdPs to simplify user provisioning, enable single sign-on (SSO) and enforce conditional access controls.

**Citrix Secure Private Access** — Yes, (Kerberos, SCIM, Okta, AzureAD, Ping, OneLogin, ... Others)

**Google Chrome Enterprise** — Yes, (SCIM, Okta, AzureAD, Ping, OneLogin, ... Others)

**TalonWork** — Yes, (SCIM, Okta, AzureAD, Ping, OneLogin, ... Others)

**Citrix is more secure** using Kerberos authentication and the same SCIM integrations as the Google and Talon solutions. All three of these vendors can integrate with other identity providers. Some provide more native integration, but each allows SAML integration with other IdPs.



## 2.0 Browsing Controls

### 2.1 Website Control

Website access controls are an essential feature of any Enterprise Browser. Every Enterprise Browser at least supports basic allow list/deny list functionality. Some vendors support more advanced or granular access controls.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** as they can control which websites users can visit based on users, groups, devices, and policies. They have varying policy control capabilities, but they all support this feature. This is a must-have feature for all vendors.

### 2.2 Control App Logins

This feature lets you control access to specific URLs, web applications, or website categories based on a user's login credentials. You can use it to prevent employees from accessing personal accounts at work. For example, you could prevent users from copying business data to a personal cloud storage account (e.g., allow the user to access Dropbox only when using their corporate login credentials). The Enterprise Browser will block access if they try to log in to Dropbox using their personal credentials.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** as they allow the control of application logins based on their policies and controls.

## 2.3 Browser Jailbreak Prevention

This feature can prevent users from escaping the browser session to open other applications. This can help ensure that the user can only access the specified resources and no other items and escape this controlled enclave.

Citrix Secure Private Access — Partial (Remote Browser Limitations)

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Google and Talon are more secure** as they can help prevent access to sites defined within policy from other sources on the endpoint. Citrix is a close second place as they can limit access to internal applications if it's the only path to the application, but with fewer policy controls than the others. All three vendors can also be integrated with IdP providers to prevent external applications access too.

## 3.0 Data Leak Prevention

### 3.1 Watermark

This feature lets you add a semi-transparent watermark to the browser display to defend against data theft or copyright infringement if a user photographs or capture a screen. The watermark could include identifying information such as the username, agent name, client IP, or other session details.

Citrix Secure Private Access — Yes (Per URL)

Google Chrome Enterprise — No

**TalonWork** — Yes (Per URL/App/Category)

**Citrix and Talon are more secure** as they allow the ability for a watermark to be applied to the browser session, so if the screen is captured locally or by another device, it could help with the incident response. Google is in third place as they do not support this feature.

### 3.2 Screen Capture Protection

This feature can prevent the endpoint's screen from being captured locally by a malicious program or productivity tool. This has been a growing attack vector with the rise of Stealer Logs that aim to log all keystrokes and sell them to the highest bidder for effective and consistent identity theft, extortion, and other criminal activities with this data. This has always been a weakness within many application delivery systems until 2010, when Citrix was introduced to the mainstream outside of an endpoint protection product solution space and added to their VDI product. This has been carried over to many other systems since.

Citrix Secure Private Access — Yes (Per URL)

Google Chrome Enterprise — No

**TalonWork** — Yes (Per URL)

**Citrix and Talon are more secure** as they can prevent the capture of their screens by redacting the content with a blank screen on a per-URL/category or SaaS application basis. Google is in third place as they don't support this feature.

### 3.3 Keylogger Protection

This feature can prevent the endpoint's keystrokes from being captured locally by a malicious program. This has been a growing attack vector with the rise of Stealer Logs that aim to log all keystrokes and sell them to the highest bidder for effective and consistent identity theft, extortion, and other criminal activities with this data. This has always been a weakness within many application delivery systems until 2010, when Citrix was introduced to the mainstream outside of an endpoint protection product solution space and added to their VDI product. This feature has been carried over to other solutions since.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — No

TalonWork — Yes

**Citrix and Talon are more secure** as they prevent keystrokes from being logged from the endpoint. Google is in third place as they don't support this feature.

### 3.4 Control File Downloads\Uploads

This feature can prevent the downloading or uploading of files within the defined browser configuration. This is one of the primary data leak protections that most clients think of when they want to protect their web applications more than just the traditional deployment methods. When a web application hosts sensitive data that could be exfiltrated intentionally or unintentionally and could damage the business and the customers, it becomes essential to have this feature.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes (Granular)

**Talon is more secure** as it can control file uploads and downloads based on file type, content, MIP/AIP tags, and on a per-URL/category or SaaS application basis. Citrix and Google are tied for second place as they have fewer controls than Talon.

### 3.5 Encrypt Downloads

This feature can allow a user to download content from their browser but in a controlled manner where it may only be used in the same secure browser after being downloaded. This can allow the administrator to enable downloads but know that this one-way encryption protects the data and that the users must use the browser to access, which has all the security controls we are discussing in this analysis.

Citrix Secure Private Access — No

Google Chrome Enterprise — No

TalonWork — Yes

**Talon is more secure** as they allow the ability to create a predefined set of sites that the user can access and not. Citrix and Google are tied for second place as they don't support this feature.

### 3.6 Malicious File Scanning

This feature will allow scanning the files accessed through the browser and downloaded. This can help protect the users by blocking access to known and potentially malicious files. This ability is critical since many attacks start from executing a single file.

Citrix Secure Private Access — Partial (IBOSS)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Google and Talon are more secure** as they allow administrators to configure some level of download reputation-based scanning. Google and Talon have built-in file scanning abilities and integrations with CrowdStrike Falcon Intelligence for additional reputation and machine learning enrichments. Talon also integrates with OPSWAT for CDR (Content Disarm and Reconstruction) scanning. Citrix is in third place with its default settings of the Chromium-based installation in their Citrix Remote Isolation Browser and their Enterprise Browser product bundled with Citrix Workspace App installations. However, since Citrix has integration with IBOSS, it is in third place because it requires another solution, and there isn't strong policy integration with both of their delivery methods.

### 3.7 USB Control

This feature can prevent USB storage devices from downloading or uploading data into the session. This is still a standard attack avenue where a malicious document is loaded onto a storage device and is activated by its execution by a user. The abilities of each vendor will vary, but blocking these devices is essential in high-security deployments, and in some compliance, bodies are required. When a web application hosts sensitive data that could be exfiltrated intentionally or unintentionally and could damage the business and the customers, it becomes essential to have this feature.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — No

TalonWork — Yes

**Citrix and Talon are more secure** as they can prevent using USB devices within their session policies. Google is in third place as they do not support this feature.

### 3.8 Clipboard Directional Control

This feature can prevent the user from copying and pasting into or out of the web session. Having the ability to control the directionality is critical for this feature. In most deployments, it's recommended to use a password manager, and preventing users from pasting their password into the session could significantly impact their workflows. This is commonly overlooked as a possible attack avenue. It's just seen as text. When a web application hosts sensitive data that could be exfiltrated intentionally or unintentionally and could damage the business and the customers, it becomes essential to have this feature.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — No

TalonWork — Yes

**Citrix and Talon are more secure** as they can control the clipboard and its directionality to specific user groups within the deployment. Google is in third place as they do not support this feature.

### 3.9 Clipboard App Control (Source\Destination)

This feature allows you to control the clipboard between the sources and destinations within the browser outside the overall clipboard control previously evaluated above. This is the next level of granular clipboard control, as this can allow administrators to copy or paste to specific locations based on the URL of the source and target.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** due to their ability to control clipboard sources and destinations users can have based on users, groups, devices, and policies.

### 3.10 Printing Control

This feature allows printing control within the web session based on the policy configured. This is commonly overlooked as a possible attack avenue. It's just seen as printing without realizing the physical and digital impacts based on the print jobs' contents. When a web application hosts sensitive data that could be exfiltrated intentionally or unintentionally and could damage the business and the customers, it becomes essential to have this feature.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes

**TalonWork** — Yes (Per URL/App/Category)

**Citrix and Talon are more secure** as they can control with more granular policy controls. Google is in third place as it can block printing without as many controls as other vendors.

### 3.11 Printer List Control

This feature only allows the user to print to a specific printer beyond the previous, more extensive printing control policy above within this analysis. This is a more granular policy control used in high-security web applications where print jobs must be controlled beyond the essential ability to print. This could be used when the company wants to restrict print only to office printers or in healthcare to allow the print to virtual printers that are fully logged.

Citrix Secure Private Access — No

Google Chrome Enterprise — No

TalonWork — Yes

**Talon is more secure** as they allow this ability to control which specific printers a user can print to. Citrix and Google are tied in second place as they do not support this feature.

### 3.12 Audio and Microphone Control

This feature allows the control of audio out and audio in via a microphone device. This will commonly be the lowest risk in a rule hierarchy, but depending on the use case, this can be important to a business's overall security. Audio is most commonly a risk in the healthcare, call center, and legal industries as the dictations played could contain sensitive health, legal, identity, and credit information that could damage the customers or the business if leaked.

Citrix Secure Private Access — No

Google Chrome Enterprise — Partial (Microphone Only)

TalonWork — Yes

**Talon is more secure** as it can control the audio output and input per URLs, content categories, or SaaS applications. Google is in second place as they can block just the microphone, but they still need the granularity per URL. Citrix is in third place as they don't support this feature. Citrix has this ability in their VDI\DaaS platform, but it hasn't been ported to the browser offering yet.

### 3.13 Webcam Control

This feature allows the administrator to control if the webcam can be accessed during a web session. While this, in some cases, is more of a privacy control than a typical corporate compliance control, this is still an excellent control.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes (Per URL)

TalonWork — Yes (Per URL/App/Category)

**Google and Talon are more secure** as they can control the webcam per URL. Citrix is in second place as they don't support this feature.



## 4.0 Threat Prevention

### 4.1 Malicious URL Protection

This feature will evaluate the URLs entered into the browser session to check their risk level before allowing the users or presenting a block or warning. Many modern browsers will have this ability, especially Chromium-based browsers, but they differ in the depth of protection they offer.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes

TalonWork — Yes (More integrations)

Talon is more secure as it has more external connections to check if the URLs are potentially unsafe. Talon uses the native Chromium Safe Browsing capabilities like the other vendors. Also, it integrates with external threat intelligence services from vendors like CrowdStrike, Avira, and Webroot to automatically detect and block access to malicious sites such as phishing or credential harvesting sites. Citrix and Google are tied for second place as they have fewer URL threat detection integrations. Each system has varying policy capabilities regarding the URLs users can navigate based on users, groups, devices, and policies.

### 4.2 Read-Only Website Access

This feature lets you protect against phishing attacks and credential theft by granting users “read-only” access to untrusted websites and preventing them from entering their credentials.

Citrix Secure Private Access – No

Google Chrome Enterprise – No

TalonWork – Yes

Talon is the most secure as they support this feature. Citrix and Google do not support this capability.

### 4.3 Leaked Credential Monitoring and Notification

This feature automatically notifies the user if they attempt to log into a site using credentials that are known to be compromised in a third-party data breach. This feature also typically creates notifications and reports in the management console for the administrators to review.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — No

**Google is more secure** as they support this feature. Citrix and Talon are tied for second place by not having this feature. We recommend that solutions have this protection as this is a common attack avenue with stealer logs and other attack methods.

### 4.4 Browser Patch Process

This feature describes the vendors' ability to patch the browser when there are security vulnerabilities. With browsers being a primary application for most users worldwide, vulnerabilities are found to become an immediate risk for all organizations and users when released. Most browsers are updated at least monthly, depending on the severity of the vulnerabilities found. Depending on which Enterprise Browser solution you use and which browser they use will determine how long it will take for patches to make it to your systems and users. This relates to the Version Upgrade Control feature in section one but looks specifically at how long it will take to update the base browser.

Citrix Secure Private Access — Secondary Update

Google Chrome Enterprise — Primary Update

Talon Security — Secondary Update

**Google Chrome Enterprise is ahead** in this category as they are the primary update source for the Chromium-based browser they use for their solution. Citrix and Talon are tied for second place by waiting until Google Chrome is updated before their solutions can be updated. All the solutions we have seen thus far with this vendor group use a Chromium-based browser, so they will always be in the secondary update channel compared to Google. There is a two-week Beta window where all vendors have a chance to update before a stable release is made, and they could be released at the same time, but they also may have a couple of days behind, depending on how the changes impacted them.

## 5.0 Endpoint Filters

### 5.1 Endpoint Filter — OS Version

This feature will require the operating system to be a specific version before the user can access the browser. This can be especially helpful in managed but especially in an unmanaged deployment where you may want to limit unsupported operating systems' ability to access a web application. Unsupported operating systems can cause user performance problems and increase the probability of a successful attack on an endpoint.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** due to their ability to control access based on the endpoint operating system.

### 5.2 Endpoint Filter – Disk Encryption

This feature will require the endpoint to enable disk encryption before accessing a specified resource. Many compliance bodies need local disk encryption enabled, no matter the type of data accessed.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** due to their ability to require an endpoint to have disk encryption before accessing resources.

### 5.3 Endpoint Filter – Require Screen Lock

This feature will require the endpoint to have a password-enabled screen lock configuration. Many compliance bodies need these to be configured. Leaving an endpoint unattended and idle can be a dangerous recipe for any organization, and the ability to audit this configuration is essential. This feature comes up a lot as a requirement when I perform audits for my clients. More solutions should be able to check this basic compliance configuration on endpoints before providing access to resources.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Google and Talon are tied for first place** due to their ability to require an endpoint to have a password-enabled lock before accessing resources. Citrix is in third place as they do not support this feature.

### 5.4 Endpoint Filter – Require Antivirus

This feature will require the endpoint to enable endpoint protection before accessing a specified resource. This has become a standard for most endpoints and validating that the system has this control should lower the probability of the endpoint being compromised.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** due to their ability to require an endpoint to have an endpoint protection solution before accessing resources, they have varying capabilities, but the core is there.

## 5.5 Endpoint Filter – Serial Number Filtering

This feature will require the endpoint to have a specific serial number before accessing the resources. This would typically only be set up in high-security deployments, but many use cases could benefit from this configuration.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Google and Talon are more secure** as they can require an endpoint to have a specific device serial number before accessing resources. Citrix is in third place as they don't support this feature.

## 5.6 Endpoint Filter – Certificates

This feature will require the endpoint to have a local certificate before accessing the resources. This would typically only be set up in high-security deployments, but many use cases could benefit from this configuration.

Citrix Secure Private Access — Yes

Google Chrome Enterprise — Yes (BeyondCorp Enterprise)

TalonWork — Yes

**Citrix, Google, and Talon are equally secure** as they require an endpoint to have a certificate installed before accessing resources.

## 6.0 Extension Controls

### 6.1 Allow or Block Extension Selection

This feature allows the administrator to Allow or Block browser extensions within the session. With so many Browser extensions out there, it's essential that you can enable users to add safe extensions as needed and block known malicious extensions. Most administrators are surprised when they audit the browser extensions installed on end-user systems because, in many cases, it's just assumed that their end users need a browser and not an extension to do their job. Since we cannot live without extensions in many deployments, having the ability to allow or block extensions is critical.

Citrix Secure Private Access — Yes (Tech Preview)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Citrix, Google, and Talon are all tied for first place** due to their ability to Allow or Block Extensions users can navigate to based on their group membership, devices, and policies. Each vendor has different dashboard and reporting capabilities but meets a good minimum feature set.

### 6.2 Restrict Extensions Permissions

This feature allows you to control what permissions specified extensions have and what permissions any extension can have. This can help prevent what known or unknown extensions can do within the browser to reduce its attack surface. There have been extensions that have been hijacked in the past that became malicious, and the ability to control what permissions the extension has to the browser and, ultimately, the endpoint can help reduce the risk and impact of those types of attacks.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes

TalonWork — Yes

**Google and Talon are more secure** as they can restrict browser and machine extension permissions. Citrix is in third place as they do not support this feature.

### 6.3 Prevent Apps from communicating with Extensions

This feature will prevent applications from communicating with extensions which can be very beneficial. When extensions are typically installed, anyone with access to the browser will have access to the extension by their machine access and the rules within each operating system.

Citrix Secure Private Access — No

Google Chrome Enterprise — Yes

TalonWork — Yes

**Google and Talon are tied for first place** as they can prevent applications from communicating with extensions. Citrix is in third place as they do not support this feature.

### 6.4 Force Extension Install

This feature will force the installation of the specified extension on the browser. This can be very important for deployments that require password managers to be configured and when specific extensions are necessary for an application to function as expected. Since many extensions are related to security use cases, this was added as a feature because this can make the user experience more secure along with the applications accessed through the browser.

Citrix Secure Private Access — Yes (Tech Preview)

Google Chrome Enterprise — Yes

TalonWork — Yes

**Citrix, Google, and Talon are tied for first place** as they can require an extension to be installed before accessing resources.

## 6.5 Extension Request Workflow

This feature allows end users to request access to install specific extensions, and admins can allow or deny them. This feature will have a more significant impact in an unmanaged deployment because you don't know what extensions the users are using, and in a managed device deployment too. Most deployments won't have a browser extension inventory for all devices or users. This feature becomes a security feature as having a workflow to request, track, deny, or install extensions lets you know which extensions you should monitor for vulnerabilities.

**Citrix Secure Private Access** — No

**Google Chrome Enterprise** — Yes

**Talon Security** — No

**Google are more secure** as they have the ability for users to request new extensions natively. Google lets you see a summary of the request to help analyze and prioritize requests based on your enterprise security requirements. Citrix and Talon are tied for second place as they do not support this feature.

## 7.0 Advanced Browser Options

### 7.1 Set Custom Header\User-Agent

This feature is powerful when paired with other content control software, firewall, and other solutions to log and control aspects of the user's web sessions. This configuration can identify the secure browser against other security products, such as firewalls, to apply relevant policies.

**Citrix Secure Private Access** — Partial

**Google Chrome Enterprise** — No

**TalonWork** — Yes

**Citrix and Talon are more secure** as they allow the ability to set each of these items. Google is in third place as they do not support this feature.



## 7.2 Basic Browser Audit

### Browser Audit Results

This analysis was to understand what default settings these browsers use to understand their default security stance. Since all the browsers validated are, Chromium-based, we used the BrowserAudit.com website to probe each browser to check their security policies. This will always be a varying score because new tests are added regularly, and then some tests could be skipped because of networking timeouts and many other factors. This was the only way we could find a way to quantify the out-of-the-box settings for each of these solutions. We plan to do more testing on the recommended lockdown settings of Chromium-based browsers to see how much we can improve the scores below. Many of these solutions can also configure every Chromium-based policy like Google and Talon, allowing each of these to be secured further along with customizing the expected experience for your users.

	Base Google Chrome	Citrix Secure Private Access	Citrix Remote Browser Isolation	Google Chrome Enterprise	Talon Cyber Security
Passed	365	365	360	365	367
Warning	18	18	21	18	16
Critical	1	1	1	1	1
Skipped	20	20	22	20	20

**Talon is more secure** as they have fewer warning findings. Google is in second place, and Citrix is in third based on its two delivery options averaged, whereas if both settings were the same, it would have been a tie for first place. Overall, these findings were very similar between each vendor, and I'm sure the results will change over time as they make changes to their policies and as the Browser Audit team creates new tests.


## Summary of Results

With all the 47 features compared between these vendors, we can see that the TalonWork secure enterprise browser wins with the highest security feature score. We want to add more vendors early later this year to see how it compares against many of the others in this emerging space.


As a reminder, we used a ranked scoring system to identify the best solution in each feature category. Each vendor started with a perfect 100/A+ score. The best vendor in each category had zero points deducted. We deducted points from the other vendors to reflect feature deficiencies or security gaps compared to the best vendor. In some cases, two or all three vendors received identical scores. We applied the deductions to create our final grade for each solution.

### Security Feature Rank Overviews


#### *Delivery and Integration – Rank*

<b>Delivery &amp; Integration Rank Matrix v1.0-March-2023</b>			
 <b>VOISEC</b>	<b>Citrix Secure Private Access</b>	<b>Google Chrome Enterprise</b>	<b>Talon Cyber Security</b>
<b>Ranks</b>	<b>@VDIHacker</b>		
<b>Delivery Type</b>	1	2	2
<b>Endpoint Operating Systems Support</b>	2	1	3
<b>Enrollment Type</b>	2	3	1
<b>VPN-less Access (Internal Apps)</b>	1	1	3
<b>Browser Use Enforcement</b>	1	1	3
<b>Version Upgrade Control</b>	3	1	1
<b>Policy Update Times</b>	2	2	1
<b>Conditional Access Controls</b>	2	2	1
<b>Idle Timeout Control</b>	1	3	1
<b>Browser Timeout Passcode</b>	2	2	1
<b>Endpoint Protection Agent Integration</b>	3	1	1
<b>SIEM Integration</b>	1	1	1
<b>Chromium Browser Policies</b>	3	1	1
<b>Authentication Integration</b>	1	2	2


Browsing Controls – Rank

<b>Browsing Controls Rank Matrix v1.0-March-2023</b>			
 <b>VDISEC</b> Ranks @VDIHacker	<b>Citrix Secure Private Access</b>	<b>Google Chrome Enterprise</b>	<b>Talon Cyber Security</b>
<b>Website Control</b>	1	1	1
<b>Control App Logins</b>	1	1	1
<b>Browser Jailbreak Prevention</b>	3	1	1


Data Leak Prevention – Rank

<b>Data Leak Prevention Rank Matrix v1.0-March-2023</b>			
 <b>VDISEC</b> Ranks @VDIHacker	<b>Citrix Secure Private Access</b>	<b>Google Chrome Enterprise</b>	<b>Talon Cyber Security</b>
<b>Watermark</b>	1	3	1
<b>Screen Capture Protection</b>	1	3	1
<b>Keylogger Protection</b>	1	3	1
<b>Control File Downloads\Uploads</b>	2	2	1
<b>Encrypt Downloads</b>	2	2	1
<b>Malicious File Scanning</b>	3	1	1
<b>USB Control</b>	1	3	1
<b>Clipboard Directional Control</b>	1	3	1
<b>Clipboard App Control (Source\Destination)</b>	1	1	1
<b>Printing Control</b>	1	3	1
<b>Printer List Control</b>	2	2	1
<b>Audio and Microphone Control</b>	3	2	1
<b>Webcam Control</b>	3	2	1


Threat Prevention – Rank


Threat Prevention Ranks Matrix v1.0-March-2023			
 <b>VDISEC</b> @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
<b>Ranks</b>			
<b>Malicious URL Protection</b>	2	2	1
<b>Read-Only Website Access</b>	2	2	1
<b>Leaked Credential Monitoring &amp; Notification</b>	2	1	2
<b>Browser Patch Process</b>	2	1	2

Endpoint Filters – Rank

Endpoint Filters Rank Matrix v1.0-March-2023			
 <b>VDISEC</b> @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
<b>Ranks</b>			
<b>Endpoint Filter - OS Version</b>	1	1	1
<b>Endpoint Filter – Disk Encryption</b>	1	1	1
<b>Endpoint Filter – Require Screen Lock</b>	3	1	1
<b>Endpoint Filter – Require Antivirus</b>	1	1	1
<b>Endpoint Filter – Serial Number</b>	3	1	1
<b>Endpoint Filter – Certificates</b>	1	1	1

Extension Controls – Rank

Extension Controls Rank Matrix v1.0-March-2023			
 <b>VDISEC</b> @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
<b>Ranks</b>			
<b>Allow or Block Extension Selection</b>	1	1	1
<b>Restrict Extensions Permissions</b>	3	1	1
<b>Prevent Apps from communicating with Extensions</b>	3	1	1
<b>Force Extension Install</b>	1	1	1
<b>Extension Request Workflow</b>	2	1	2


Advanced Browser Options Rank Matrix v1.0-March-2023				
 <b>VDISEC</b> @VDIHacker		Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
<b>Ranks</b>				
<b>Set Custom Header\User-Agent</b>		2	3	1
<b>Browser Audit Results</b>		3	2	1

### Security Feature Rank Summary

Overall, there was a good spread of ties and first places, which is good. There were more three-way ties than in our previous VDI and Endpoint comparisons. It’s good to see the ranking to know which are better in each category and which are tied.

Rank Count March 2023	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
1st Place	21	25	39
2nd Place	14	13	5
3rd Place	12	9	3

### Final Score Summary

Browser Security Feature Scores - March 2023			
 <b>VDISEC</b> @VDIHacker	Score	Grade	Rank
<b>Citrix Secure Private Access</b>	79.7	C+	3
<b>Google Chrome Enterprise</b>	82.8	B-	2
<b>Talon Cyber Security</b>	93.0	A	1

## Conclusion

An enterprise browser can clearly help any business reduce the security risks posed by modern web apps and SaaS solutions and by remote workers and unmanaged devices. The market is just starting, but we found that the early entrants already provide an unexpectedly broad array of features to help prevent data loss and malicious attacks. We were surprised by the feature differences between the three products we examined. We trimmed the list down to 46 mutual features for our first report, but we could have easily added twice as many.


Talon edged out Citrix in our first report. Google received a passing grade for their Chrome Enterprise Browser, including BeyondCorp Enterprise. The Enterprise Browser market is highly competitive and evolving rapidly. We plan to update this report quarterly to include additional vendors and features and provide additional insights for the community.

Please get in touch with me on [Twitter](#) or [LinkedIn](#) if you have any questions or comments. Let us know if there are additional vendors, products, features, or security policies you would like us to look at in future reports.


## Scoring Appendix

The below summaries show the scores used per feature that were totaled and then subtracted from the 100 perfect scores for having all the features. A zero score is the best score, as the vendor doesn't have a partial or full-point deduction for the feature we are comparing. Like a typical test in school, the fewer deductions, the higher your score will be.


### *Delivery and Integration – Score*

<b>Delivery &amp; Integration Score Matrix v1.0-March-2023</b>			
 <b>VOISEC</b>	<b>Citrix Secure Private Access</b>	<b>Google Chrome Enterprise</b>	<b>Talon Cyber Security</b>
<b>Ranks</b>	<b>@VDIHacker</b>		
<b>Delivery Type</b>	0	1	1
<b>Endpoint Operating Systems Support</b>	0.5	0	1
<b>Enrollment Type</b>	0.5	1	0
<b>VPN-less Access (Internal Apps)</b>	0	0	0.5
<b>Browser Use Enforcement</b>	0	0	0.5
<b>Version Upgrade Control</b>	0.5	0	0
<b>Policy Update Times</b>	0.5	0.5	0
<b>Conditional Access Controls</b>	0.5	0.5	0
<b>Idle Timeout Control</b>	0	0.5	0
<b>Browser Timeout Passcode</b>	1	1	0
<b>Endpoint Protection Agent Integration</b>	0.5	0	0
<b>SIEM Integration</b>	0	0	0
<b>Chromium Browser Policies</b>	1	0	0
<b>Authentication Integration</b>	0	0.5	0.5

Browsing Controls – Score


Browsing Controls Score Matrix v1.0-March-2023			
 <b>VDISEC</b> Ranks <span style="float: right;">@VDIHacker</span>	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
	Website Control	0	0
Control App Logins	0	0	0
Browser Jailbreak Prevention	0.5	0	0

Data Leak Prevention – Score


Data Leak Prevention Score Matrix v1.0-March-2023			
 <b>VDISEC</b> Ranks <span style="float: right;">@VDIHacker</span>	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
	Watermark	0	1
Screen Capture Protection	0	1	0
Keylogger Protection	0	1	0
Control File Downloads\Uploads	0.5	0.5	0
Encrypt Downloads	1	1	0
Malicious File Scanning	0.5	0	0
USB Control	0	1	0
Clipboard Directional Control	0	1	0
Clipboard App Control (Source\Destination)	0	0	0
Printing Control	0	0.5	0
Printer List Control	1	1	0
Audio and Microphone Control	1	0.5	0
Webcam Control	1	0.5	0




Endpoint Filters – Score

Endpoint Filters Score Matrix v1.0-March-2023			
 <b>VDISEC</b> Ranks @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
Endpoint Filter - OS Version	0	0	0
Endpoint Filter – Disk Encryption	0	0	0
Endpoint Filter – Require Screen Lock	1	0	0
Endpoint Filter – Require Antivirus	0	0	0
Endpoint Filter – Serial Number	1	0	0
Endpoint Filter – Certificates	0	0	0


Extension Controls – Score

Extension Controls Score Matrix v1.0-March-2023			
 <b>VDISEC</b> Ranks @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
Allow or Block Extension Selection	0	0	0
Restrict Extensions Permissions	1	0	0
Prevent Apps from communicating with Extensions	1	0	0
Force Extension Install	0	0	0
Extension Request Workflow	1	0	1

Advanced Browser Options – Score

Advanced Browser Options Score Matrix v1.0-March-2023			
 <b>VDISEC</b> Ranks @VDIHacker	Citrix Secure Private Access	Google Chrome Enterprise	Talon Cyber Security
Set Custom Header\User-Agent	0.5	1	0
Browser Audit Results	0.8125	0.75	0.5

## Other Scoring Summary Matrix

<b>Enterprise Secure Browser Score Matrix v1.0-March-2023</b>			
<b>@VDIHacker Security Item  VDISEC</b>	<b>Citrix Secure Private Access</b>	<b>Google Chrome Enterprise</b>	<b>Talon Cyber Security</b>
<b>Security Feature Score</b>	79.69	82.75	93.00
<b>Security Feature Grade</b>	C+	B-	A
<b>Security Total Rank</b>	3	2	1
<b>Security Average Score</b>	0.43	0.37	0.15

### Copyright

This publication is copyrighted by VDISEC Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise, to persons not authorized to receive it without the express consent of VDISEC is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, don't hesitate to contact the Author on [Twitter](#) or [LinkedIn](#).