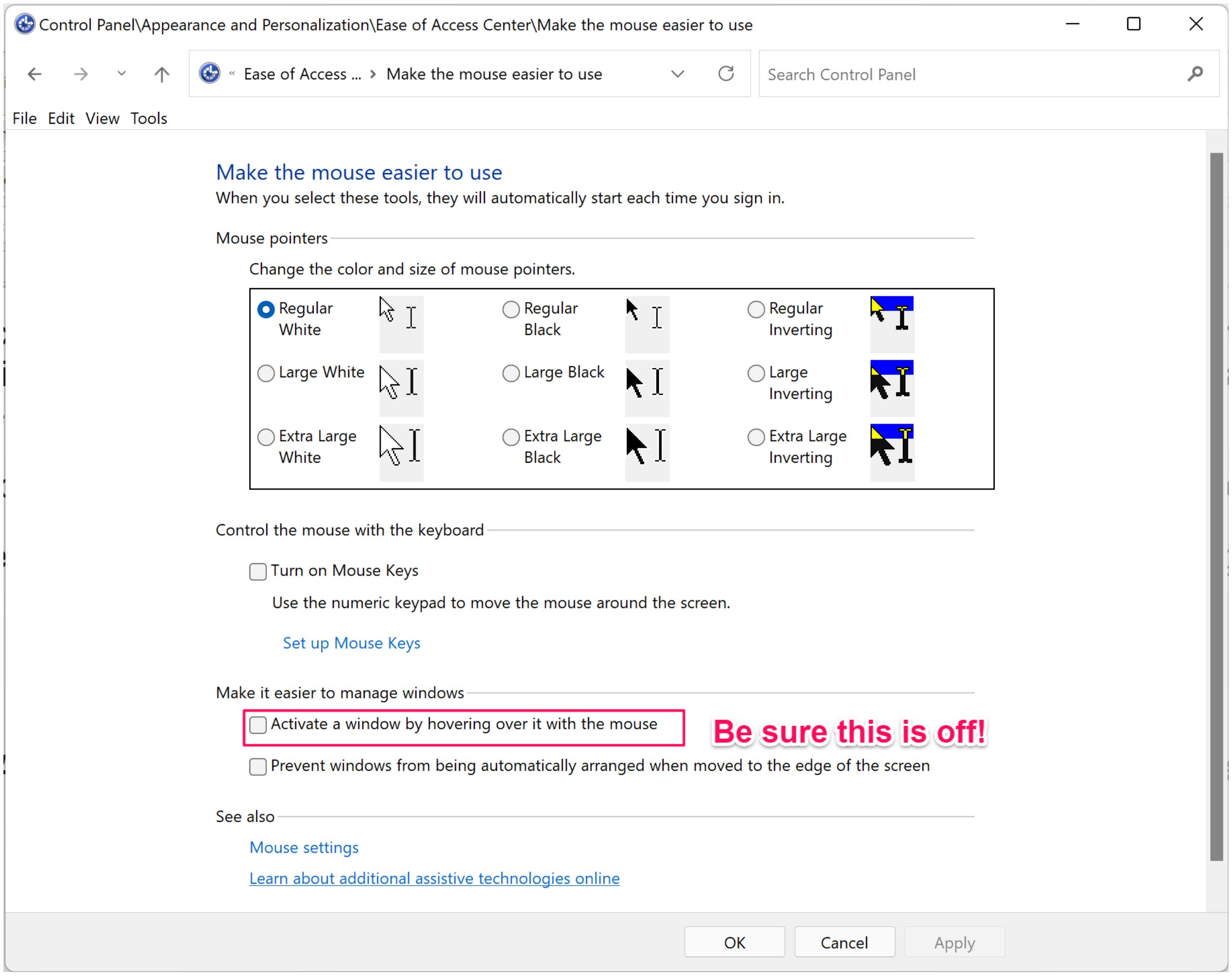
Browser Guards - No Real Malware!

Control Panel, Appearance and Personalization, Ease of Access Center, Make the mouse easier to use.



Control Panel\Appearance and Personalization\Ease of Access Center\Make the mouse easier to use

Ease of Access ... › Make the mouse easier to use

Search Control Panel

File Edit View Tools

Make the mouse easier to use

When you select these tools, they will automatically start each time you sign in.

Mouse pointers

Change the color and size of mouse pointers.

● Regular White

○ Regular Black

○ Regular Inverting

○ Large White

○ Large Black

○ Large Inverting

○ Extra Large White

○ Extra Large Black

○ Extra Large Inverting

Control the mouse with the keyboard

□ Turn on Mouse Keys

Use the numeric keypad to move the mouse around the screen.

Set up Mouse Keys

Make it easier to manage windows

□ Activate a window by hovering over it with the mouse

Be sure this is off!

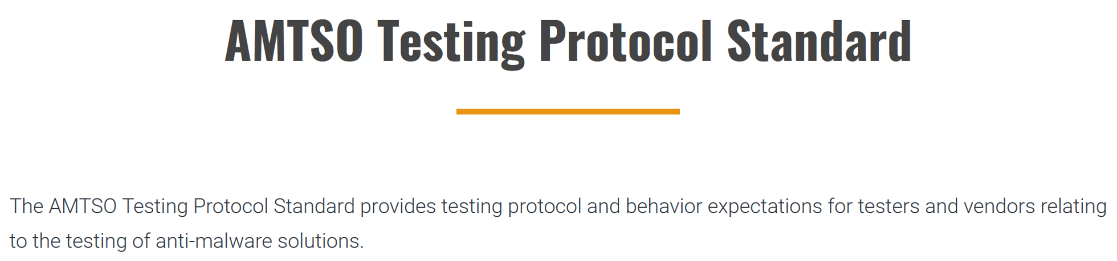
□ Prevent windows from being automatically arranged when moved to the edge of the screen

See also

Mouse settings

Learn about additional assistive technologies online

How to VERIFY!



AMTSO Testing Protocol Standard

The AMTSO Testing Protocol Standard provides testing protocol and behavior expectations for testers and vendors relating to the testing of anti-malware solutions.

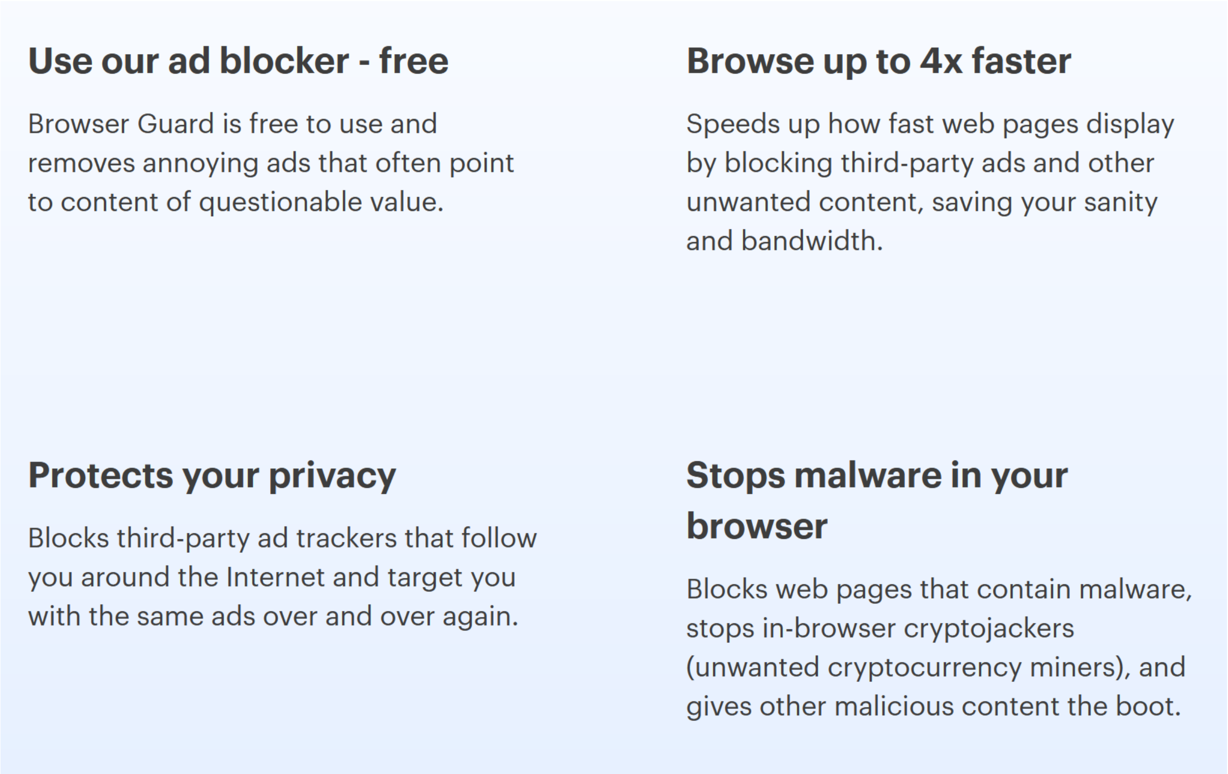
Anti-Malware Testings Standards Organization

AntiVirus/Malware software testing site.

https://www.amtso.org/security-features-check/

Malwarebytes Browser Guard

Claims



Use our ad blocker - free

Browser Guard is free to use and removes annoying ads that often point to content of questionable value.

Browse up to 4x faster

Speeds up how fast web pages display by blocking third-party ads and other unwanted content, saving your sanity and bandwidth.

Protects your privacy

Blocks third-party ad trackers that follow you around the Internet and target you with the same ads over and over again.

Stops malware in your browser

Blocks web pages that contain malware, stops in-browser cryptojackers (unwanted cryptocurrency miners), and gives other malicious content the boot.

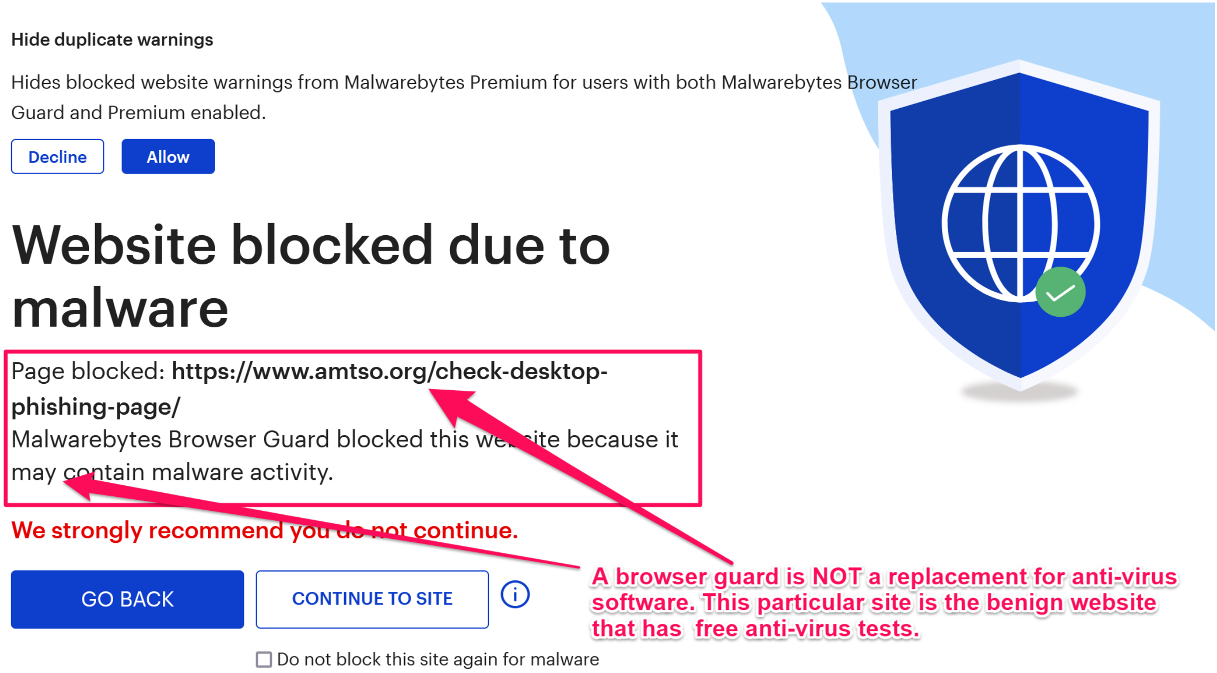
https://www.malwarebytes.com/browserguard

Malwarebytes Browser guard for Safari
https://support.malwarebytes.com/hc/en-us/articles/4413290281747-Install-Malwarebytes-Browser-Guard-on-Safari-Browser

Malwarebytes Browser guard for Google Chrome
https://chrome.google.com/webstore/detail/malwarebytes-browser-guar/ihcjicgdanjaechkgeegckofjjedodee?hl=en

Malwarebytes Browser guard for Mozilla Firefox
https://addons.mozilla.org/en-US/firefox/addon/malwarebytes/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

Malwarebytes Browser guard for Microsoft Edge
https://chrome.google.com/webstore/detail/malwarebytes-browser-guar/ihcjicgdanjaechkgeegckofjjedodee/related



Hide duplicate warnings

Hides blocked website warnings from Malwarebytes Premium for users with both Malwarebytes Browser Guard and Premium enabled.

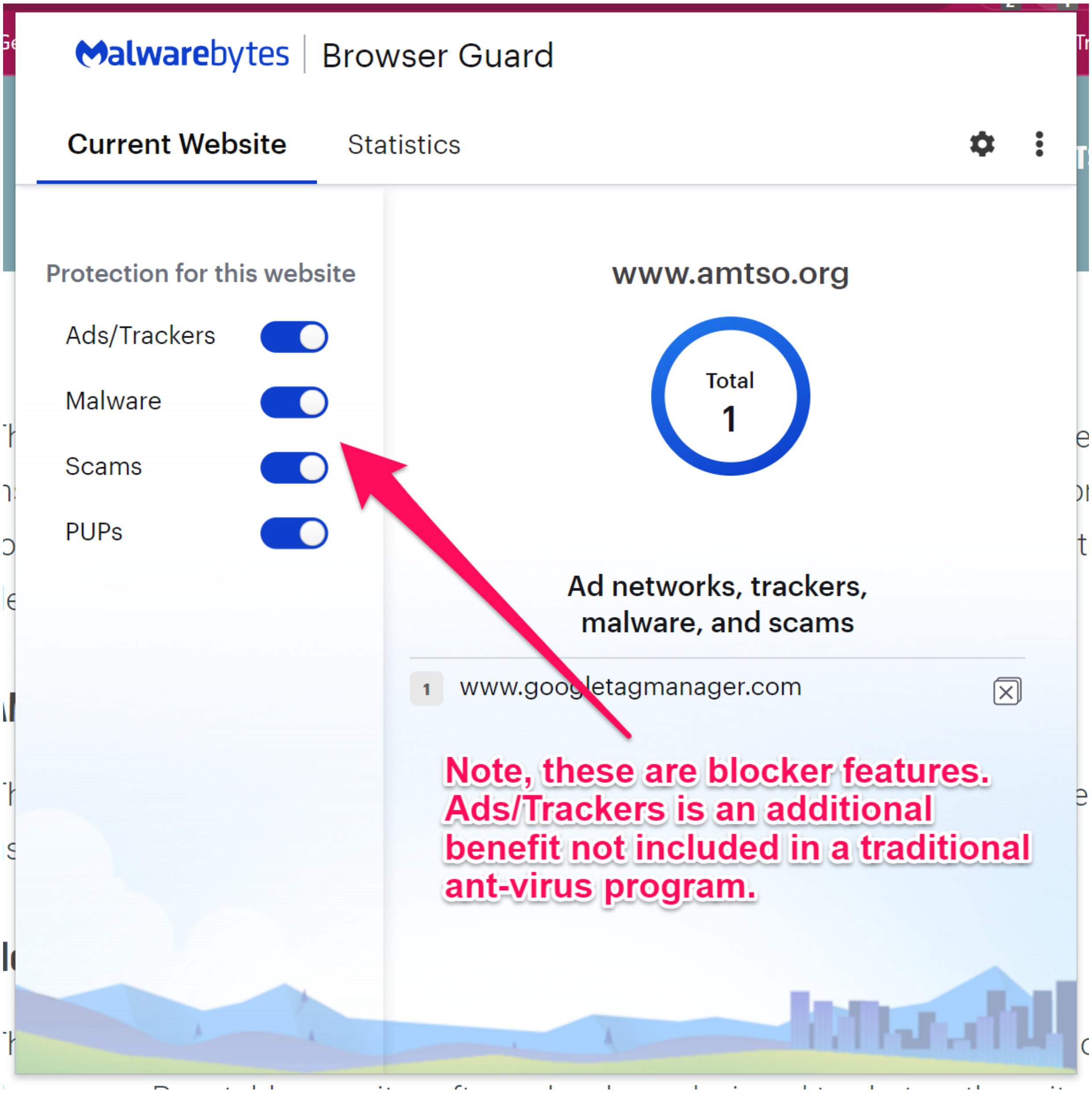
Website blocked due to malware

Page blocked: **https://www.amtso.org/check-desktop-phishing-page/**
Malwarebytes Browser Guard blocked this website because it may contain malware activity.

We strongly recommend you do not continue.

☐ Do not block this site again for malware

A browser guard is NOT a replacement for anti-virus software. This particular site is the benign website that has free anti-virus tests.



Malwarebytes | Browser Guard

Current Website | Statistics

Protection for this website

- Ads/Trackers ●
- Malware ●
- Scams ●
- PUPs ●

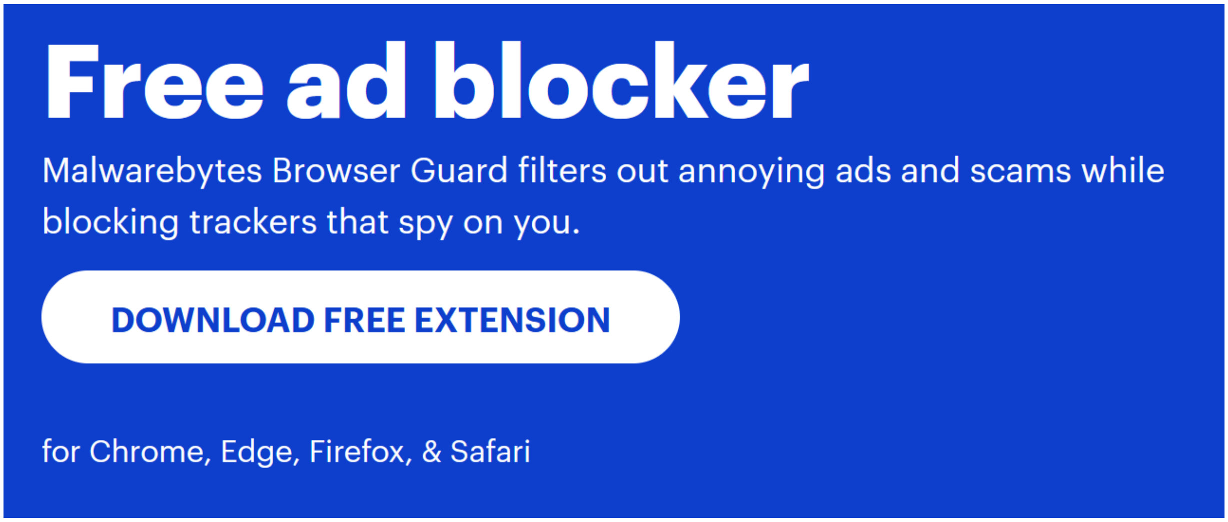
www.amtso.org

Total
1

Ad networks, trackers, malware, and scams

1 www.googletagmanager.com ☒

Note, these are blocker features. Ads/Trackers is an additional benefit not included in a traditional ant-virus program.

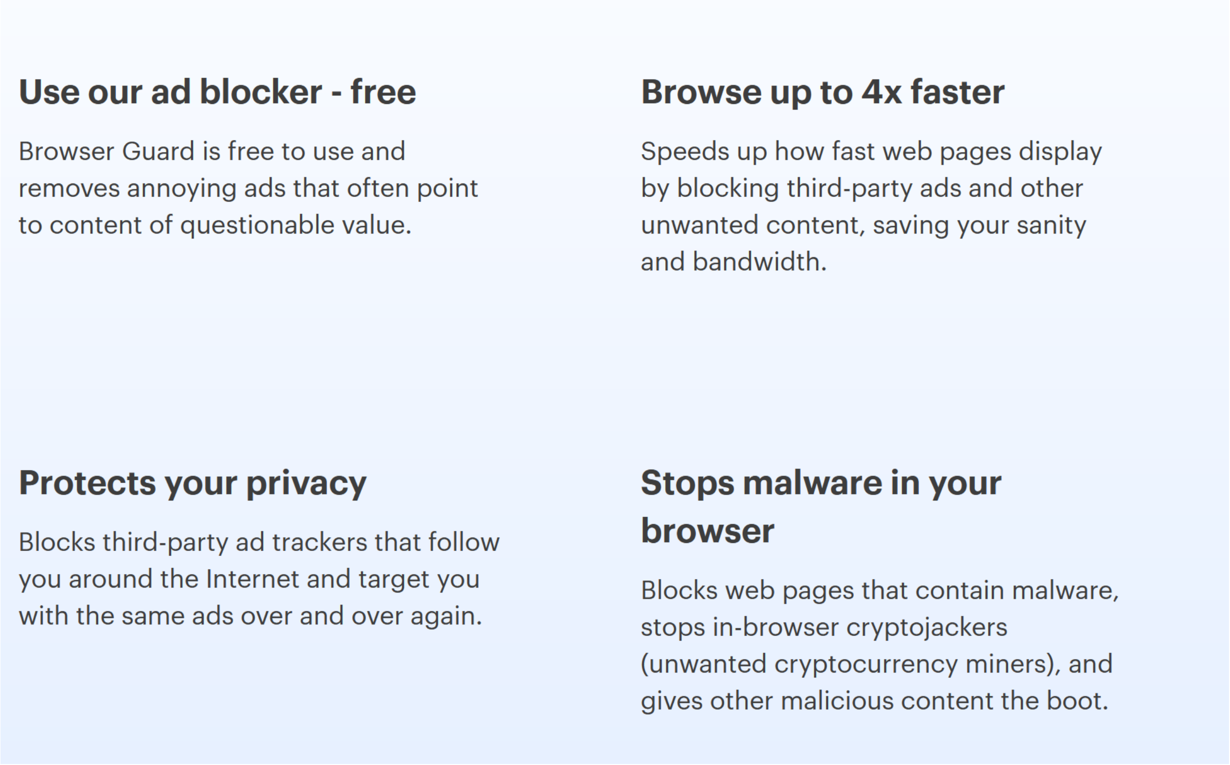


Free ad blocker

Malwarebytes Browser Guard filters out annoying ads and scams while blocking trackers that spy on you.

DOWNLOAD FREE EXTENSION

for Chrome, Edge, Firefox, & Safari



Use our ad blocker - free

Browser Guard is free to use and removes annoying ads that often point to content of questionable value.

Browse up to 4x faster

Speeds up how fast web pages display by blocking third-party ads and other unwanted content, saving your sanity and bandwidth.

Protects your privacy

Blocks third-party ad trackers that follow you around the Internet and target you with the same ads over and over again.

Stops malware in your browser

Blocks web pages that contain malware, stops in-browser cryptojackers (unwanted cryptocurrency miners), and gives other malicious content the boot.

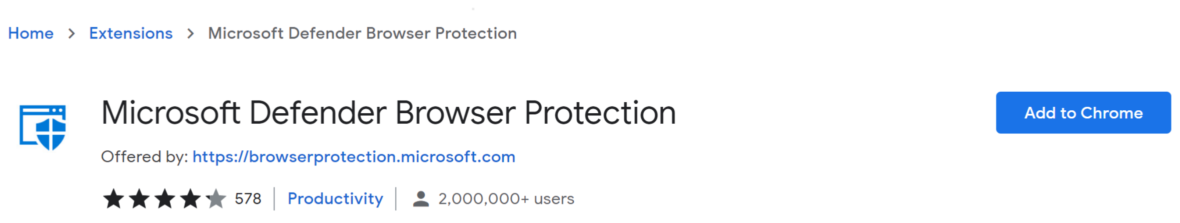
SHOW OFF AVAST V.S. MALWAREBYTES AD TRACKING (Firefox)

https://www.zdnet.com/

Microsoft Defender Browser Protection

https://chrome.google.com/webstore/detail/microsoft-defender-browse/bkbeeeffjjeopflfhgeknacdieedcoml?hl=en-US

https://chrome.google.com/webstore/search/microsoft%20defender%20browser%20protection?hl=en-US



Microsoft Defender Browser Protection

Offered by: https://browserprotection.microsoft.com

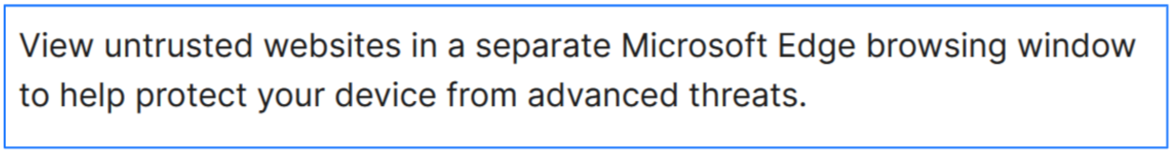
★★★★☆ 578 | Productivity | 2,000,000+ users

Claims

Protect yourself against online threats, like phishing and malicious websites, with real-time protection from Microsoft.

Microsoft Defender Application guard Extension

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/install-md-app-guard#review-system-requirements

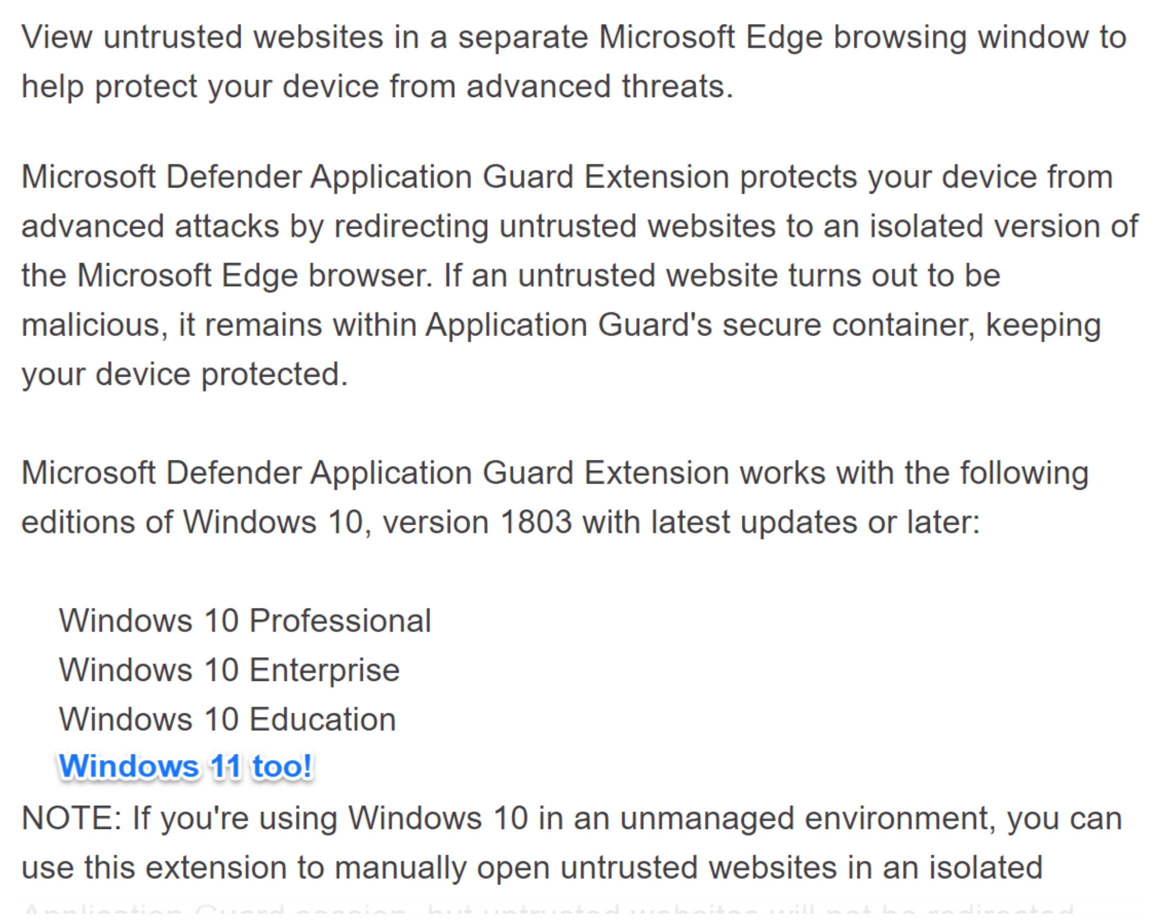


View untrusted websites in a separate Microsoft Edge browsing window to help protect your device from advanced threats.

https://addons.mozilla.org/en-US/firefox/addon/application-guard-extension/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

1. On the local device, download and install the Application Guard extension for Google Chrome and/or Mozilla Firefox.
2. Install the Microsoft Defender Application Guard companion app from the Microsoft Store. This companion app enables Application Guard to work with web browsers other than Microsoft Edge or Internet Explorer.
3. Restart the device.

Microsoft Defender Application Guard Extension - Windows security | Microsoft Docs



View untrusted websites in a separate Microsoft Edge browsing window to help protect your device from advanced threats.

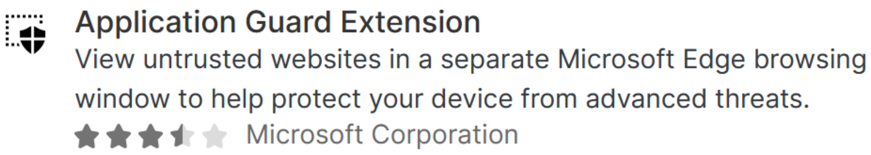
Microsoft Defender Application Guard Extension protects your device from advanced attacks by redirecting untrusted websites to an isolated version of the Microsoft Edge browser. If an untrusted website turns out to be malicious, it remains within Application Guard's secure container, keeping your device protected.

Microsoft Defender Application Guard Extension works with the following editions of Windows 10, version 1803 with latest updates or later:

Windows 10 Professional
Windows 10 Enterprise
Windows 10 Education
Windows 11 too!

NOTE: If you're using Windows 10 in an unmanaged environment, you can use this extension to manually open untrusted websites in an isolated Application Guard session, but untrusted websites will not be redirected

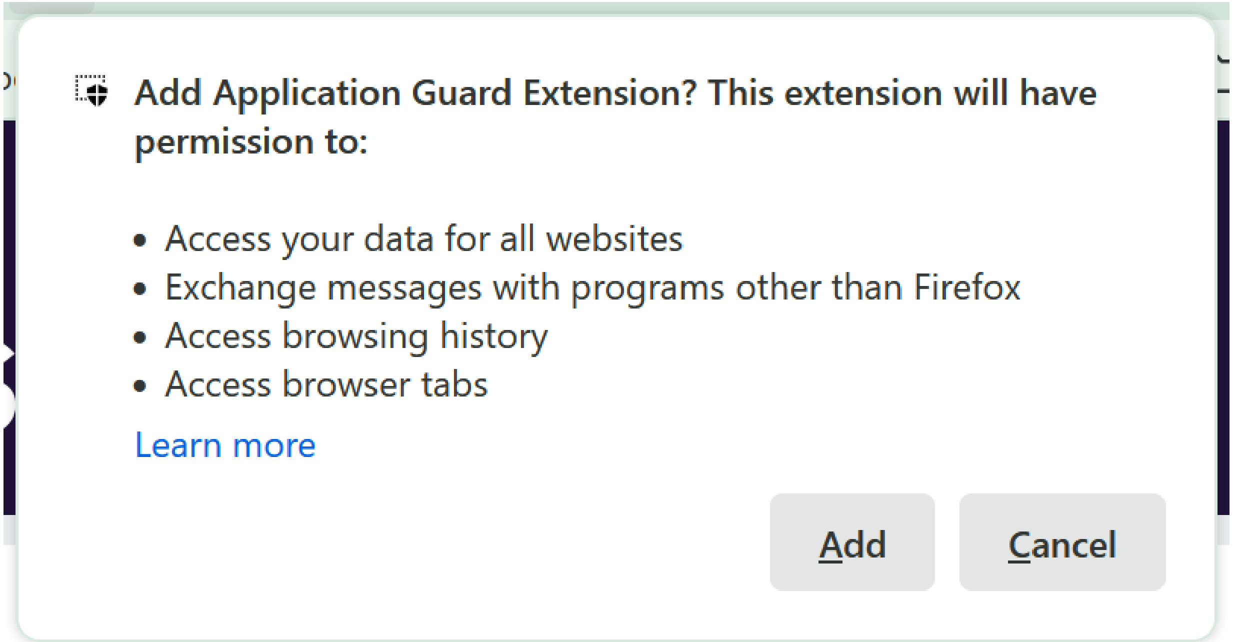
Also supported on Windows 11.



Application Guard Extension

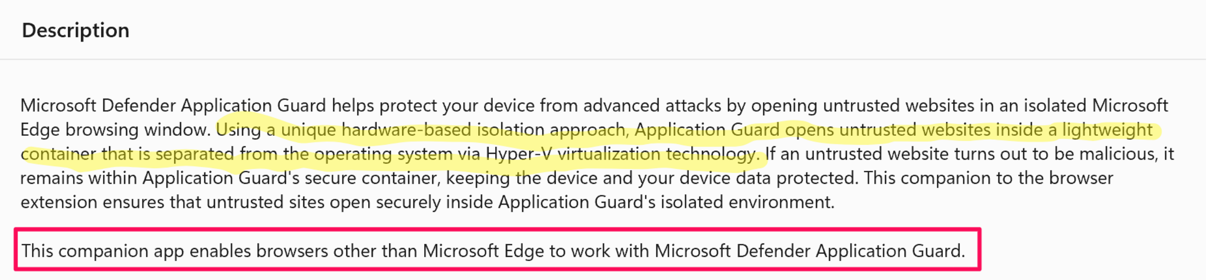
View untrusted websites in a separate Microsoft Edge browsing window to help protect your device from advanced threats.

★★★⯪☆ Microsoft Corporation



Add Application Guard Extension? This extension will have permission to:

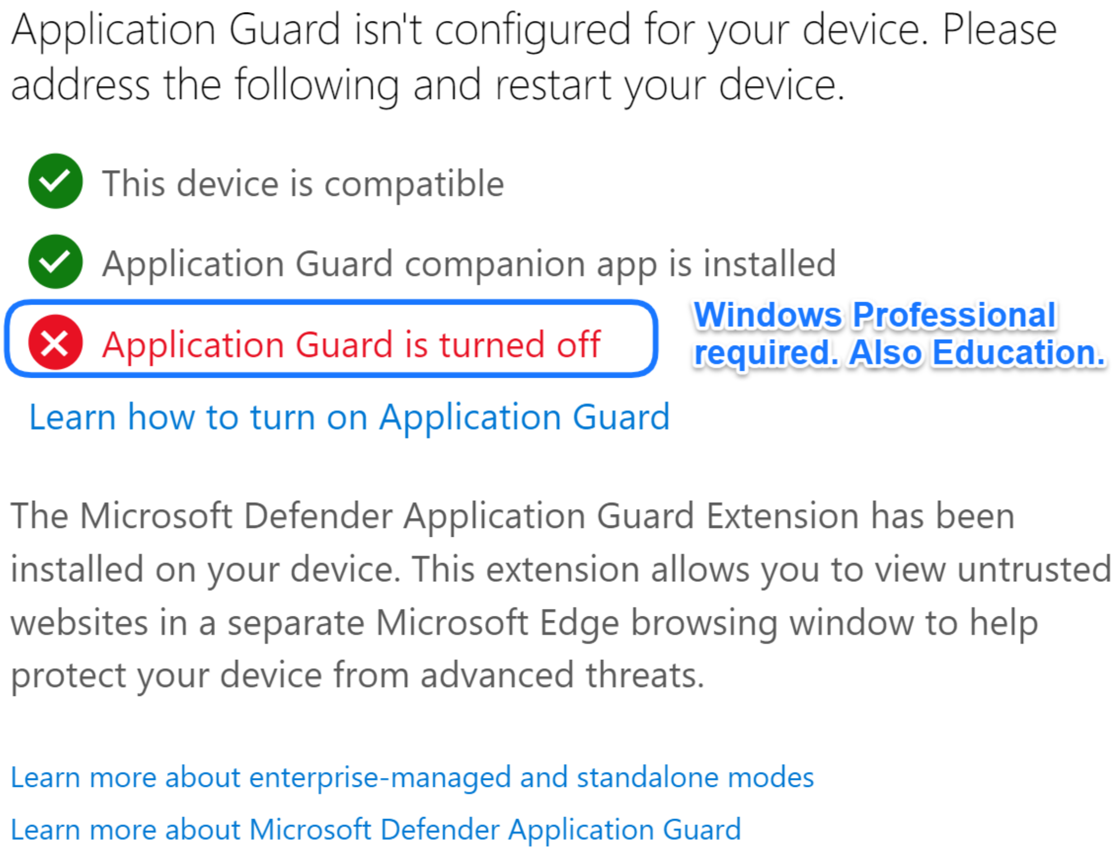
- Access your data for all websites
- Exchange messages with programs other than Firefox
- Access browsing history
- Access browser tabs



Description

Microsoft Defender Application Guard helps protect your device from advanced attacks by opening untrusted websites in an isolated Microsoft Edge browsing window. Using a unique hardware-based isolation approach, Application Guard opens untrusted websites inside a lightweight container that is separated from the operating system via Hyper-V virtualization technology. If an untrusted website turns out to be malicious, it remains within Application Guard's secure container, keeping the device and your device data protected. This companion to the browser extension ensures that untrusted sites open securely inside Application Guard's isolated environment.

This companion app enables browsers other than Microsoft Edge to work with Microsoft Defender Application Guard.



Application Guard isn't configured for your device. Please address the following and restart your device.

✓ This device is compatible

✓ Application Guard companion app is installed

✗ Application Guard is turned off

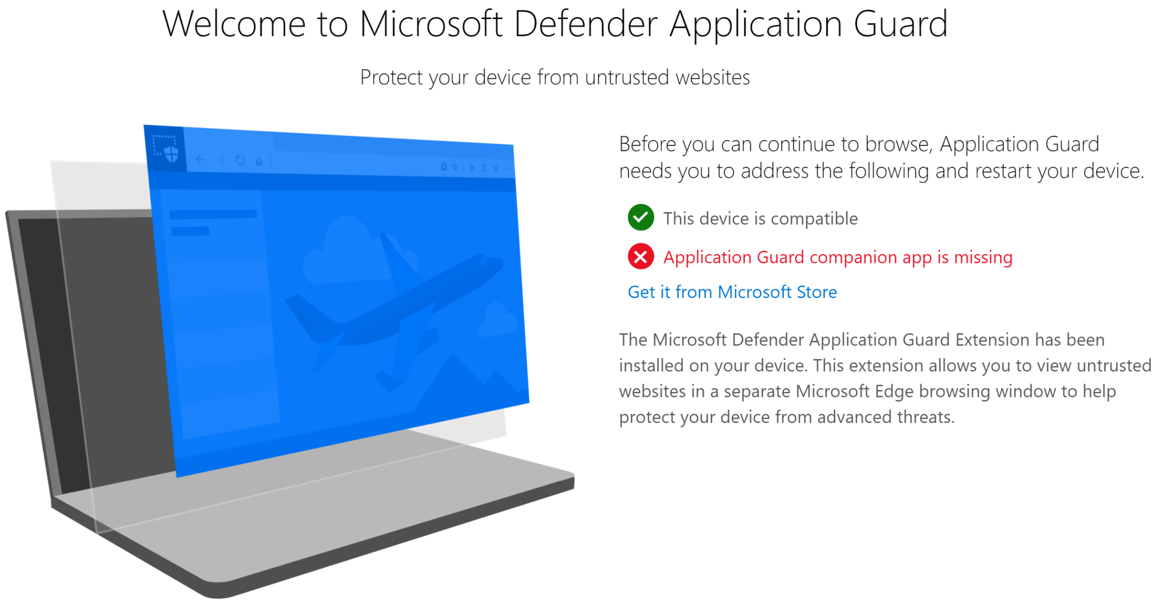
Windows Professional required. Also Education.

Learn how to turn on Application Guard

The Microsoft Defender Application Guard Extension has been installed on your device. This extension allows you to view untrusted websites in a separate Microsoft Edge browsing window to help protect your device from advanced threats.

Learn more about enterprise-managed and standalone modes

Learn more about Microsoft Defender Application Guard



Welcome to Microsoft Defender Application Guard

Protect your device from untrusted websites

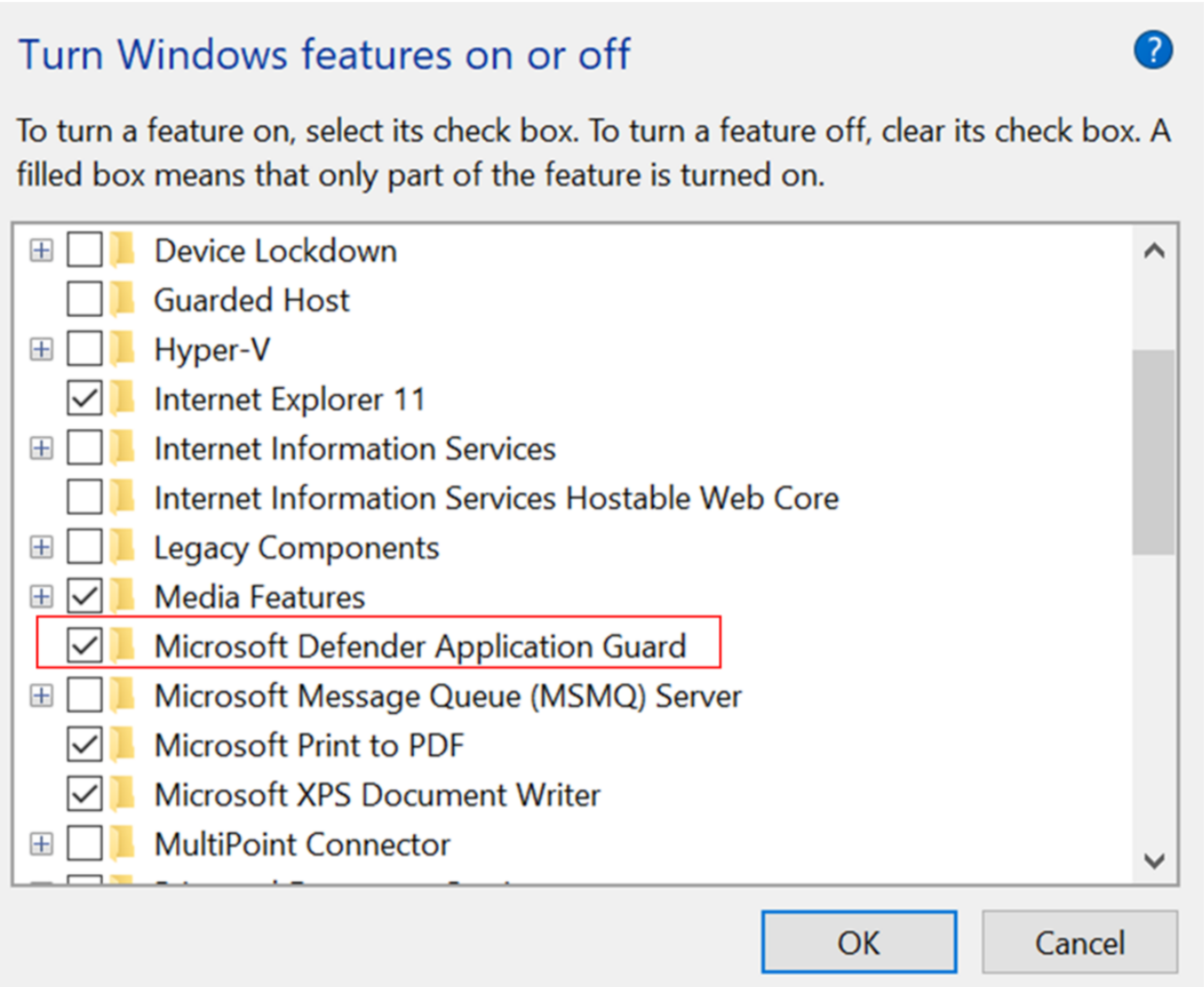
Before you can continue to browse, Application Guard needs you to address the following and restart your device.

✓ This device is compatible

✗ Application Guard companion app is missing

Get it from Microsoft Store

The Microsoft Defender Application Guard Extension has been installed on your device. This extension allows you to view untrusted websites in a separate Microsoft Edge browsing window to help protect your device from advanced threats.



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ Device Lockdown
- ☐ Guarded Host
- ☐ Hyper-V
- ☑ Internet Explorer 11
- ☐ Internet Information Services
- ☐ Internet Information Services Hostable Web Core
- ☐ Legacy Components
- ☑ Media Features
- ☑ Microsoft Defender Application Guard
- ☐ Microsoft Message Queue (MSMQ) Server
- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer
- ☐ MultiPoint Connector

Prepare for Microsoft Defender Application Guard

Before you can install and use Microsoft Defender Application Guard, you must determine which way you intend to use it in your enterprise. You can use Application Guard in either Standaloneor Enterprise-managedmode.

Standalone mode

Applies to:

- Windows 10 Enterprise edition, version 1709 or higher
- Windows 10 Pro edition, version 1803

- Windows 11

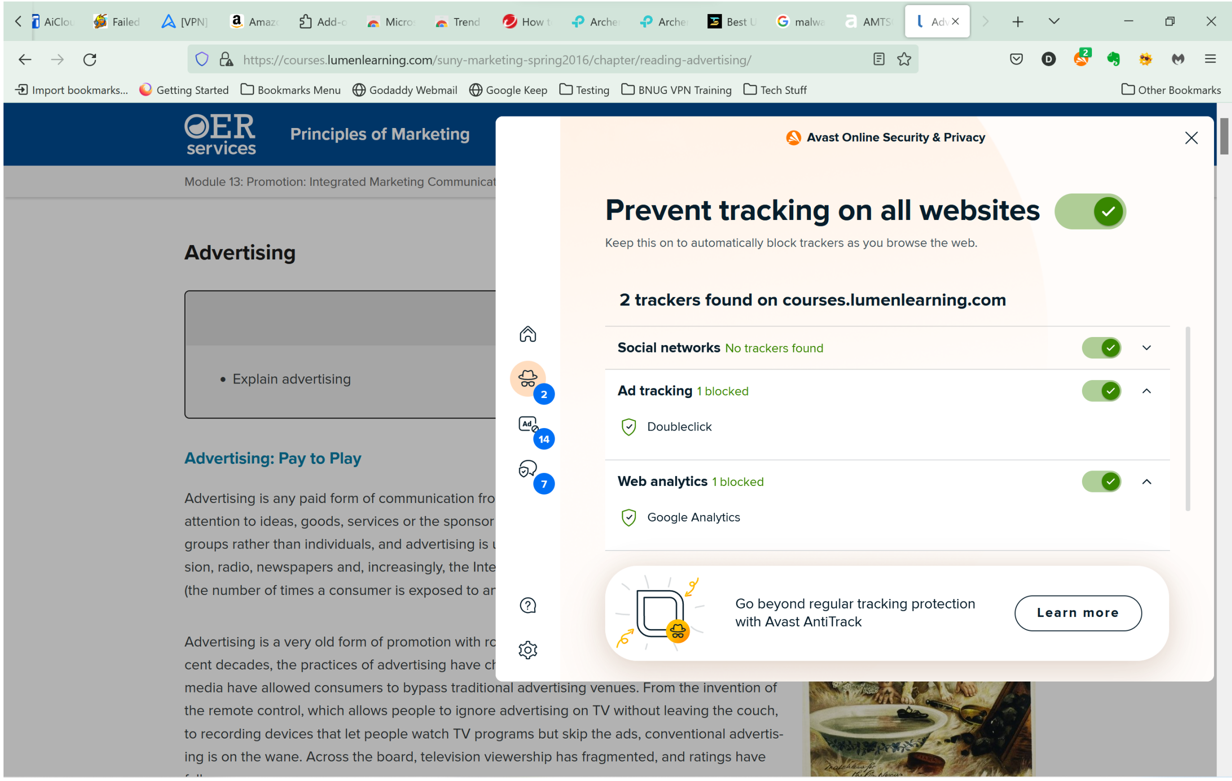
Employees can use hardware-isolated browsing sessions without any administrator or management policy configuration. In this mode, you must install Application Guard and then the employee must manually start Microsoft Edge in Application Guard while browsing untrusted sites. For an example of how this works, see the Application Guard in standalone modetesting scenario.

Enterprise-managed mode

Applies to:

- Windows 10 Enterprise edition, version 1709 or higher
- Windows 11

You and your security department can define your corporate boundaries by explicitly adding trusted domains and by customizing the Application Guard experience to meet and enforce your needs on employee devices. Enterprise-managed mode also automatically redirects any browser requests to add non-enterprise domain(s) in the container.



Avast Online Security & Privacy

Prevent tracking on all websites ✓

Keep this on to automatically block trackers as you browse the web.

2 trackers found on courses.lumenlearning.com

Social networks No trackers found ✓

Ad tracking 1 blocked ✓

Doubleclick

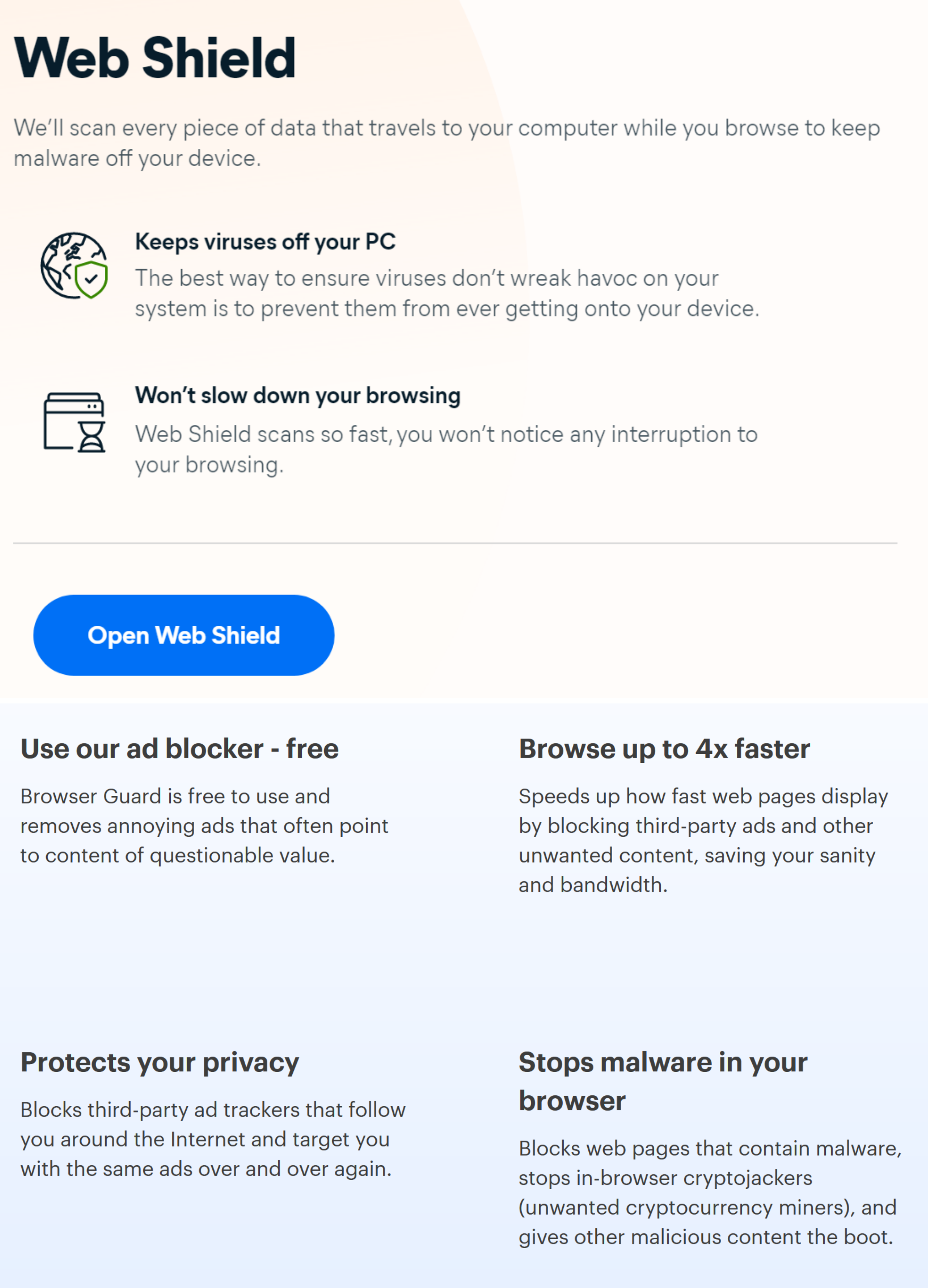
Web analytics 1 blocked ✓

Google Analytics

Go beyond regular tracking protection with Avast AntiTrack

Learn more

Show Avast Web Shield



Web Shield

We'll scan every piece of data that travels to your computer while you browse to keep malware off your device.

Keeps viruses off your PC

The best way to ensure viruses don't wreak havoc on your system is to prevent them from ever getting onto your device.

Won't slow down your browsing

Web Shield scans so fast, you won't notice any interruption to your browsing.

Open Web Shield

Use our ad blocker - free

Browser Guard is free to use and removes annoying ads that often point to content of questionable value.

Browse up to 4x faster

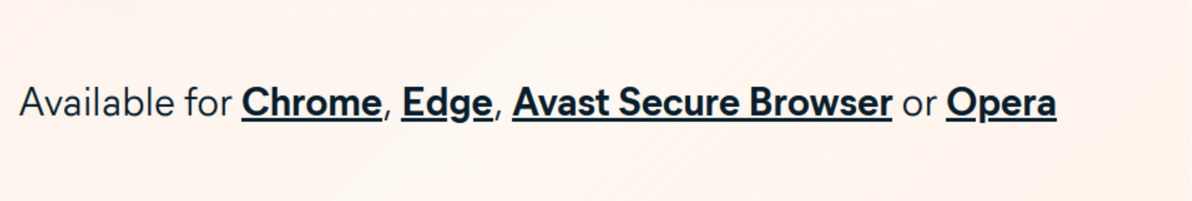
Speeds up how fast web pages display by blocking third-party ads and other unwanted content, saving your sanity and bandwidth.

Protects your privacy

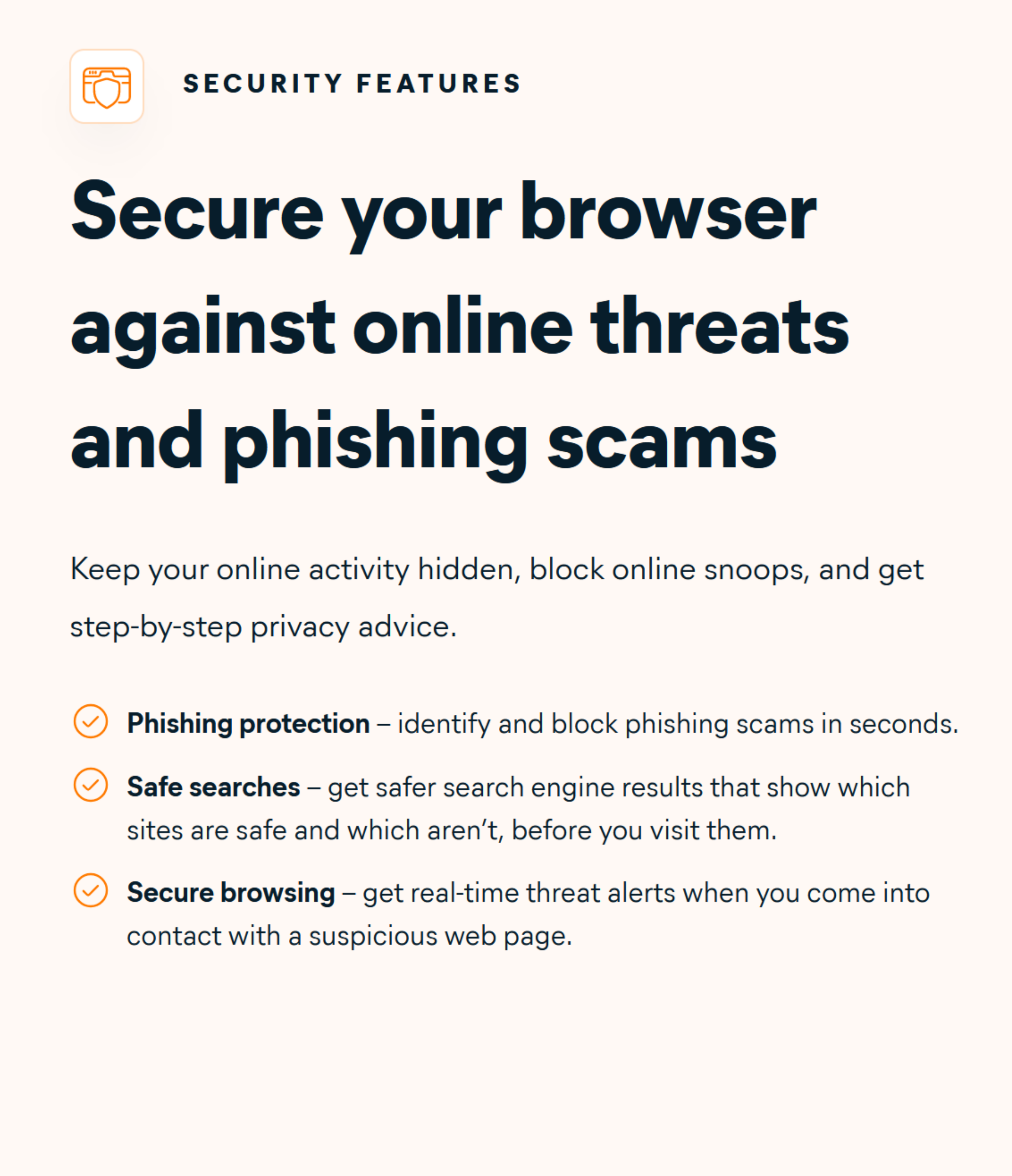
Blocks third-party ad trackers that follow you around the Internet and target you with the same ads over and over again.

Stops malware in your browser

Blocks web pages that contain malware, stops in-browser cryptojackers (unwanted cryptocurrency miners), and gives other malicious content the boot.



Available for **Chrome**, **Edge**, **Avast Secure Browser** or **Opera**



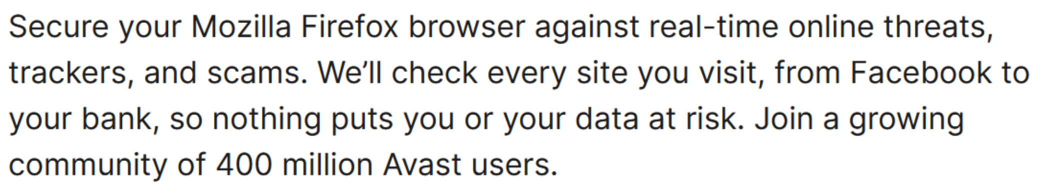
SECURITY FEATURES

Secure your browser against online threats and phishing scams

Keep your online activity hidden, block online snoops, and get step-by-step privacy advice.

- ✓ **Phishing protection** – identify and block phishing scams in seconds.
- ✓ **Safe searches** – get safer search engine results that show which sites are safe and which aren't, before you visit them.
- ✓ **Secure browsing** – get real-time threat alerts when you come into contact with a suspicious web page.

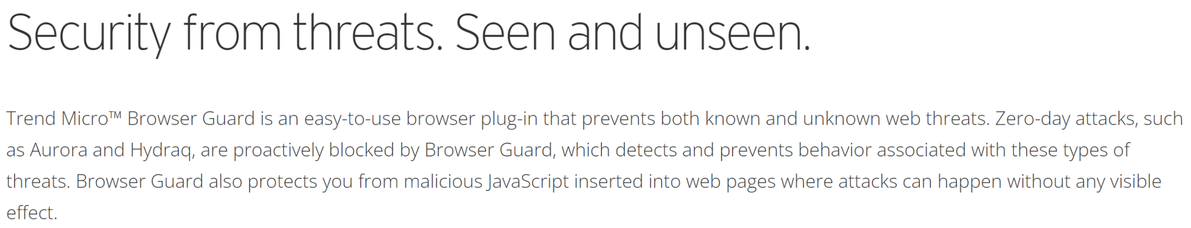
Claim



Secure your Mozilla Firefox browser against real-time online threats, trackers, and scams. We'll check every site you visit, from Facebook to your bank, so nothing puts you or your data at risk. Join a growing community of 400 million Avast users.

Show Avast Web Shield

Trend Micro Check - Browser Security

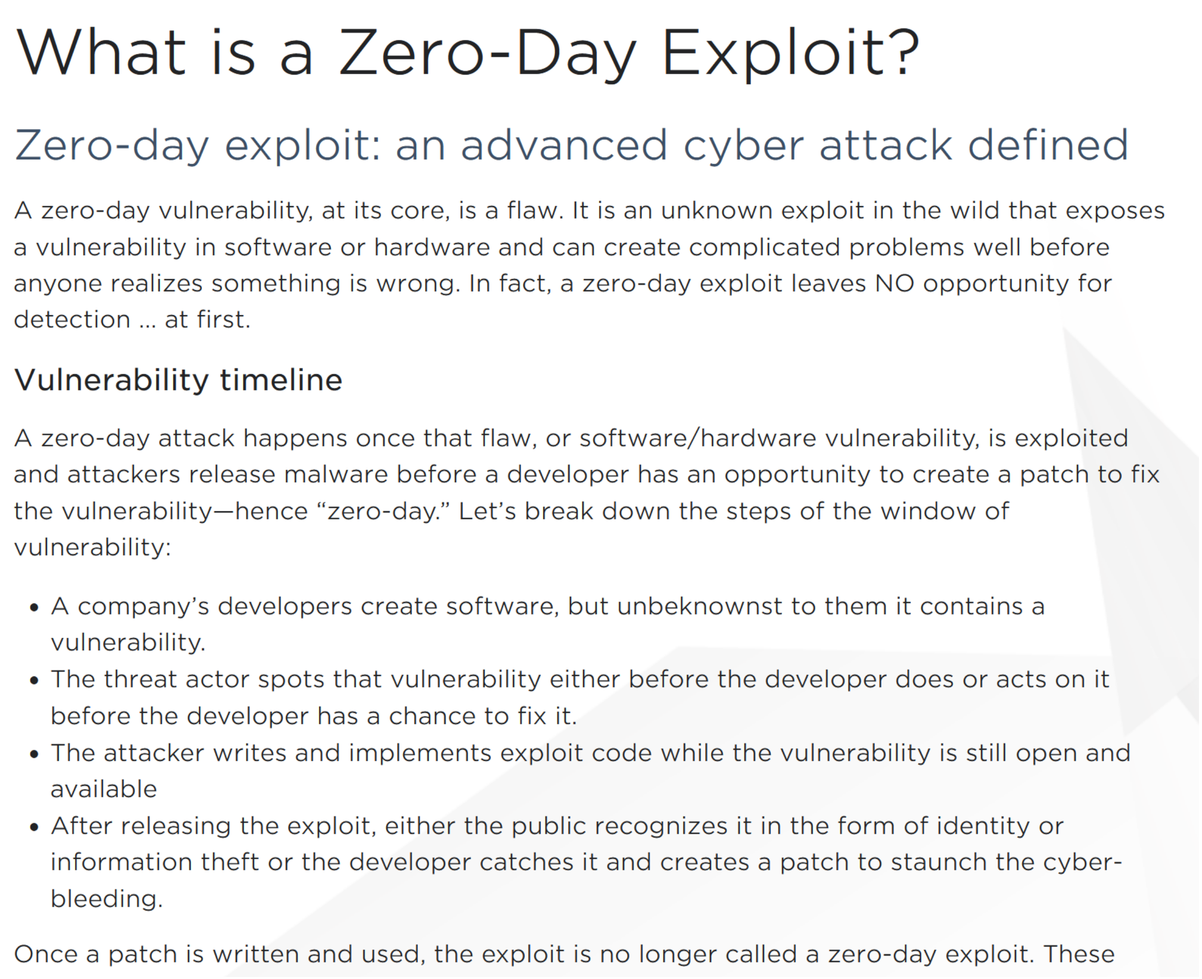


Security from threats. Seen and unseen.

Trend Micro™ Browser Guard is an easy-to-use browser plug-in that prevents both known and unknown web threats. Zero-day attacks, such as Aurora and Hydraq, are proactively blocked by Browser Guard, which detects and prevents behavior associated with these types of threats. Browser Guard also protects you from malicious JavaScript inserted into web pages where attacks can happen without any visible effect.

Known & Unknown

https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html



What is a Zero-Day Exploit?

Zero-day exploit: an advanced cyber attack defined

A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection ... at first.

Vulnerability timeline

A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day." Let's break down the steps of the window of vulnerability:

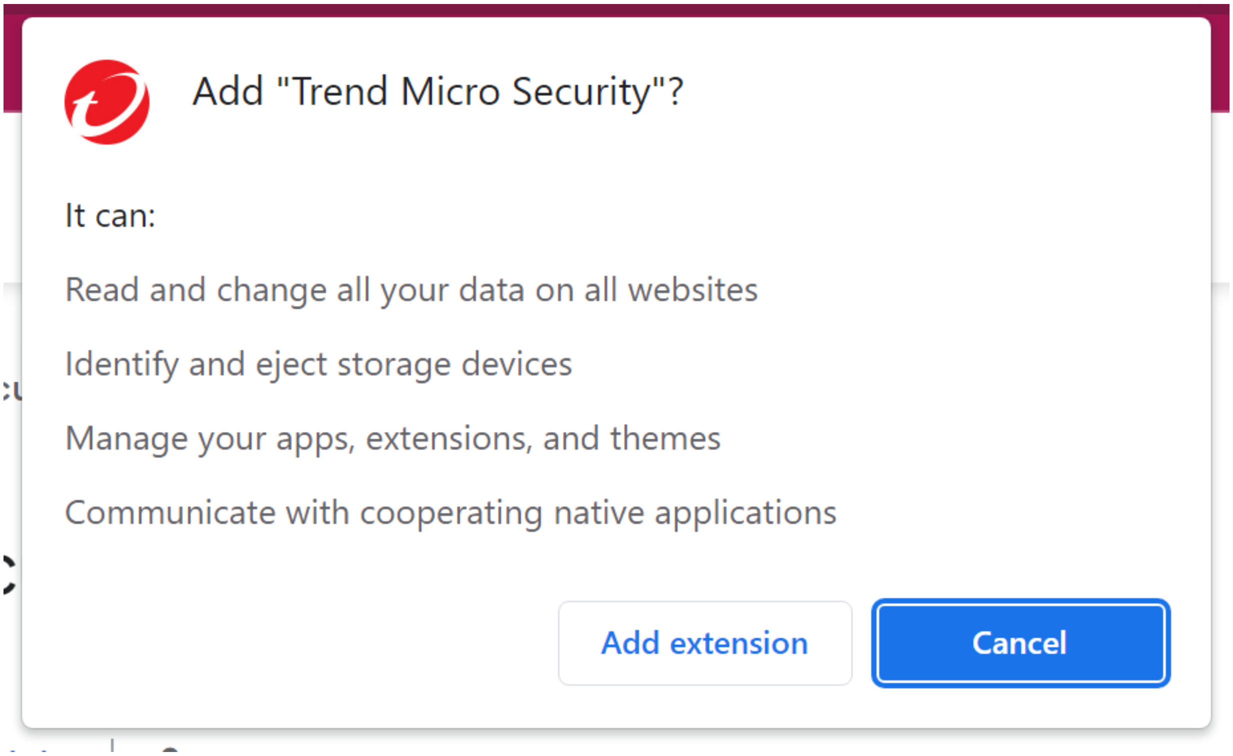
- A company's developers create software, but unbeknownst to them it contains a vulnerability.
- The threat actor spots that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
- The attacker writes and implements exploit code while the vulnerability is still open and available
- After releasing the exploit, either the public recognizes it in the form of identity or information theft or the developer catches it and creates a patch to staunch the cyber-bleeding.

Once a patch is written and used, the exploit is no longer called a zero-day exploit. These

https://www.trendmicro.com/en_no/forHome/products/free-tools/browser-guard.html

Trend Micro Security for Microsoft Edge
Trend Micro Check - Browser Security - Microsoft Edge Addons

Trend Micro Security for Google Chrome
https://chrome.google.com/webstore/detail/trend-micro-security/ibojepnlfiefkikckgmljdaogmgopbnn



Add "Trend Micro Security"?

It can:

Read and change all your data on all websites

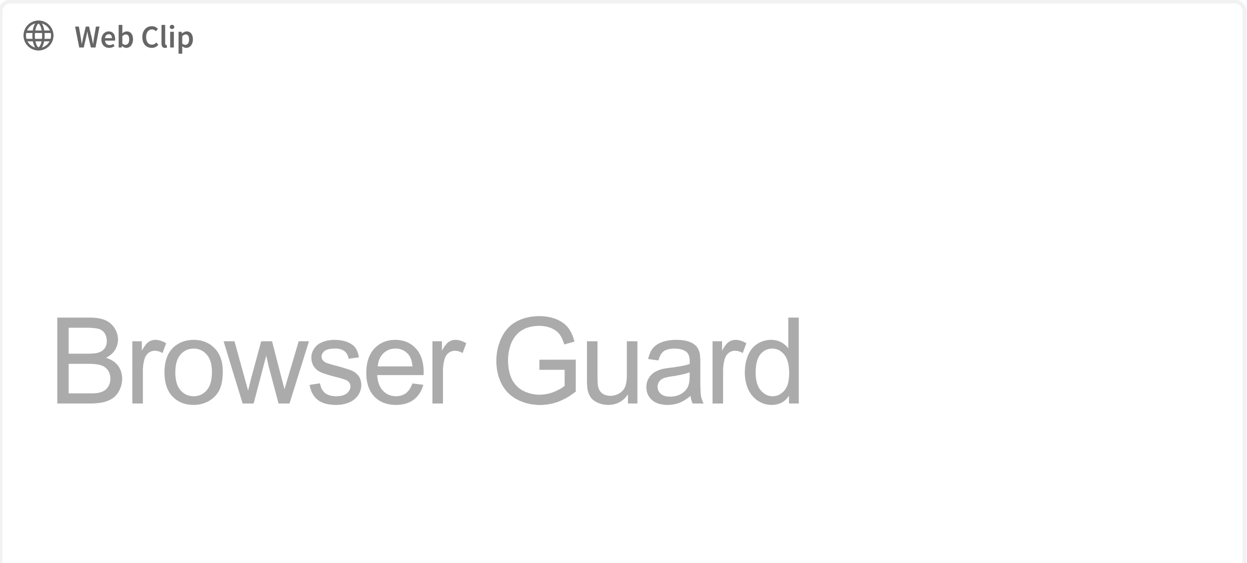
Identify and eject storage devices

Manage your apps, extensions, and themes

Communicate with cooperating native applications

Trend Micro for Safari Requires License

Trend Micro for Mozilla Firefox not available



Web Clip

Browser Guard

Proactively protect your browser against new web threats.

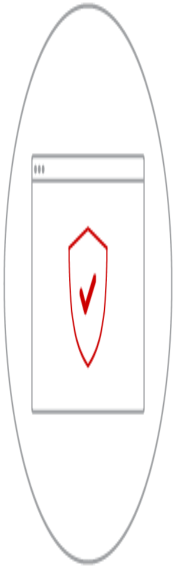
Download

Security from threats. Seen and unseen.

Trend Micro™ Browser Guard is an easy-to-use browser plug-in that prevents both known and unknown web threats. Zero-day attacks, such as Aurora and Hydraq, are proactively blocked by Browser Guard, which detects and prevents behavior associated with these types of threats. Browser Guard also protects you from malicious JavaScript inserted into web pages where attacks can happen without any visible effect.

Browser Guard has zero-day vulnerability prevention and protects against malicious JavaScript using advanced heuristics and emulation technologies.

Browser Guard is quickly and continuously updated to deliver the most secure and up-to-date technology. The latest version includes detection enhancement for Web Trojans, and for tracing infection chains.



Browser Guard

Protects against zero-day exploits

Detects buffer-overflow and heap-spray attacks

Protects against execution of shell code

Analyzes and protects against malicious JavaScript

Communicates with the Trend Micro Smart Protection Network

System requirements

Hardware	At least 300MHz Intel® Pentium^{TM} processor or equivalent 256MB of RAM (512MB recommended) At least 200MB available disk space
Operating System	Windows Vista®(32-bit, 64-bit) Ultimate, Business, Home Premium, or Home Basic with SP1 or SP2 Windows® 7 (32-bit, 64-bit) Windows® 8 (32-bit, 64-bit) Windows® 8.1 (32-bit, 64-bit) Windows® 10 (32-bit, 64-bit)

Terms & Conditions

These free antivirus services are provided on an "AS IS" basis. Trend Micro reserves the right to change the terms of this free antivirus site offerings without advance notice. Trend Micro also reserves the right to refuse service to any Web site at its sole discretion. For more information, please see our **legal notice**.