GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

W

Web Protection: How Browser and Network Defenses Work

Learn how browser reputation, DNS filtering, TLS, isolation, endpoint controls, and safe habits work together—and what web protection cannot guarantee.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	4 min

CONTENTS

In this guide

01 What does web protection do?

02 What web protection can inspect

03 Browser protection and reputation warnings

04 DNS filtering and network gateways

05 Browser isolation and endpoint controls

06 What HTTPS does and does not prove

07 Web protection checklist for users

08 Web protection for organizations

09 When a malicious page was opened

Web protection is a set of controls that reduces risk from malicious websites, downloads, scripts, tracking, and stolen web sessions. It can operate in the browser, on the device, through DNS or a network gateway, or in a remote browser-isolation service.

No single layer can guarantee that a page is safe. Effective protection combines reputation, content and behavior analysis, timely updates, identity security, and a user-visible way to handle warnings.

01 What does web protection do?

Web protection checks a requested site, connection, page, or download before or while the user interacts with it. Depending on the product, it can warn about phishing, block a known malicious domain, stop a harmful download, apply an organization's browsing policy, or isolate active web content from the device.

"Web protection" is a category, not one universal feature. A browser's safe-browsing warning, an antivirus web shield, a DNS filter, and a secure web gateway see different parts of the request and should not be assumed to provide identical coverage.

02 What web protection can inspect

- Requested domains and URLs against reputation or threat intelligence.
- DNS queries before a browser connects.
- Downloaded files, scripts, and browser behavior.
- TLS certificate and connection errors.
- Page characteristics associated with phishing or impersonation.
- Network requests through a web security gateway.

Encrypted HTTPS hides page content from ordinary network observers. A managed inspection gateway can decrypt approved traffic only when devices trust its certificate and policy permits it, creating privacy, security, and operational responsibilities.

03 Browser protection and reputation warnings

Modern browsers compare destinations and downloads with security services and may show a full-page warning. Do not bypass it merely because a link came from a friend or search result. Verify the exact hostname and contact the organization through a known channel. A newly created phishing site may not yet have a poor reputation, so appearance and HTTPS alone are not proof of legitimacy.

04 DNS filtering and network gateways

DNS filtering can prevent resolution of known malicious or disallowed domains. It is fast and broadly deployable, but it may not see a full URL and can be bypassed by direct IP access or unapproved encrypted DNS. Gateways can apply more context, authentication, download scanning, and policy, but must be configured for remote as well as office users.

05 Browser isolation and endpoint controls

Browser isolation executes web content away from the endpoint and streams a safer representation to the user. It can reduce exposure to browser exploits but may affect downloads, uploads, accessibility, and interactive applications. Endpoint protection can still inspect processes and files that reach the device. Use isolation for higher-risk categories or users rather than assuming it replaces all endpoint controls.

06 What HTTPS does and does not prove

HTTPS encrypts traffic and authenticates control of the site name covered by the certificate. It does not prove that the site owner is honest, a download is safe, or a login request is expected. Treat certificate warnings as a stop condition; changing the clock or installing an unknown certificate to remove the warning can make interception easier.

07 Web protection checklist for users

1. Keep the browser, extensions, operating system, and document readers updated.
2. Remove extensions you no longer need and restrict their site access.
3. Use a password manager and phishing-resistant MFA.
4. Navigate to sensitive sites from a bookmark or typed address.
5. Check the complete hostname before entering credentials or payment data.
6. Do not enable notifications, paste commands, or install software at a page’s request without independent verification.

08 Web protection for organizations

Define acceptable-use and privacy policies, protect managed browsers, enforce updates, and collect enough telemetry to investigate without retaining unnecessary personal data. Provide a fast false-positive review path so users do not learn to bypass controls. Test policies on representative business applications and monitor coverage for off-network devices.

09 When a malicious page was opened

Close the page and do not interact further. If credentials were entered, change them from a clean device, revoke sessions, and review MFA and recovery settings. If a file ran or the browser behaved unexpectedly, disconnect the device as appropriate, preserve details, and run the organization’s incident-response or security-scan process.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com