

Microsoft Edge for Business: AI and protection in one secure enterprise browser

Bolster your Zero Trust architecture with built-in security and native support for Microsoft security solutions

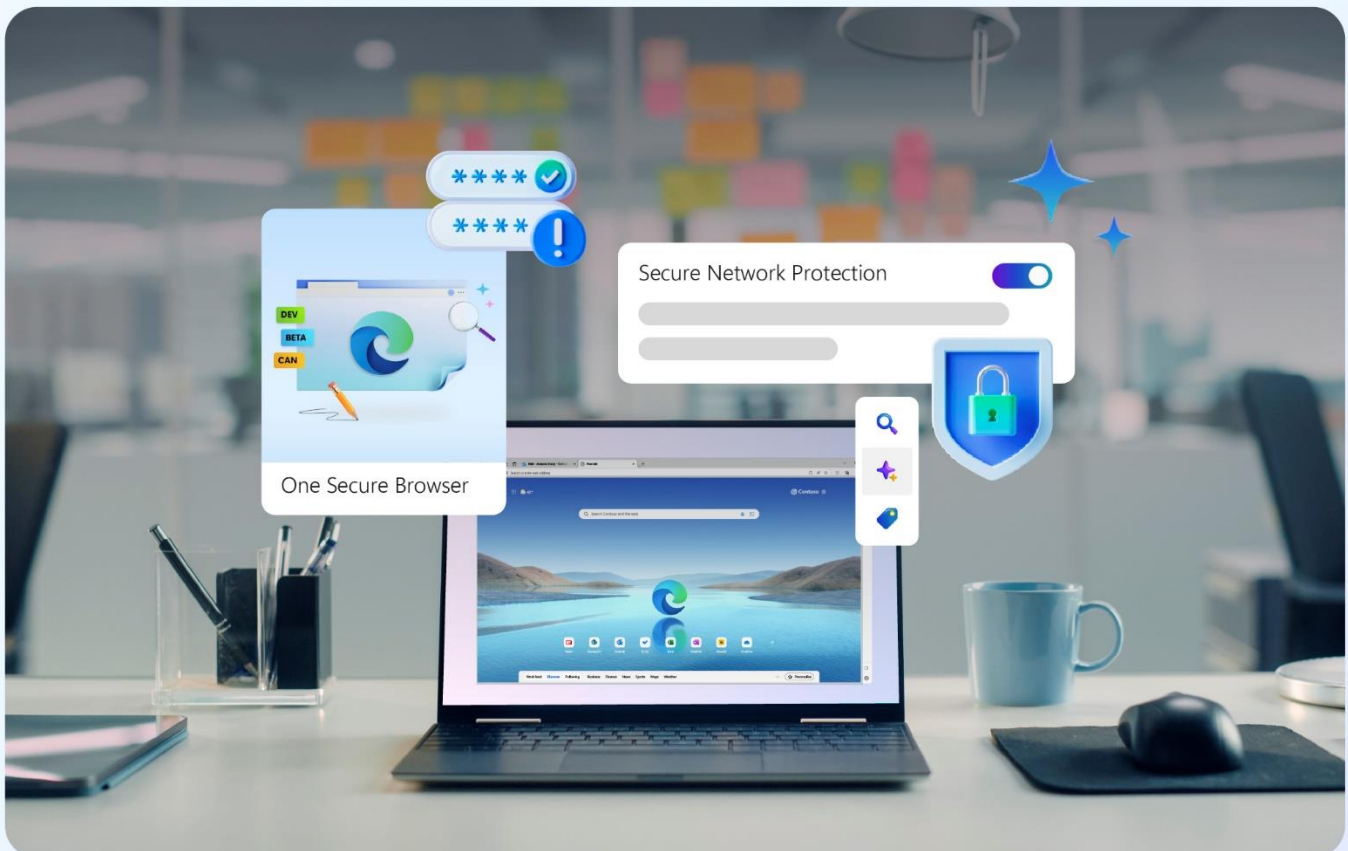


TABLE OF CONTENTS

INTRODUCTION.....	3
WHAT IS A SECURE ENTERPRISE BROWSER?	4
ZERO TRUST CHANGES THE SECURITY GAME	5
MICROSOFT EDGE FOR BUSINESS COMPLEMENTS ZERO TRUST.....	6
GENERATIVE AI WEBCHAT WITH ENTERPRISE DATA PROTECTION	8
SAFEGUARD SENSITIVE ENTERPRISE DATA.....	9
PHISHING AND MALWARE PROTECTION	10
SAFEGUARD AGAINST MEMORY-RELATED VULNERABILITIES	12
REDUCE RISK OF MISSPELLED URLs	15
IDENTITY SIGNALS TO ENFORCE ACCESS POLICIES	16
PASSWORD ALERTS AND STRONG PASSWORDS	17
DEDICATED AND GUIDED MANAGEMENT EXPERIENCE	19
MANAGED BROWSER ON PERSONAL AND BYOD DEVICES.....	21
SECURE ACCESS ON MOBILE.....	22
CONCLUSION.....	24



INTRODUCTION

As the digital landscape continues to grow and transform at a fantastic rate, so does the increase in threat vectors and risk factors. Cyberattacks are growing at a rate of 490% year-over-year,¹ and the cost of these attacks is projected to surpass \$10.5 trillion annually by 2025.² Combined with the hybrid working world of today and the growing prevalence of AI use, the need for enhanced security measures for users, devices, and data has never been stronger. The answer to this challenge revolves around security solutions that align to a Zero Trust security model. Instead of assuming everything behind an organization's firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network.

When organizations seek to adopt a Zero Trust model and implement tools and policies around it, internet browsers often fall down the list of strategic priorities. But the fact is, users spend most of their time in the browser accessing trusted—or untrusted—content. With vulnerability exploitations rising at 180% annually,³ maximizing browser security is an imperative to reducing organizational risk. Of course, focusing on browser security also comes with the added benefit of making it easier for users to see how their activities are being protected. Seeing various security tools in action can help users grasp their organization's overall security strategy, and when users better understand the organization's motives and actions, they are more likely to engage in safer behavior and be more conscious about their role in protecting company assets. As such, a secure enterprise browser is a must-have for any organization.

1. [Identity Theft Resource Center Sees Third-Most Data Breach Victims in a Quarter in Q2 2024](#)
2. [Cybercrime To Cost The World \\$10.5 Trillion Annually By 2025](#)
3. [Verizon 2024 Data Breach Investigations Report](#)

WHAT IS A SECURE ENTERPRISE BROWSER?

All browsers perform the same basic job of enabling users to view and interact with content online while offering some security measures. But not all browsers have what an organization needs.

The question isn't just whether your organization's current browser is secure, but whether it provides you with the enterprise-grade security and controls

needed to address the latest business scenarios—ideally at no additional cost. That's where Edge for Business comes in. Edge for Business is a secure enterprise browser that helps organizations keep up with the emerging threat landscape by providing them with:

Organizational needs include:

- Device health and identity checks
- Data loss prevention
- Personal and unmanaged device support
- Generative AI controls
- Comprehensive management tools

Seamless integration – Edge for Business is included out-of-the-box in Windows, helping streamline deployment and fulfill enterprise security requirements without the need for additional browsers.

Advanced security at no additional cost – Expand your protections without the hassle of extensions using comprehensive security capabilities built into Microsoft 365 E3 and E5 subscriptions.

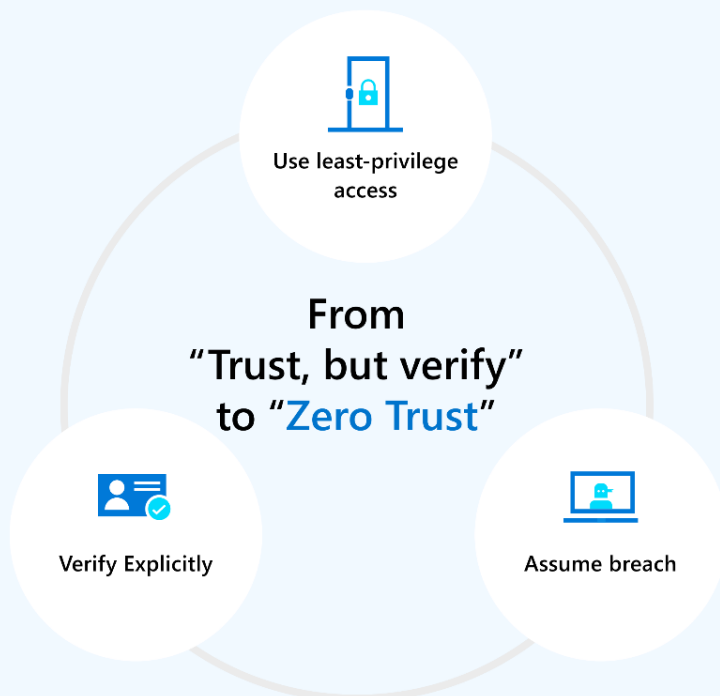
Optimized for enterprise generative AI – Supports enterprise data protection, safeguarding generative AI prompts and responses.

Proven security leadership – Microsoft is a recognized leader in security, compliance, identity, and endpoint management and is uniquely positioned to address the evolving cybersecurity threat landscape.

At Microsoft, we are committed to helping our customers stay ahead of the evolving threat landscape. Edge for Business is ready to meet your organization's needs for a secure enterprise browser today, and as we move forward, we are continuing to enhance our security capabilities to ensure Edge for Business remains the trusted choice for a secure, productive browsing experience.

ZERO TRUST CHANGES THE SECURITY GAME

The [Zero Trust](#) methodology gives organizations a different approach to security and has become the standard for organizations. Prior best practices revolved around the model of “trust but verify,” however attacks in today’s landscape can take advantage of the trust inherent in that model, driving a need for change in tackling this challenge. These attacks are costing organizations more each year, as seen with the average cost of a data breach reaching \$4.88M in 2024.⁴ As a result, organizations are changing their security strategy to align with three principles based on the concept of “*never trust, always verify*”:



Verify explicitly – always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least-privilege access – limiting user access via just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.

Assume breach – minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

4. [Cost of a data breach Report 2024 \(IBM\)](#)

MICROSOFT EDGE FOR BUSINESS COMPLEMENTS ZERO TRUST

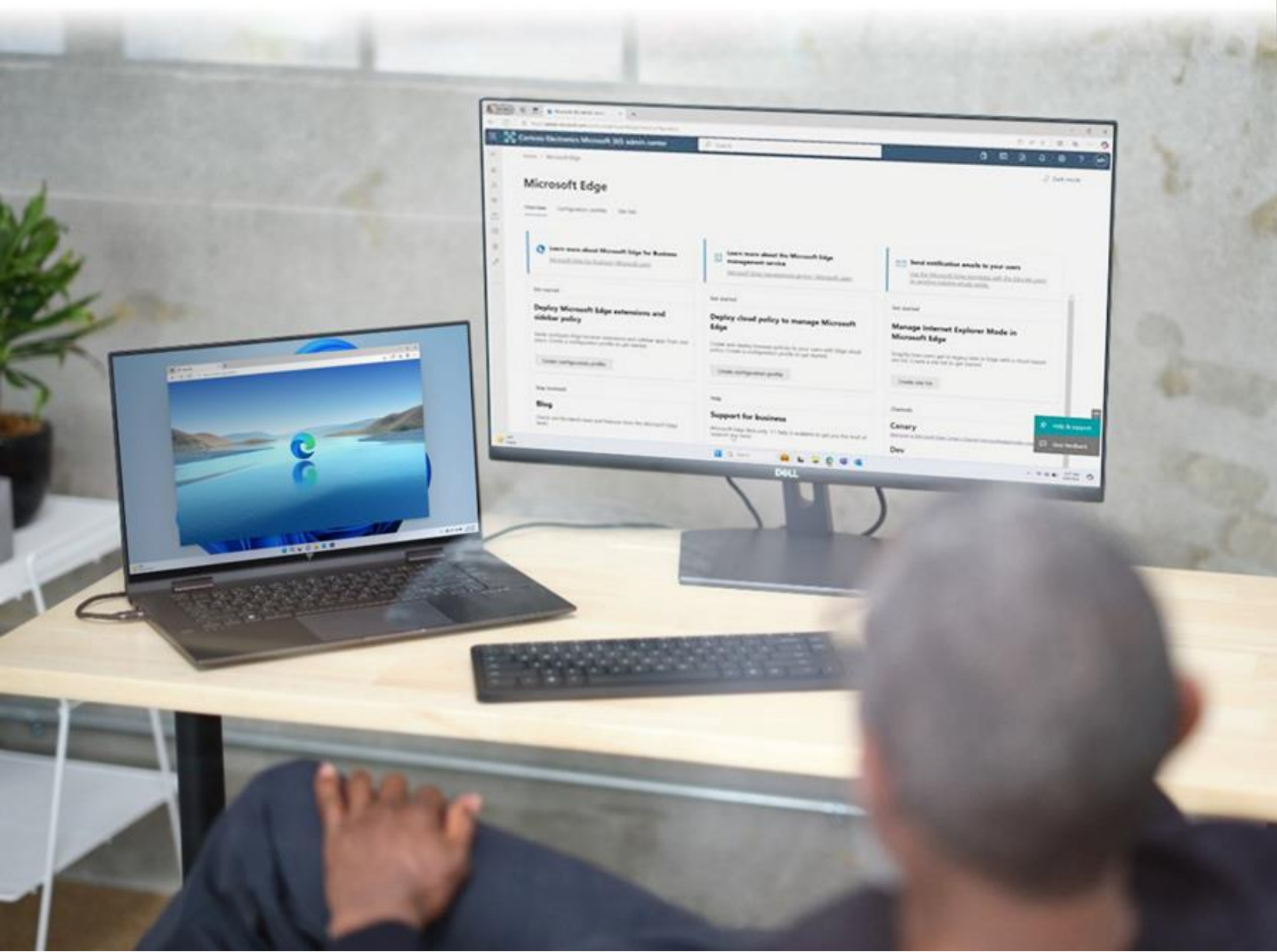
Microsoft Edge for Business is available on supported desktop platforms along with iOS and Android and built with Chromium, giving it the well-engineered and tested security architecture design at its foundation. Because of this foundation, Edge releases security updates and patches quickly to help stay ahead of security threats, such as zero-day exploits, to minimize the impact of compromise.

As a secure enterprise browser, Edge for Business expands on the security features of Chromium by seamlessly integrating with Microsoft Security solutions and offering features that support a Zero Trust security model. These features include:

Microsoft Entra Conditional Access	Ensure that only compliant devices can access corporate resources
Microsoft Purview Data Loss Prevention (DLP)	Protect sensitive data from unauthorized access and sharing
Microsoft Intune Mobile Application Management	Extend security controls to personal and unmanaged devices, mitigating risks associated with BYOD policies
Microsoft Defender SmartScreen	Safeguard users from phishing and malicious websites
Enhanced security mode (ESM)	Safeguard against memory-related vulnerabilities
Website typo protection	Prevent users from inadvertently visiting harmful sites due to typos
Password Monitoring and Generator	Alert users to compromised credentials and help them generate strong passwords
Edge management service	Provide admins with a dedicated, guided management experience for Edge for Business

Our goal is for Edge for Business to provide the most secure experience for end users across all browsers. With no extensions to manage for these protections, IT admins can maintain their environments more easily. There are less concerns of a performance hit and less attack vectors that could potentially become compromised since there are no extensions in use for these features.

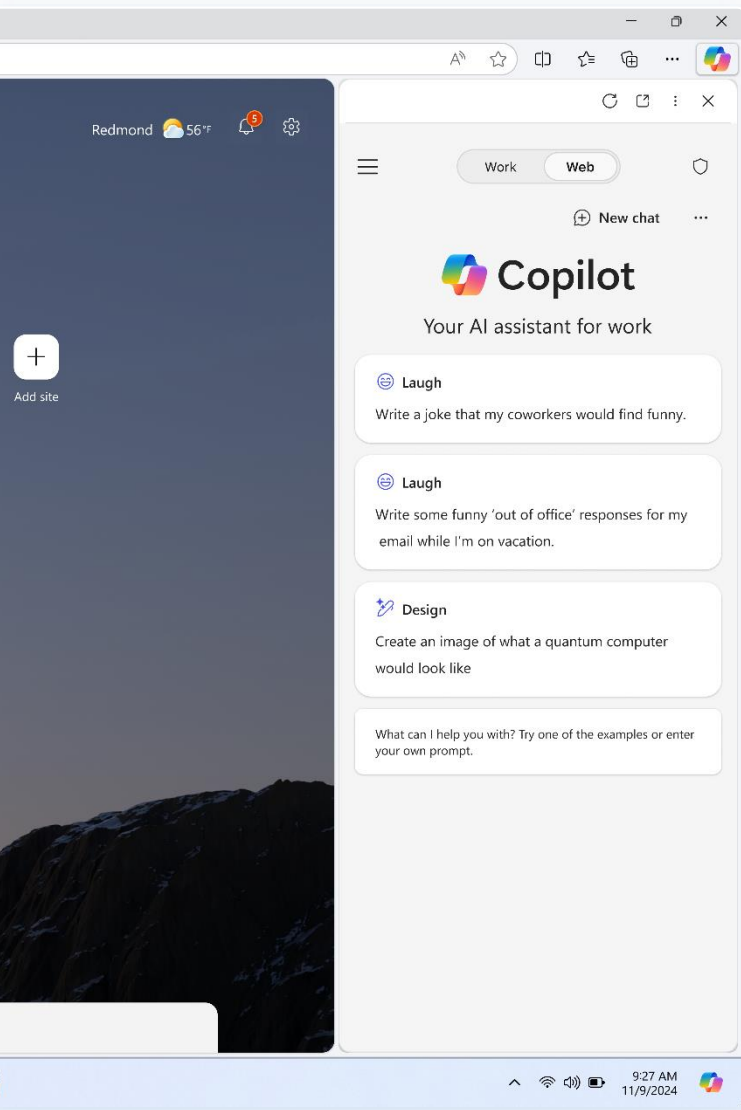
With these capabilities, detailed over the next pages, Edge for Business aligns itself with the Zero Trust principles. The threat detection and prevention features align with the *"assume breach"* principle, and the management features and native support align with the principles to *"use least-privilege access"* and *"verify explicitly."*



GENERATIVE AI WEBCHAT WITH ENTERPRISE DATA PROTECTION

Microsoft Copilot

People are looking to use AI tools to help them unlock creativity and productivity at work—in fact, 75% of global knowledge workers surveyed in our Work Trend Index Annual Report said they’re already using AI at work today.⁵ But using public AI tools that are not built for the enterprise inadvertently puts sensitive business data at risk. As organizations adopt AI, they want to be confident that their data is protected—and some companies have even felt the need to block all AI use in response.



The good news is that it’s possible to move forward with AI and protect confidential data. Microsoft Copilot is an AI-optimized chat experience grounded in web data from the Bing search index. When users sign in with their work or school (Entra ID) accounts, they will receive enterprise data protection (EDP).

Microsoft Copilot offers the same enterprise terms available in our Microsoft 365 commercial offerings. Use of Microsoft Copilot involves prompts (entered by users) and responses (content generated by Copilot). With EDP, prompts and responses are protected by the same contractual terms and commitments widely trusted by our customers for their emails in Exchange and files in SharePoint.

5. [2024 Work Trend Index Annual Report](#)

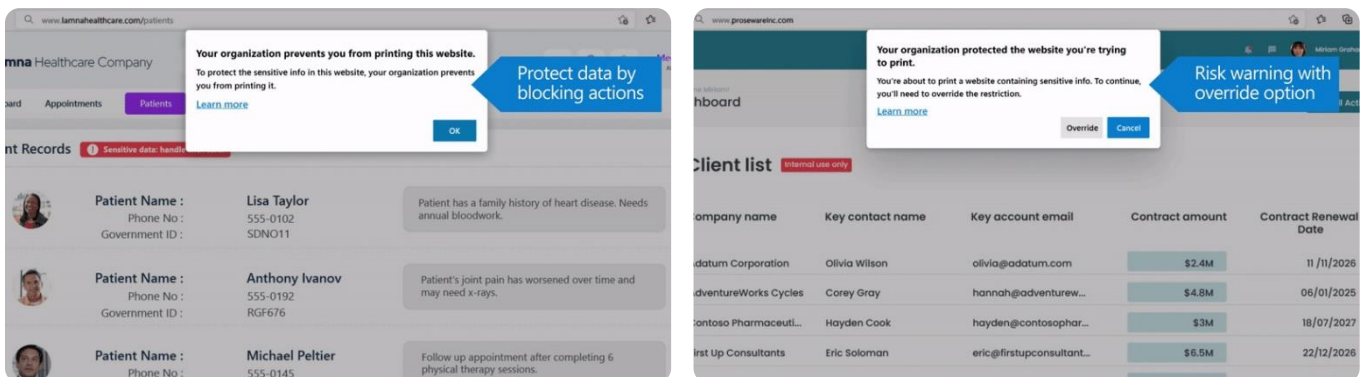
SAFEGUARD SENSITIVE ENTERPRISE DATA

Microsoft Purview Data Loss Prevention

Microsoft Purview Data Loss Prevention (DLP) is a system of technologies that identifies and safeguards sensitive enterprise data from unauthorized disclosure. This technology is built into Microsoft Edge and utilizes the [sensitive service domains](#) feature. This enforces admin-configured policies for sensitive files, and records audit events for non-compliant activities. Some of the user activities that you can audit and manage on devices include the following:

- Print from a website
- Copy data from a website
- Save websites as local files
- Upload or drag/drop a sensitive file to an excluded website
- Paste sensitive data into an excluded website

For the print, copy data, and save actions, each website must be listed in a website group. When [configured](#), IT admins can "audit," "block with override," or "fully block" user activity when users attempt to take any unauthorized action.

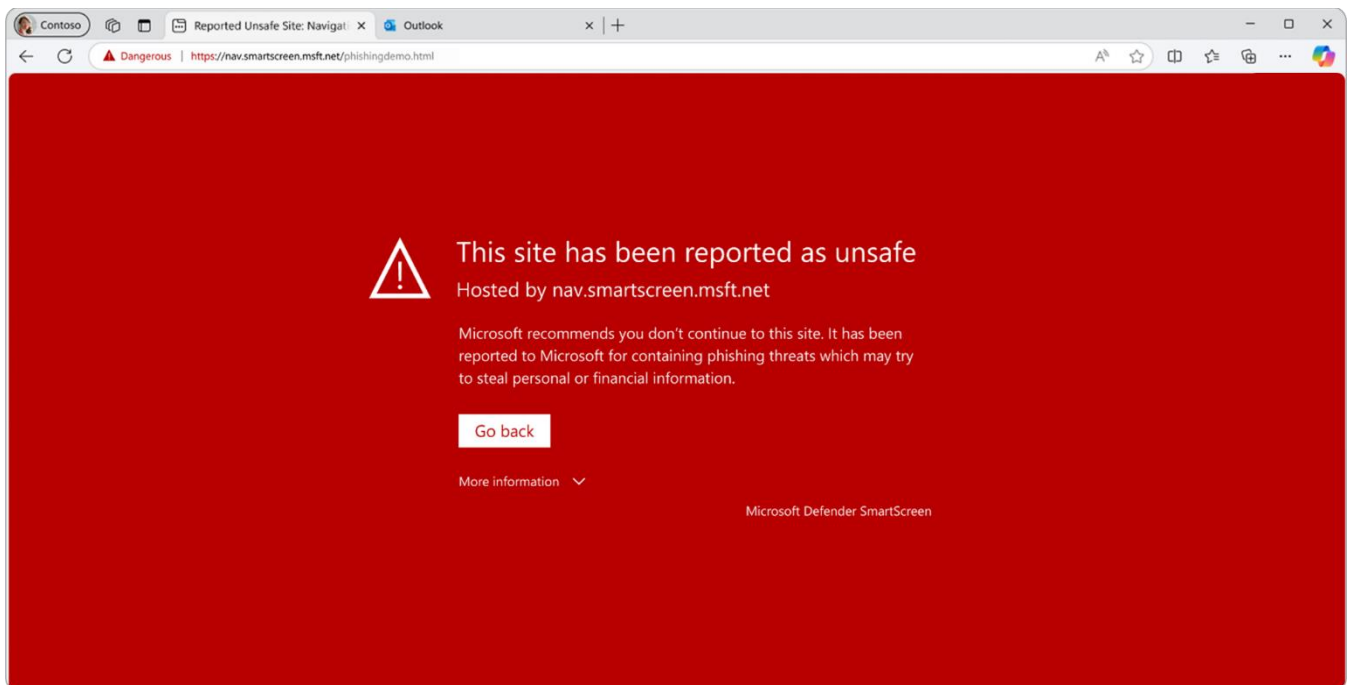


PHISHING AND MALWARE PROTECTION

Microsoft Defender SmartScreen

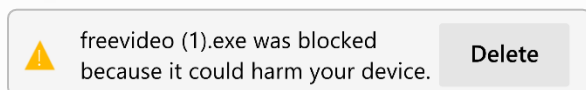
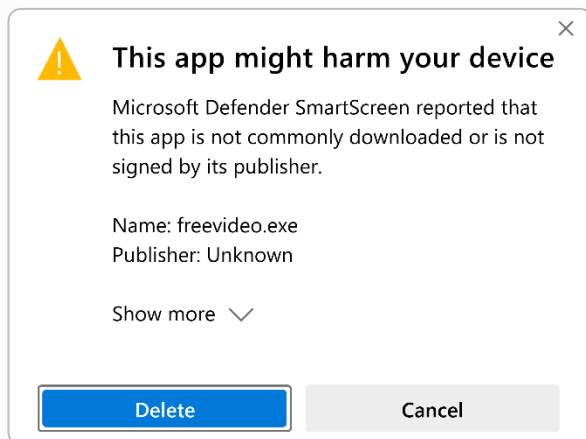
Microsoft Defender SmartScreen is a service that helps keep users safe while browsing the web by notifying them of potentially suspicious websites. SmartScreen does a real-time reputation check of websites and downloads and is part of the Microsoft Intelligent Security Graph, which draws signals and insights generated from Microsoft's large network of global assets, researchers, and partners. With this, Microsoft Edge provides an early warning system against websites that might engage in phishing attacks or attempt to distribute malware through a focused attack. Policies can be configured using group policy, Intune, or Mobile Device Management (MDM). It provides several benefits for added protection:

- Anti-phishing and anti-malware support
- Reputation-based URL and app protection
- Operating system integration
- Improved heuristics and diagnostic data
- Management through Group Policy and Microsoft Intune
- Blocking URLs associated with potentially unwanted applications



How it works:

Utilizing data received from user feedback, data providers, and intelligence models, Microsoft Defender SmartScreen determines whether a site is potentially malicious by analyzing visited webpages for indications of suspicious behavior and checking the site against a dynamic record of reported phishing sites. If a site is determined to be malicious, the user will see a screen warning them that the site has been reported as unsafe, with an option to report the site as safe or unsafe.



To protect users from downloading compromised files, SmartScreen will analyze the file based on criteria including download traffic, download history, past anti-virus results, and URL reputation. If a file is safe, no action is taken on the download. If the file is unsafe and reported as malicious, it will be blocked. If the file has inconclusive results and is unknown, the user will be given an advisory warning and can choose to delete the file or continue the download after selecting “*Show more.*”

SmartScreen stores data about reputation checks and builds a database of known malicious URLs and files. The data is stored on secure Microsoft servers and is used only for Microsoft security services. The data is never used for identification or targeting purposes in any way. Clearing the browsing cache clears all locally stored SmartScreen URL data. Clearing the download history removes any locally stored SmartScreen data about file downloads. [Scenario testing](#) is available to see how SmartScreen will respond to different situations.

SAFEGUARD AGAINST MEMORY-RELATED VULNERABILITIES

Enhanced security mode

Enhanced security mode in Microsoft Edge helps safeguard against memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections for the browser. There are multiple protections included in this protective mode including the following:

- [Arbitrary Code Guard \(ACG\)](#)
- [Code Integrity Guard \(CIG\)](#)
- [Control Flow Guard \(CFG\)](#)
- [Hardware-enforced Stack Protection](#)

Arbitrary Code Guard (ACG):

ACG helps protect against a malicious attacker loading the code of their choice into memory through a memory safety vulnerability and being able to execute that code. It protects an application from executing dynamically generated code (code that is not loaded, for example, from the .exe itself or a .dll). It works by preventing memory from being marked as executable. When an application attempts to allocate memory, the protection flags are checked. If the allocations attempt to include the “*execute*” protection flag, then the memory allocation fails and returns an error code. If the application attempts to change the protection flags that have been allocated and include the “*execute*” protection flag, then the permission change will fail.

Code Integrity Guard (CIG):

CIG ensures that all binaries loaded into a process are digitally signed by Microsoft. It includes Windows Hardware Quality Labs (WHQL) signatures, which allow WHQL approved drivers to run within the process. This mitigation is implemented within the memory manager, which blocks the binary from being mapped into memory. If a binary that is not signed by Microsoft attempts to be loaded, the memory manager will give an error. By blocking at the memory manager level, this prevents both binaries loaded by the process and binaries injected into the process.

Control Flow Guard (CFG):

CFG is a protection for applications compiled with CFG support. It mitigates the risk of attackers using memory corruption vulnerabilities by protecting indirect function calls. This mitigation is provided by injecting another check at compilation time. Before each indirect function call, another instruction is added which verifies that the target is a valid call target before it is called. If the target is not a valid call target, then the application is terminated.

The check for a valid target is provided by the Windows kernel. When executable files are loaded, the metadata for indirect call targets is extracted at load time and marked as valid call targets. Additionally, when memory is allocated and marked as executable (such as for generated code), these memory locations are also marked as valid call targets, to support mechanisms such as JIT compilation.

Hardware-enforced Stack Protection:

Hardware-enforced Stack Protection is an exploit mitigation that will protect the return address, and work with other Windows mitigations to prevent exploit techniques that aim to achieve arbitrary code execution. Two policies that are prominent in this protection are shadow stack and instruction pointer validation.

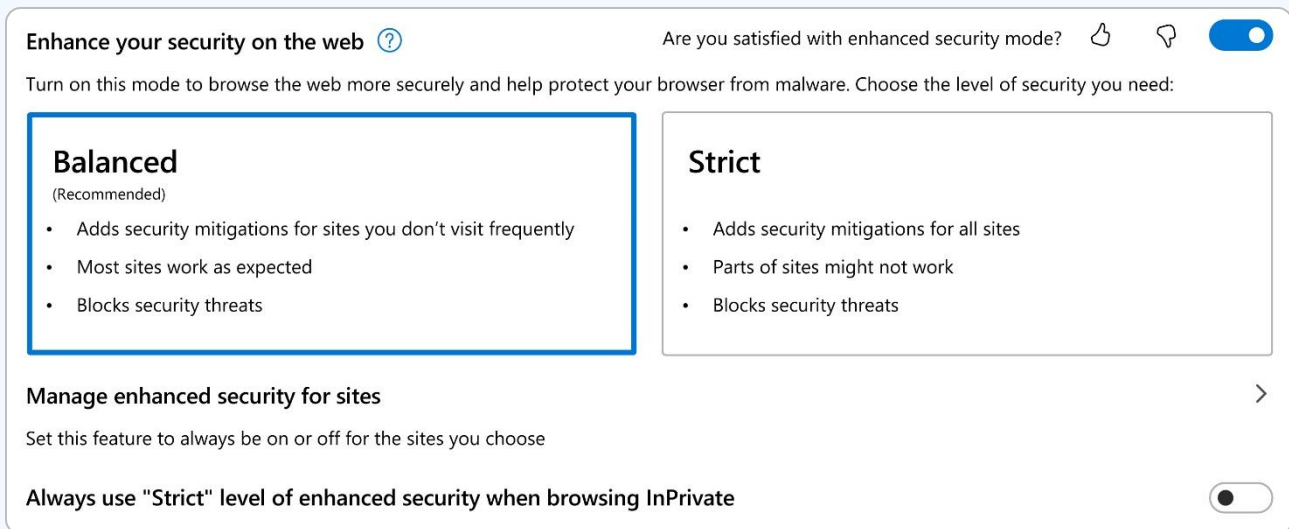
Shadow stack is a hardware-enforced read-only memory region that can be activated to help keep record of the intended control-flow of the program. Call instructions will push the return address on both stacks and return instructions will compare the values and issue a CPU exception if there is a return address mismatch.

Instruction pointer validation mitigates control flow hijacking to corrupt the instruction pointer value inside the *"context"* structure passed into system calls that redirect thread execution. This step mitigation is active during exception handling. With this feature enabled, the user-supplied instruction pointer will be checked to see if it is on the shadow stack or in the EH continuation data (EHCONT), before allowing the call to proceed or the call will fail. Note that if the binary does not contain EHCONT data (legacy binary), then the call is allowed to proceed.

Enhance Security Configuration

Enhanced security mode is turned off by default. The following settings are available:

- Off (Default): Feature is turned off.
- Balanced (Recommended): Microsoft Edge will apply added security protections when users visit their less familiar sites but bypass those protections for commonly visited sites. This combination provides a practical level of protection against attackers while preserving the user experience for a user's usual tasks on the web.
- Strict: Microsoft Edge will apply added security protections for all the sites a user visits. Users may report some challenges accomplishing their usual tasks.



In both modes, exceptions can be created for users' trusted websites. IT admins can configure this security feature using [Group Policy settings](#), including creating "Allow" and "Deny" lists to explicitly enhance security for their users when visiting certain sites, or disable the mode for other users.

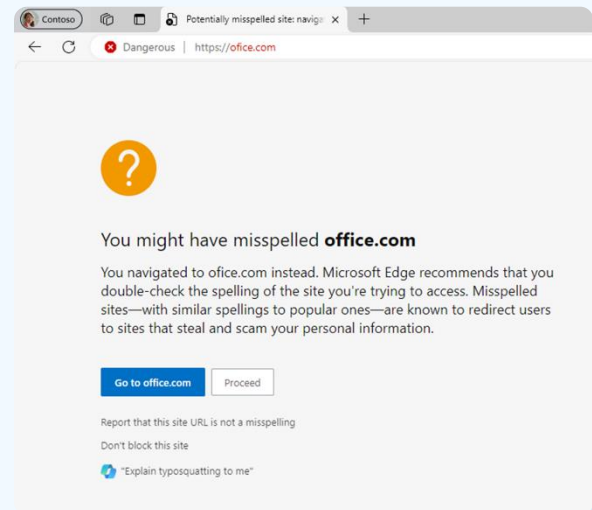
REDUCE RISK OF MISPELLED URLs

Website typo protection

Threat actors use typosquatting to prey on users who misspell a URL. And while users may not be aware, there has been a recent resurgence of typosquatting attacks using fake domains, as well as scam sites that impersonate brands or offer fake hiring information.⁶ Microsoft Edge includes a typosquatting checker that can warn users if they appear to have mistyped a common web address and may be directed to a malicious site. With this growing threat, website typo protection brings a piece of mind to users and IT in case of accidental typos.

How it works:

Once configured through [policy](#) or in Edge settings, users are given an interstitial warning page suggesting that the site might have been misspelled. A corrected URL is suggested, and users are given a choice to which website to access.

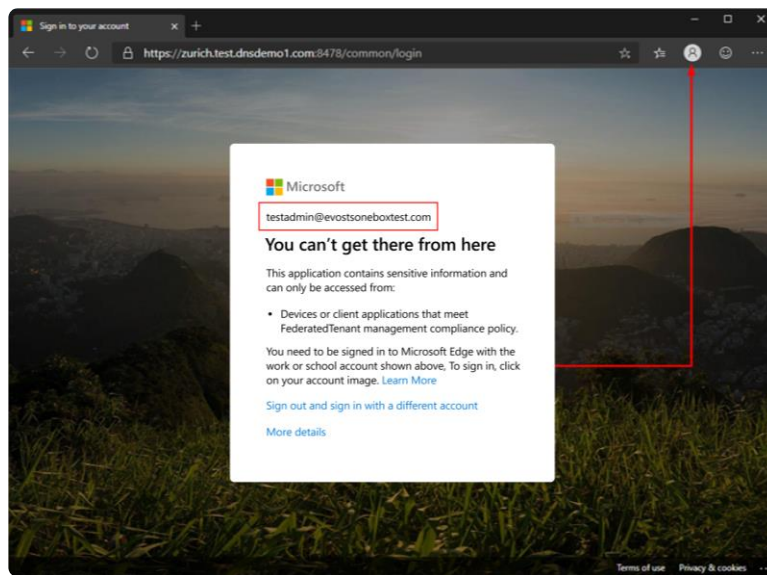


6. [Typosquatting Wave Shows No Signs of Abating](#)

IDENTITY SIGNALS TO ENFORCE ACCESS POLICIES

Microsoft Entra Conditional Access

Microsoft Edge for Business natively supports [Microsoft Entra Conditional Access](#) (formerly known as Azure Active Directory (Azure AD) Conditional Access). Conditional Access is an advanced policy engine that extends security measures well beyond basic authentication. Conditional Access takes in vast amounts of data in real-time to ascertain the context of a user's access request such as device, location, group, and role. Each signal is analyzed to accurately grant or deny access or seek additional authentication. When signed into a Microsoft Edge profile with Microsoft Entra ID credentials, Edge allows seamless access to enterprise cloud resources protected using Conditional Access on managed and unmanaged devices.



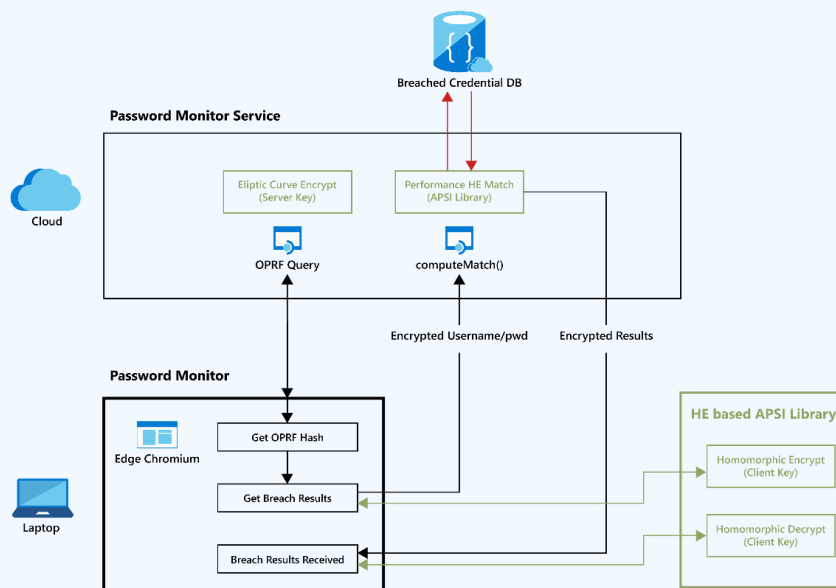
How it works:

On a compliant device, the identity accessing the resource should match the identity on the profile. If there is no match, an error denying access will be displayed. Improperly configured personal devices will not be able to access company resources but properly configured devices will be, therefore allowing end users the best balance of safety and convenience.

PASSWORD ALERTS AND STRONG PASSWORDS

Password monitoring and generator

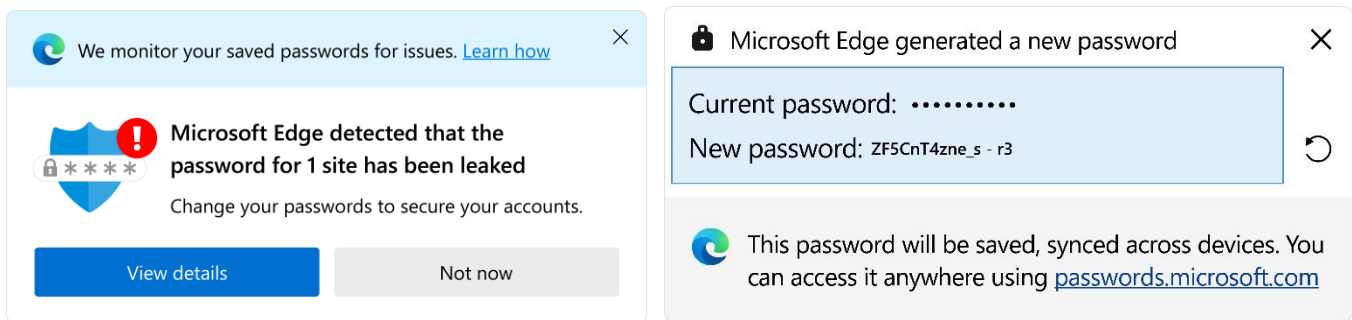
Microsoft Edge for Business stores passwords encrypted on disk. They're encrypted using AES256 and the encryption key is saved in an operating system (OS) storage area using Chromium's OSCrypt. The cryptographic primitive used is [homomorphic encryption](#), which allows computing on encrypted data without decrypting the data first. Password Monitor helps users protect their online accounts by informing them if any of their passwords have been found in an online leak.



This feature is controlled via the [PasswordMonitorAllowed](#) group policy. After the policy is enabled, users will be notified if any of their saved passwords have been compromised due to a breach in third-party apps or websites. If the feature is configured as strictly enabled or disabled using group policy, users can't override this setting. If the feature is set as recommended enabled, the user interface in Settings remains in the 'Off' state. However, a briefcase icon is displayed adjacent to it. When hovered over, it shows the message - "Your organization suggests a particular value for this setting and you have selected a different value". Users have the option to activate this through a consent pop-up or directly from Wallet settings > Passwords.

How it works:

When [Password Monitor](#) is turned on for the first time, all saved passwords will be scanned to see if any have been compromised. If any of the passwords match those in the list of known leaked passwords, a notification is sent to the user.

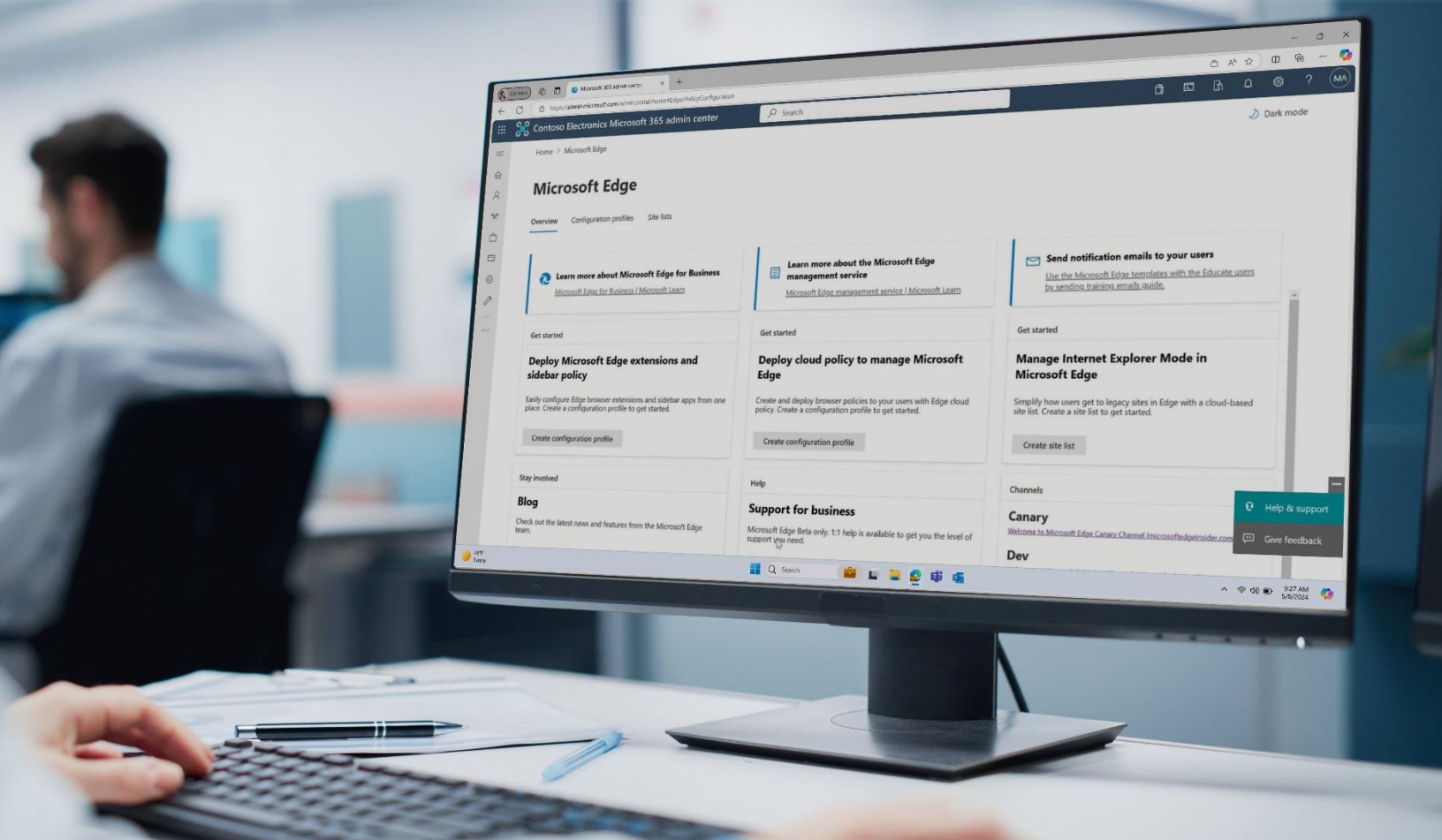


This notification appears only once each time a new password is found to be unsafe. A user can select "View details" to see more information or "Not now" to dismiss this notification. If dismissed, there is a small badge visible in the "Settings and more" menu to access it again. At any point, if a user wants to have a new password created for them, they can do so with the [Password Generator](#) feature. This will generate a highly-secure password for the desired website and save it in Edge for the user.

DEDICATED AND GUIDED MANAGEMENT EXPERIENCE

Microsoft Edge management service

To configure your secure enterprise browser, you need a robust management solution. If you're a pro at policy management or are an enterprise customer, you likely use Microsoft Intune to configure policies, and you can manage Edge for Business there, too. For browser specialists, small or medium sized businesses, or those that want a guided experience, we recommend the [Edge management service in the Microsoft 365 admin center](#). The configurations are stored in the cloud and can be applied to browsers using group assignments or group policies. A configuration profile contains all the browser policy configurations, including extension settings. Each configuration profile can be assigned to multiple Microsoft Entra groups, and a group can be assigned to multiple configuration profiles. When a group is assigned to multiple configuration profiles, the settings will merge if there are no conflicting settings. If a user is a member of multiple Microsoft Entra groups with conflicting policy settings, then the profile priority is used to determine which policy setting is applied.



How it works:

Once a configuration profile is created and applied, the Click-to-Run service used by Edge management service checks with Cloud Policy regularly to see if there are any configuration profiles that pertain to the user. If there are, then the appropriate policy settings are applied and take effect the next time the user opens Edge.

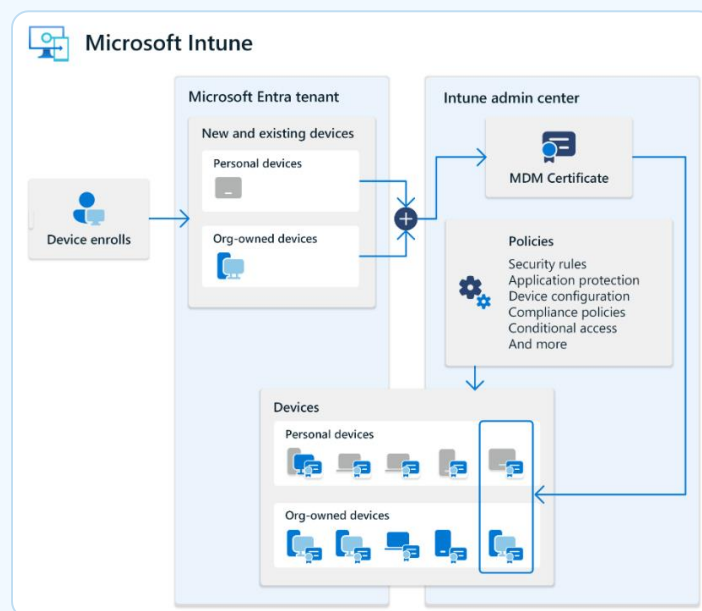
- When a user signs into Microsoft Edge on a device for the first time, a check is immediately made to see if there's a configuration profile that pertains to the user.
- If the user is not a member of a Microsoft Entra group that's assigned a configuration profile, then another check is made again in 24 hours.
- If the user is a member of a Microsoft Entra group that's assigned a configuration profile, then the appropriate policy settings are applied. A check is made again in 90 minutes.
- If there are any changes to the configuration profile since the last check, then the appropriate policy settings are applied, and another check is made again in 90 minutes.
- If there are not any changes to the configuration profile since the last check, another check is made again in 24 hours.
- If there's an error, a check is made when the user next opens Microsoft Edge.
- If Edge is not running when the next check is scheduled, then the check will be made the next time the user opens Microsoft Edge.

MANAGED BROWSER ON PERSONAL AND BYOD DEVICES

Microsoft Intune Mobile Application Management

Mobile Application Management (MAM) enables admins to publish, push, configure, secure, monitor, and update mobile apps for users on managed or unmanaged devices, such as a personal or bring your own devices (BYOD). MAM protects an organization's data within an application by using Intune app protection policies that help secure data and prevent data loss. Intune app protection policies can be used independent of any mobile-device management (MDM) solution to help secure organization data with or without enrolling devices in a device management solution. By implementing these account-level policies, access to company resources is restricted and data is kept within the purview of admins. MAM is supported in Microsoft Edge for Business on unmanaged Windows devices and Edge for mobile. This capability uses the following functionality:

- [Intune Application Configuration Policies \(ACP\)](#) to customize the org user experience in Microsoft Edge.
- [Intune Application Protection Policies \(APP\)](#) to secure org data and ensure the client device is healthy when using Microsoft Edge.
- Windows Security Center threat defense integrated with Intune APP to detect local health threats on personal Windows devices.
- Application Protection Conditional Access to ensure the device is protected and healthy before granting protected service access via Entra ID (AAD).



SECURE ACCESS ON MOBILE

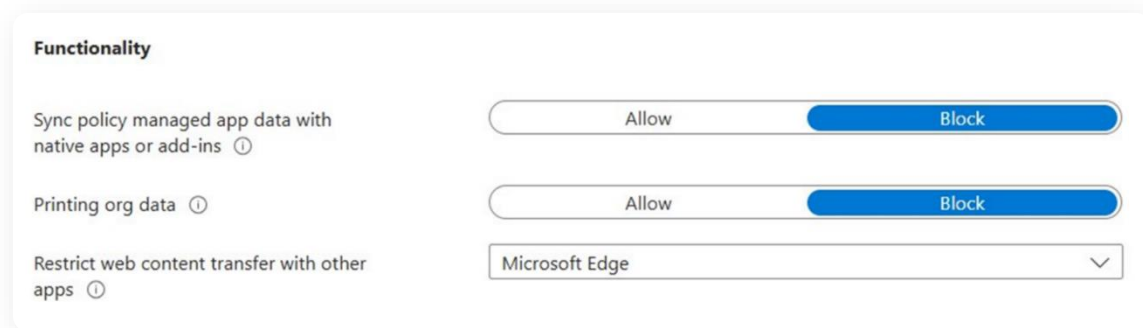
Microsoft Edge for Mobile

As flexible working environments become the norm, using devices beyond desktops and laptops for email and chat increases the risk of data exposure and compromise. Microsoft Edge for mobile protects company data in a few ways:

With [Conditional Access](#) policies, data is available only to those designated to see it. Configuration includes a policy admins can set that requires an approved client app or an app protection policy when using iOS/iPadOS or Android devices.

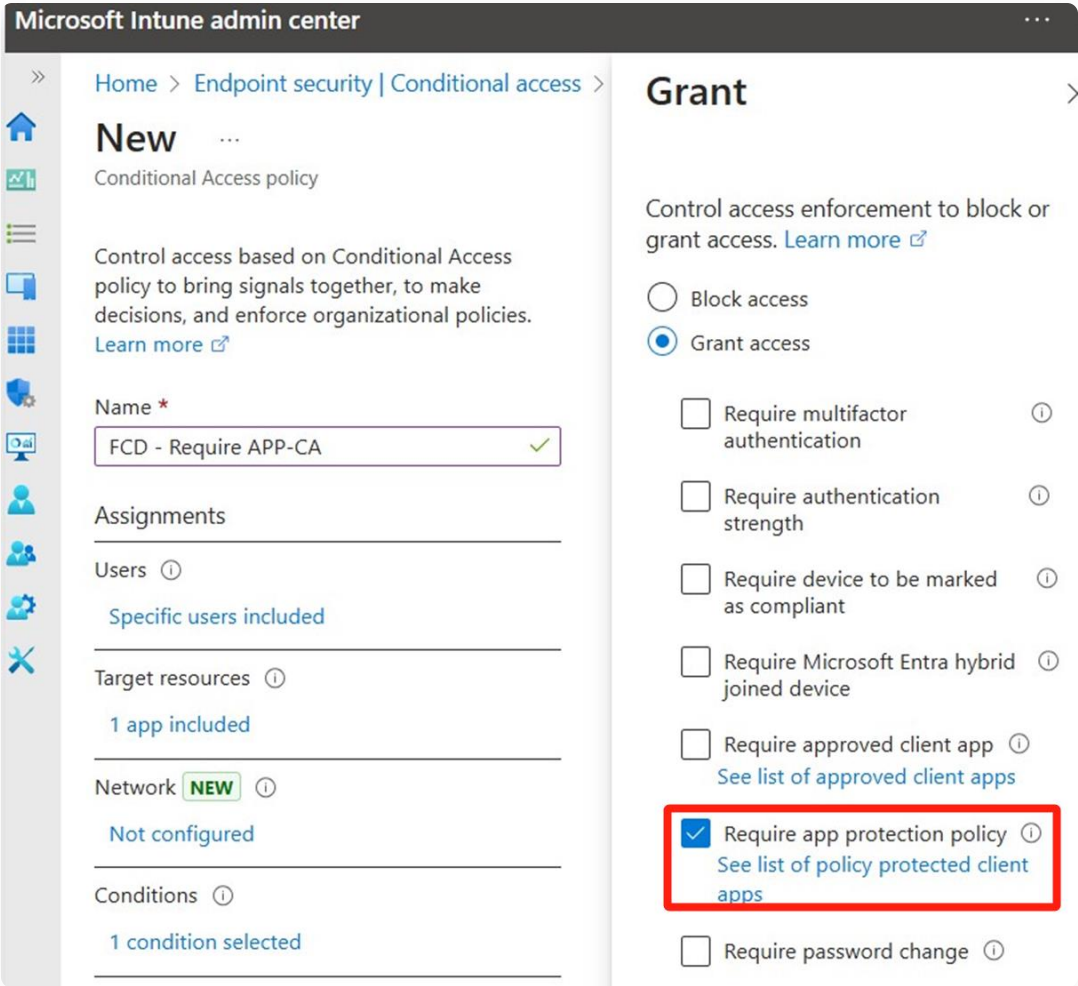
Edge for mobile supports [Microsoft Defender SmartScreen](#) to protect against potentially suspicious websites.

With support for Microsoft Intune [Application Protection Policies](#) (APP) IT admins can implement controls akin to DLP for specific applications at various levels. Level 1 provides the minimum level of data protection to enforce reasonable data access, while minimizing user impact on application usage. Level 3 is the highest level of protection, and the recommended standard for organizations with sophisticated security architectures. This APP configuration includes all settings from levels 1 and 2 and adds more security such as more stringent mobile device unlock settings and blocking devices entirely if they are rooted or jailbroken. Additional configurations include the ability to restrict web content transfer with other apps, preventing unauthorized sharing of web content between Microsoft Edge and other applications.



Furthermore, using Edge for mobile enhances security for admins who are already configuring Intune for other Microsoft apps like Outlook and Teams. This setup ensures that links opened in these apps default to Edge for mobile. With support for [Microsoft Entra application proxy](#), the configuration to URL mapping can be specified by IT admins. This is recognized by Edge for mobile to facilitate the access from the mobile browser to corporate IT infrastructure. By turning on the support in Intune MAM policy, access from a users' Edge for mobile instance will be automatically translated into the designated public URLs to have an access funnel through the enforced endpoints and routed to the correct web resource inside the internal network.

With [Microsoft Tunnel](#), users can seamlessly access resources deployed behind the network perimeter without manually establishing a VPN connection first.



CONCLUSION

As threat actors gain more skill and knowledge, IT and cybersecurity professionals face the challenge of keeping systems and people current on the latest threats. With the reasonable assumption that the upward trend in attacks and complexity will continue in the future, there's never been a more important time for organizations to reassess the role and importance of internet browsers in keeping organizations and users secure.

Edge for Business was designed from the ground up as a secure enterprise browser optimized for AI, with industry-leading, native security and data protection capabilities from Microsoft built on top of its Chromium base. It defends against the spectrum of modern threats, from unauthorized data access to phishing and malware compromise. Microsoft Edge for Business is a holistic solution that delivers added protection to your organization's users and assets, no matter where or what they are, without sacrificing productivity and familiarity.

Get started today by [learning more about managing Edge for Business](#).

Get the latest on Microsoft Edge for Business:

- Read our [blogs](#)
- Follow [@MSEdgeDev](#) on X (formerly Twitter)
- Check out the [Microsoft Edge release notes](#)
- Follow the [Microsoft 365 Roadmap](#)
- Check out the [Microsoft Edge for Business security features license matrix](#)

