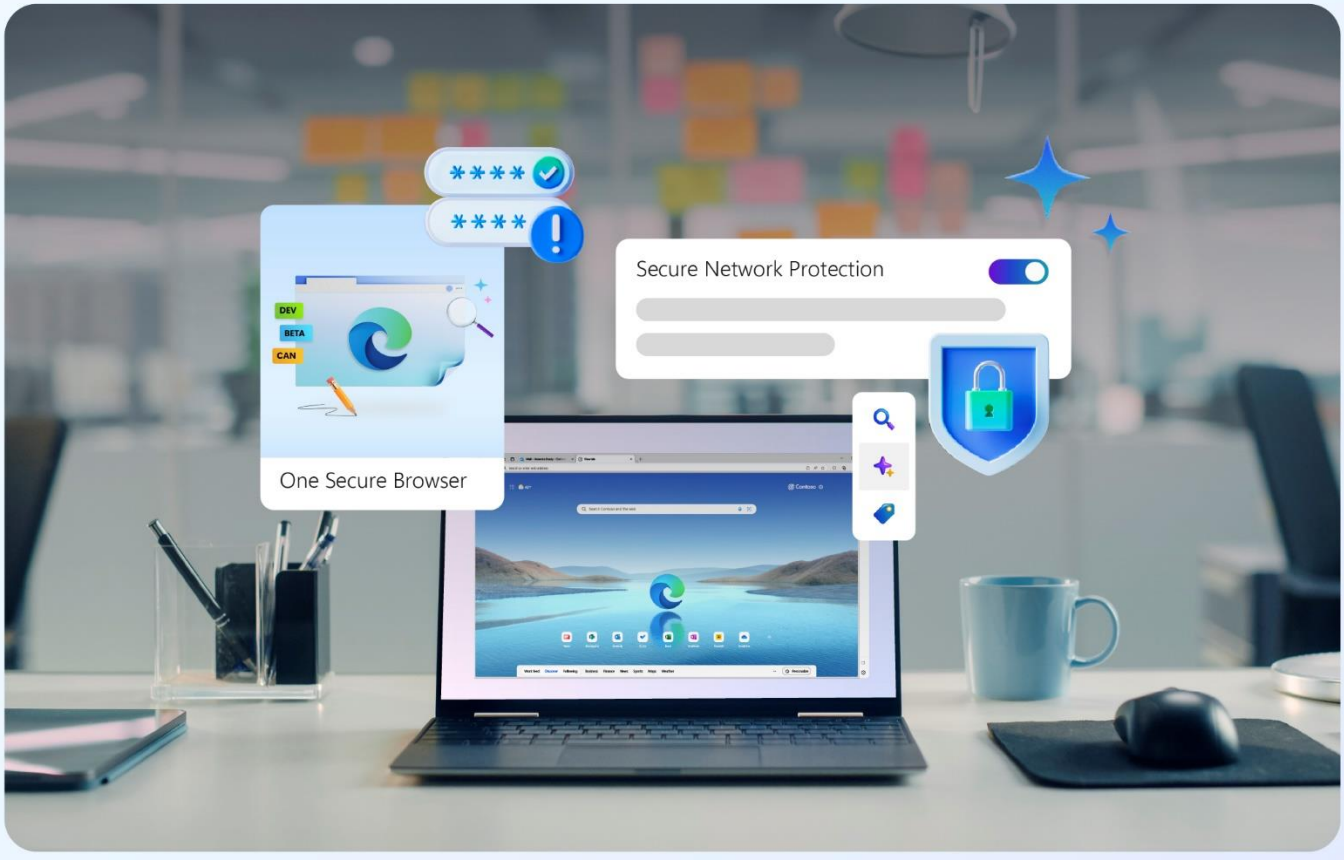
Microsoft Edge

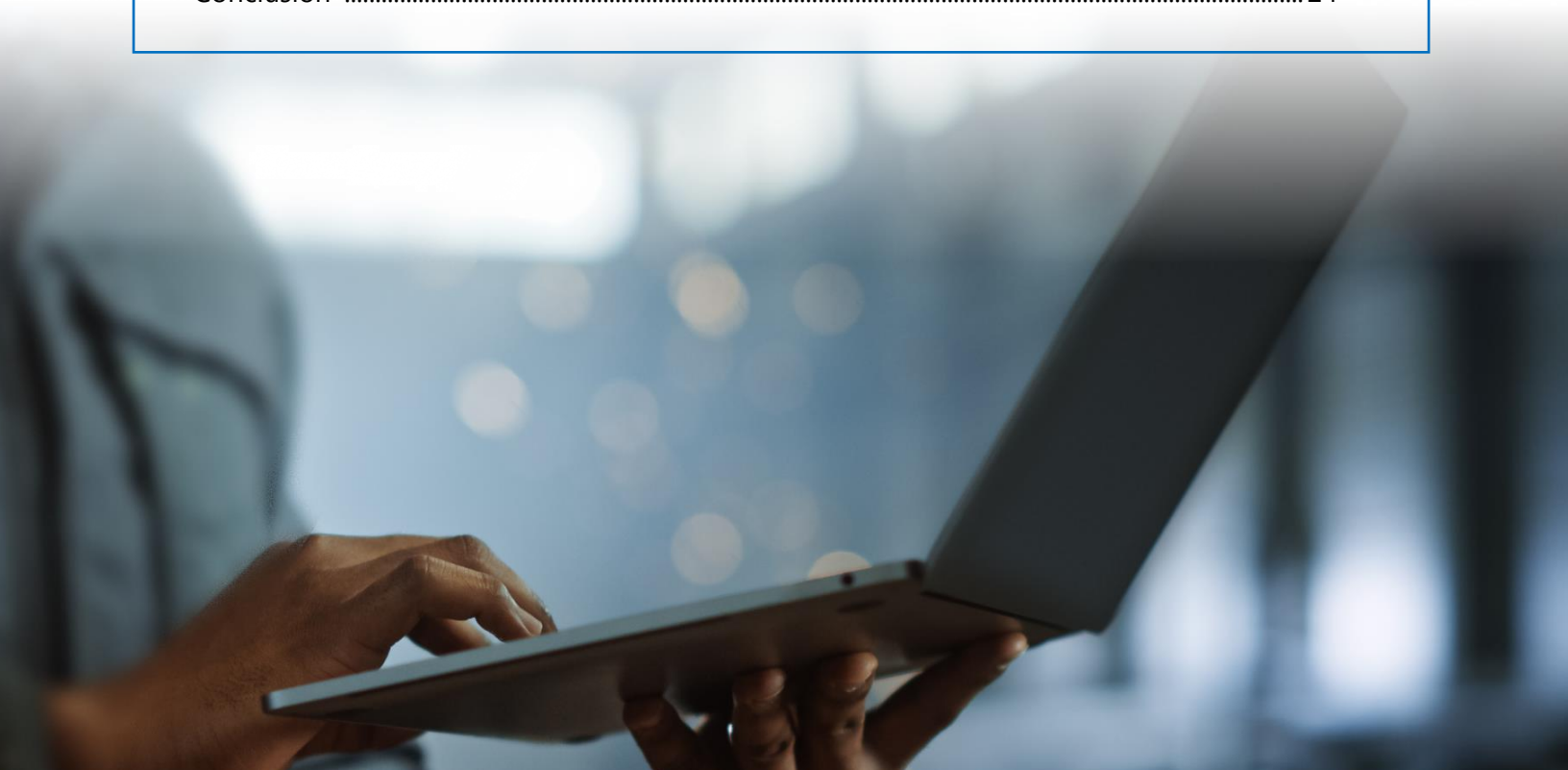
Microsoft Edge for Business: AI and protection in one secure enterprise browser

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



V 2.0

TABLE OF CONTENTS



INTRODUCTION

As the digital landscape continues to grow and transform at a fantastic rate, so does the increase in threat vectors and risk factors. Coupled with the hybrid and remote working world of today, 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 follow the Zero Trust security model. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network.

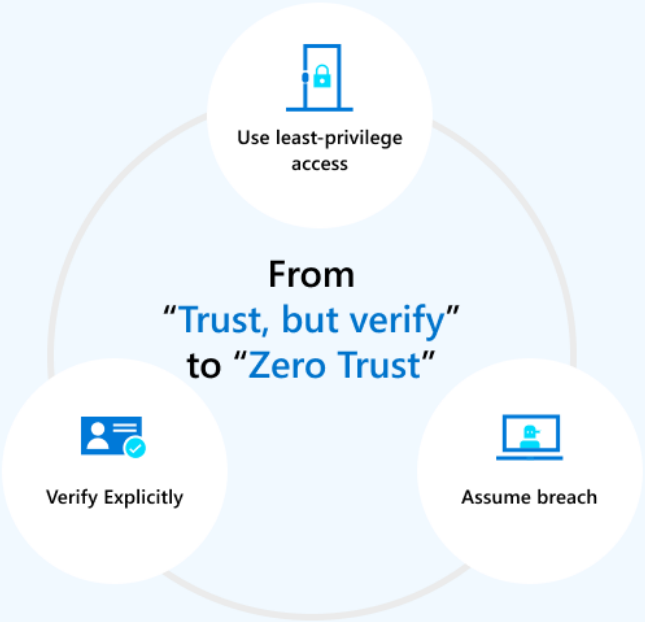
When organizations seek to adopt this model and implement tools and policies around it, one area that is often lower on the list of strategic priorities is the internet browser. However, with users spending over 55 percent of their time in the browser accessing trusted or untrusted content and 38% more cyber-attacks each week on corporate networks[1], it is an important asset to all security models and solution implementations. Additionally, it is a familiar outlet for end users to understand how their activity is protected when they face difficulty comprehending the larger security strategy and range of tools their organizations employ. 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 where applicable in their roles. As such, a secure enterprise browser is a must-have for any organization.

Microsoft Edge for Business is a secure enterprise browser due to its secure by default design and capabilities for protection. In addition to built-in security features to bolster defenses, it natively supports security features employed by other Microsoft technologies across Microsoft 365, Windows, and other Microsoft products. Edge for Business reduces the need for extensions, eliminating unnecessary management and saving IT administrators time for other tasks. With Edge for Business, organizations get a secure enterprise browser that brings added protection to their users and assets, no matter where their users are.

1. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Blog

ZERO TRUST CHANGES THE SECURITY GAME

The Zero Trust methodology aims to bring a new way of thinking to how an organization should approach security, and is increasingly becoming the standard for security strategy. 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. 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.

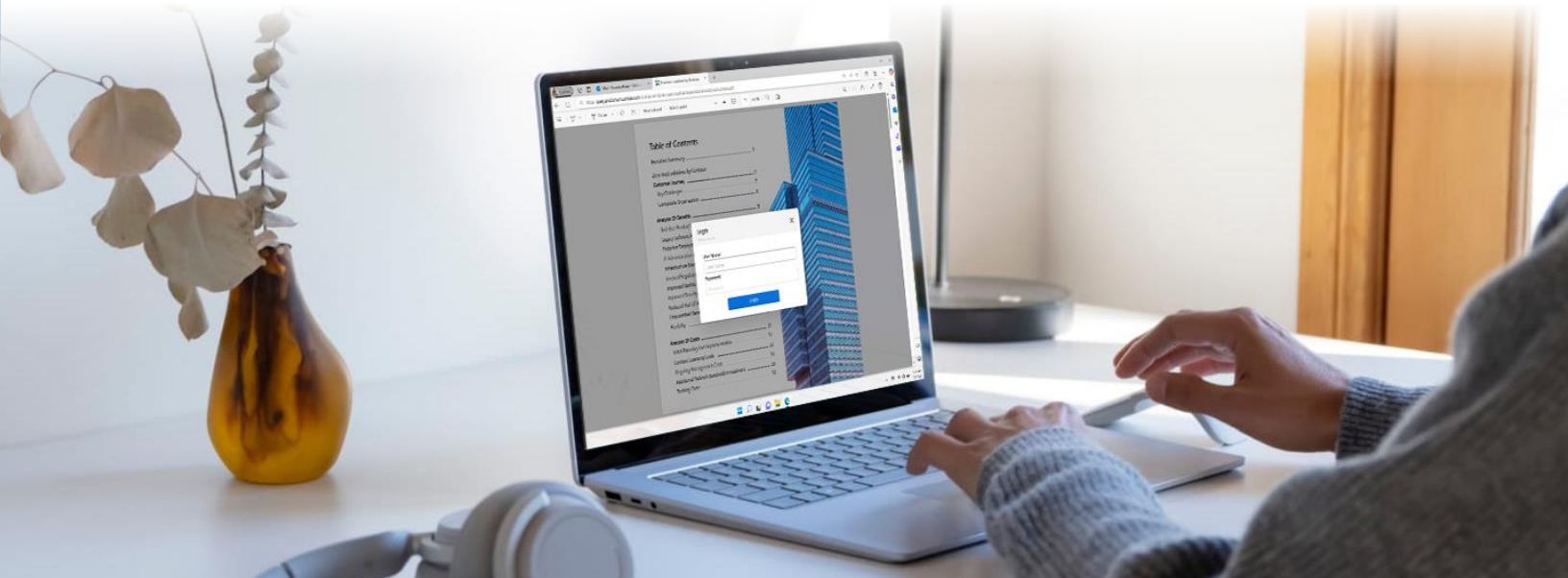
Assume breach – minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

MICROSOFT EDGE FOR BUSINESS COMPLEMENTS ZERO TRUST

Microsoft Edge for Business is 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. Additionally, Edge is built with its own unique protection features on top of Chromium and supports Microsoft Security solutions from Microsoft Defender, Microsoft Entra (formerly known as Azure Active Directory), and Microsoft Purview. Currently, Microsoft Edge for Business offers the following features that support the Zero Trust methodology:

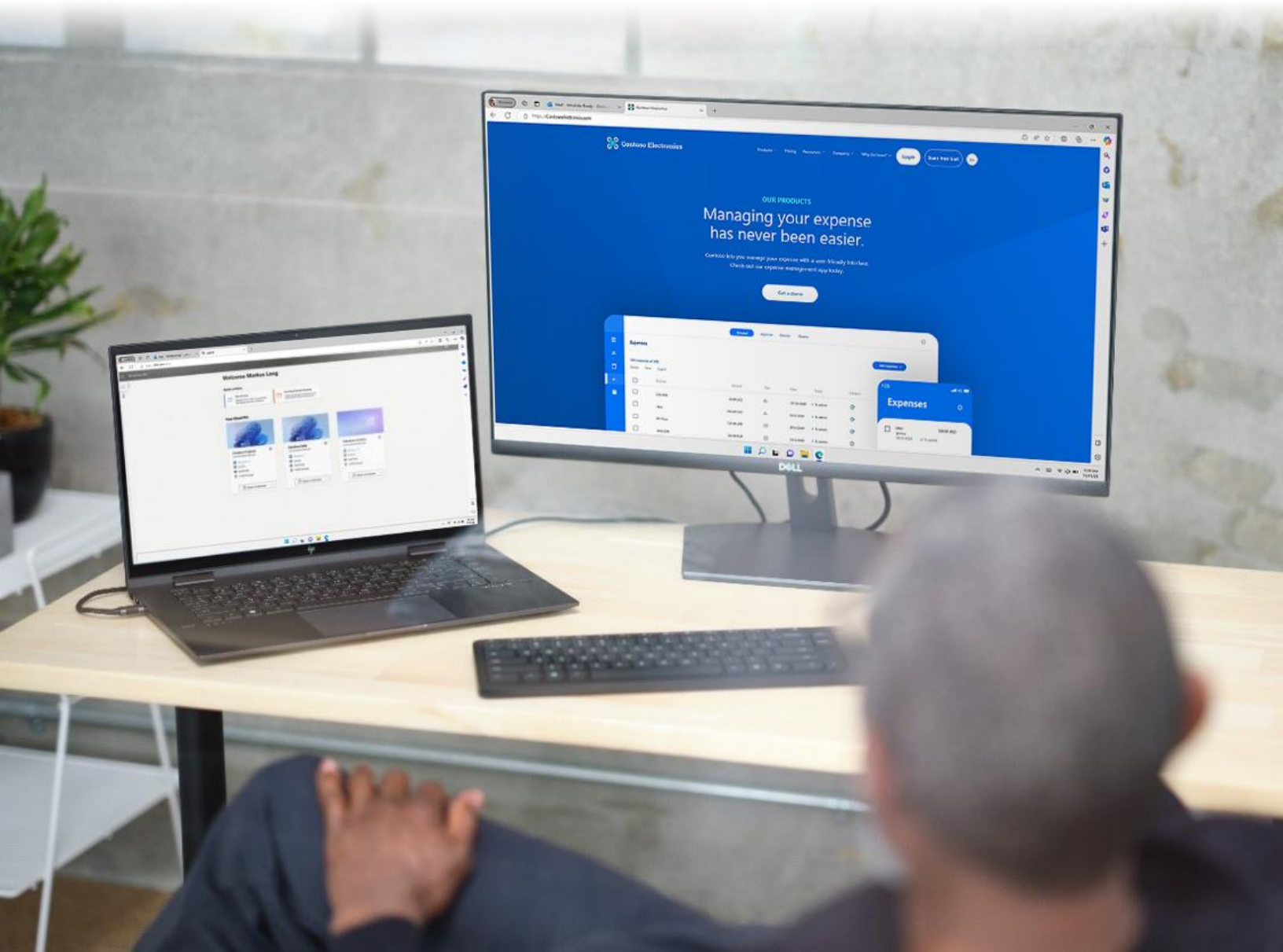
- Microsoft Purview Data Loss Prevention (DLP)*
- Microsoft Defender SmartScreen*
- Enhanced security mode (ESM)
- Website typo protection
- Native support for Microsoft Entra Conditional Access*
- Password Monitoring and Generator
- Microsoft Edge management service (EMS)
- Unmanaged device support with Microsoft Intune Mobile Application Management (MAM)*

*Requires separate licensing



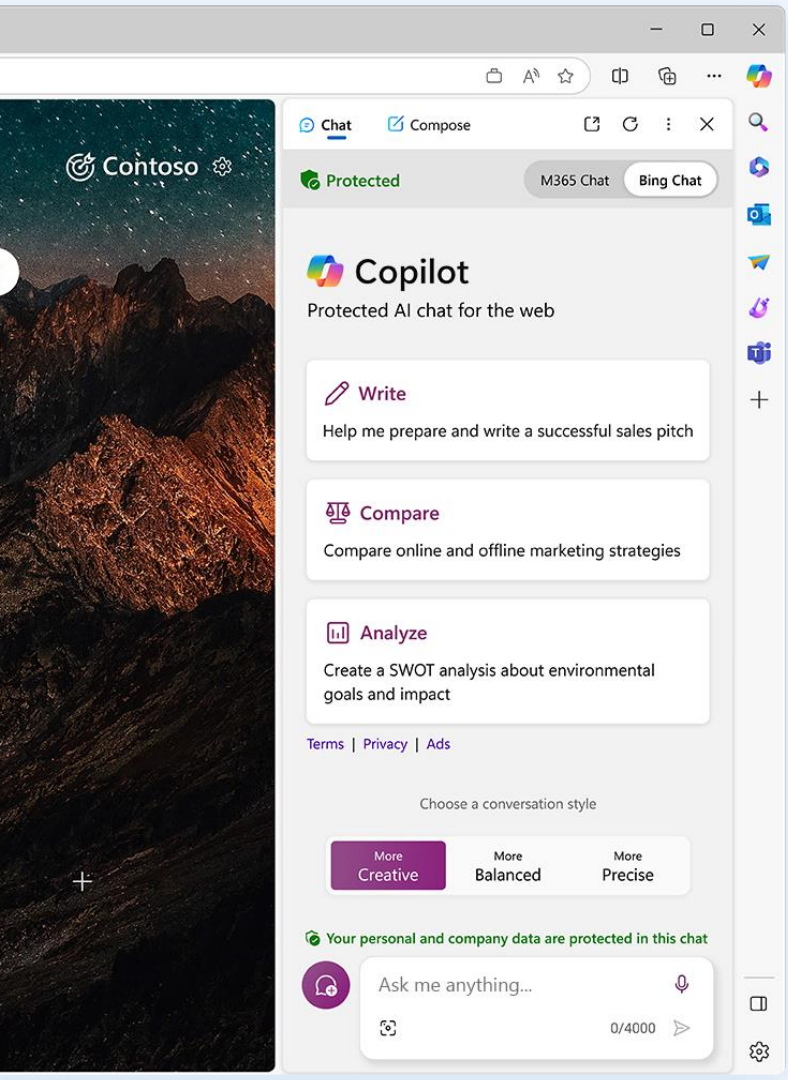
Our goal is for Edge for Business to provide the most secure experience for end users across all browsers. With no extensions to manage for these protections, IT admins can maintain their environments more easily. There are less concerns of a performance hit and less attack vectors that could potentially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



COPILOT

Employees are looking to use AI tools to help them unlock creativity and productivity at work—in fact, among technical professionals and business decision makers that we surveyed, 92% of them say that they have used or tried an AI tool or service already[2]. 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.

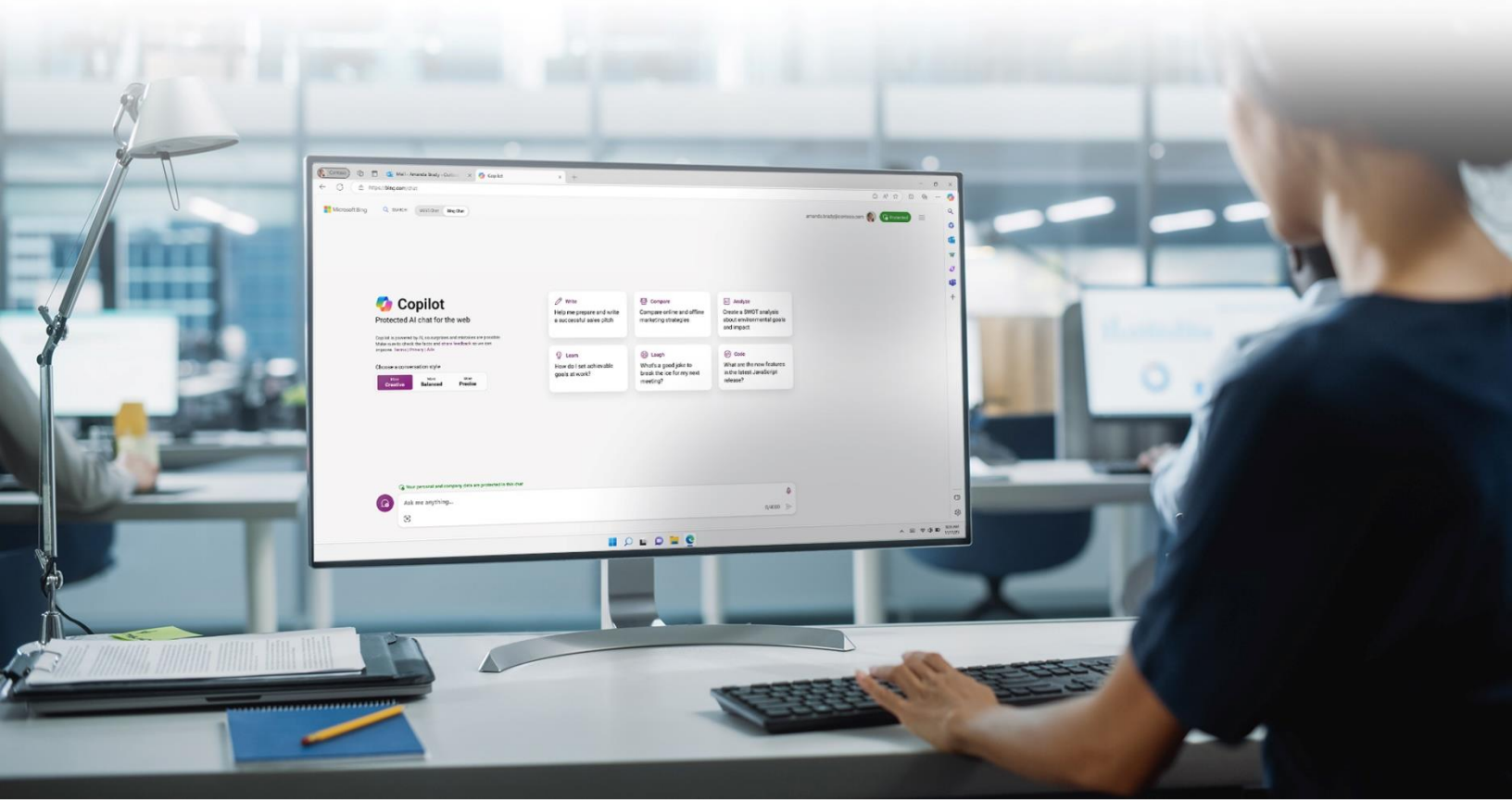


The good news is that it's possible to move forward with AI and protect your confidential data. Copilot is an AI-optimized chat experience for the web with commercial data protection. It is a generative AI service grounded in public web data in the Bing search index. User and business data are protected and will not leak outside the organization. What goes in—and comes out—remains protected. Chat data is not saved, and Microsoft has no eyes-on access, which means your data is not used to train the AI models. It does not have access to organizational resources or content within Microsoft 365, such as documents in OneDrive, emails, or other data in the Microsoft 365 Graph.

Whether you are a multinational enterprise or a startup with new IP, Copilot is a great first step to get your organization into AI. Copilot makes use of GPT-4 for text and DALL-E 3 for images and is transparent with users on its sources of data, providing citations that users can examine. In addition, Copilot can answer questions with up-to-date information, as there is no knowledge cut off limitations by the AI model. This AI-powered web chat with commercial data protection is available at no additional cost to customers with the appropriate license[3].

2. "*State of AI,*" Microsoft Tracking Study, June 2023
3. Check for the latest information on license eligibility

Users can safely create content, images, and ask the internet for answers to complex questions at Bing.com/chat, when they are logged in with their work accounts. When accessed through Copilot in Microsoft Edge, users can tap into capabilities unique to Edge. Copilot in the Edge sidebar lets you view and summarize whole webpages, documents, and PDFs, eliminating the difficulties of copy-and-pasting large sections of documents into the chat input box. Copilot in Edge also makes it easy to create



When a user is signed into Microsoft Edge for Business, they can automatically get the Copilot experience through Copilot in the Edge sidebar, provided the user is on an eligible license. The copilot in the sidebar experience inherits the commercial data protection capability of Copilot and respects the controls of Microsoft Purview Data Loss Prevention. IT Admins and end users also have the ability to control whether Copilot can view webpages or PDFs in Microsoft Edge for Business.

Copilot follows responsible AI principles to help provide a private AI experience that is reliable and trustworthy.

Commercial data protection:

When organizations and employees use generative AI services, it's important to understand how these services handle user and chat data. Because employee chats may contain sensitive data, Copilot has the following measures in place to protect this information:

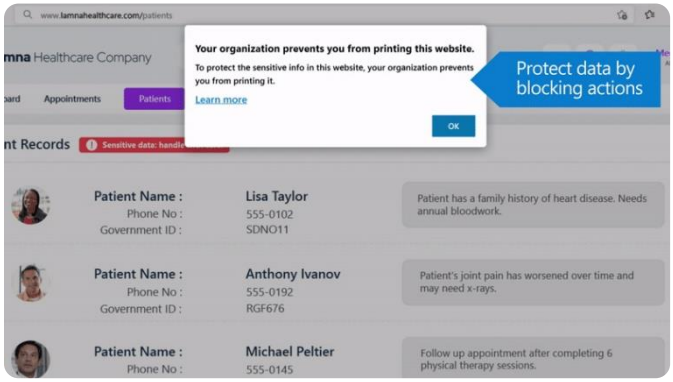
- Copilot uses Microsoft Entra ID (formerly known as Azure Active Directory) for authentication and only allows users to access it with their work account.
- Tenant and user identity information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible to access Copilot. Search queries triggered by prompts are not linked to users or organizations by Bing.
- Microsoft does not retain prompts or responses from users in Copilot. Prompts and responses are maintained for a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards all prompts and responses.
- Chat data sent to and from Copilot is encrypted in transit and at rest (during the chat session). Microsoft has no 'eyes-on' access to it.
- Because Microsoft does not retain prompts and responses, they cannot be used as part of a training set for the underlying large language model.
- These data protections extend to Copilot in Edge and Copilot in Windows when Copilot is enabled.

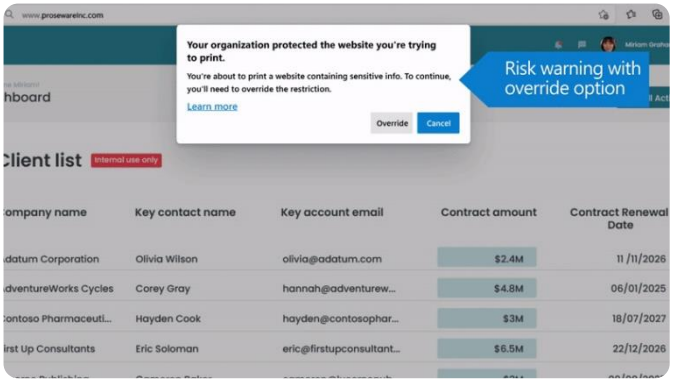
MICROSOFT PURVIEW DATA LOSS PREVENTION

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 a website 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.

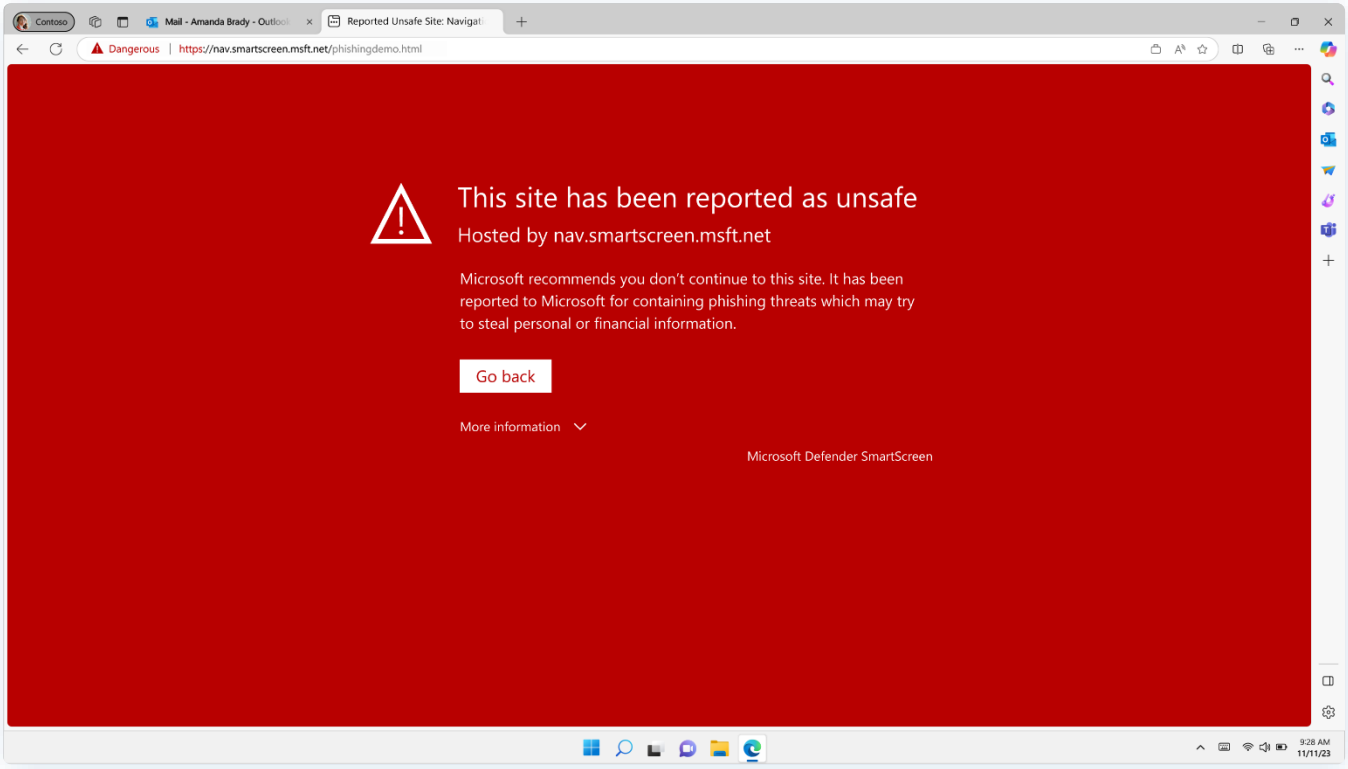




MICROSOFT DEFENDER SMARTSCREEN

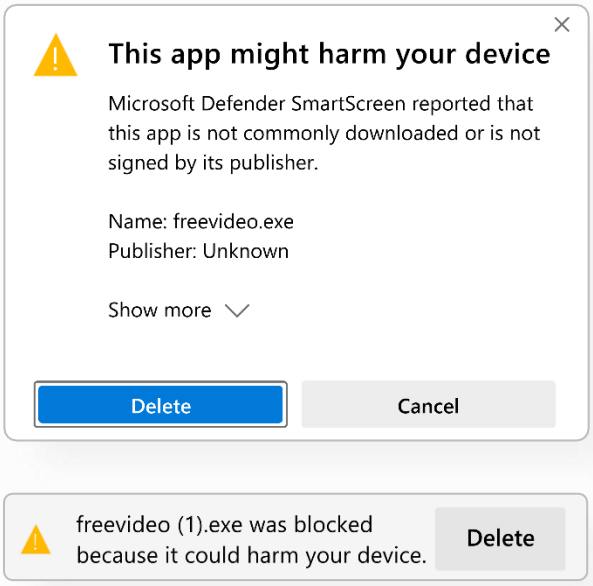
Microsoft Defender SmartScreen is a service that helps keep users safe while browsing the web. SmartScreen does a real-time reputation check of websites and downloads and is part of the Microsoft Intelligent Security Graph, which draws signals and insights generated from Microsoft's large network of 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.

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.

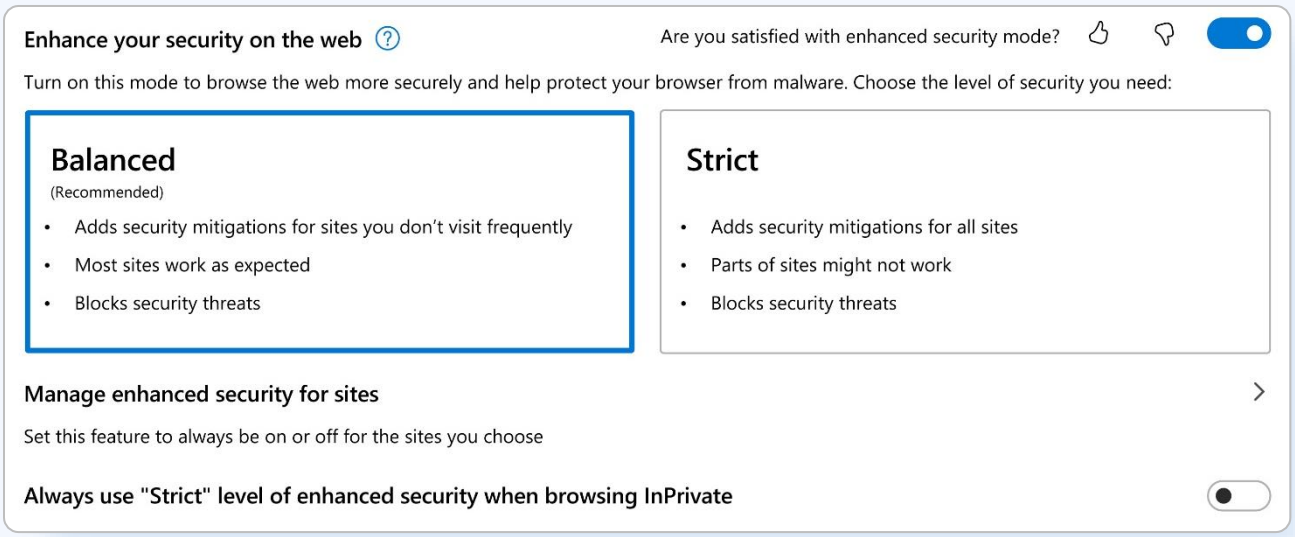
Shadow stack is a hardware-enforced read-only memory region that can be activated to help keep record of the intended control-flow of the program. Call instructions will push the return address on both stacks and return instructions will compare the values and issue a CPU exception if there is a return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



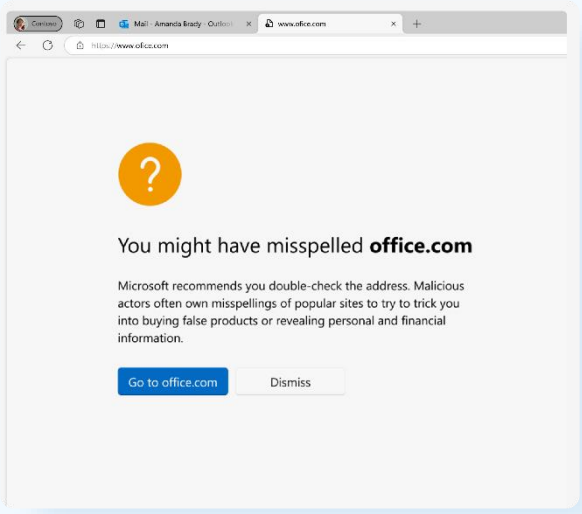
In both modes, exceptions can be created for users' trusted websites. IT admins can configure this security feature using Group Policy settings, including creating "*Allow*" and "*Deny*" lists to explicitly enhance security for their users when visiting certain sites, or disable the mode for other users.

WEBSITE TYPO PROTECTION

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. Between 2020 to 2022, typosquatting attacks grew 29%, from 4,204 to 5,423[4]. With this growing threat, website typo protection brings a piece of mind to users and IT in case of accidental typos.

How it works:

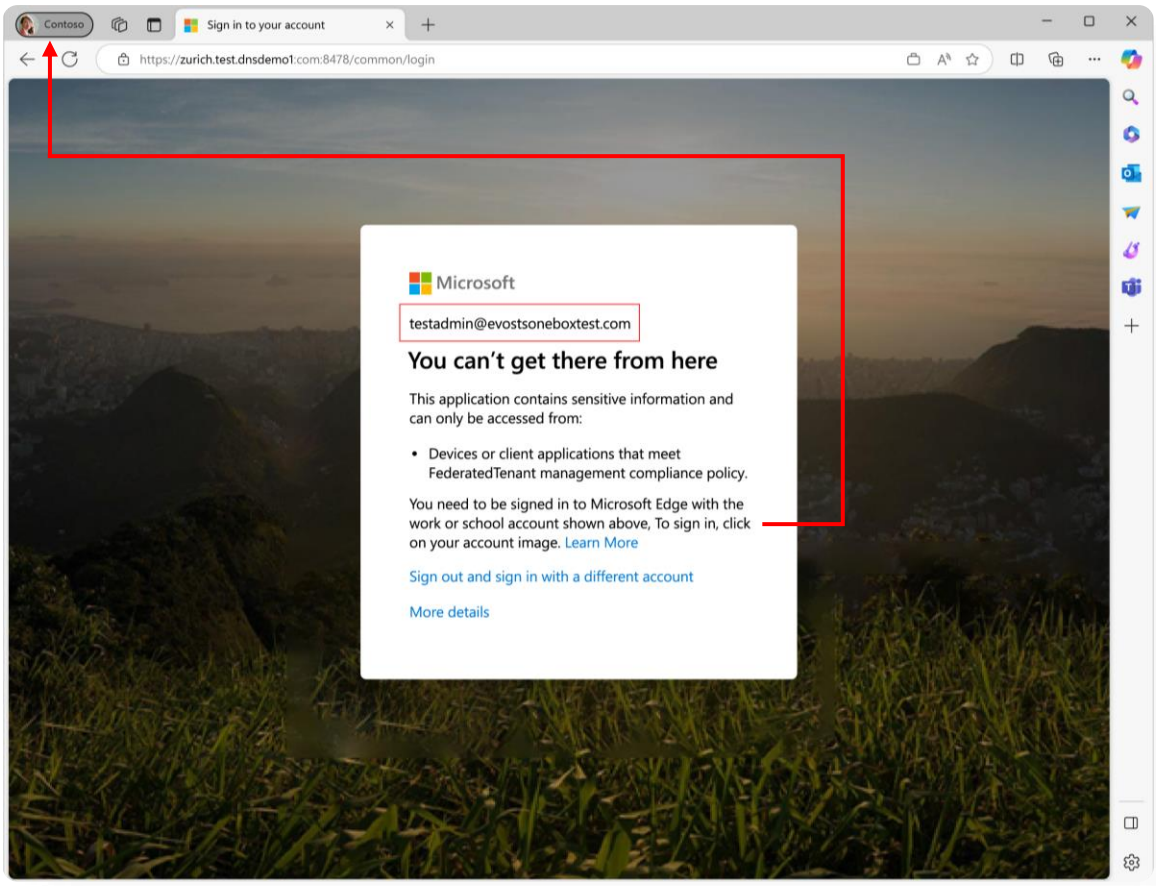
This can be configured via policy or in Edge settings. Once configured, users are given an interstitial warning page suggesting that the site might have been misspelled. A corrected URL is suggested when a potentially compromised misspelled site is identified (for example, a SaaS URL). Users are required to confirm before continuing to the website as typed.



4. Cybersquatting: most domain name dispute filings 2022 | Statista

MICROSOFT ENTRA CONDITIONAL ACCESS

Microsoft Edge for Business natively supports Microsoft Entra Conditional Access (formerly known as Azure Active Directory (Azure AD) Conditional Access). When signed into a Microsoft Edge profile with Microsoft Entra ID credentials, Edge for Business allows seamless access to enterprise cloud resources protected using Conditional Access on managed and unmanaged devices.

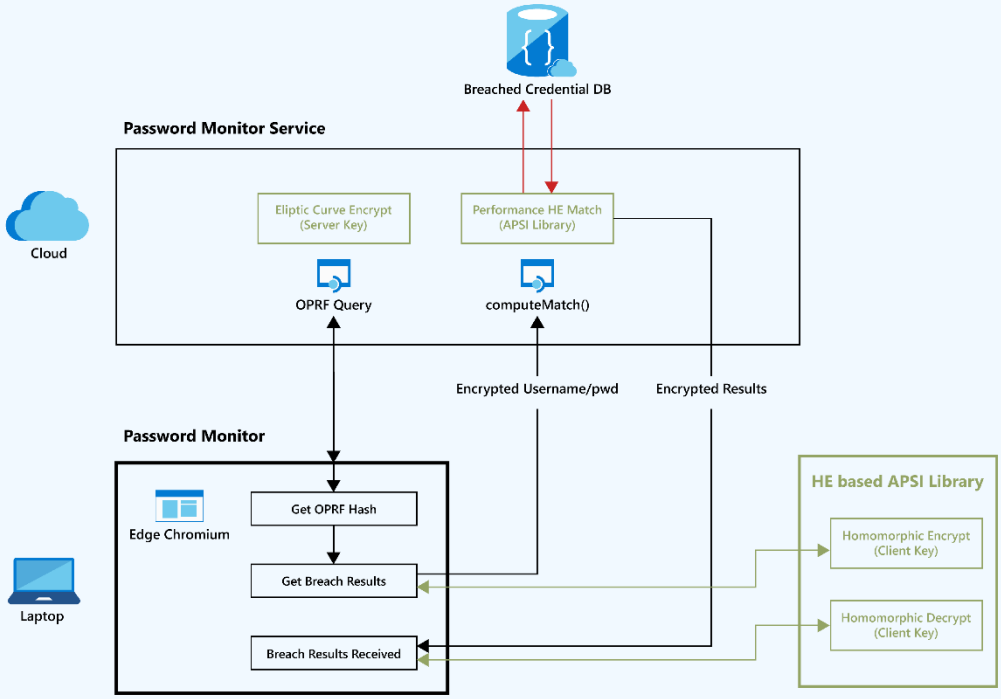


How it works:

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 MONITORING AND GENERATOR

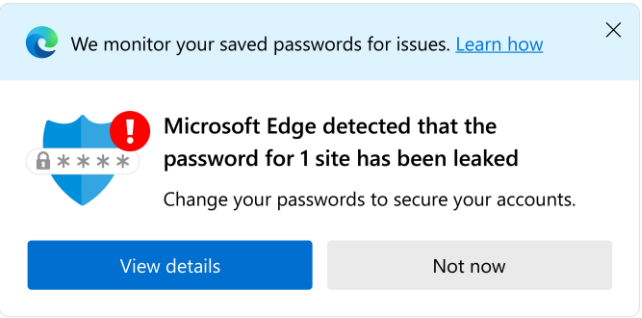
Microsoft Edge for Business stores passwords encrypted on disk. They're encrypted using AES256 and the encryption key is saved in an operating system (OS) storage area using Chromium's OSCrypt. The cryptographic primitive used is homomorphic encryption, which allows computing on encrypted data without 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.

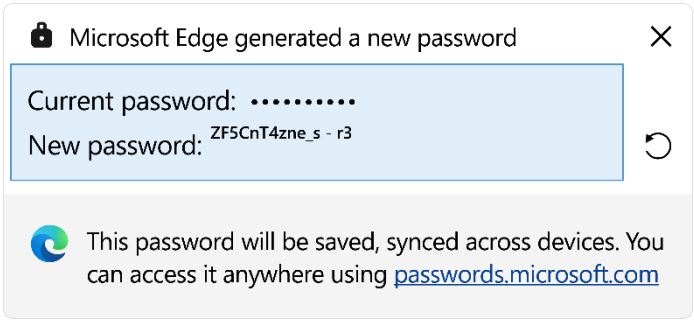


This feature is controlled via the PasswordMonitorAllowed group policy. After the policy is enabled, users still need to provide consent to turn on the feature either by giving explicit consent or acknowledgment of the auto-enabled policy when signed into their work account. Consent is required because the feature contains sensitive and personal data (passwords). If the feature is disabled using group policy, users cannot override this setting.

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.

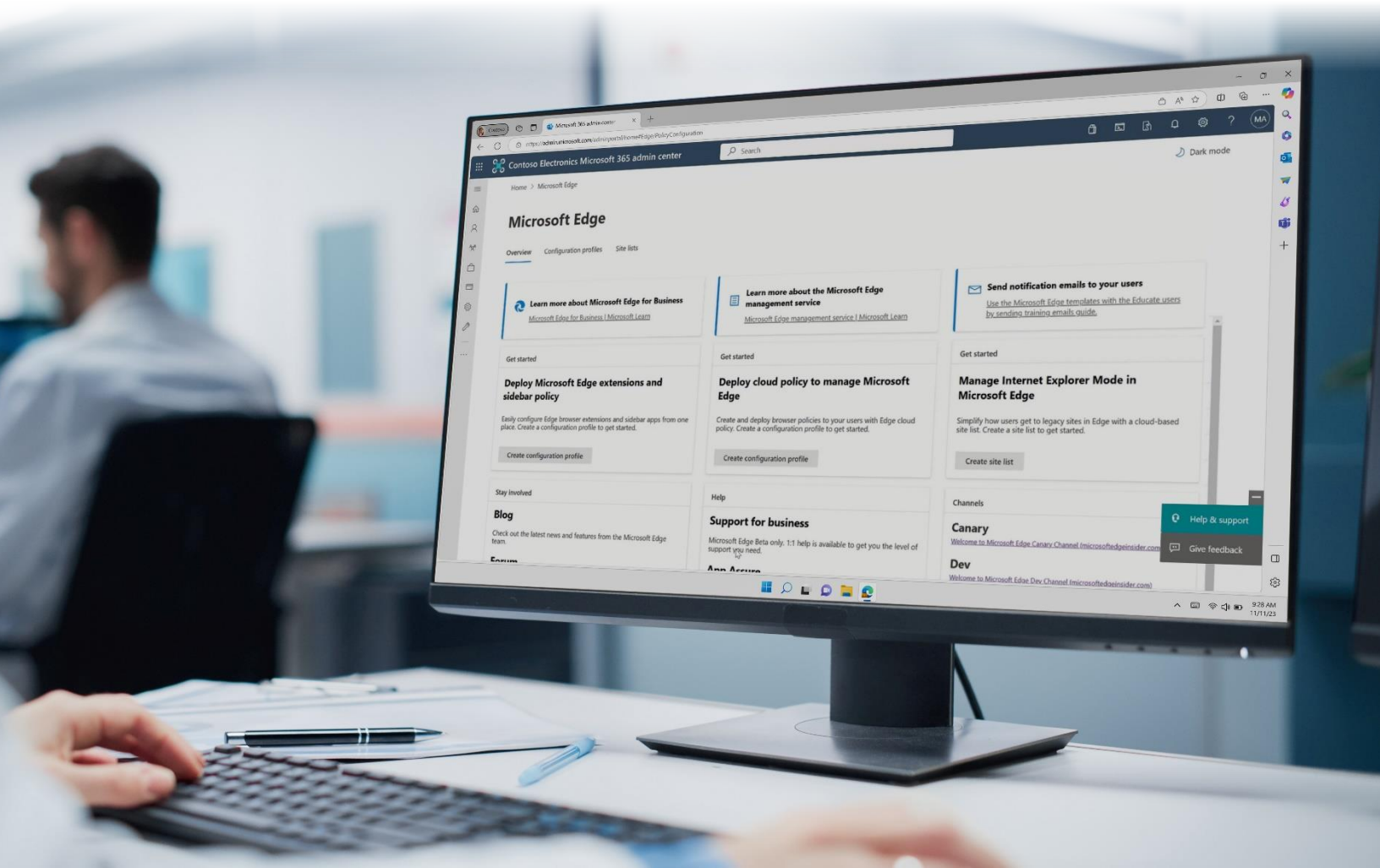




This notification appears only once each time a new password is found to be unsafe. A user can select "*View details*" to see more information or "*Not now*" to dismiss this notification. If dismissed, there is a small badge visible in the "*Settings and more*" menu to access it again. At any point, 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.

MICROSOFT EDGE MANAGEMENT SERVICE

The Microsoft Edge management service in the Microsoft 365 admin center is a tool where admins can configure Edge for Business settings for their organizations with more ease, time savings, and granularity. 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:

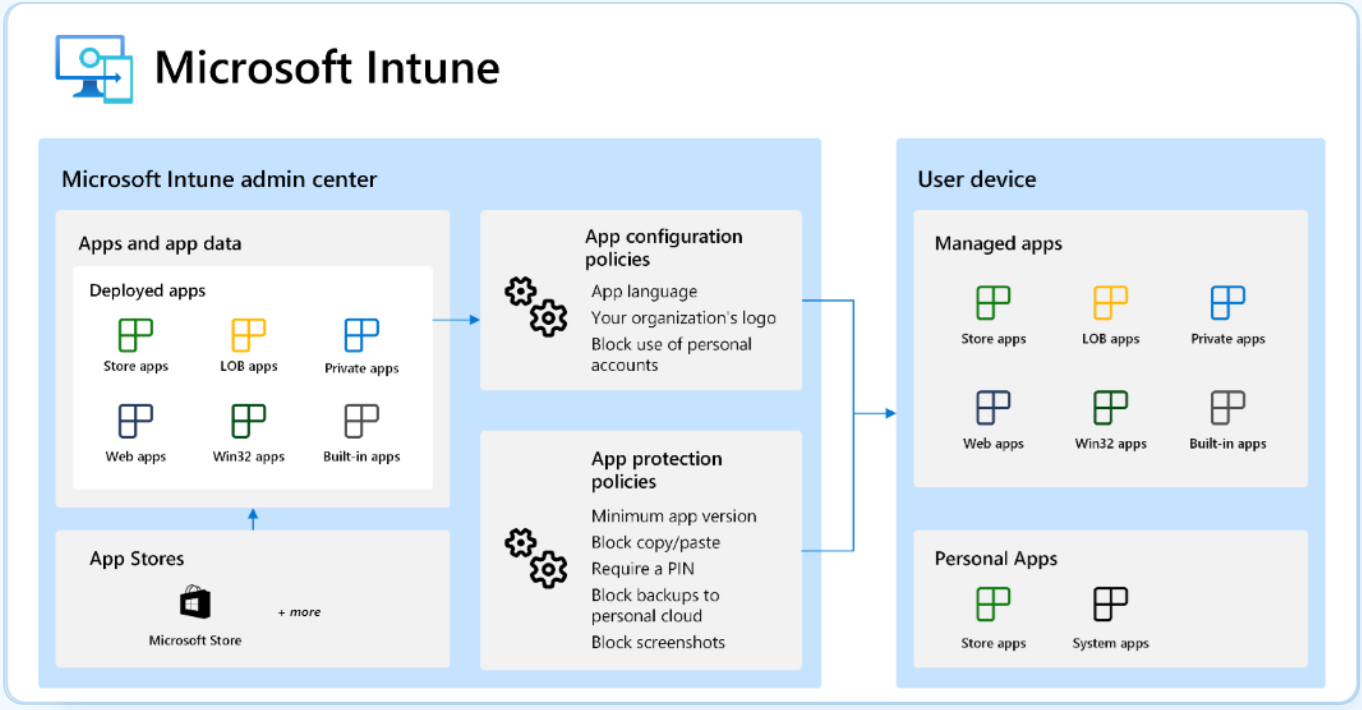
Once a configuration profile is created and applied, the Click-to-Run service used by Edge management service checks with Cloud Policy regularly to see if there are any configuration profiles that pertain to the user. If there are, then the appropriate policy settings are applied and take effect the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

MICROSOFT INTUNE MOBILE APPLICATION MANAGEMENT

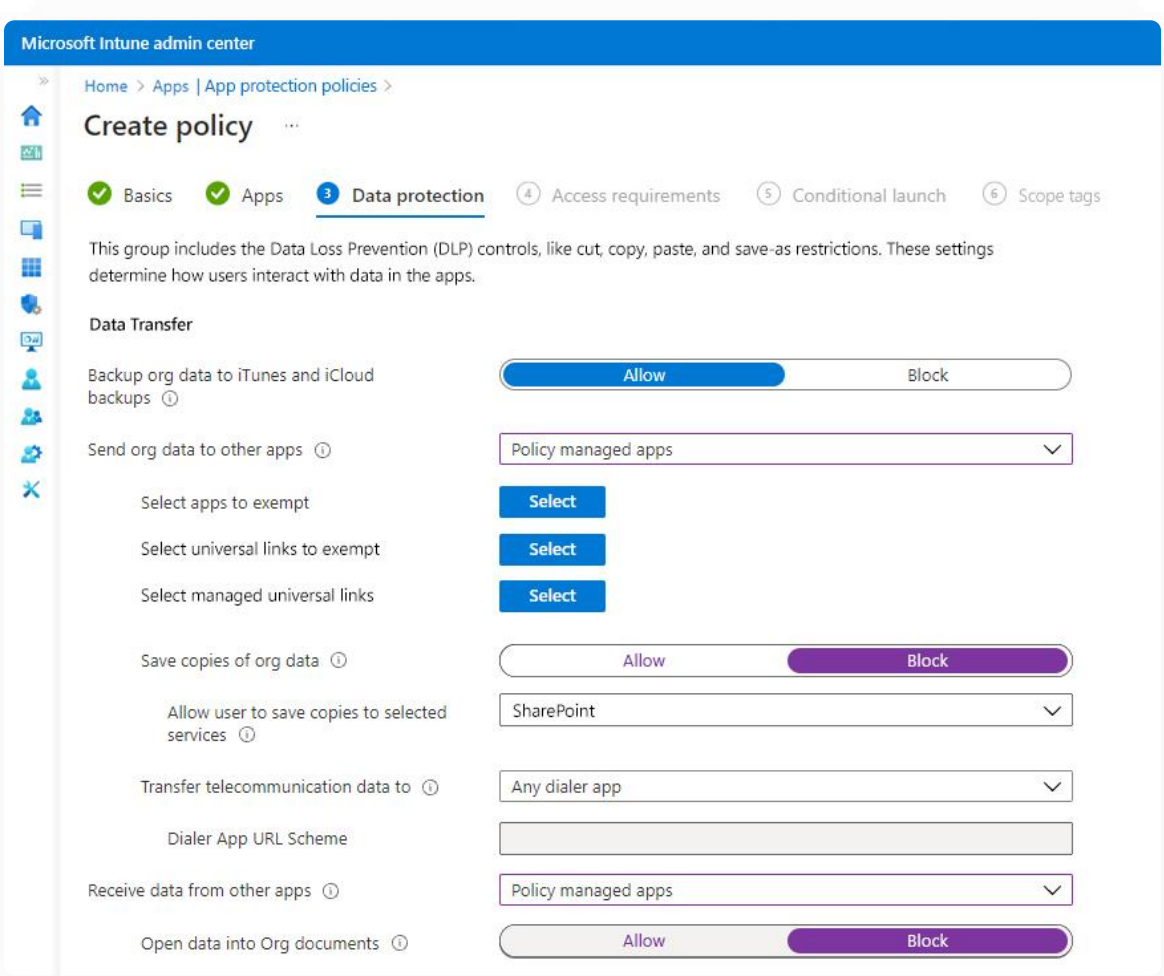
Mobile Application Management (MAM) is a tool that allows application configuration profiles to be deployed on unmanaged and bring your own devices (BYOD). This provides more security for users accessing their data on devices not owned by their organizations. MAM is supported in Microsoft Edge for Business 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).



MICROSOFT EDGE FOR MOBILE

As flexible working environments increasingly become the norm, so does working from devices outside of desktop computers and laptops. Microsoft Edge for mobile protects company data accessed via mobile devices with conditional access policies to make data available only to those designated to see it. Edge for Mobile supports Intune Application Protection Policies (APP). With APP configuration 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.



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, 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.

Learn more about Microsoft Edge for Business today:

- Read our blogs: https://blogs.windows.com/msedgedev/
- Follow us on X (Twitter): @MSEdgeDev
- Check out the release notes: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel