

Edge for Business



Petr Vlk

Microsoft MVP

Microsoft 365 Enterprise Security Architect @ KPCS CZ



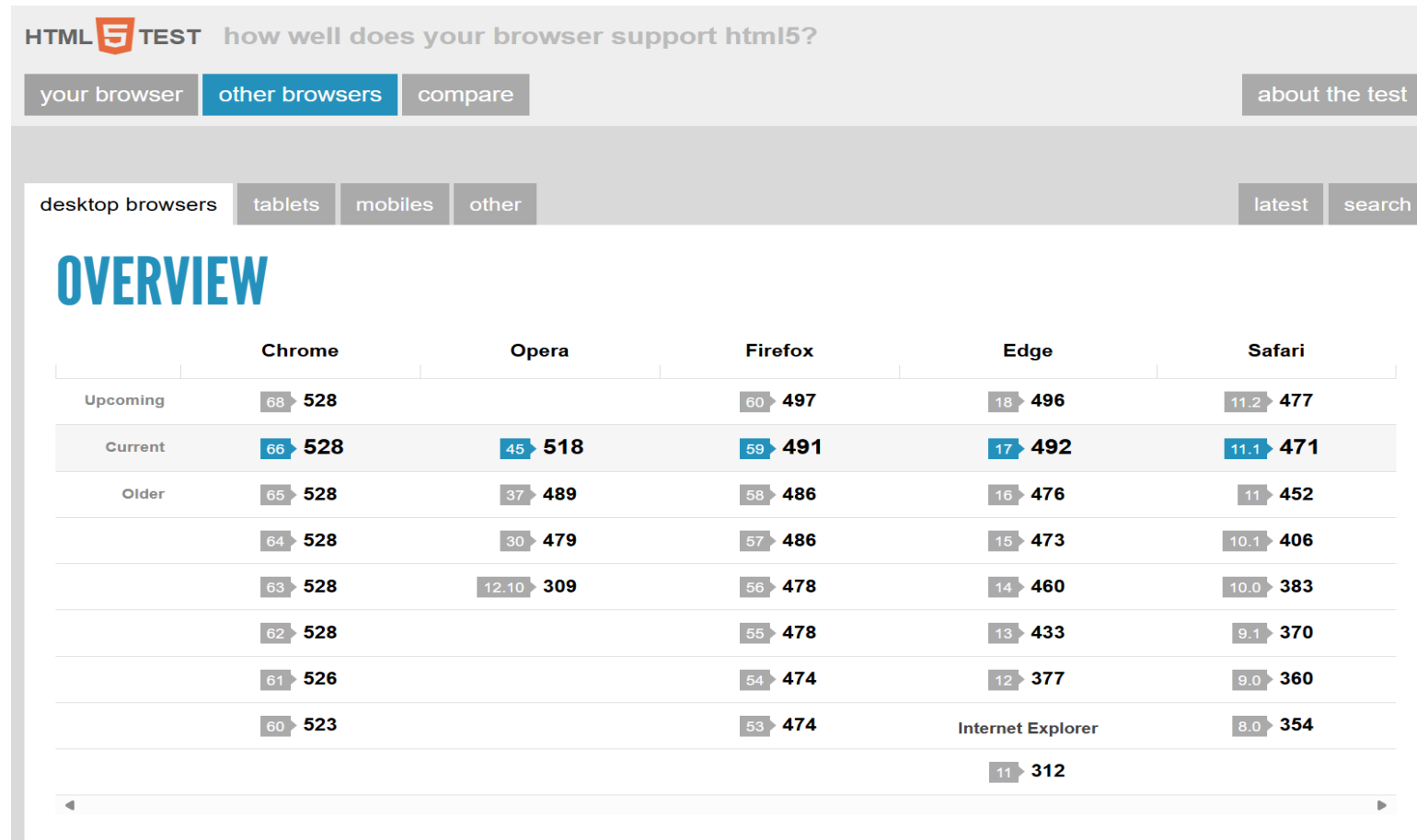
vlk@kpcs.cz

Kde se odehrává dnešní práce

- Ve webových aplikacích (SaaS)
 - Dle průzkumu více než 50 % pracovního času
- Interní uživatelé, externisté, AI agenti
 - Více než 50 uživatelů používá soukromé zařízení
- Všichni chtějí přístup na Internet
 - Poskytuje totiž přístup k AI aplikacím
- Internet je také zlé a nebezpečné místo
 - 12x nárůst phishing stránek a škodlivých rozšíření



Browser Wars

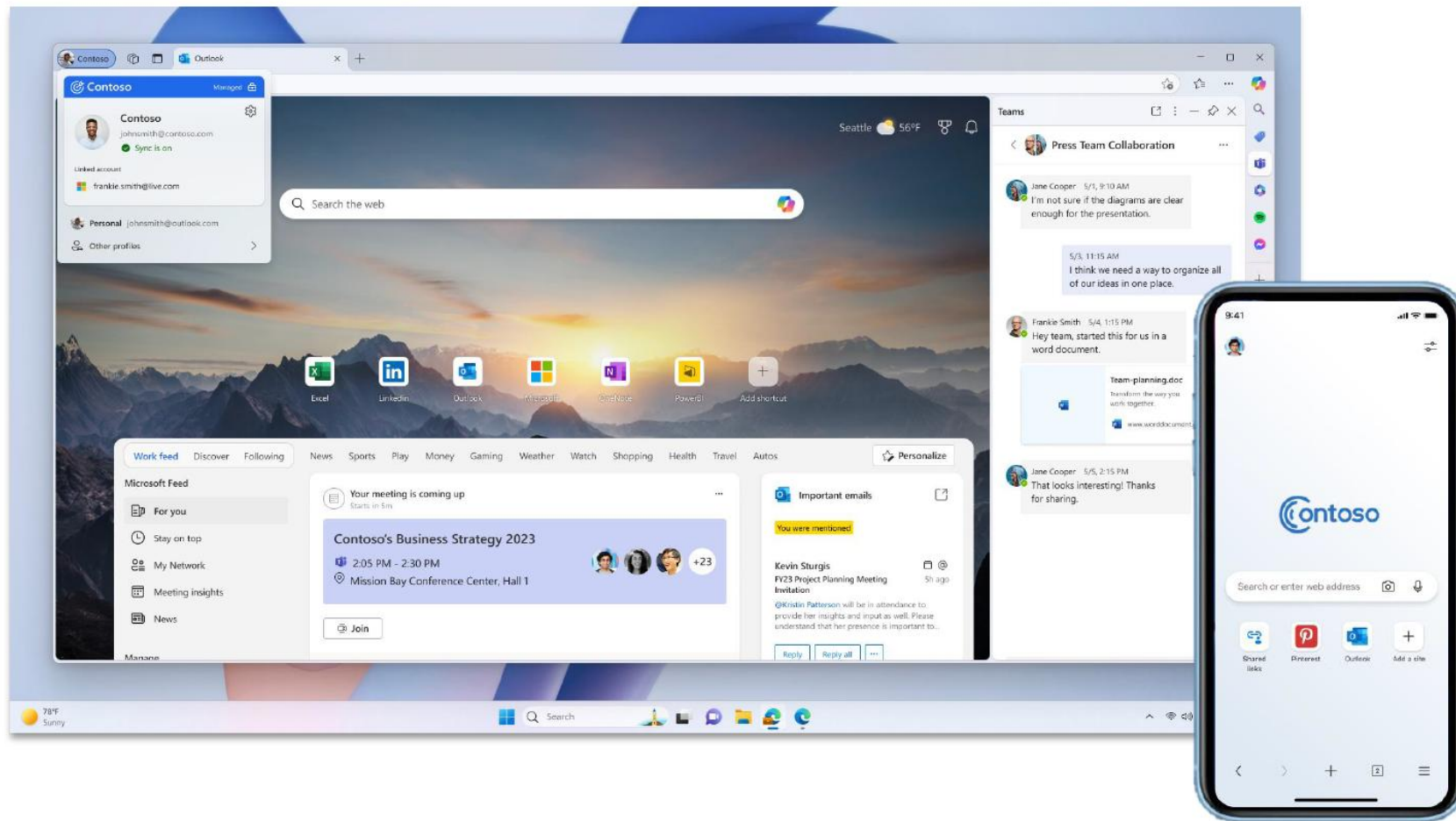


Browser Wars

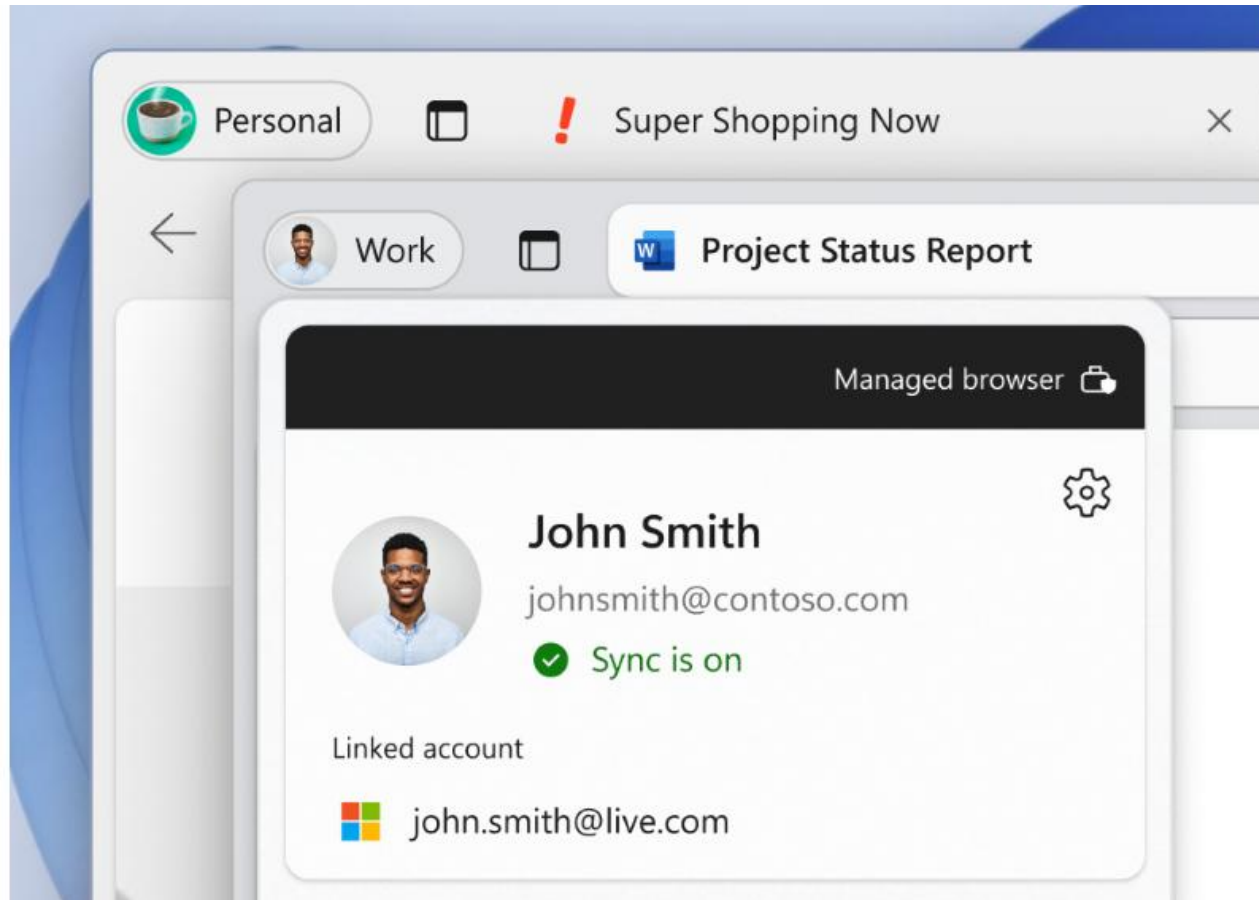
- Pamětníci Internet Explorer?
- Google Chrome (Windows, Android, ChromeOS, iOS, macOS)
- Safari (macOS a iOS)
- Microsoft Edge (Windows, macOS, iOS, Android)
 - Internet Explorer (Trident : MSHTML) aka IEMode (Legacy)
 - Microsoft Edge (EdgeHTML : Spartan)
 - Microsoft Edge (Chromium)
- Chromium Based
 - Seznam Browser
 - OpenAI Atlas



Edge for Business



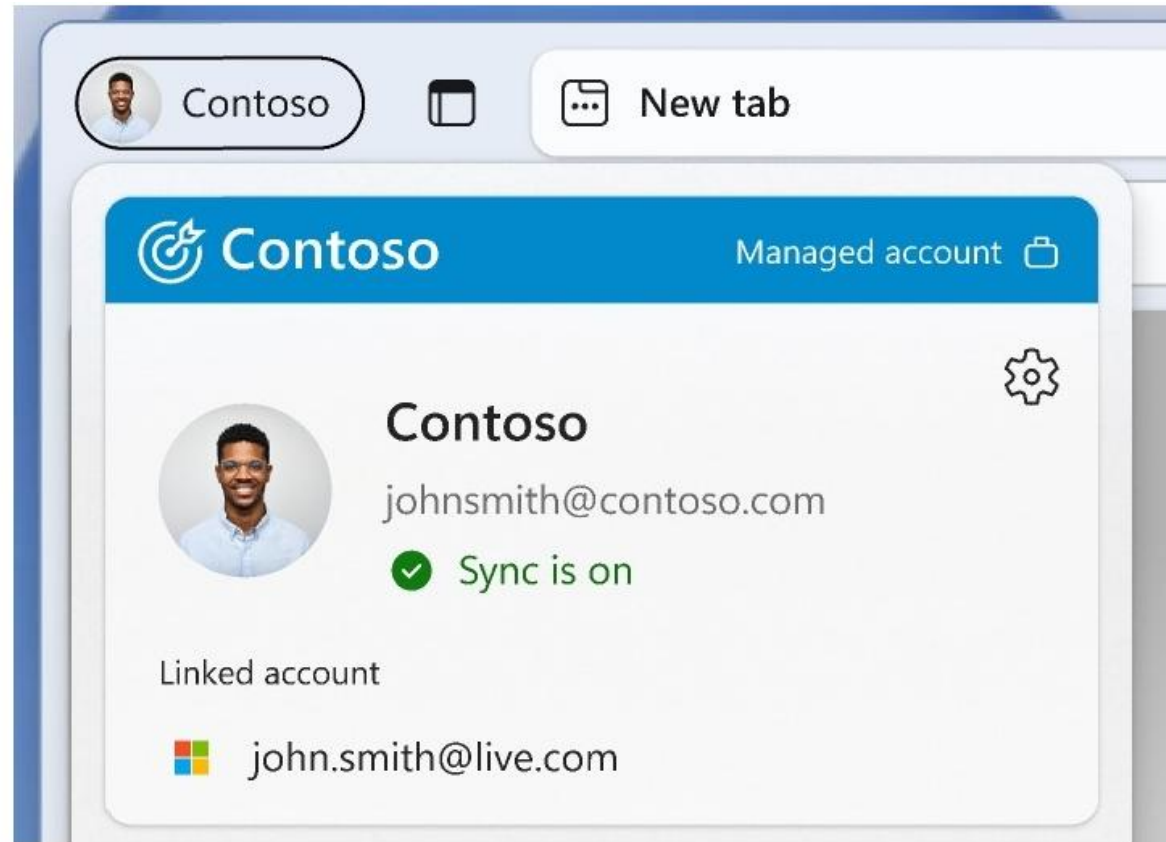
Work Profile



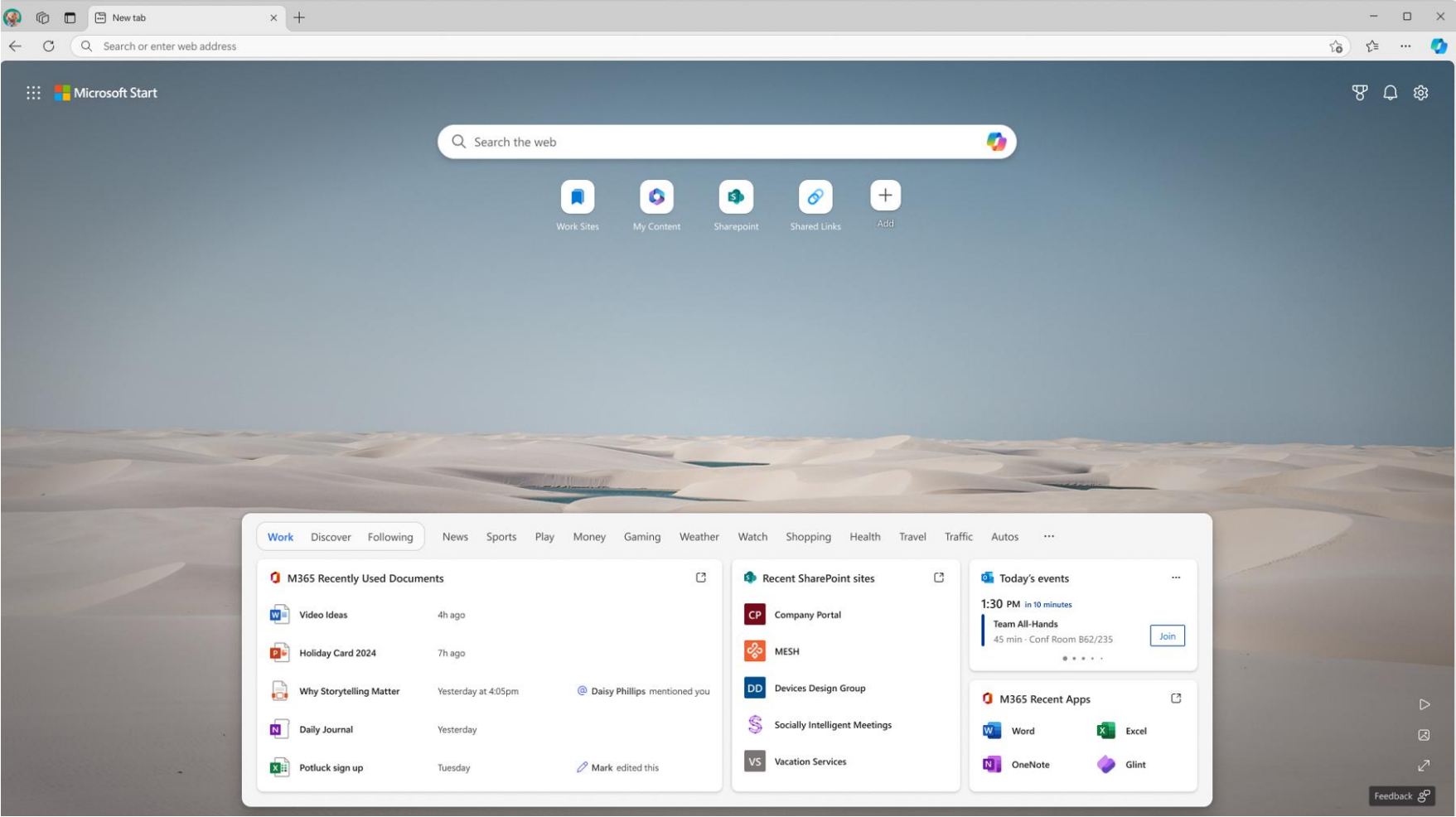
Work Identity (SSO)

Feature	Microsoft Entra ID	Microsoft Entra ID Free	On-premises AD DS	MSA
Sync	Yes	No	No	Yes
SSO with Primary Refresh Token	Yes	Yes	No	Yes
Seamless SSO	Yes	Yes	Yes	N/A
Integrated Windows Authentication	Yes	Yes	Yes	N/A
Enterprise New tab page	Requires O365	Requires O365	No	N/A
Microsoft Search	Requires O365	Requires O365	No	N/A

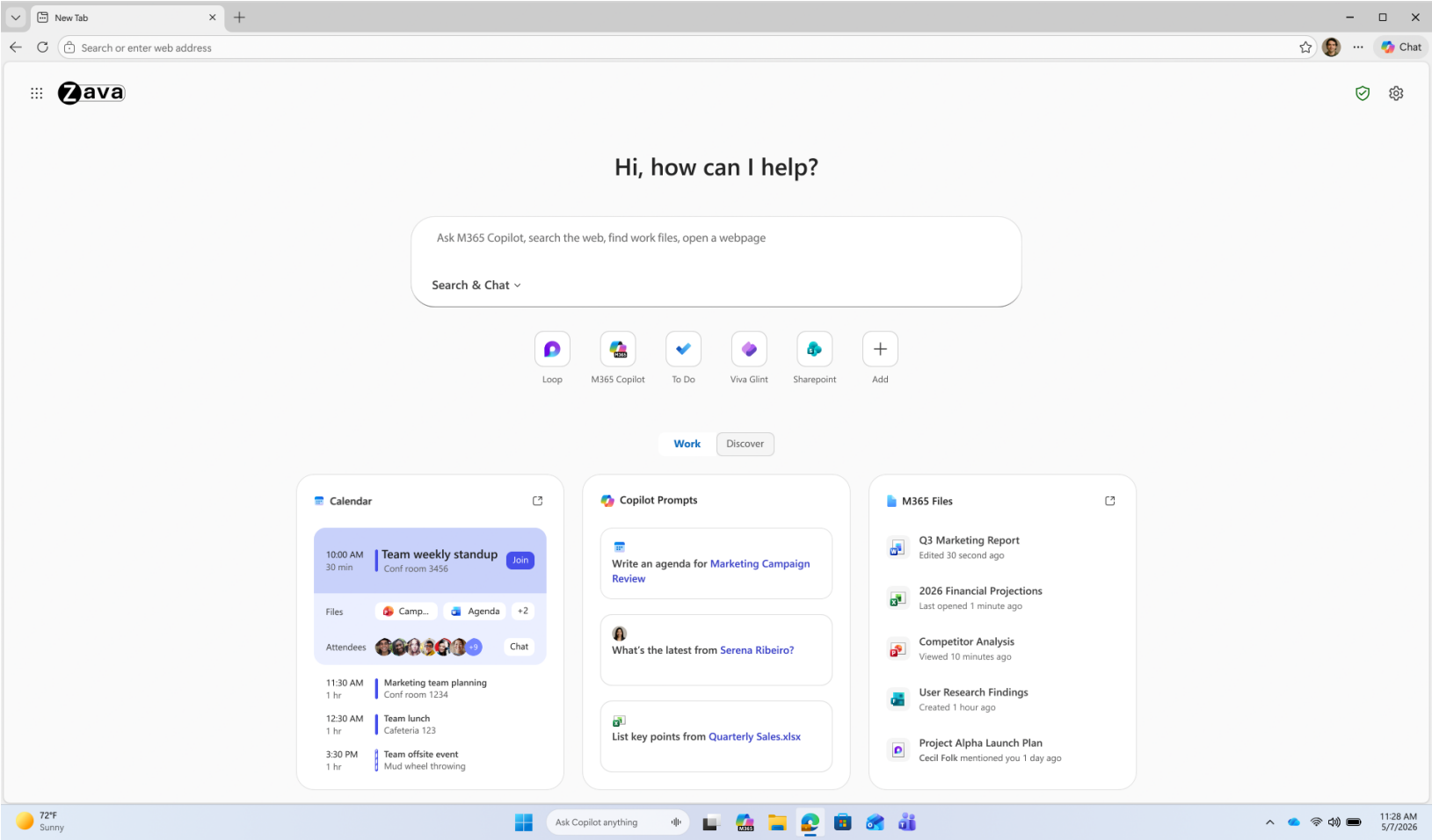
Work Branding



Enterprise Home



Copilot Home

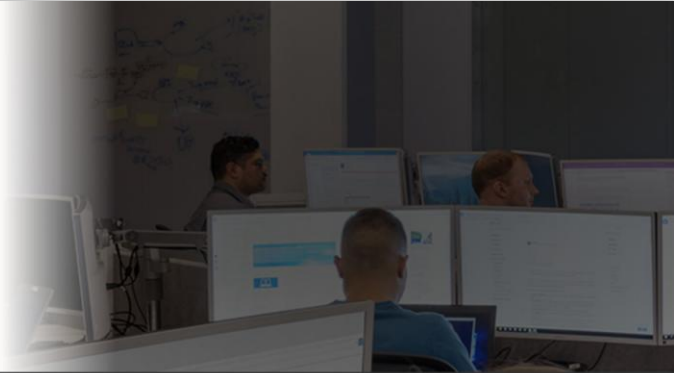


Security Baselines

Microsoft Security Baselines

Learn more: aka.ms/baselines | Download the Security Compliance Toolkit: aka.ms/SCT

53
Blog Articles



Filter by label

RSS

Follow

[Home](#) > [Security, Compliance, and Identity](#) > Microsoft Security Baselines

Options

Microsoft

2,849

Security baseline (FINAL):
Microsoft Edge,
version 91

Security baseline for Microsoft Edge version 91

Rick_Munck on 05-28-2021 07:01 AM

We are pleased to announce the enterprise-ready

Microsoft

13.1K

Security baseline (FINAL):
Windows 10, version 21H1

Security baseline (FINAL) for Windows 10, version 21H1

Rick_Munck on 05-18-2021 10:33 AM

We are pleased to announce the final release of the

Microsoft

7,438

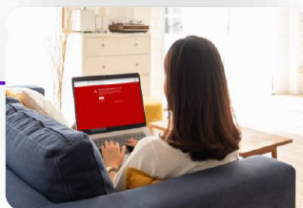
Security baseline (FINAL):
Microsoft 365 Apps for enterprise,
version 2104

Security baseline for Microsoft 365 Apps for enterprise...

Rick_Munck on 04-29-2021 01:10 PM

Microsoft is pleased to announce the final release of

Ochrana uživatelů



Protect users & devices

Protect users and devices from phishing & malware.

Industry leading phishing protection

Microsoft Defender SmartScreen

Integrated with industry leading Microsoft Defender SmartScreen (verified by 3rd parties) protecting against phishing, drive-by exploits, tech call scams, malware, malvertising, backed by the Microsoft Intelligent Security Graph.

Increased Zero-day protection

Enhanced Security Mode (ESM)

Edge safeguards against memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections such as Hardware-enforced Stack Protection and Arbitrary Code Guard (ACG).

Enhance your security on the web ⓘ

Are you satisfied with enhanced security mode? ⤴ ⤵ ☒

Turn on this mode to browse the web more securely and help protect your browser from malware. Choose the level of security you need:

Balanced

(Recommended)

- Adds security mitigations for sites you don't visit frequently
- Most sites work as expected
- Blocks security threats

Strict

- Adds security mitigations for all sites
- Parts of sites might not work
- Blocks security threats

Typosquatting protection

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.



You might have misspelled **twitter.com**

You navigated to `twiterr.com` instead. Microsoft Edge recommends that you double-check the spelling of the site you're trying to access. Misspelled sites—with similar spellings to popular ones—are known to redirect users to sites that steal and scam your personal information.

[Go to twitter.com](#)

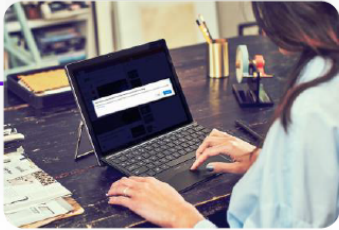
[Proceed](#)

[Report that this site URL is not a misspelling](#)

[Don't block this site](#)

["Explain typosquatting to me"](#)

Ochrana dat



Protect sensitive organization data

Leverage built-in, seamless controls for data security while keeping users productive.

Prevent sensitive data leak

Microsoft Purview DLP (E5)

Native support for DLP for better and more productive end user experience. No need to install or manage extensions, resulting in lower cost.

Prevent sensitive data leak across tenants

Microsoft Entra TRv2

Built in with advanced data-exfil protection to protect from sensitive data leaking across tenants.

Manage Insider Risk

Microsoft Insider Risk Management (E5)

Integrated with Microsoft IRM for policy-based risk monitoring and alerting. Supports detailed auditing for incident forensic and mitigation.

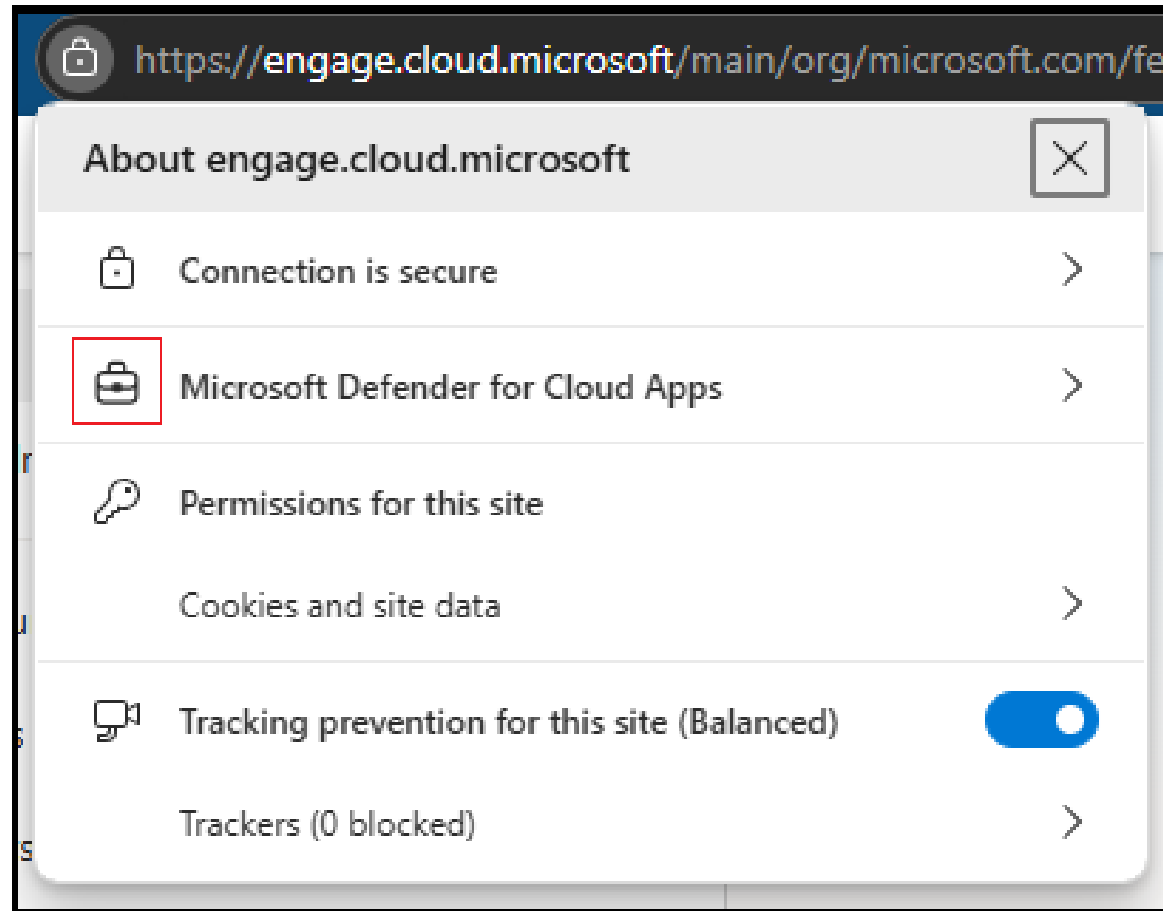
Integrate s Purview

Insider risk management > New insider risk policy

- ✓ Policy template
- ✓ Name and description
- ✓ Users and groups
- ✓ Content to prioritize
- Triggering event
- Indicators
- Finish

- ✓ Using a browser to upload files to the web
- ☐ Sharing SharePoint files with people outside the organization
- ☐ File copied to remote desktop session
- Select which sequences will trigger this policy**
- ✓ Download from Microsoft 365 location then exfiltrate
- ✓ Download from Microsoft 365 location, obfuscate, then exfiltrate
- ✓ Download from Microsoft 365 location, exfiltrate, then delete
- ✓ Download from Microsoft 365 location, obfuscate, exfiltrate, then delete
- ☐ Archive then exfiltrate
- ☐ Archive, obfuscate, then exfiltrate
- ☐ Archive, exfiltrate, then delete
- ☐ Archive, obfuscate, exfiltrate, then delete
- ☐ Downgrade or remove label then exfiltrate
- ☐ Downgrade or remove label, download, then exfiltrate
- ☐ Downgrade or remove label, download, exfiltrate, then delete
- ☐ Downgrade or remove label, download, obfuscate, then exfiltrate
- ✓ Download from third-party site then exfiltrate
- ✓ Download from third-party site, exfiltrate, then delete
- ✓ Download from third-party site, obfuscate, exfiltrate, then delete
- ✓ Download from third-party site, obfuscate, then exfiltrate
- ✓ Download from unallowed domain then exfiltrate
- ✓ Download from unallowed domain, exfiltrate, then delete
- ✓ Download from unallowed domain obfuscate exfiltrate then delete

Integrate s Defender for Cloud Apps



Conditional Access a App Protection

How Entra, Intune, and Edge work together to enable MAM on Windows



Entra CA

Conditional Access policy

Requires app protection for browser access to protected resources



Intune App Protection (MAM)

App Protection (MAM) policy

Defines data protection controls for Edge work profiles



Edge for Business

Enforcement in Edge work profile

Protections applied per-profile using Edge and Intune policies

Enterprise Connectors

- Data Loss Prevention
- Device Identity

Connector	Documentation Link
Symantec DLP	Set up a Symantec DLP Data Loss Connector
Trellix	Set up a Trellix Data Loss Connector

Connector	Documentation Link
Cisco Duo	Set up a Cisco Duo Device Trust Connector
RSA	Set up a RSA Device Trust Connector
Omnissa	Set up an Omnissa Trust Device Connector
Ping Identity	Set up a Ping Identity Trust Device Connector
HYPR	Set up a HYPR Identity Trust Device Connector
Clever	Set up a Clever Identity Trust Device Connector

Aktualizace

Channel	Primary purpose	How often updated with new features	Supported?
Stable	Broad Deployment	~four weeks	Yes
Extended Stable	An enterprise release option for Stable aligned to a longer release cycle	~eight weeks	Yes
Beta	Representative validation in the organization	~four weeks	Yes
Dev	Planning and developing	Weekly	No
Canary	Bleeding edge content	Daily	No

Doplňky

← Installed extensions / Office



Office

Size 5.1 MB Version 2.2.4

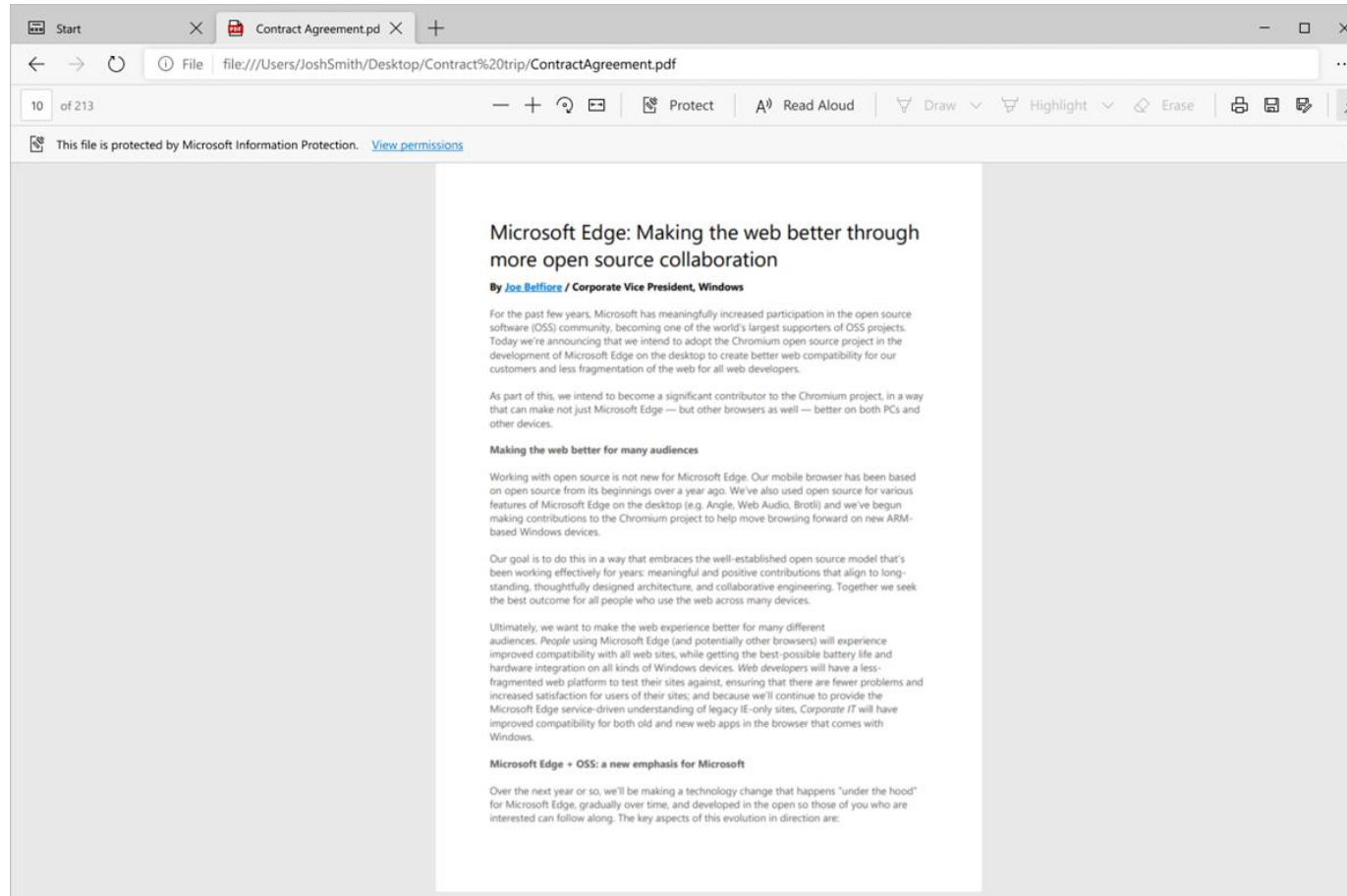
Description

View, edit, and create Office documents in your browser.

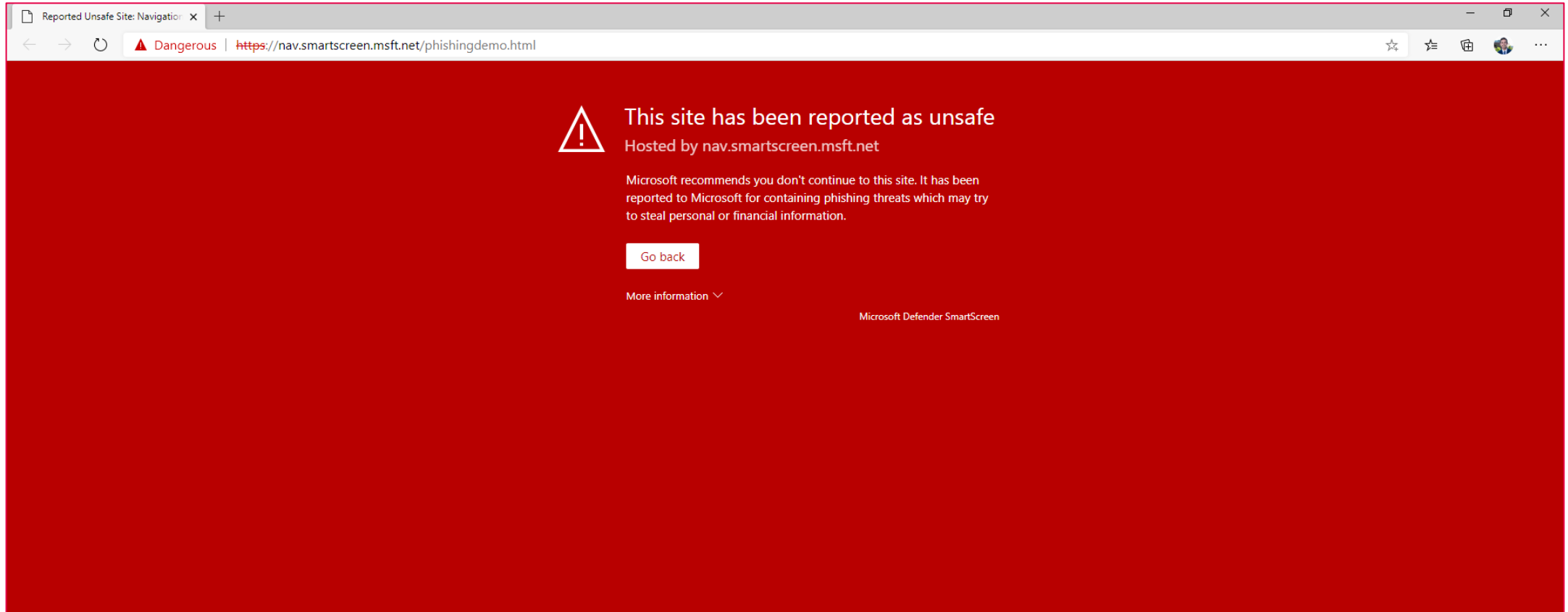
Permissions

- Read your browsing history
- Display notifications
- Read and modify data you copy and paste
- Communicate with cooperating native applications

PDF Reader



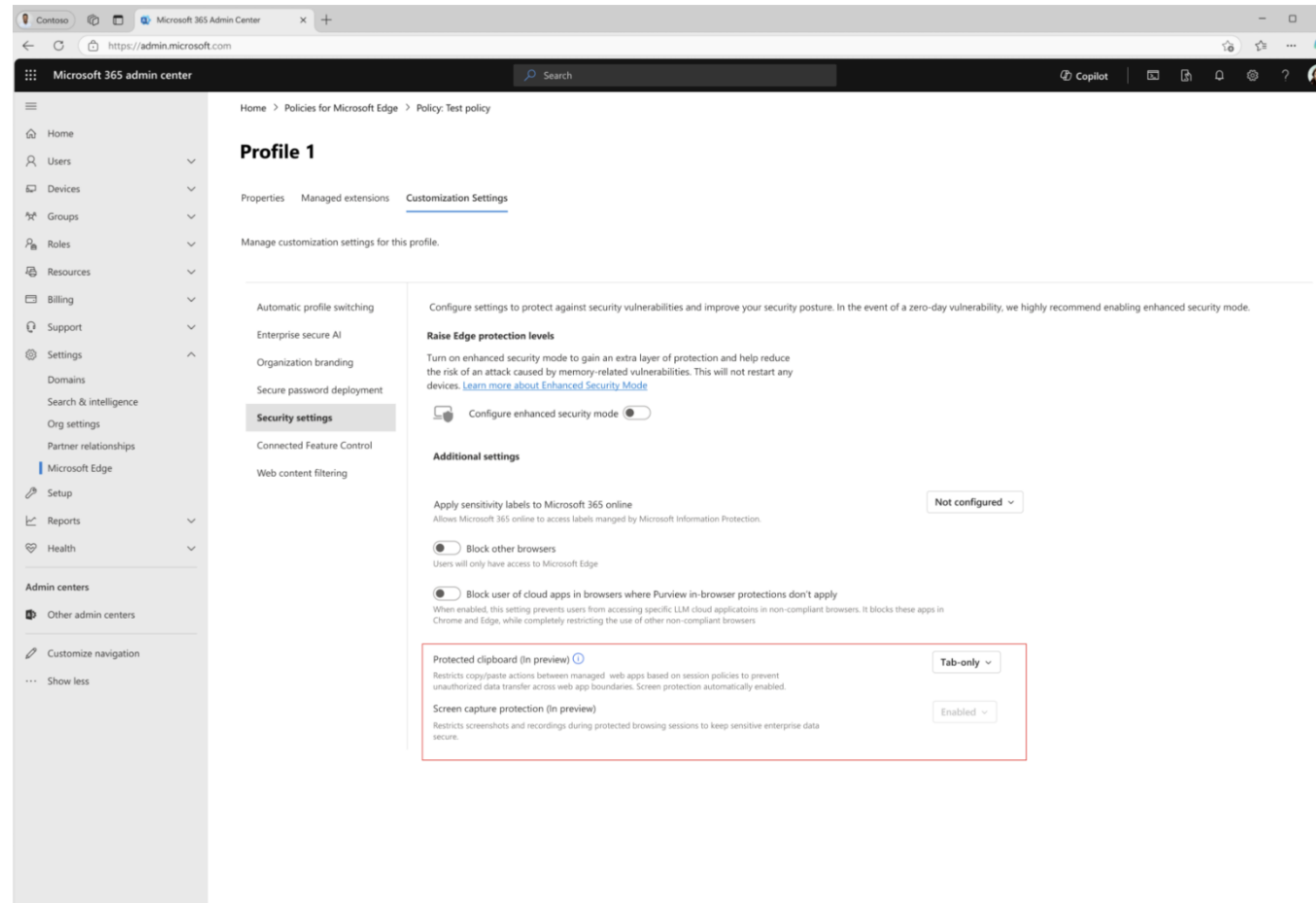
SmartScreen



Data Policy Controls

Activity	Device Type	App Type	Supported Policy Actions
Upload text	Managed	Unmanaged	allow, block, both actions audited
Upload file	Managed, Unmanaged	Managed, Unmanaged	allow, block, both actions audited
Download file	Managed, Unmanaged	Managed	allow, block, both actions audited
Cut/copy data	Managed, Unmanaged	Managed	allow, block, both actions audited
Paste data	Managed, Unmanaged	Managed	allow, block, both actions audited
Print data	Managed, Unmanaged	Managed	allow, block, both actions audited
Protected clipboard (Preview)	Managed, Unmanaged	Managed	See Microsoft Edge Protected Clipboard (preview)
Screen capture (Preview)	Managed, Unmanaged	Managed	See Microsoft Edge Protected Clipboard (preview)

Protected Clipboard / Screenshots



Enterprise AI Policy (preference Copilot)

Model Name	Model Company
Arc AI	arc.ai
Canva	canva.com
CapCut	capcut.com
Character.ai	character.ai
ChatGPT	chat.openai.com , chatgpt.com
Claude	claude.ai
Cohere	cohere.com/coral
DeepAI	deepai.org
DeepL	deepl.com
Deepseek	deepseek.me , deepseek.com
DiaAI	diaai.org
ElevenLabs	elevenlabs.io
Google Gemini	bard.google.com , gemini.google.com
Grammarly	grammarly.com
Grok (xAI)	x.com
Markcopy.AI	markcopy.ai
Meta AI	meta.com
Murf.ai	murf.ai
Ninja Tech AI	myninja.ai
Notion	notion.so
n8n	n8n.io
Otter.ai	otter.ai
Perplexity AI	perplexity.ai
Rea	rea.com

Automatická ochrana obsahu

The screenshot shows a web browser window displaying a Microsoft Word document titled "Contoso Acquisition Brief.docx". The browser address bar shows "https://contoso.sharepoint.com". The document is titled "Contoso Acquisition Brief" and has a ribbon with tabs: File, Home, Insert, Layout, References, Review, View, and Help. The "Home" tab is active, showing a font face of "Calibri Light" and a size of "20". The document content includes a title "Acquisition Brief – Trey Research", a section "Executive Summary", and a "Budget" table.

Acquisition Brief – Trey Research

Executive Summary

This brief outlines the plan for Contoso, Ltd. to acquire Trey Research in Q3 of 2026 for \$8,500,000 USD.

This acquisition is designed to strengthen Contoso's research and development capabilities while expanding its presence in emerging markets. By integrating Trey Research's innovative solutions and talent pool, Contoso aims to accelerate product innovation and deliver enhanced value to customers. The combined resources will enable operational efficiencies, foster collaboration across teams, and position the organization for sustained growth in a competitive landscape.

The acquisition will also create a platform for long-term strategic alignment between Contoso and Trey Research. By leveraging shared expertise and complementary technologies, the combined entity can accelerate time-to-market for new solutions and strengthen its competitive edge. This integration is expected to unlock synergies across product development, customer engagement, and operational processes—ultimately driving innovation at scale and delivering measurable business impact.

Budget

Category	Estimated Cost
Purchase Price	\$8,500,000
Legal & Due Diligence Fees	\$450,000

Page 1 of 2 385 words English (U.S.) TTVR: 2.62s | EUPL: 2.4s Text Predictions: On Editor Suggestions: Showing Outer Ring (PPE) : TIL1

58°F Sunny 11:28 AM 11/18/2025

Podpora DLP

The screenshot displays a Microsoft Word document titled "Contoso Workforce Overview and Strategic Implications" within a web browser window. The document is marked as "Confidential - Internal Use Only" and contains several paragraphs of text, including a section on "Headcount Composition" with a bulleted list of employee statistics. The document is protected by DLP, as evidenced by the "Ask Copilot anything" watermark and the "Confidential - Internal Use Only" label. The browser window shows the URL "https://contoso.sharepoint.com" and the document is open in the "Contoso Human Resources" workspace. The Word ribbon is visible at the top, showing the "Home" tab and various editing options. The status bar at the bottom indicates the temperature is 58°F and the date is 11/18/2025.

Human Resources Contoso Inc. Confidential - Internal Use Only

Contoso Workforce Overview and Strategic Implications

As of the latest reporting period, Contoso maintains a robust and growing workforce totaling almost **5,000 employees (4,258 to be precise)**. This includes **213 newly onboarded employees**, reflecting the company's continued investment in talent acquisition and organizational expansion.

Headcount Composition

- **Full-Time Employees (FTEs):** 4,258
- **New Full-Time Hires:** 184 out of the 213 newly onboarded employees
- **Remaining New Hires (Part-Time, Contract, or Interns):** 29

This distribution underscores Contoso's strategic emphasis on full-time roles, which continue to form the backbone of its operational and innovation capacity.

Talent Acquisition Trends

The recent onboarding wave of 213 employees marks a significant milestone in Contoso's hiring strategy. The majority of these hires were placed in full-time roles, indicating a prioritization of long-term workforce stability and deeper integration into core business functions.

Departments that saw the highest influx of new talent include:

- **Engineering and Product Development**
- **Sales and Customer Success**
- **Security and Compliance Operations**

These areas align with Contoso's current business priorities, including scaling its cloud offerings, enhancing customer engagement, and strengthening its enterprise-grade security posture.

Dynamický Watermarking

Experiences_Built_for_Focus.docx x Contoso Human Resources x +

https://contoso.sharepoint.com

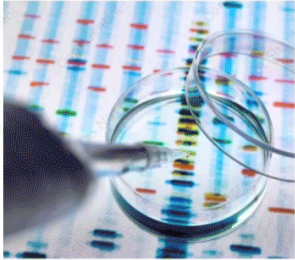
Experiences_Built_for_Focus

File Home Insert Layout References Review View Help

Cambria (Body) 11 A B I U ab X X' W Y Z ... List Paragraph Caption TOC Heading Q Find Dictate Sensitivity Editor Add-ins

Classified as Contoso Highly Confidential

Confidential - Internal Use Only



Experiences built for focus

Experiences Built for Focus

This document outlines a series of user experiences designed to enhance focus and productivity. These features are part of a confidential initiative aimed at improving cognitive engagement through digital interfaces. The information contained herein is highly sensitive and intended solely for internal demonstration purposes.

Focus-Driven Features

- Adaptive Notification Filtering
- Ambient Sound Integration
- Dynamic Task Prioritization
- Cognitive Load Balancing
- Real-Time Distraction Alerts

Sensitive User Scenarios

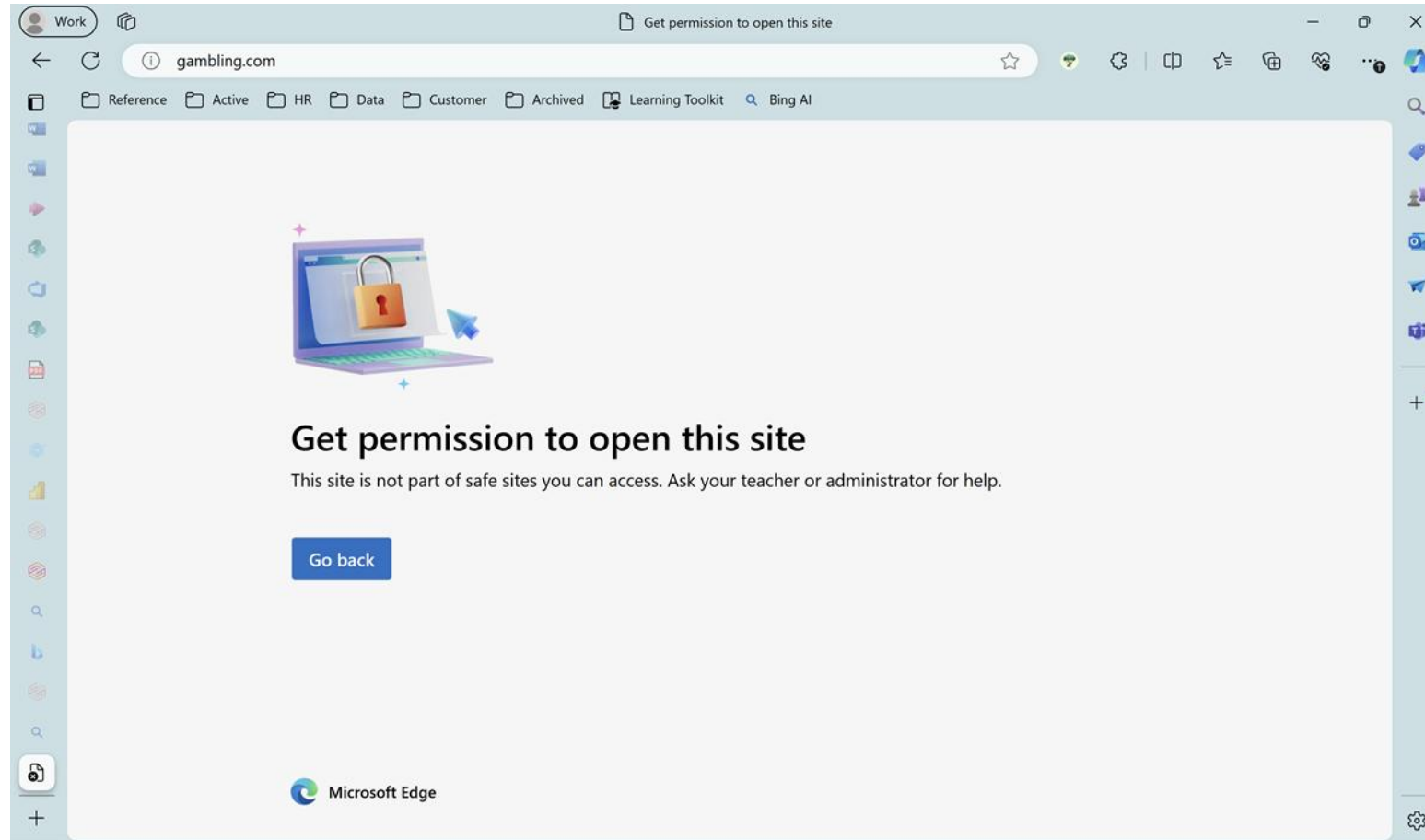
Scenario ID	Description	Sensitivity Level
SCN-001	Executive using focus mode	High

58°F Sunny

Ask Copilot anything

11:28 AM 11/18/2025

Web Content Filtering



Detekce PUA



freevideo.exe has been blocked as a potentially unwanted app by Microsoft Defender SmartScreen.

Delete

...

Password Monitor

×

Save password

monakane@outl... .. Edit

☒

Let Microsoft Edge check passwords you've saved in the browser and alert you if they've been compromised on the internet.
[Learn more](#)



OK

Not now

▼



Edge Management Service

A další možnosti správy prohlížeče Edge

Možnosti nastavení

Platforma Funkce	GPO	MDM (Intune)	Mobile Application Management	Edge Management Service
Windows	Ano	Ano	Ano	Ano
macOS	Ne	Ano	Ne	Ano
iOS	Ne	Částečně	Ano	Ano
Android	Ne	Částečně	Ano	Ano
Reporty	Ne	Částečně	Částečně	Ano

Ke zvážení

- Potřebné URL v rámci firewall pravidel pro jednotlivé služby
- Politiky se aplikují po restartu prohlížeče
 - Standardně se kontrolují každých 24 hodin
 - Přiřazení na skupinu uživatelů pak každých 90 minut
- Vyvarovat se konfliktu politik
 - Vyhrává Intune nad Edge Management Service (pokud neřekne politika jinak)
 - Vyhrává Defender a Purview nad Intune (bez ohledu na politiku)
- Network Protection v Defender for Endpoint
 - Na některých platformách jediná možnost získání všech dat
- DNS over HTTPS a QUICK
 - Šifrované hlavičky jsou bezpečné, ale těžko se hlídají

Zdroje a další postup

- Chcete poznat Edge for Business?
 - [An Industry-Leading Secure Enterprise Browser | Microsoft Edge for Business](#)
- Chcete Edge for Business nasadit vlastními silami?
 - [Plan your deployment of Microsoft Edge | Microsoft Learn](#)
 - [Get started with configuration policies | Microsoft Learn](#)
- Chcete Edge for Business nasadit externími silami?
 - [Kontakt | KPCS](#) 

Dotazy a diskuse



Petr Vlk

Microsoft MVP

Microsoft 365 Enterprise Security Architect @ KPCS CZ



vlk@kpcs.cz

Že už používáte a platíte za služby Microsoft 365?
Využijte jejich benefitů na maximum!



Definujte priority bezpečnosti: [Zero Trust Workshop by KPCS](#)

Ověřte si realitu IT prostředí: [Security Risk Assessment by KPCS](#)