Protecting your corporate data on managed Windows devices - Your options

Start 13:00

Peter van der Woude

Albert Hoitingh

Protecting your corporate data on managed Windows devices - Your options

Peter van der Woude & Albert Hoitingh

Experts Live Netherlands

Sprekers

Peter van der Woude

Principal Consultant @ InSpark
Security MVP (Intune) |
Windows and Devices MVP
(Windows)

Albert Hoitingh

Technical Architect @
Microsoft Innovation Hub
CEH | CISSP

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

What are we going to discuss?

- Why is it important to protect corporate data (on managed devices)
- What are the options for protecting corporate data on managed Window devices
- A closer look at Personal Data Encryption and Microsoft Purview
- How do the different options for protecting corporate data compare

Why is it important to protect corporate data (on managed devices)

Reasons why

- Combatting cyber threats
- Regulatory compliance (NIS2 | DORA| etc)
- Keeping customer trust and reputation
- Avoid financial losses
- Safeguarding intellectual property

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Strategic approaches to cybersecurity: "Managing your own house"

Data security

Accountability is increasingly central to the world of data security. From security strategies to new policies governing generative AI, organizations must start taking responsibility for what is going on under their own digital roof.

Key components of an effective data security strategy

In our experience, the most successful data security implementation strategies consider the following: visibility, risk detection, classification, labeling, data protection, and data leakage prevention across your multi-cloud and hybrid digital estate.

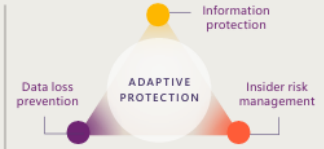
It is no longer enough to focus solely on the data; it's just as important to understand how that data moves within the organization, how users, customers or partners interact with it, and what level of risk is acceptable for the organization.

Data doesn't move on its own. It's moved by people. Because different people require different levels of access, a comprehensive data security policy must be dynamic, considering both data and user context. This lets organizations balance protection and productivity, allowing low-risk users to continue working as usual while restricting the actions of users with elevated risk.

As data types proliferate, sources get more complex, and generative AI technology gains traction, data security is inevitably becoming a pressing concern. A 2023 Microsoft study found that over 40% of enterprise (>500 employees) organizations' annual cybersecurity budget on average is now allocated to data security.

An integrated approach to data security

- Classify and label sensitive data, and prevent its unauthorized use across apps, services, and devices.
- Understand the user intent and context around the use of sensitive data to identify the most critical risks
- Assign high-risk users to appropriate DLP, data lifecycle, and Conditional Access policies



Securing organizational data has also become a multifaceted task, leading to the adoption of multiple, hard-to-manage tools. This kind of fragmented approach creates more noise from duplicated alerts, making it harder to identify and investigate actual incidents. Organizations using over 15 tools experienced nearly three times more data security incidents than organizations using fewer tools. This is why it is so important to invest in integrated, automated data security solutions to achieve the best outcomes.

How generative AI is fueling the need for data security policy implementation

Microsoft's AI products, such as Copilot, are designed to use only information you already have access to. When other generative AI apps are deployed on ungoverned data estates it can result in data oversharing or leakage as users may end up accessing sensitive data. It is difficult to protect data from AI-related security risks given many organizations don't actually know where—or even what—their sensitive data is.

Studies show 83% of organizations experience multiple data breaches over time, so getting ahead of the risks is critical. Data environments must be prepared for AI, which requires inventorying data stores, identifying sensitive data, then labeling and protecting it to ground the data and prevent its unintended exposure to AI apps.

Applying data loss prevention policies for inputs and outputs from AI apps helps to prevent both overexposure and leakage for new AI generated data, while automating data classification and labeling vastly reduces the risk of data exposure. In summary, data loss prevention policies can apply to data that AI models consume and generate.

Links

Microsoft insights and best practices in securing data | Microsoft Security Blog | Oct 2023

Empowering employee self-service with guardrails: How we're using sensitivity labUsing sensitivity labels | Apr 2024

How to use prompts in Microsoft Copilot for Security | Microsoft Security Blog | Feb 2024

Microsoft Copilot for Security in Microsoft Purview | Microsoft Learn | Sep 2024

GitHub - Azure/Copilot-For-Security

What about AI….

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Dutch privacy watchdog warns firms that use AI chatbots

August 7, 2024

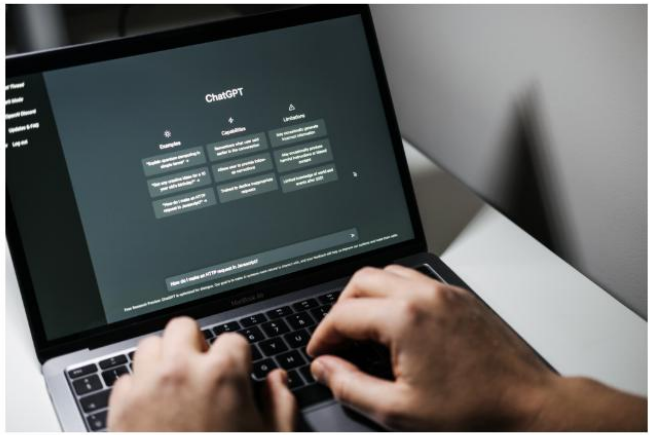


Photo: Depositphotos.com

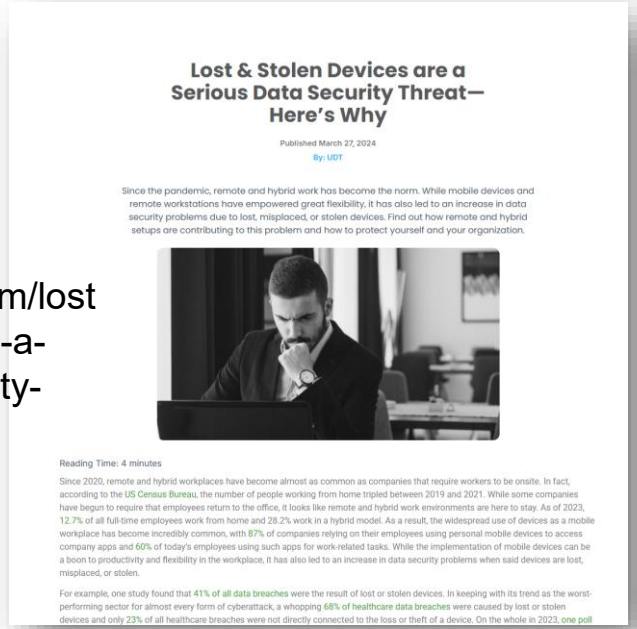
The Dutch privacy watchdog Autoriteit Persoonsgegevens has issued a warning about the use of AI-driven chatbots by companies, following several leaks of private information, including medical details.

Workers who use digital assistants such as ChatGPT to answer questions from customers or summarise large files, may save time, but they also pose a risk to data protection, the AP said.

In one case, a family doctor's assistant fed private information about patients into a ChatGPT-based programme, which was then stored on the tech company's servers and potentially used to train the software, the AP said.

https://www.dutchnews.nl/2024/08/dutch-privacy-watchdog-warns-firms-that-use-ai-chatbots/

https://udtonline.com/lost-stolen-devices-are-a-serious-data-security-threat-heres-why/



Lost & Stolen Devices are a Serious Data Security Threat—Here's Why

Published March 27, 2024

By: UDT

Since the pandemic, remote and hybrid work has become the norm. While mobile devices and remote workstations have empowered great flexibility, it has also led to an increase in data security problems due to lost, misplaced, or stolen devices. Find out how remote and hybrid setups are contributing to this problem and how to protect yourself and your organization.

Reading Time: 4 minutes

Since 2020, remote and hybrid workplaces have become almost as common as companies that require workers to be onsite. In fact, according to the US Census Bureau, the number of people working from home tripled between 2019 and 2021. While some companies have begun to require that employees return to the office, it looks like remote and hybrid work environments are here to stay. As of 2023, 12.7% of all full-time employees work from home and 28.2% work in a hybrid model. As a result, the widespread use of devices as a mobile workplace has become incredibly common, with 87% of companies relying on their employees using personal mobile devices to access company apps and 60% of today's employees using such apps for work-related tasks. While the implementation of mobile devices can be a boon to productivity and flexibility in the workplace, it has also led to an increase in data security problems when said devices are lost, misplaced, or stolen.

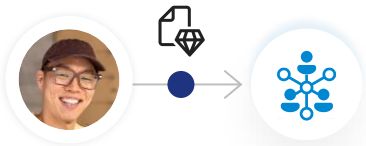
For example, one study found that 41% of all data breaches were the result of lost or stolen devices. In keeping with its trend as the worst-performing sector for almost every form of cyberattack, a whopping 68% of healthcare data breaches were caused by lost or stolen devices and only 23% of all healthcare breaches were not directly connected to the loss or theft of a device. On the whole in 2023, one poll

Security concerns associated with AI

Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

1

Data leak:
Users may inadvertently leak sensitive data to AI apps

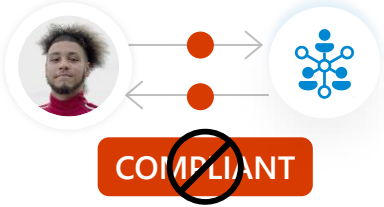


2

Data oversharing:
Users may access sensitive data via AI apps they are not authorized to view or edit

3

Non-compliance usage:
Users use AI apps to generate unethical or other high-risk content

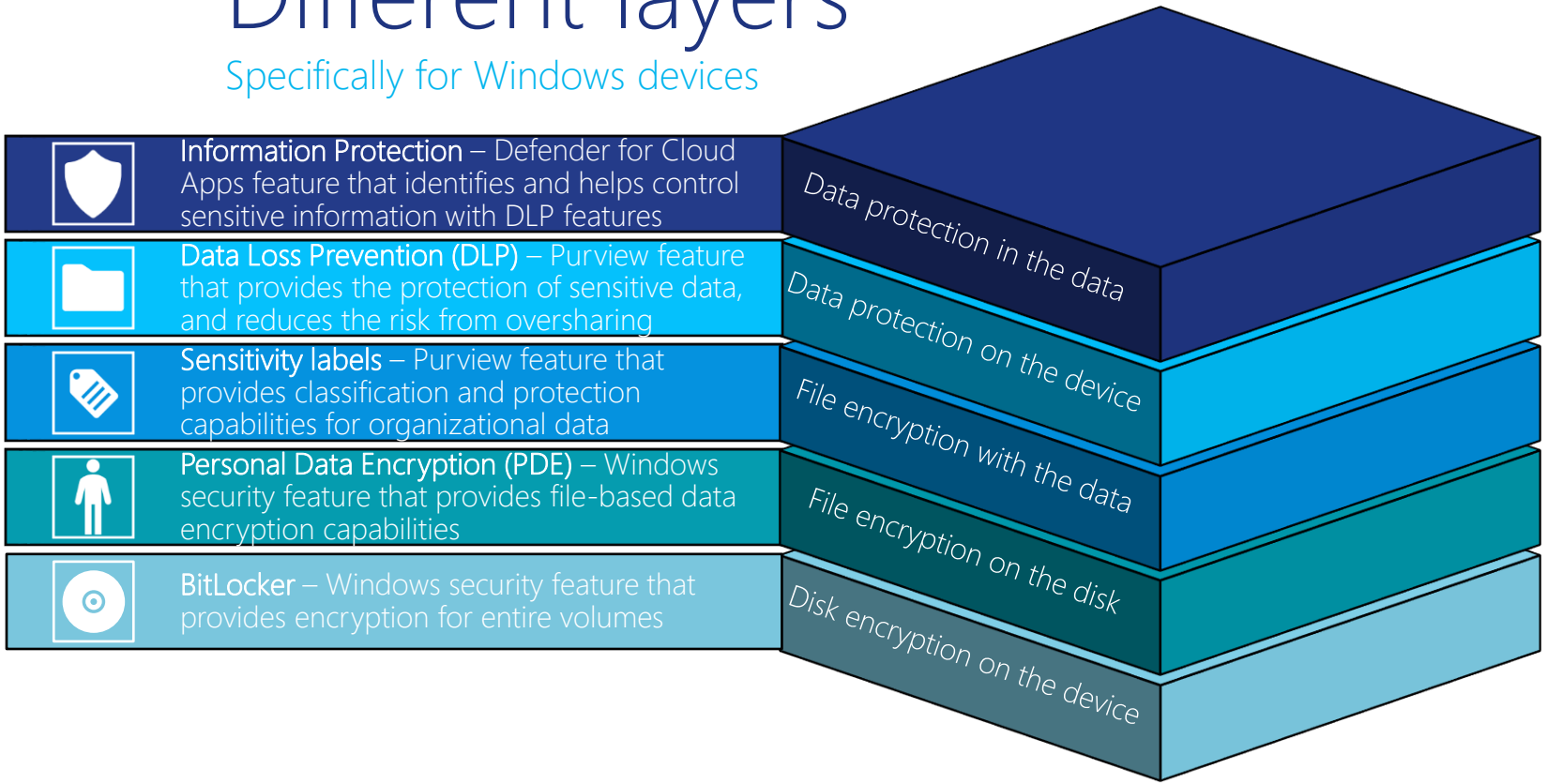


Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

What are the options for protecting corporate data on managed Window devices

Different layers

Specifically for Windows devices



Specifically for Windows devices

What are the realistic options?

BitLocker – Windows security feature that provides encryption for entire volumes

Relies on TPM and UEFI

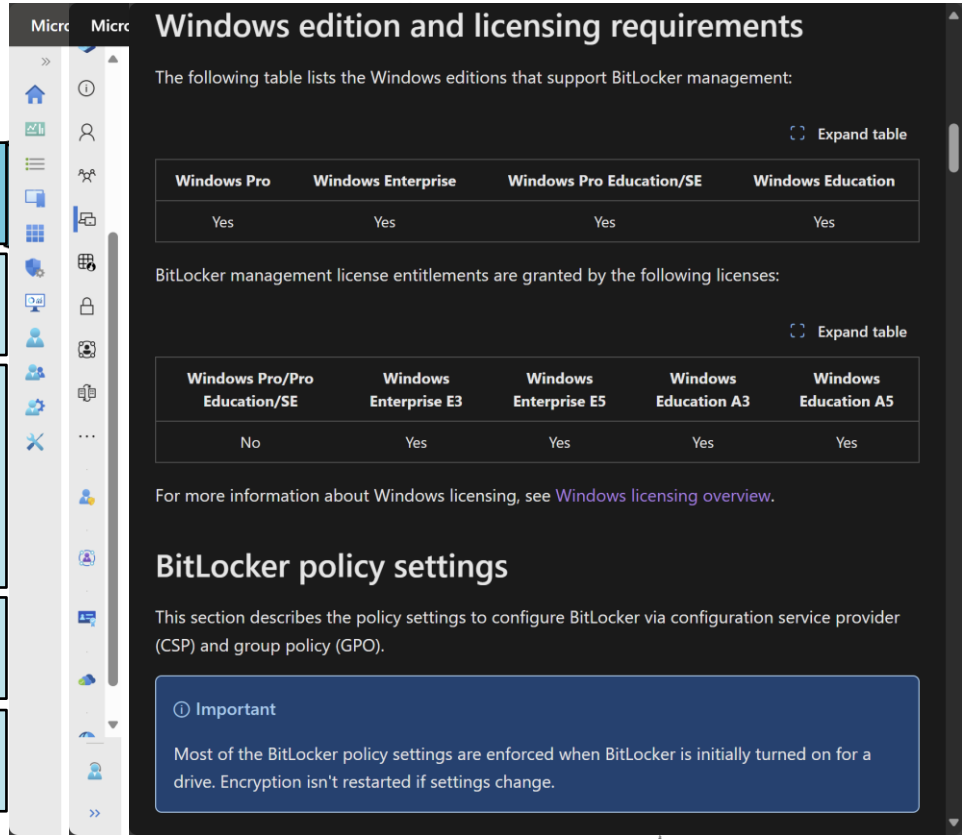
Management via Microsoft Intune

- Ability to require TPM startup PIN
- Ability to use full disk encryption
- Ability to configure encryption method

Recovery key storage in Microsoft Entra

- Ability to allow self service recovery

Advise: Make sure that the required licensing is available for BitLocker management



Windows edition and licensing requirements

The following table lists the Windows editions that support BitLocker management:

Expand table

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
Yes	Yes	Yes	Yes

BitLocker management license entitlements are granted by the following licenses:

Expand table

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
No	Yes	Yes	Yes	Yes

For more information about Windows licensing, see Windows licensing overview.

BitLocker policy settings

This section describes the policy settings to configure BitLocker via configuration service provider (CSP) and group policy (GPO).

Important

Most of the BitLocker policy settings are enforced when BitLocker is initially turned on for a drive. Encryption isn't restarted if settings change.

Specifically for Windows devices

What are the realistic options?

Personal Data Encryption (PDE) – Windows security feature that provides file-based data encryption capabilities

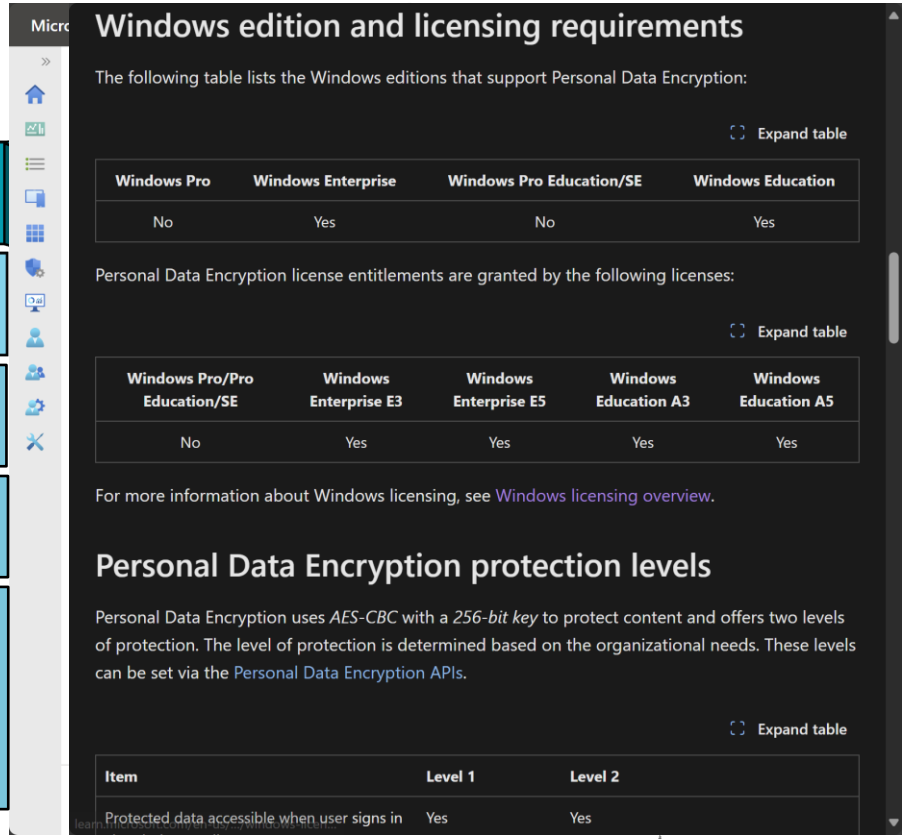
Relies on Windows Hello

Management via Microsoft Intune

- Ability to configure protected folders

Advise: Make sure that the required licensing is available for management and usage

More details later ☺



Windows edition and licensing requirements

The following table lists the Windows editions that support Personal Data Encryption:

Expand table

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
No	Yes	No	Yes

Personal Data Encryption license entitlements are granted by the following licenses:

Expand table

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
No	Yes	Yes	Yes	Yes

For more information about Windows licensing, see Windows licensing overview.

Personal Data Encryption protection levels

Personal Data Encryption uses *AES-CBC* with a *256-bit key* to protect content and offers two levels of protection. The level of protection is determined based on the organizational needs. These levels can be set via the Personal Data Encryption APIs.

Expand table

Item	Level 1	Level 2
Protected data accessible when user signs in	Yes	Yes

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Specifically for Windows devices

What are the realistic options?

Sensitivity labels – Purview feature that provides classification and protection capabilities for organizational data

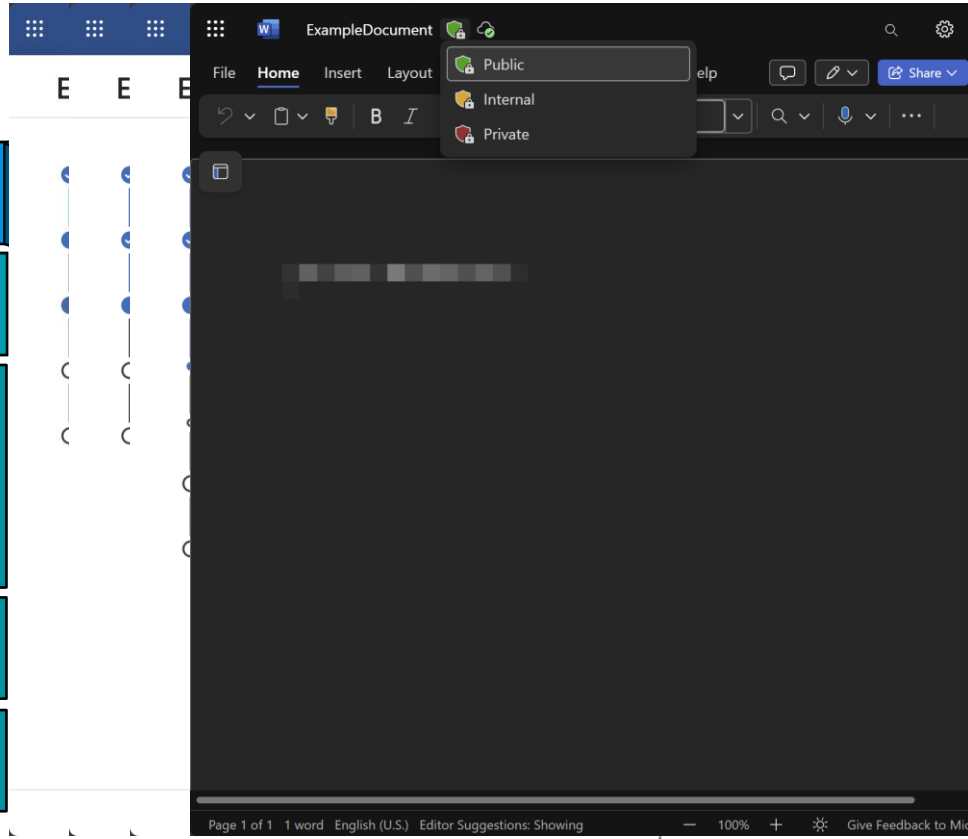
Offers encryption on the data level. The label and protection always stays with the data.

Management via Microsoft Purview

- Ability to specify data assets and containers
- Ability to specify encryption and permissions
- Ability to mark content

Ability to use Double Key Encryption for protecting highly sensitive data

Advise: The technical implementation is the easy part. Don't forget the user!



Specifically for Windows devices

What are the realistic options?

Data Loss Prevention (DLP) – Purview feature that provides the protection of sensitive data, and reduces the risk from oversharing

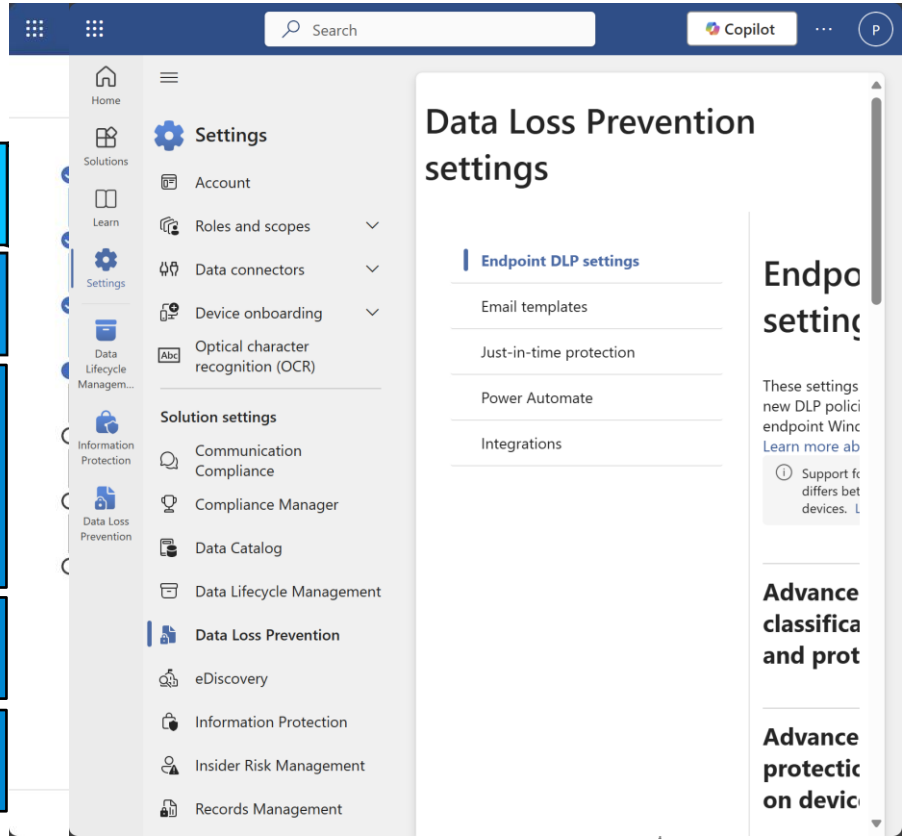
Covers all Microsoft 365 workloads, including on-premises and the device.

Management via Microsoft Purview

- Ability to specify locations and scopes
- Ability to specify data type and actions
- Ability to configure policy mode

Ability to configure specific Endpoint DLP settings for protecting content on Windows

More details later ☺



Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Specifically for Windows devices

What are the realistic options?

Information Protection – Defender for Cloud Apps feature that identifies and helps control sensitive information with DLP features

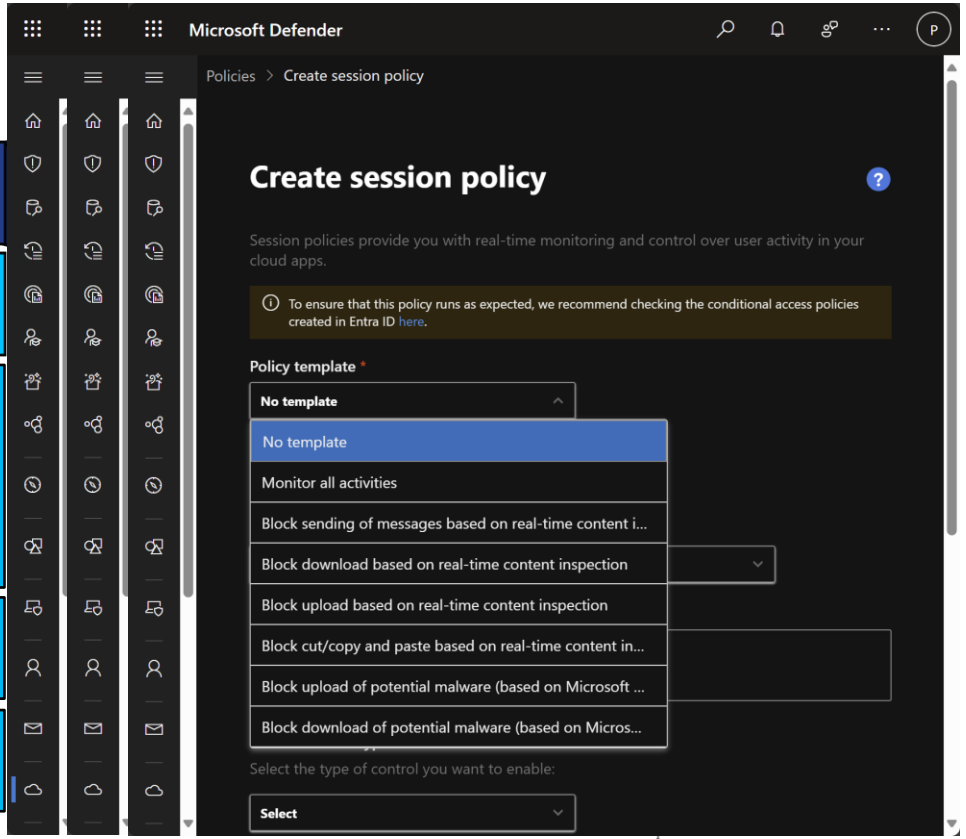
More enhanced DLP for Saas platforms that works together with Purview.

Management via Microsoft Defender

- Configure file, access and session policy
- Ability to prevent data sharing
- Ability to look in the data

With all that: the ability to contain data

Make sure that the required licensing is available for Defender for Cloud Apps!



Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

A closer look at Personal Data Encryption and Microsoft Purview

Let’s start with Personal Data Encryption

An overview

Personal Data Encryption

Personal Data Encryption **leverages the protection of Windows Hello for Business** and adds upon it.

Personal data can now be **protected based on the user who is logged in** on a device.

Personal data is **protected at rest, at lock screen, and while another user is logged in**to a machine.

Personal Data Encryption **API allows for encryption of data** with LOB apps.

Requires Windows 11, version 22H2 and later

- Personal Data Encryption for known folders is only available on Windows 11, version 24H2 and later

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Prerequisites and recommendations

Personal Data Encryption

Device should be Microsoft Entra joined, or hybrid Microsoft Entra joined

Windows Hello for Business should be deployed

- FIDO2 is currently not supported, and Windows Hello for Business PIN reset service is enabled

Winlogon automatic restart sign-on feature disabled, and Windows Information Protection not enabled.

OneDrive should be installed and configured as a mechanism for personal data backup.

How does it differ from BitLocker?

Personal Data Encryption

Personal Date Encryption encrypts files instead of whole volumes and disks

Personal Data Encryption occurs in addition to other encryption methods such as BitLocker or Purview

Personal Data Encryption doesn't release data encryption keys until a user signs in using Windows Hello for Business

When a user logs off, decryption keys are discarded and data is inaccessible, even if another user signs into the device.

Allows for multi-user device scenarios

How does it differ from Purview?

Personal Data Encryption

Personal Data Encryption has the encryption stay with the device where it is enabled.

While Personal Data Encryption offers encryption down to the files on the device, it will not travel with those files.

Personal Data Encryption files are encrypted in a way where you either have access or you do not.

What are the different protection levels?

Personal Data Encryption

Personal Data Encryption uses AES-CBC with a256-bit key to protect content and offers developers the choice of configuring the behavior of PDE to use one of two levels of protection when they enrich their application using the PDE APIs. The level of protection is determined based on the organizational needs.

1

Level 1 (L1) protection: Protects PDE enabled content and requires the user to be logged on with Windows Hello for that user to access the data.

2

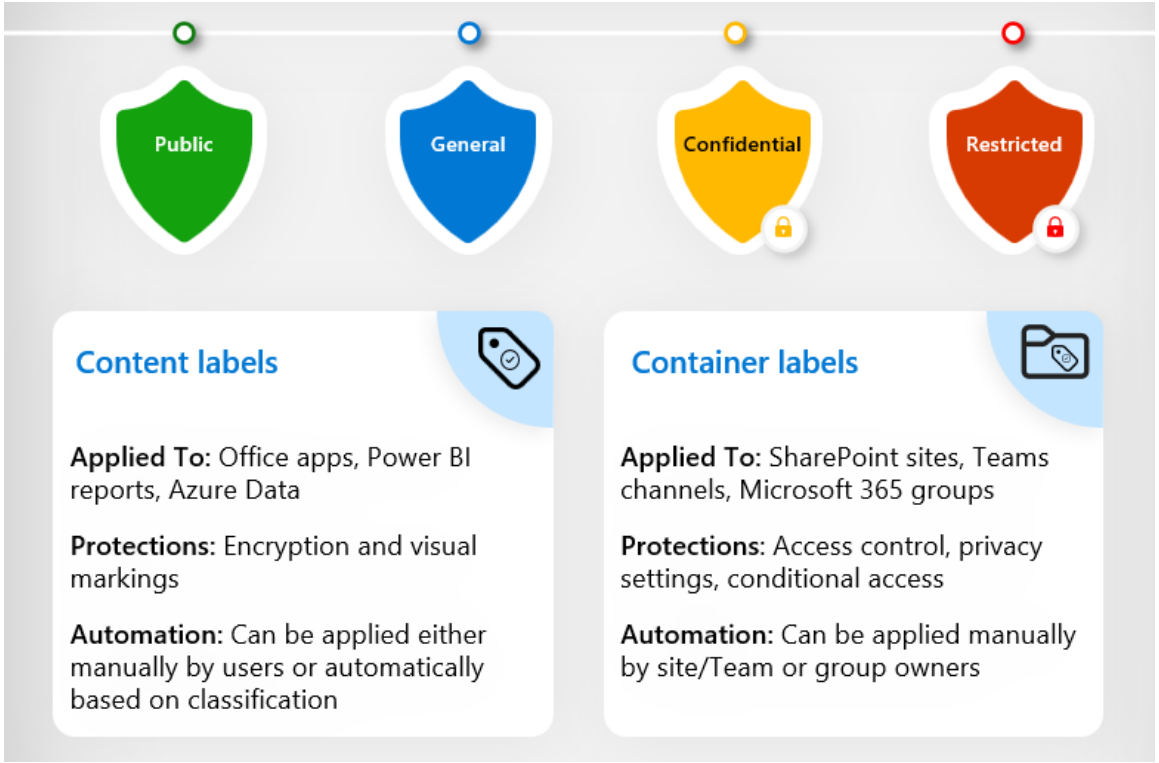
Level 2 (L2) protection: Protects PDE enabled content and requires the user to be logged on with Windows Hello for that user to access the data. Provides the additional protection that when the user is logged on, but the screen is locked, that the data is no longer accessible as the decryption key is removed from memory..

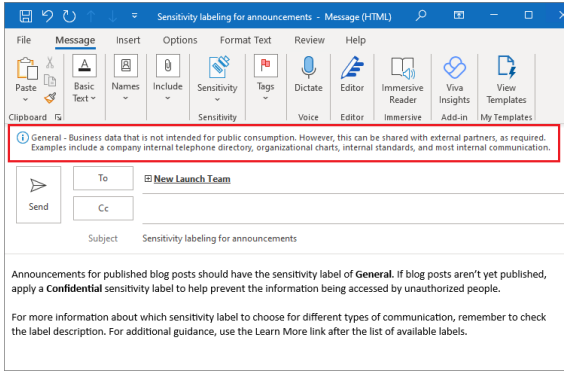
Demonstration

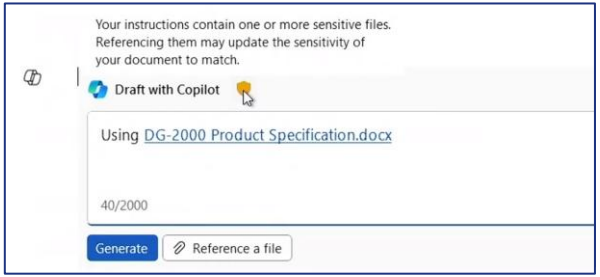
1. Configuring Personal Data Encryption
2. Looking at the sign-in experience
3. Looking at the file experience


Microsoft Purview

Sensitivity labels







Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

AutoSave On | Executive Salary 2024 | Confidential • Saved | Search | Liz Willets

File Home Insert Draw Page Layout Formulas Data Review View Automate Help | Comments | Share | Catch up

Paste | Aptos Narrow | 11 | Wrap Text | Merge & Center | General | Conditional Formatting | Format as Table | Cell Styles | Insert | Delete | Format | Sort & Filter | Find & Select | Sensitivity | Add-ins | Analyze Data | Copilot

Clipboard | Font | Alignment | Number | Styles | Cells | Editing | Sensitivity | Add-ins

RESTRICTED ACCESS Permission is currently restricted. Only specified users can access this content. Change Permission...

M5

	A	B	C	D	E
1		Base	Bonus	Stock	Total
2	Liz	$2,000,000	$500,000	$600,000	$3,100,000
3	Anna	$2,500,000	$625,000	$750,000	$3,875,000
4	Bob	$1,800,000	$450,000	$540,000	$2,790,000
5	Jeff	$1,950,000	$487,500	$585,000	$3,022,500
6	Joe	$1,500,000	$375,000	$450,000	$2,325,000
7	Jane	$1,750,000	$437,500	$612,500	$2,800,000

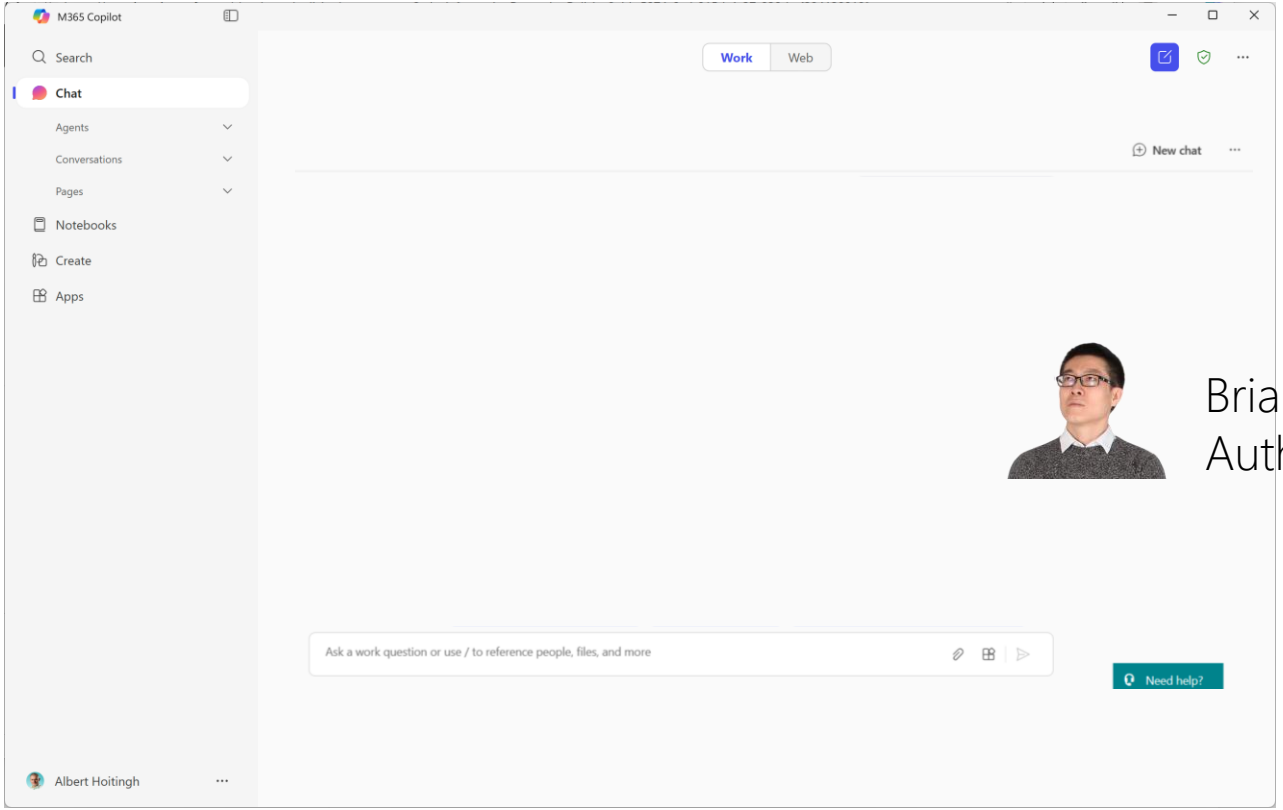
Liz – author - authorized

Brian – reader - authorized

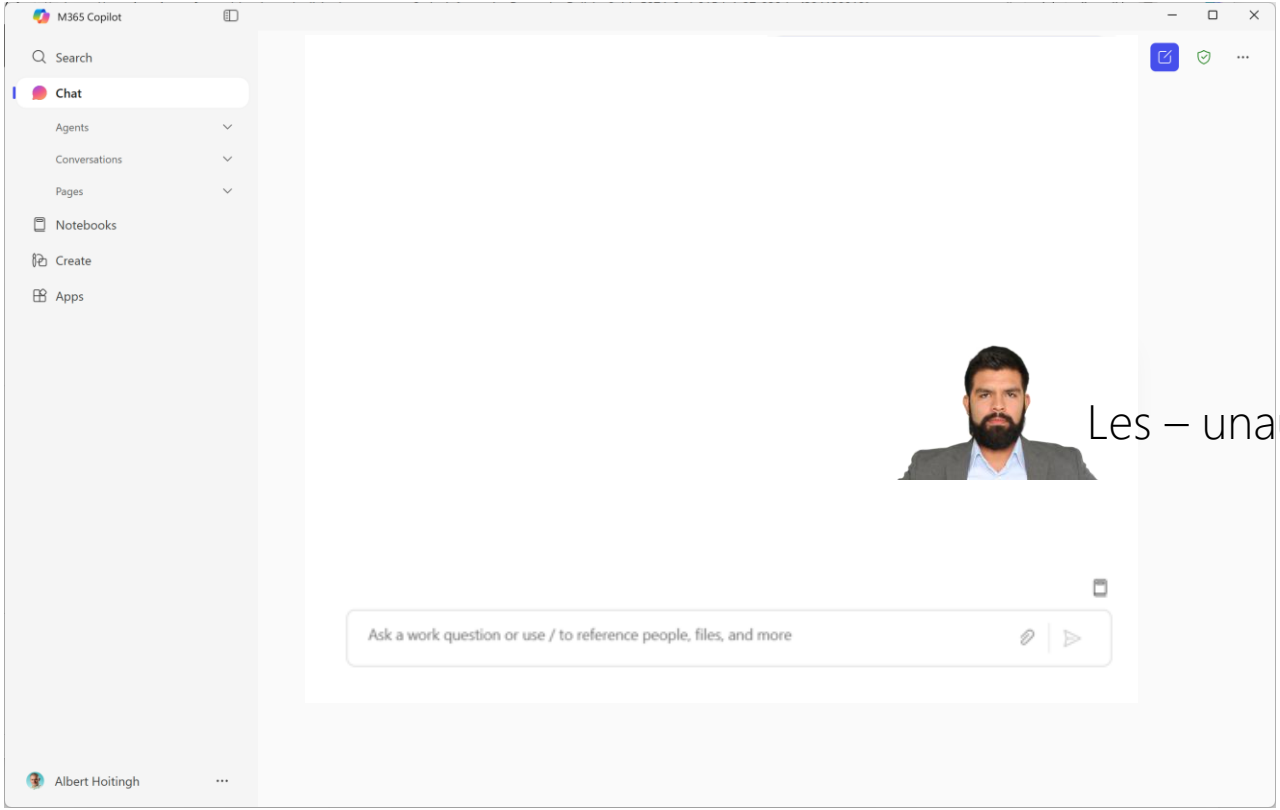
Les – unauthorized

Sheet1

Ready | Accessibility: Good to go | Display Settings | 100%



Brian – Authorized



Les – unauthorized

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Microsoft Purview Endpoint DLP

An overview

Microsoft Purview Endpoint DLP

Microsoft 365

Cloud DLP – Service based

An overview

Microsoft Purview Endpoint DLP

Device should be Microsoft Entra joined, hybrid Microsoft Entra joined or registered

Endpoint DLP extends DLP functions to Windows and MacOS devices

Monitors and restricts actions like copying, transferring, or sharing sensitive data

Integrated with Microsoft Information Protection (MIP) and Insider Risk Management

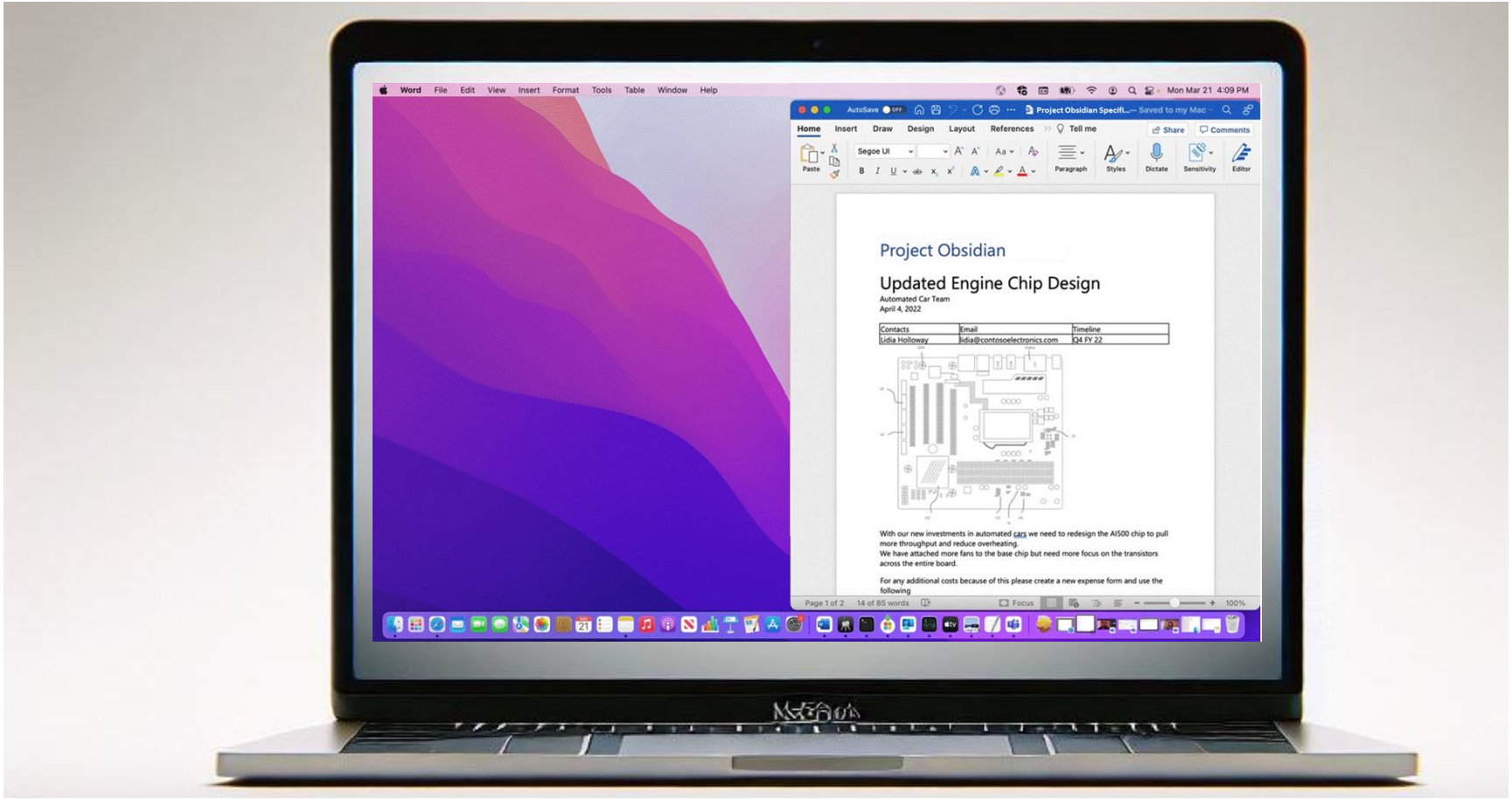
Demonstration

1. Microsoft Purview Endpoint DLP in action - Windows
2. Microsoft Purview Endpoint DLP in action - MacOS
3. Configuring Microsoft Purview Endpoint DLP

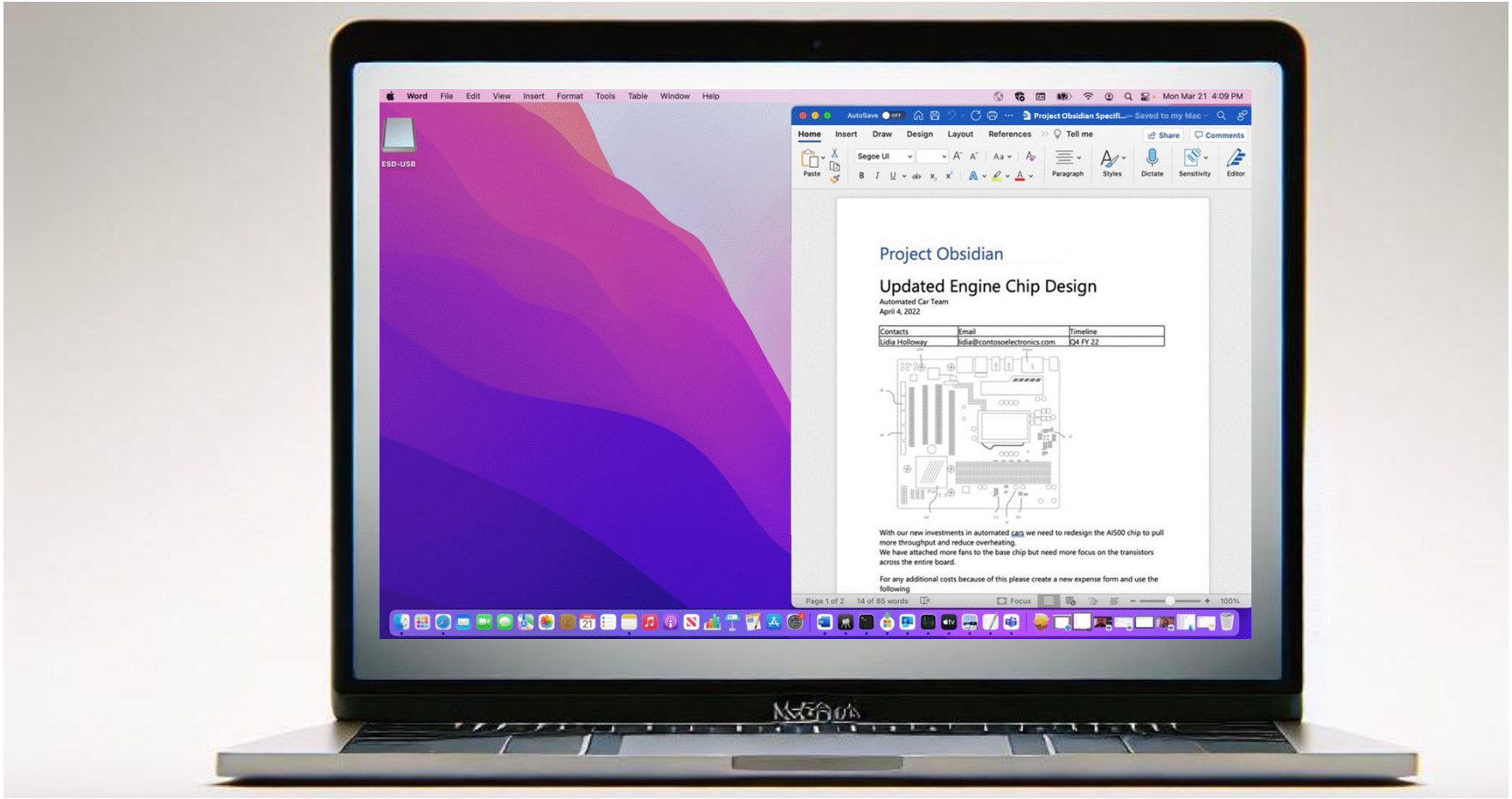
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

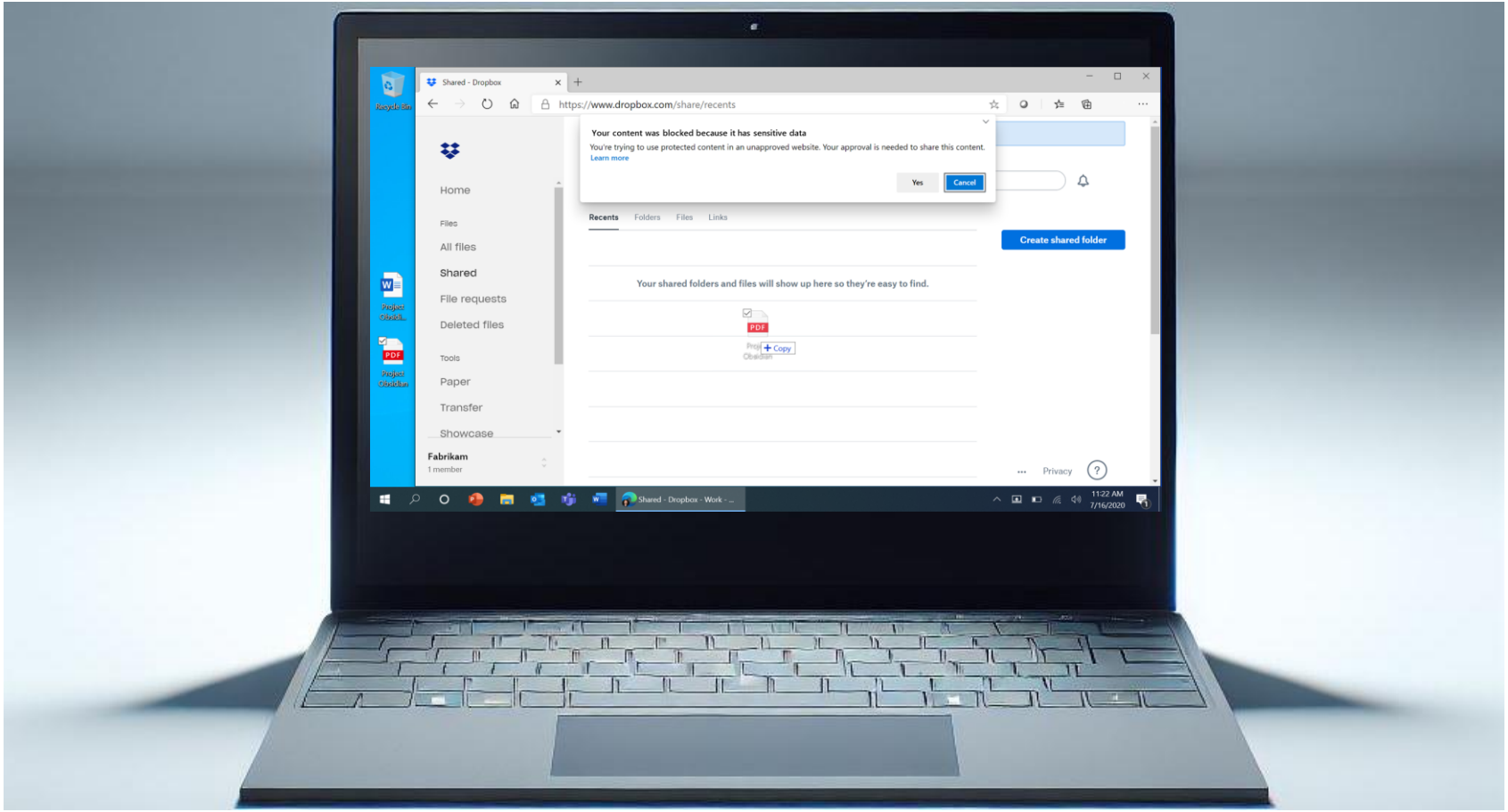
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



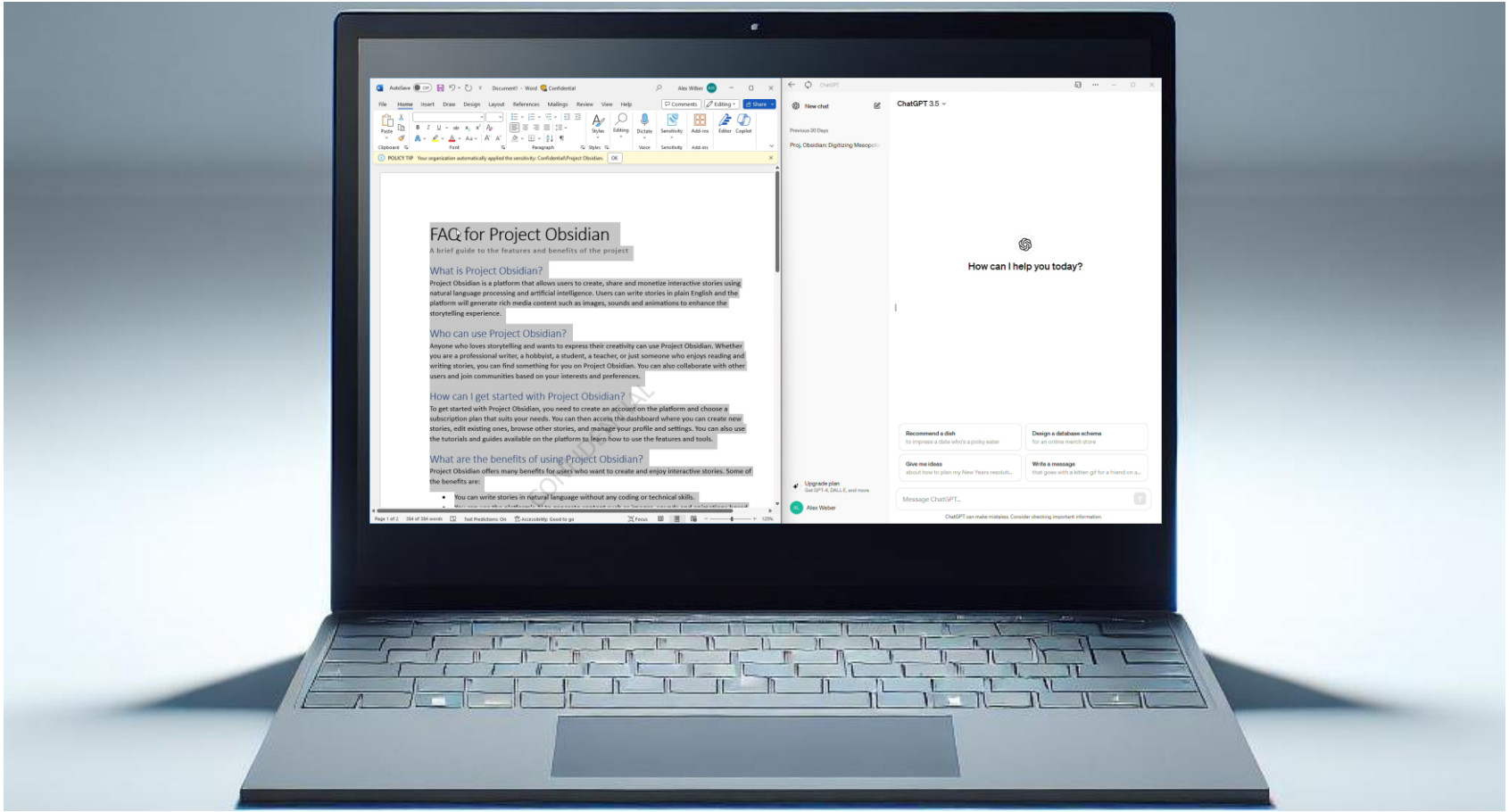
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



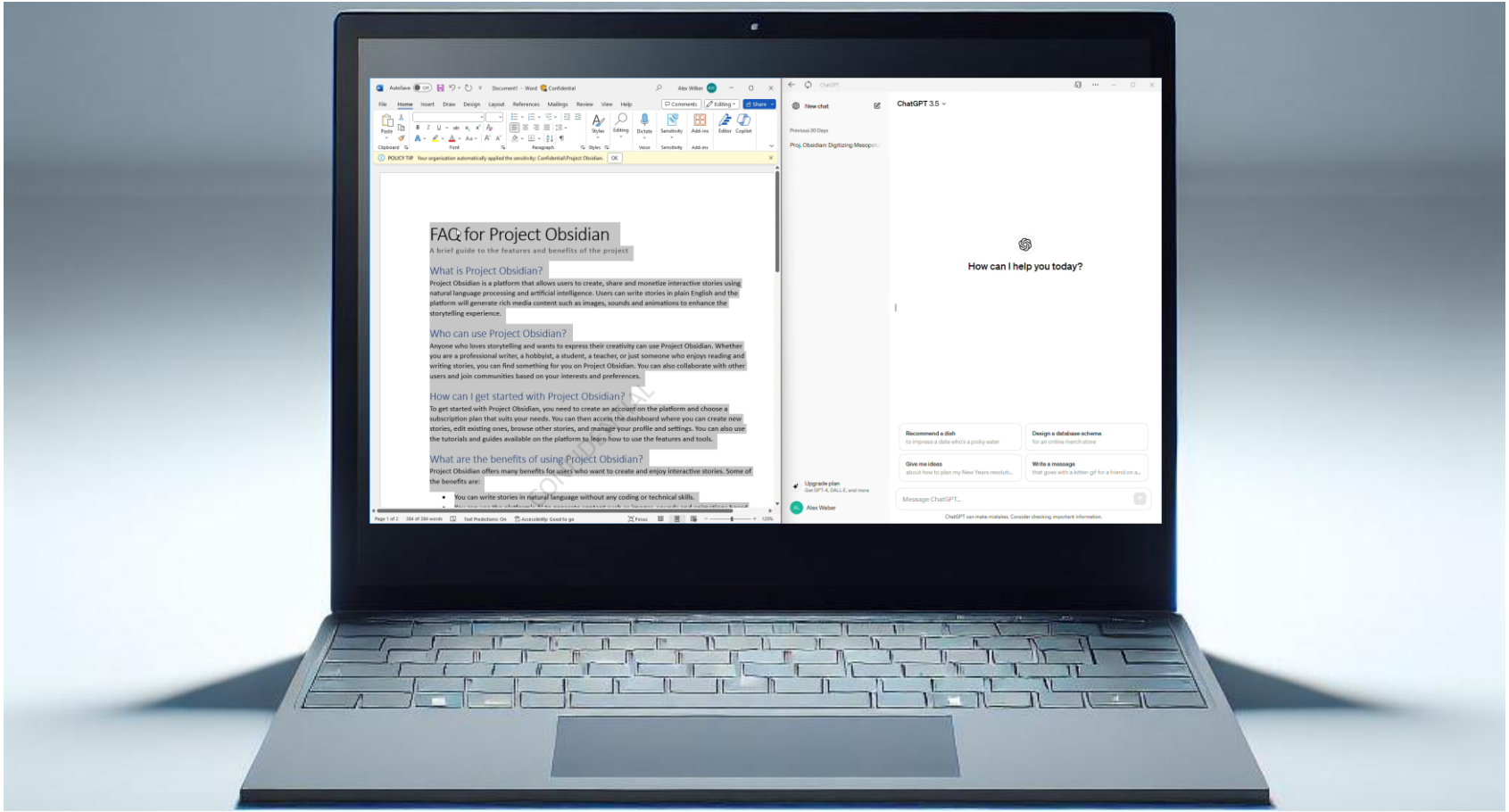
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



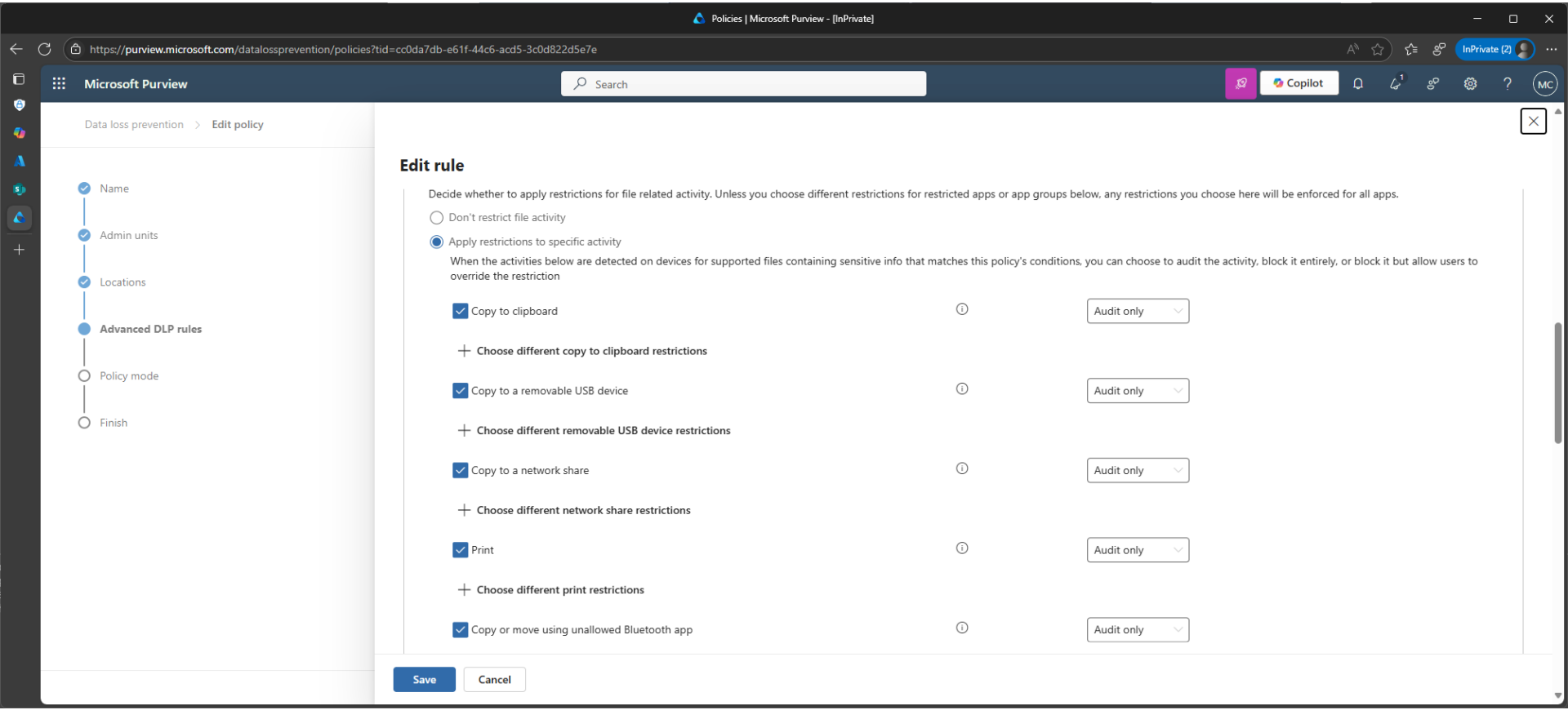
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



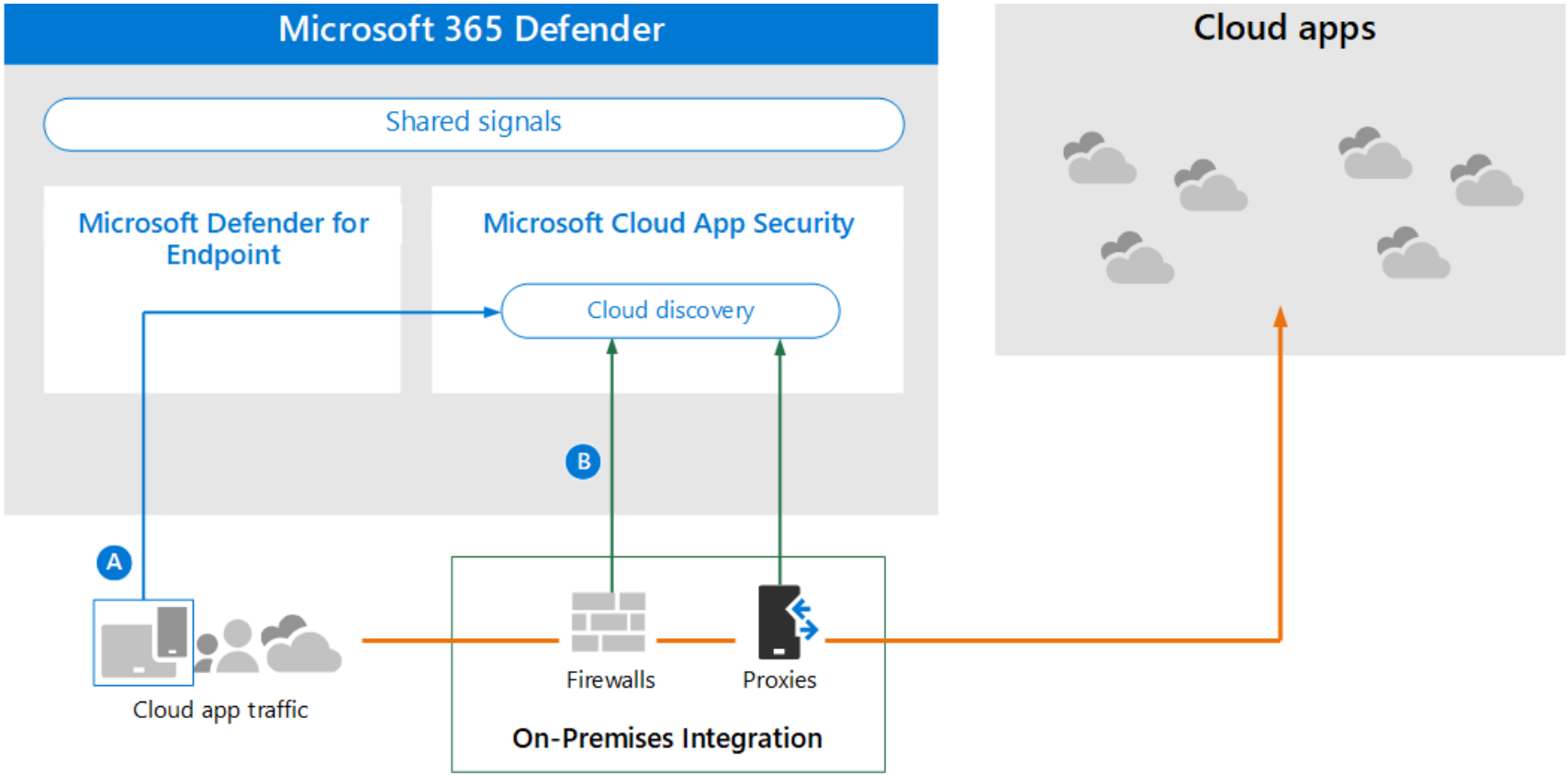
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



Defender for Cloud Apps



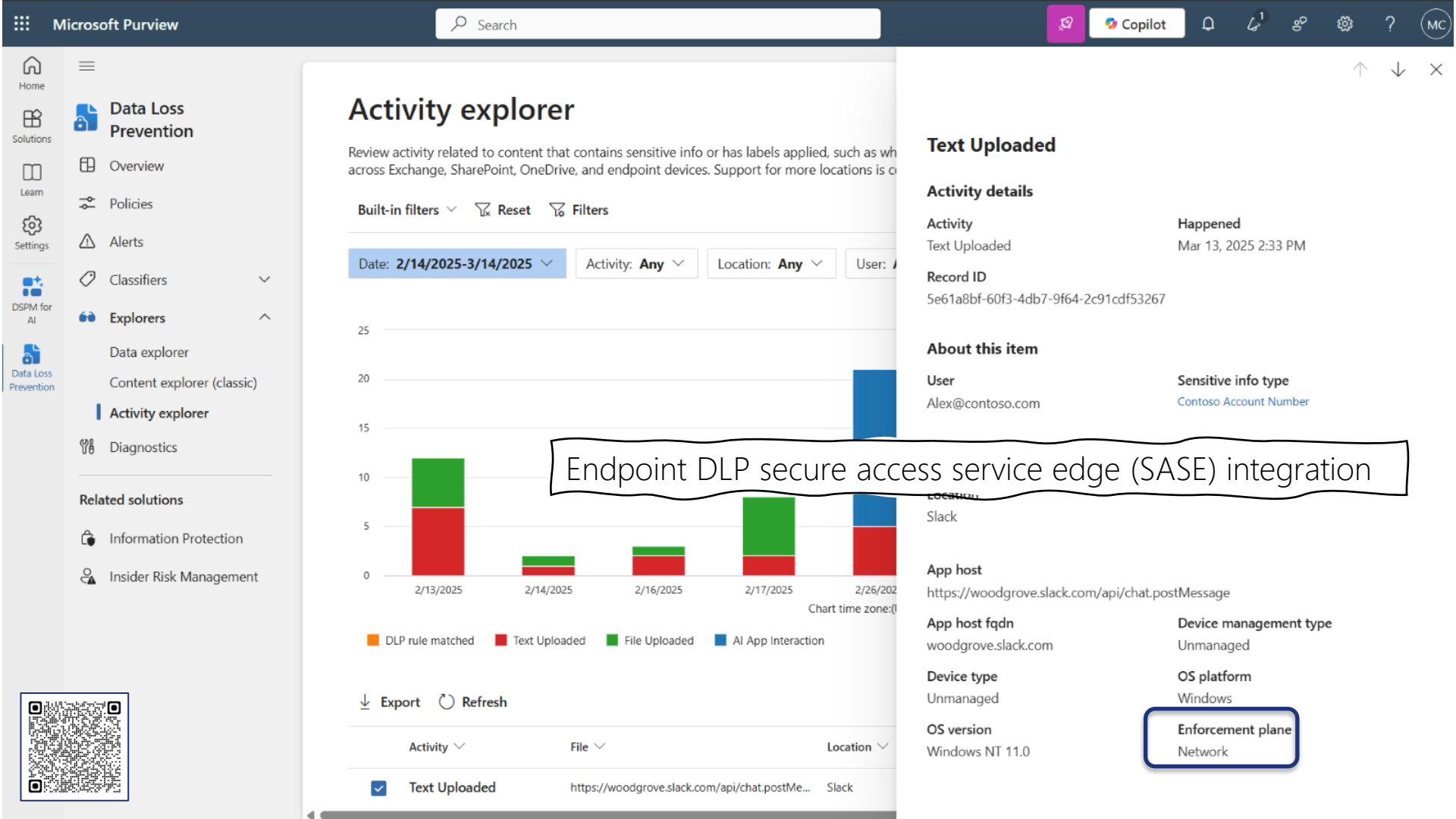
Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

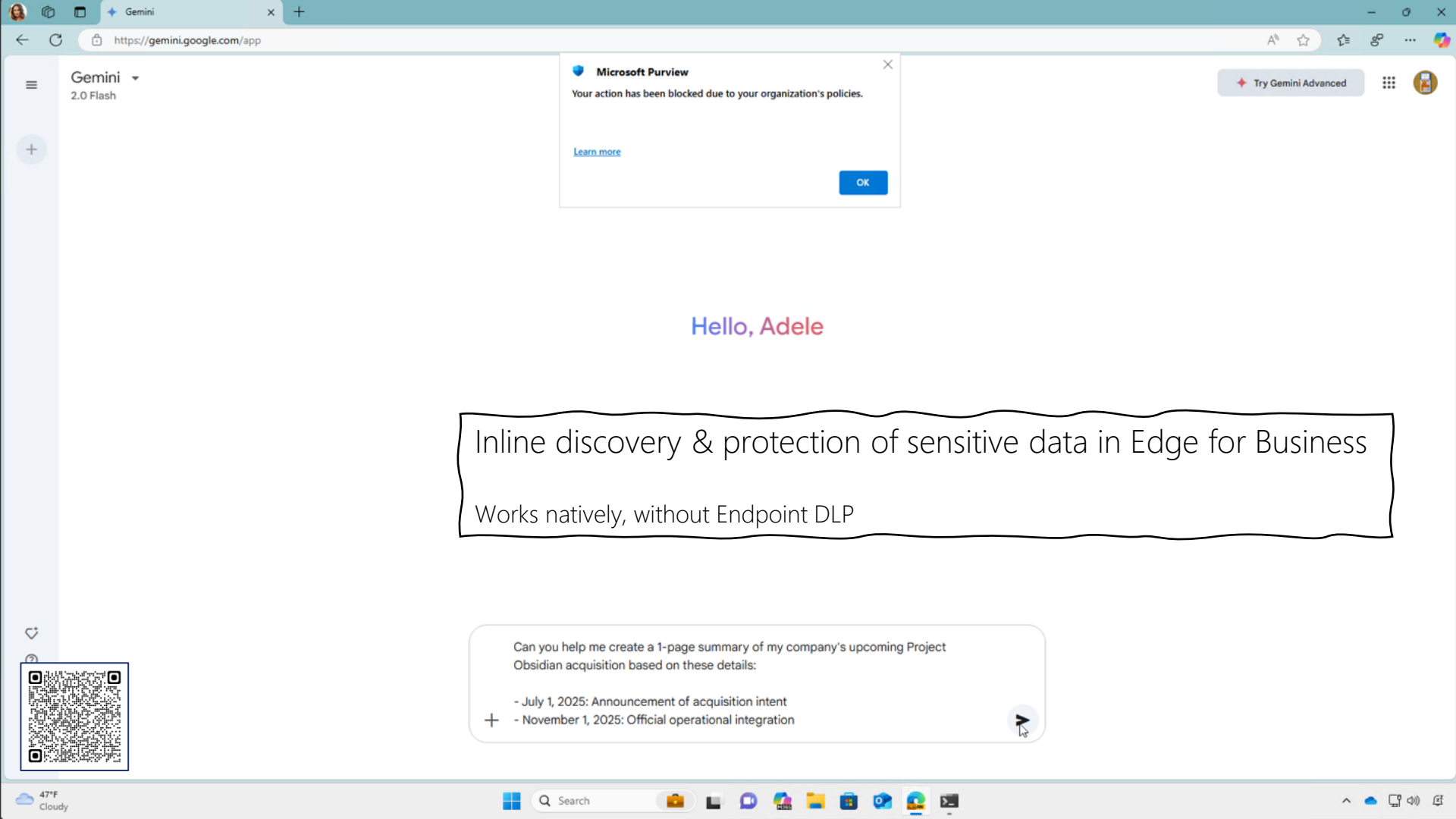
Demonstration

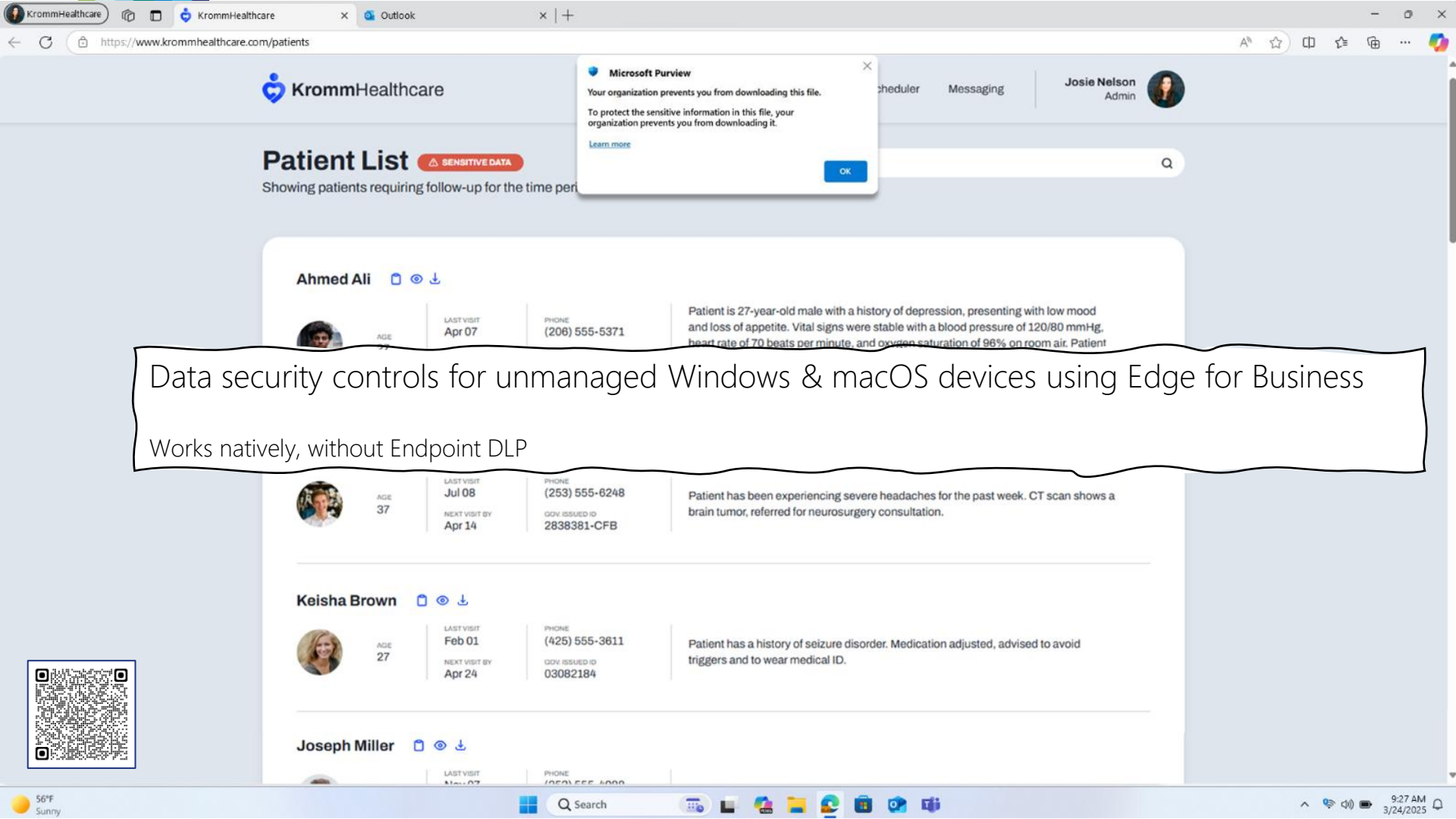
1. Blocking SharePoint Online downloads - user
2. Configuring Microsoft Defender for Cloud Apps Session settings and policies
3. Blocking SharePoint Online downloads - admin

Preview news


Microsoft Purview

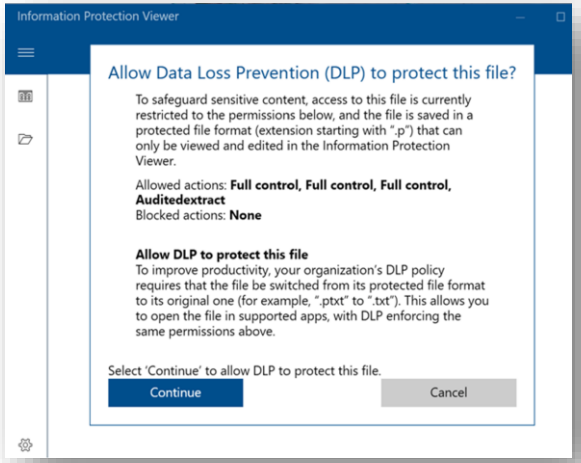

Microsoft Purview
Search
Copilot
Home
Solutions
Learn
Settings
DSPM for AI
Data Loss Prevention
Data Loss Prevention
Overview
Policies
Alerts
Classifiers
Explorers
Data explorer
Content explorer (classic)
Activity explorer
Diagnostics
Related solutions
Information Protection
Insider Risk Management
Activity explorer
Review activity related to content that contains sensitive info or has labels applied, such as wh
across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is c
Built-in filters
Reset
Filters
Date: 2/14/2025-3/14/2025
Activity: Any
Location: Any
User:
25
20
15
10
5
0
2/13/2025
2/14/2025
2/16/2025
2/17/2025
2/26/202
Chart time zone:(
DLP rule matched
Text Uploaded
File Uploaded
AI App Interaction
Export
Refresh
Activity
File
Location
Text Uploaded
https://woodgrove.slack.com/api/chat.postMe...
Slack
Text Uploaded
Activity details
Activity
Text Uploaded
Happened
Mar 13, 2025 2:33 PM
Record ID
5e61a8bf-60f3-4db7-9f64-2c91cdf53267
About this item
User
Alex@contoso.com
Sensitive info type
Contoso Account Number
Endpoint DLP secure access service edge (SASE) integration
Slack
App host
https://woodgrove.slack.com/api/chat.postMessage
App host fqdn
woodgrove.slack.com
Device management type
Unmanaged
Device type
Unmanaged
OS platform
Windows
OS version
Windows NT 11.0
Enforcement plane
Network

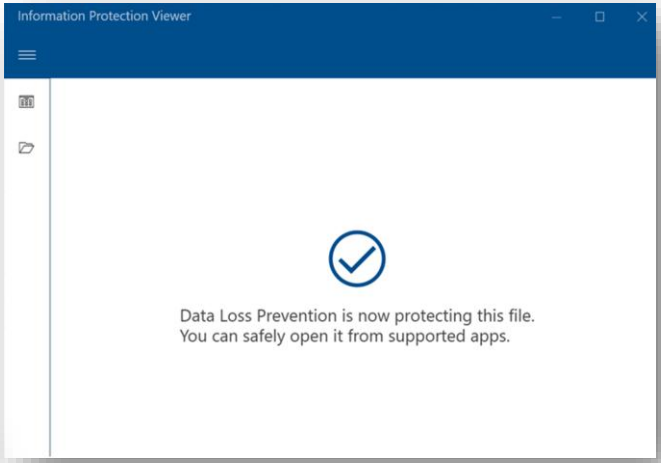

Gemini
https://gemini.google.com/app
Gemini
2.0 Flash
Microsoft Purview
Your action has been blocked due to your organization's policies.
Learn more
OK
Try Gemini Advanced
Hello, Adele
Inline discovery & protection of sensitive data in Edge for Business
Works natively, without Endpoint DLP
Can you help me create a 1-page summary of my company's upcoming Project Obsidian acquisition based on these details:
- July 1, 2025: Announcement of acquisition intent
- November 1, 2025: Official operational integration
47°F
Cloudy
Search

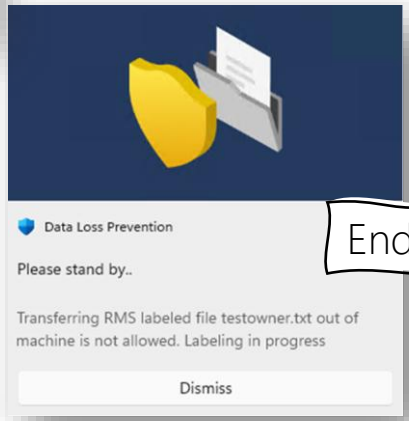


Data security controls for unmanaged Windows & macOS devices using Edge for Business

Works natively, without Endpoint DLP



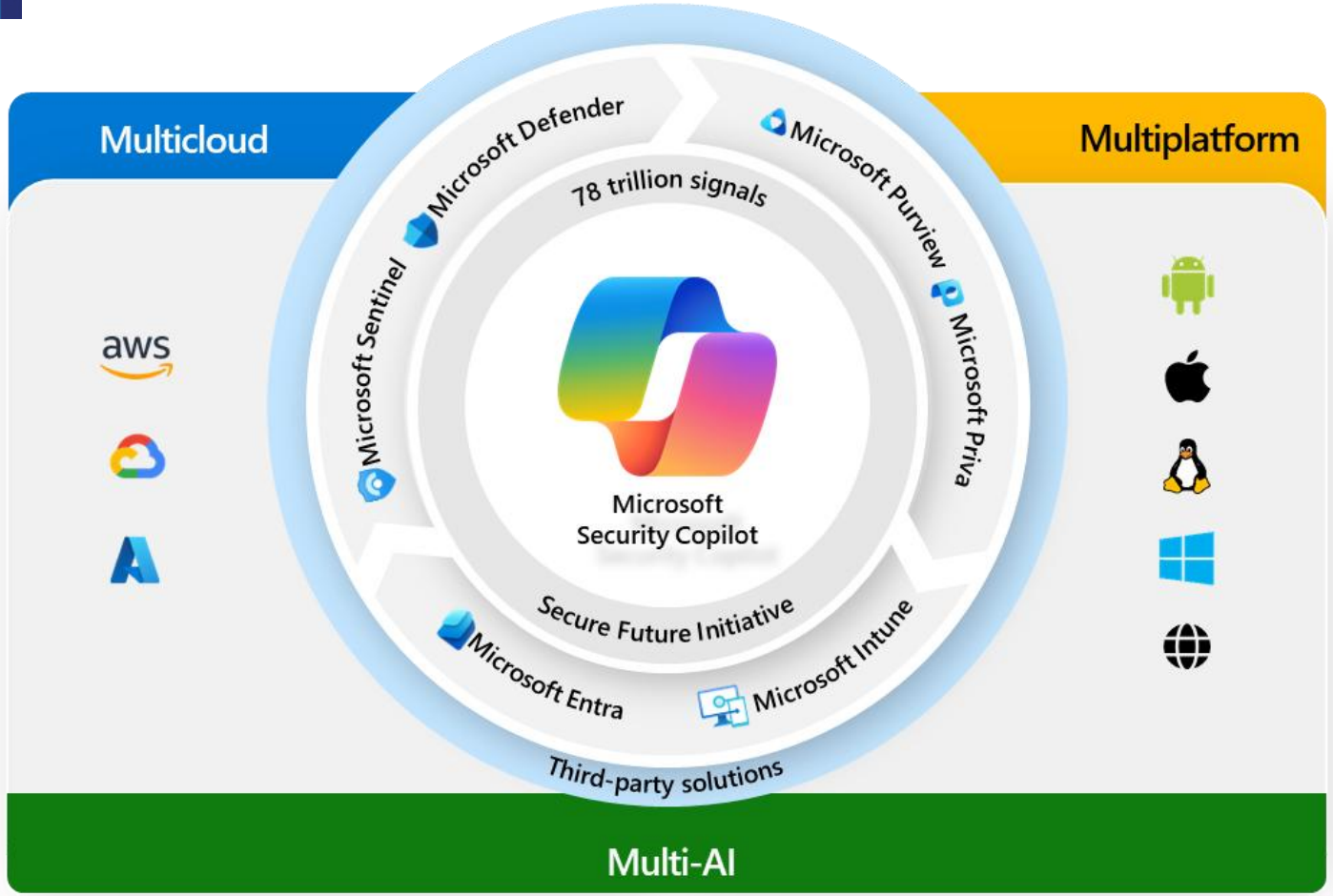




Endpoint DLP – non Office/PDF file protection

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

How do the different options for protecting corporate data compare



Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Defender vs. DLP vs. Edge for Business

Defender for Cloud Apps

Cloud-native Saas Protection

Shadow IT discovery, app governance, DLP

Cloud app data location

Cloud based deployment

Saas risk management and governance

Endpoint DLP

Endpoint level data protection

Prevent data exfiltration from devices

Local files, clipboard, USB, print, network share

Requires devices onboarding and MDE agent

Insider risk and endpoint data protection

Edge for Business

Browser-level protections, especially for AI interactions

Build-in Edge for Business, does not require Endpoint DLP

Only requires sing-in to Edge for Business

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Choose where to apply the policy

Let us know what type of data you want your policy to cover, and we'll guide you through a tailored setup experience. Learn more about these options.

- ◯ **Data stored in connected sources**
  Protect data that's stored in sources connected to your org, either automatically (like Microsoft 365 data sources) or manually (like managed devices). Policies scoped to connected data sources protect data-at-rest and data-in-use.
- ◯ **Data in browser and network activity**
  Protect data in cloud apps as its actively being used in browser and network activities. Policies scoped to cloud apps apply real-time protection to data-in-motion.

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

BitLocker vs. PDE vs. Purview

BitLocker

Disk encryption to protect the data on the device

Personal Data Encryption

Data encryption to protect the personal data on the device

Purview

Data encryption that follows the data to protect the data

Data protection to prevent data loss

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

Please evaluate this session in the App.

THANK YOU

Are there any questions?

Next session 14:00 – 14:50

Onboarding Like a Pro: Autopilot and Password-less for Secure and User-Friendly Excellence