



NIC Cloud
Connect

Oslo Spektrum
November 7 - 9

Crouching Tiger, Hidden Data. What's New in Microsoft 365 Security & Compliance

Andy Malone MVP

Visit my YouTube Channel @AndyMaloneMVP



This Session we'll Discuss ...



Identity



Security



Compliance



“This place is Going to the Dogs ...”

- Increased attacks on Critical Infrastructure Targets by Nation State Actors (Russia, Ukraine Conflict)
- Theft of Documents in transit via document transfer Systems (MoveIT Cyber attack)
- Attacks on Apps & App dev platforms. Malware found in over 190 Android apps on Google Play store (SpinOK malware is easily spread as it poses as a legitimate (SDK)
- Hackers continue to target Hybrid cloud, In particular remote workers & attacks on corporate networks
- Ransomware Continues to generate millions. A favorite of nation states
- Social engineering continues to successfully target the human element
- A.I Will become a major attack tool



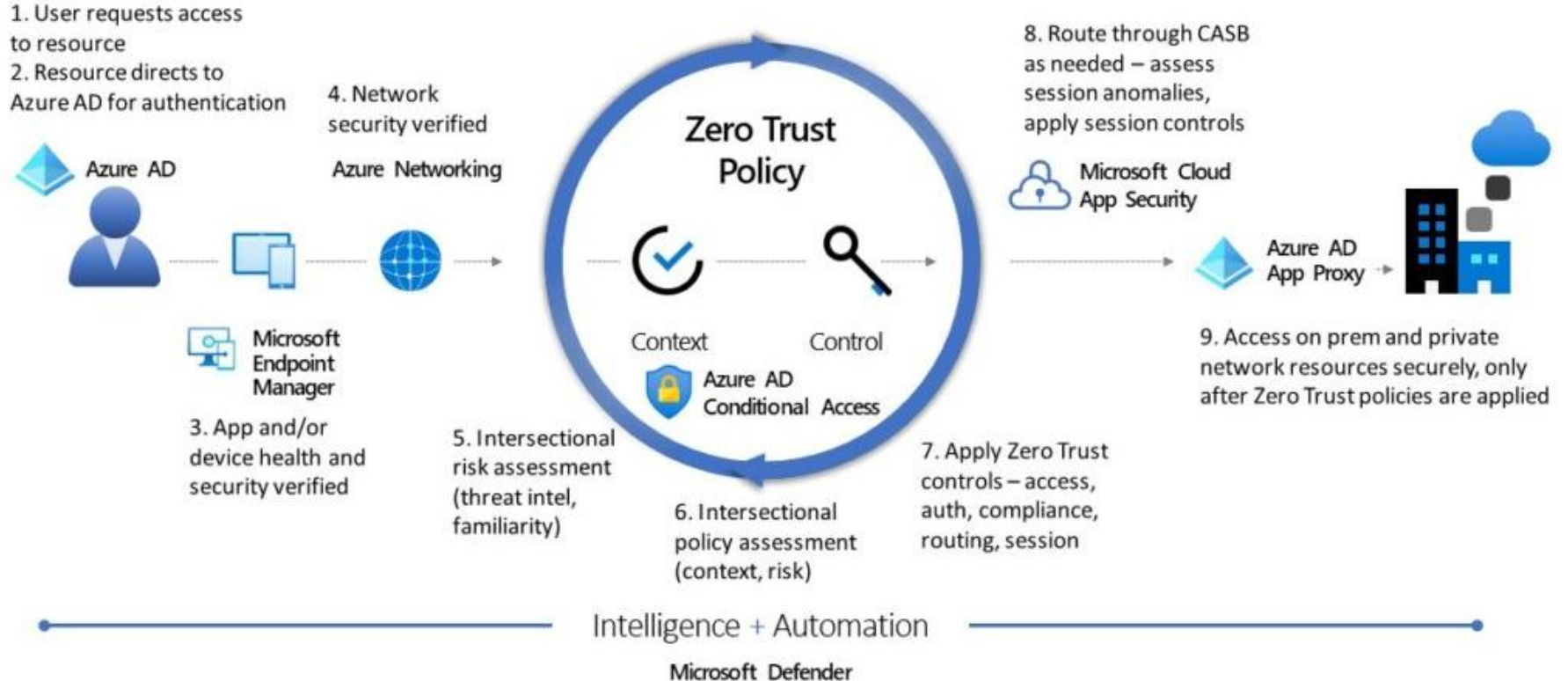
Zero Trust

Use the Principle of Always
Verify
Least Privilege
Assume Breach

“There’s always one rat.”



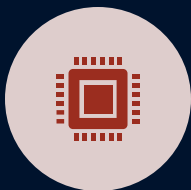
Why Zero Trust Works!



Identity is the First Line of Defence



New Entra ID Innovations



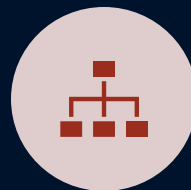
PASKEY SUPPORT
(PHISHING RESISTANT
MFA)



IDENTITY PROTECTION
NEW FEATURES



ENTRA ID TIME BASED
DYNAMIC GROUPS



RESTRICTED
MANAGEMENT ADMIN
UNITS

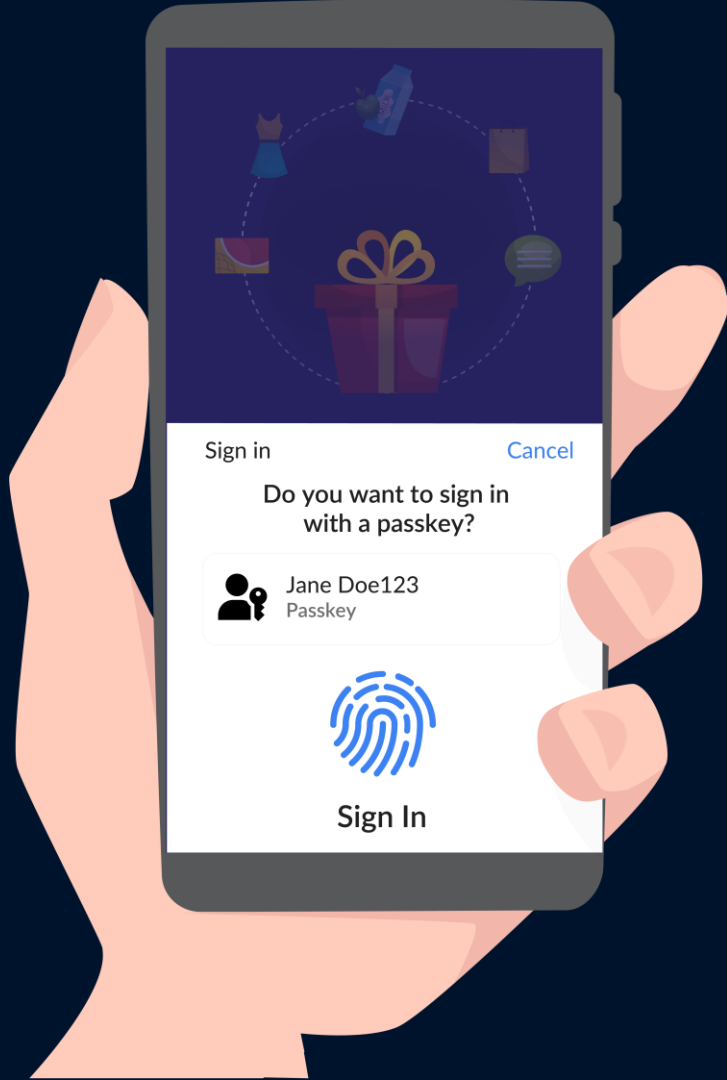


CONDITIONAL ACCESS
TOKEN BINDING
PROTECTION

Demo

1. Identity Protection New Features
2. Entra ID Time Based Dynamic groups
3. Restricted Management Admin Units
4. Conditional Access Token Binding
Protection

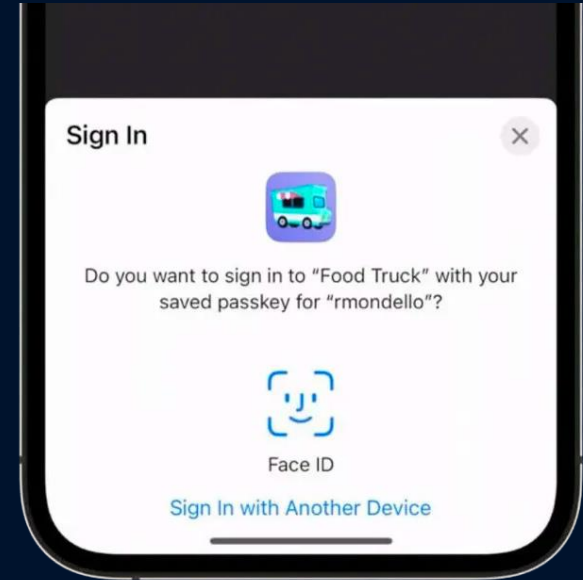




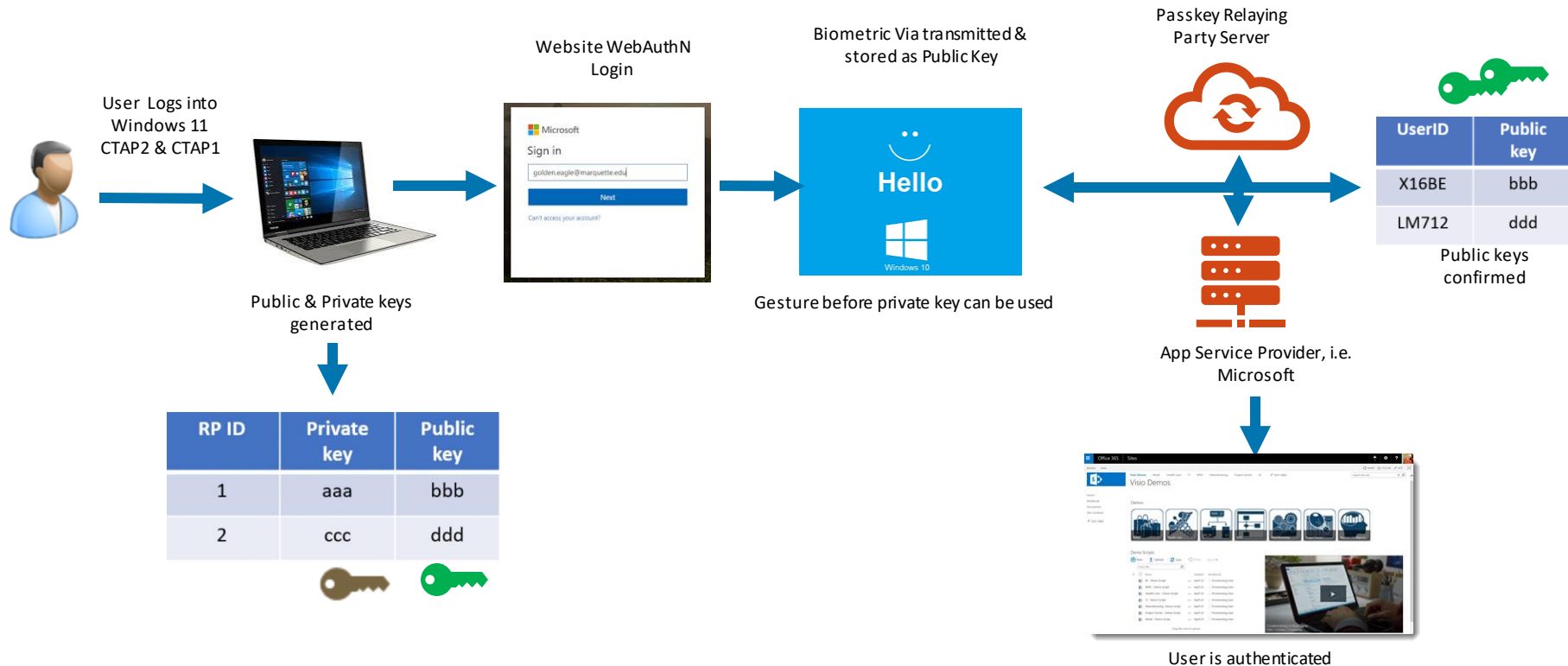
Introducing Passkeys

Introducing Passkeys

- Based on FIDO Standards
- A replacement for Passwords & provide faster, easier and more secure sign-ins to Websites & Apps
- Simplify account registration for apps & websites & work across multiple devices in close proximity
- Unlike passwords that are sent to an authenticating server, a passkey never leaves the user's device to sign in the user
- Creates a unique cryptographic key pair. Private keys NEVER leave the device. A biometric gesture is also required.
- Now incorporated in Windows 11

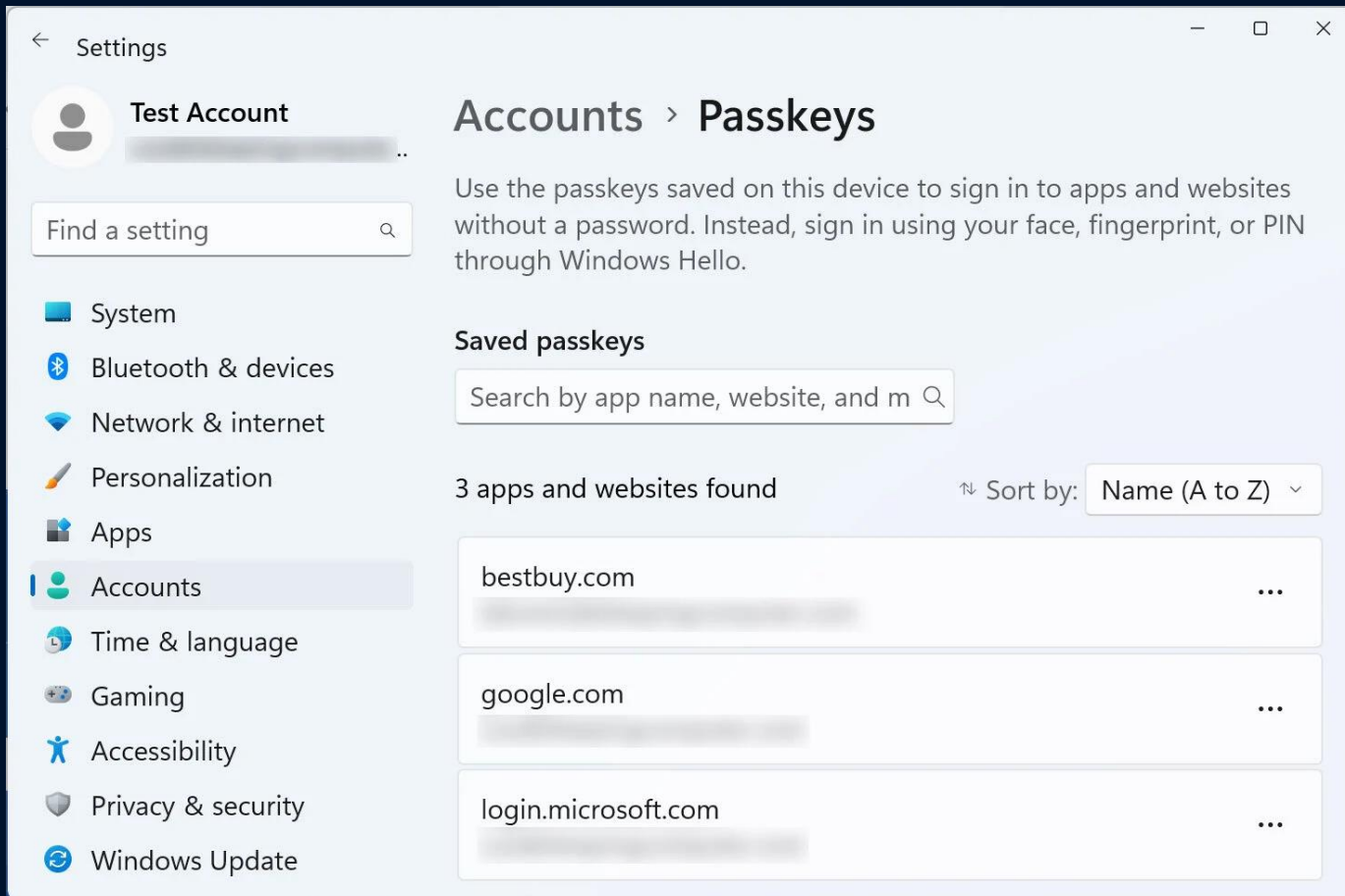


How do Passkeys work?



CTAP = Client to Authenticator Protocol
WebAuthN Web Authentication Protocol

Windows 11 is Passkey Ready



Demo

Passkeys



What is a passkey?

A passkey is a [new way to sign in](#) that works completely [without passwords](#). By using the security capabilities of your devices like Touch ID and Face ID, passkeys are way [more secure](#) and [easier to use](#) than both passwords and all current 2-factor authentication (2FA) methods.

#1 PRODUCT OF THE WEEK
User Experience

Try the passkey demo

How to use the demo? [Learn more.](#)

Sign in or sign up

hickardJ@M365x93168372.onmicrosoft.com

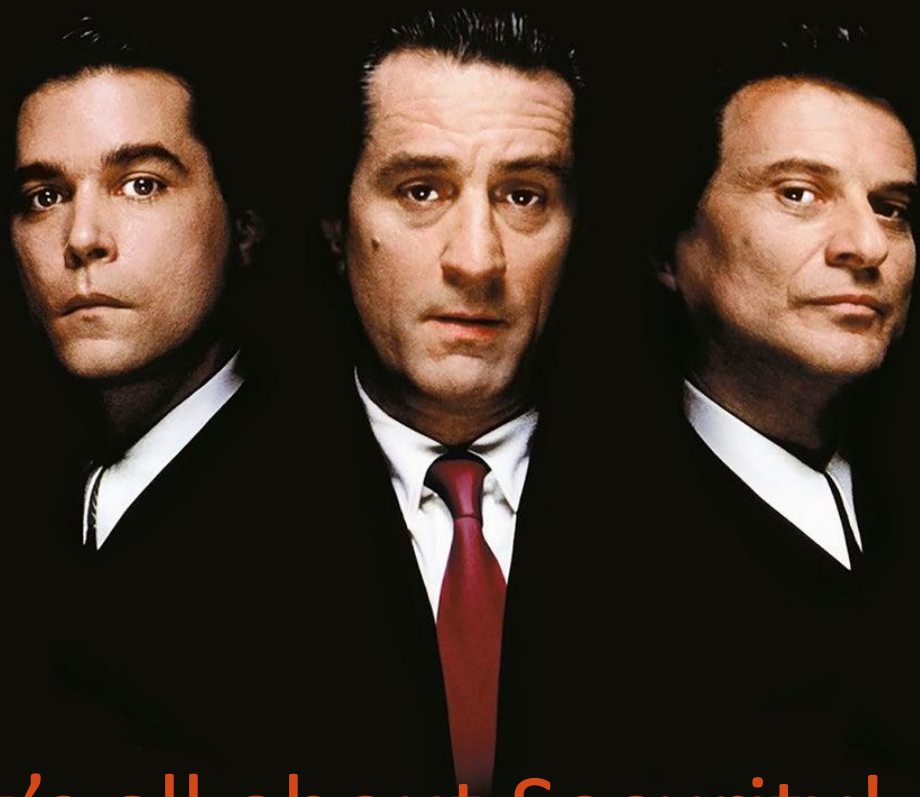
Continue

or

Sign in with a passkey

[Data privacy](#)

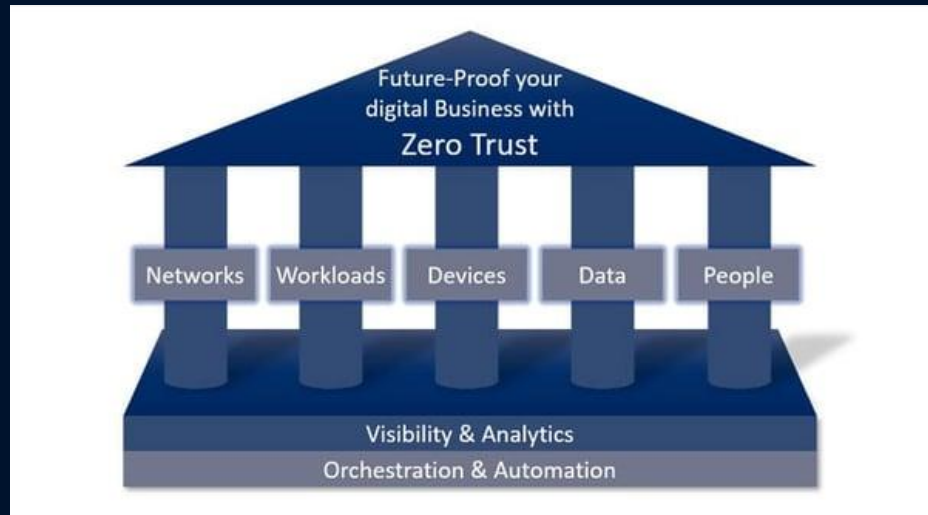
Powered by [Hanko.io](#)



It's all about Security!

Remember - The Zero Trust model

- Zero Trust guiding principles
 - Verify explicitly
 - Least privileged access
 - Assume breach
- Six foundational pillars
 - **Identities** may be users, services, or devices.
 - **Devices** create a large attack surface as data flows.
 - **Applications** are the way that data is consumed.
 - **Data** should be classified, labeled, and encrypted based on its attributes.
 - **Infrastructure** whether on-premises or cloud based, represents a threat vector.
 - **Networks** should be segmented.



Microsoft Defender

The Complete Security Solution

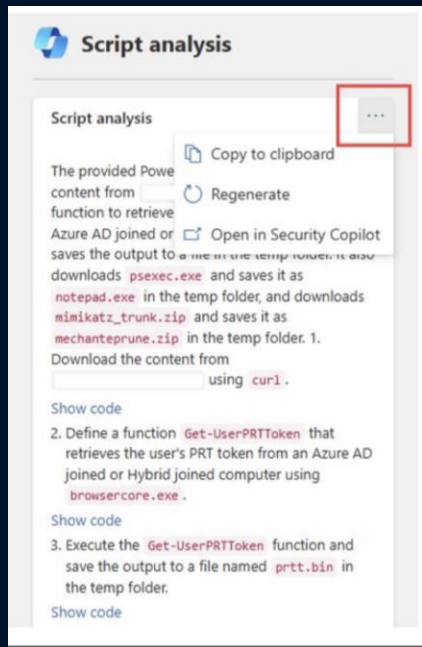
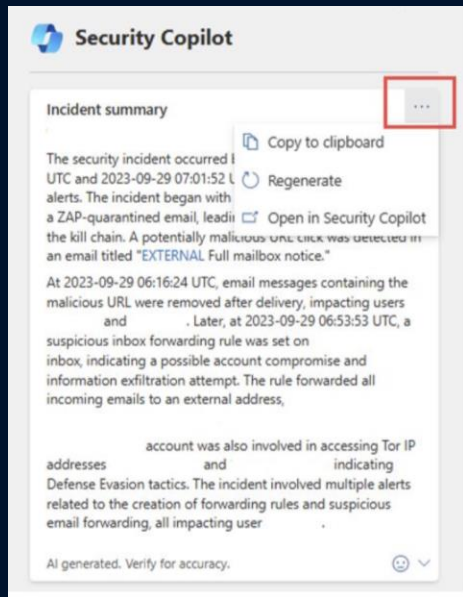
- Microsoft Encryption Solutions
- Defender for 365
- Defender for Endpoint
- Defender for CloudApps
- Defender for Identity
- Defender for Cloud
 - Databases, IoT, Storage, Compute Etc.
- Microsoft Sentinel



Microsoft Defender

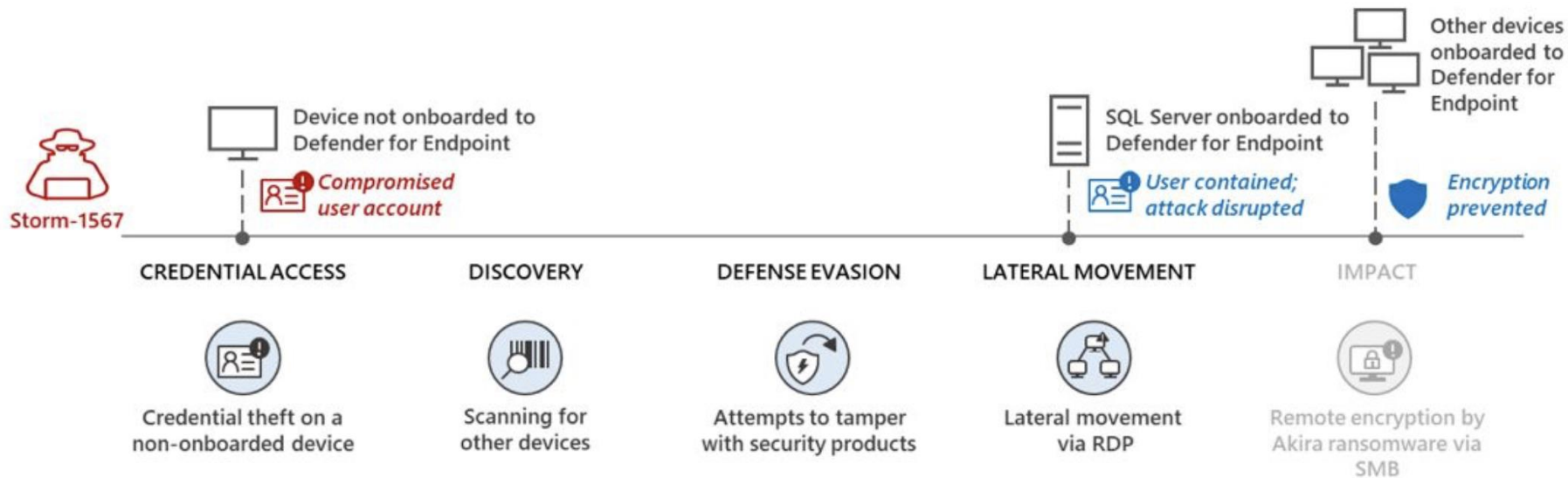
New Features

- Improved Integrated Reporting
- Device Tamper Protection
- Priority Account Protection
- New Customized Email Notification Rules
- Improved Oauth App Reporting
- Improved Threat Intelligence
- Microsoft Security Copilot integration within Microsoft 365 Defender & Sentinel



Microsoft Defender

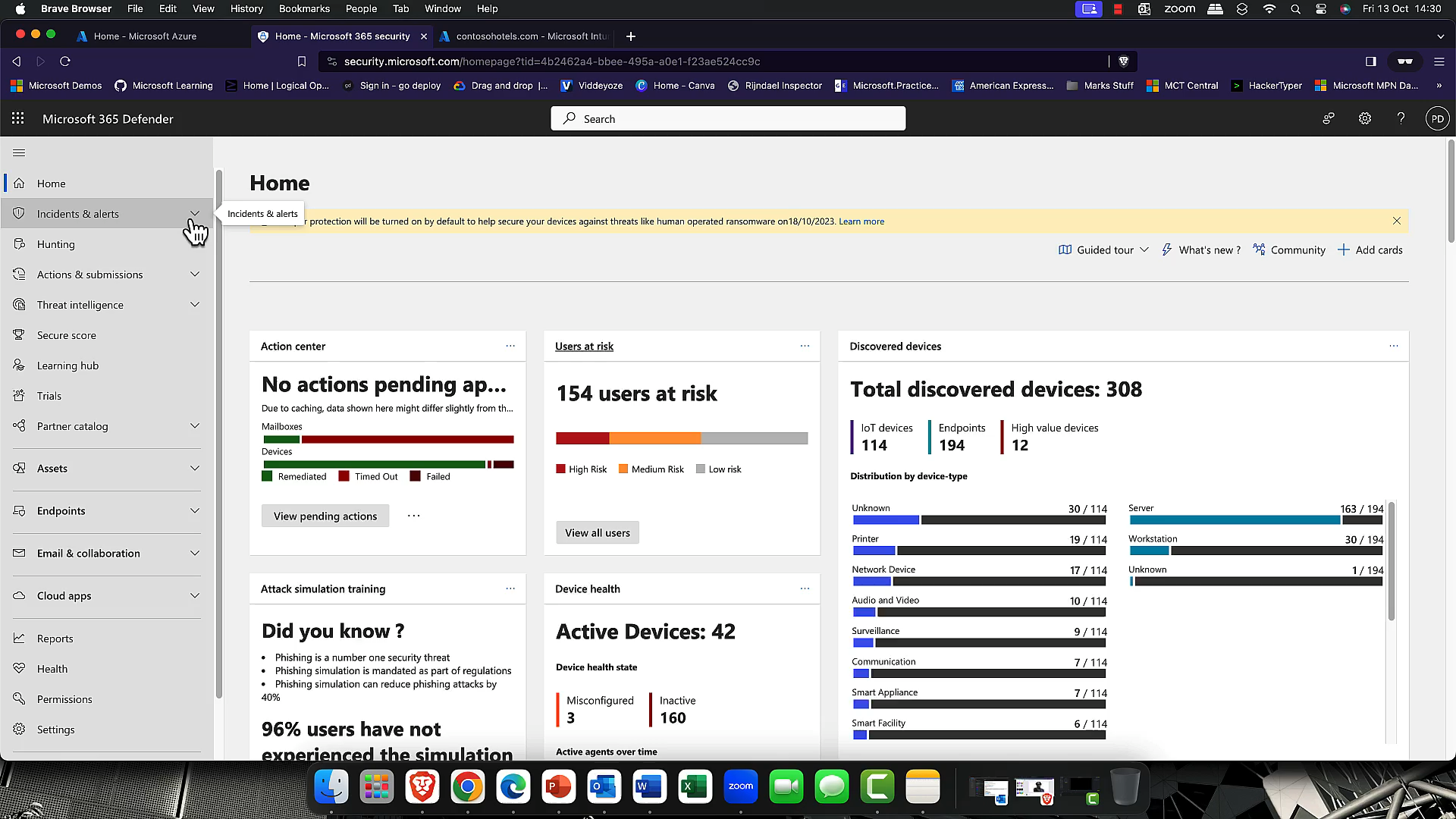
Auto Remediation from Ransomware



Demo

Microsoft Defender Security Solutions
Keeping the Bad Guy Out





What about Compliance?

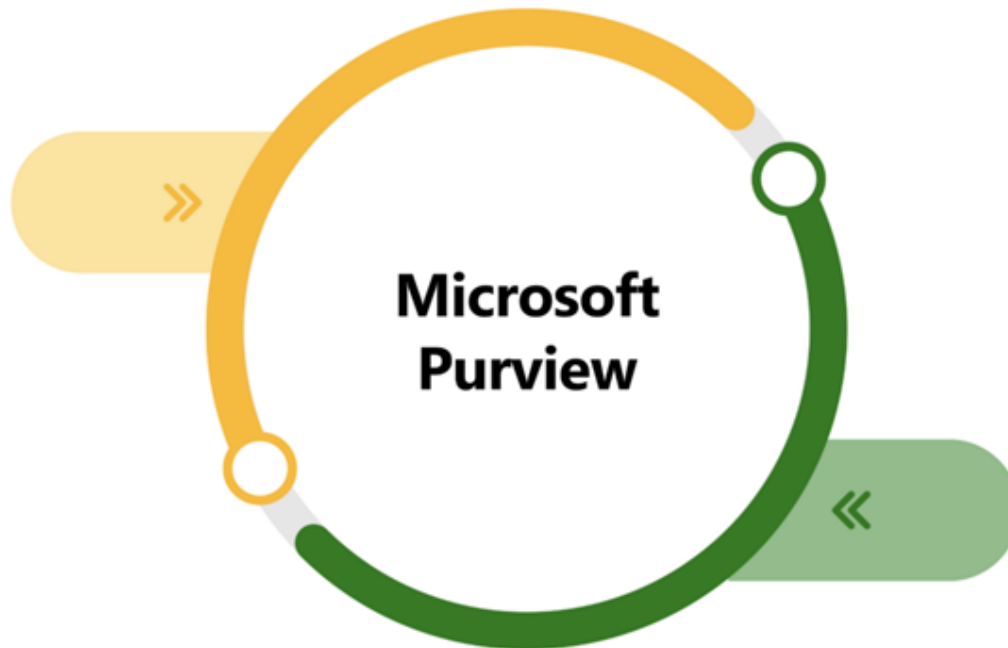


“We need to keep this hush hush”

Microsoft Purview Compliance Solutions

Risk & compliance

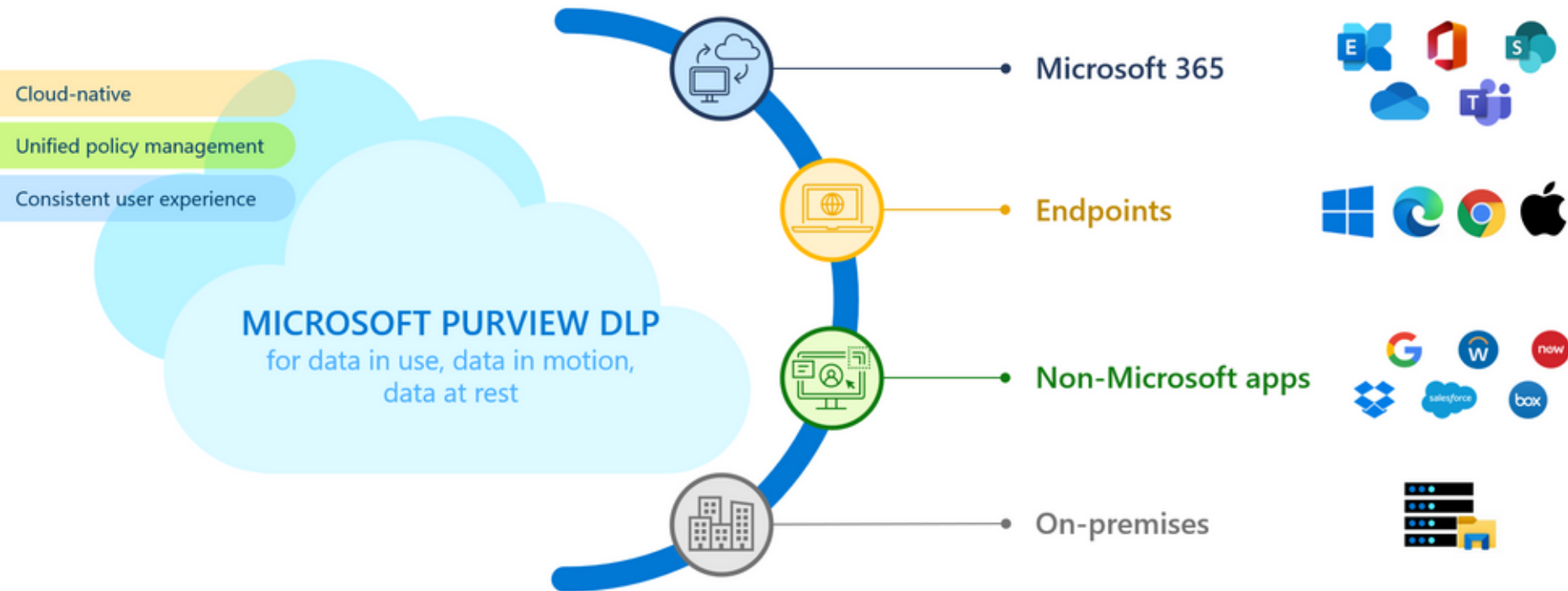
For risk, compliance,
and legal teams



Unified data governance

For data consumers, data
engineers, data officers

Microsoft Purview Data Loss Prevention



Microsoft Purview Information Protection

PHASE 1 Know Your Data

1. SENSITIVE INFO TYPES (SITs)

SITs are the PII patterns that you can look for in your data.

- What info do you need to protect?
- Is it a built-in or a custom SIT?
- Who should access this PII?

2. CONTENT EXPLORER

Find out which PII you have and where they're stored.

- Where are files with PII stored?
- Do you need to restructure your files access?
- What are the file formats?

3. TRAINABLE CLASSIFIERS

Automated or manual. Train AIP to identify the PII that matters. A first full scan of your data will be performed before you can train your own classifiers. You can use them in Sensitivity Labels as well.

4. POLICIES & INDUSTRY REGULATIONS

- Which regulations apply to your business?
- Are you already fulfilling them?
- What are the implementations expected?
- What are the control mechanisms?

Check the privacy laws for the USA here: [US Privacy Laws](#).



PHASE 2 Protect Your Data

5. CREATE SENSITIVITY LABELS

Some organizations use only a few labels while others might have one for each team, site, or set of data.

6. TEST & ASSIGN LABELS

Use policies, groups, DLs, and Sites.

Deploy the labels to the users and locations established in Phase 1. Using combinations of labels and policies, you can achieve levels of granular control.

Other Microsoft Purview Solutions You Can Use

- Sensitivity Labels
- AIP Unified Labelling Client
- Double-Key Encryption
- Office Message Encryption
- Defender for Cloud Apps
- Purview Data Map
- Rights Management Connector
- Service Encryption with Customer Key

PHASE 3 Prevent Data Loss

7. DLP POLICIES

For endpoint, cloud locations, On-premise servers, Chrome Extensions, and Microsoft Teams & Chats.

8. MONITORING & MAINTENANCE

Based on your findings, update your policies and postures.

Demo

Information Protection &
Data Loss Prevention Policies



Microsoft Purview Insider Risk Management



Helps organizations detect, investigate, and act on malicious and inadvertent activities in their organization.

“There’s always one rat.”

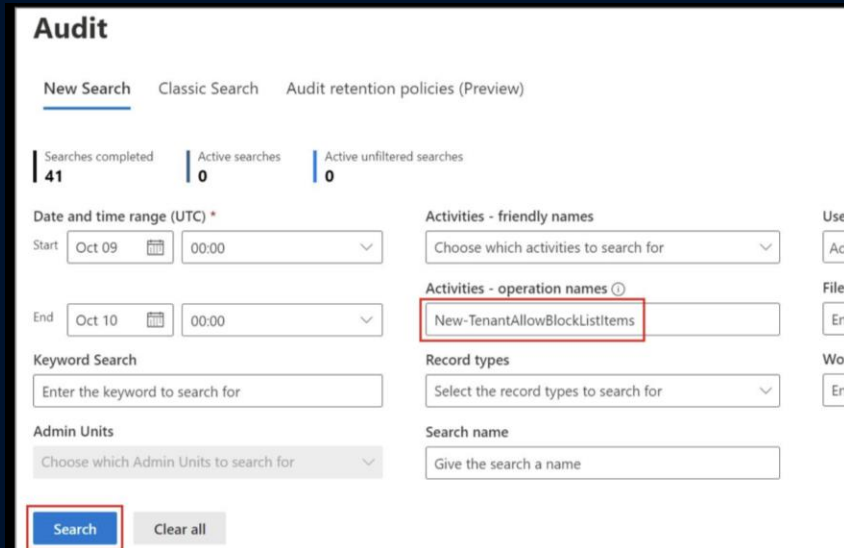
Demo

Insider Risk Management &
Communications Compliance



Microsoft Purview New Features Include

- Support for Administrative Units now in preview for all compliance features
- Colored Labels available throughout all tools
- Adaptive Scopes Now Generally Available
- New Label & encrypt PDF Support for OneDrive & Mail Attachments
- Enhanced Audit Filters & New Audit Protection Policies
- Co-Authoring for Sensitivity Labels

A screenshot of the Microsoft Purview Audit search interface. The page is titled 'Audit' and has three tabs: 'New Search' (selected), 'Classic Search', and 'Audit retention policies (Preview)'. Below the tabs, there are three status indicators: 'Searches completed' with a value of 41, 'Active searches' with a value of 0, and 'Active unfiltered searches' with a value of 0. The main search area includes several filters: 'Date and time range (UTC) *' with 'Start' and 'End' date and time pickers; 'Activities - friendly names' with a dropdown menu; 'Activities - operation names' with a dropdown menu where 'New-TenantAllowBlockListItems' is selected and highlighted with a red box; 'Keyword Search' with a text input field; 'Admin Units' with a dropdown menu; 'Record types' with a dropdown menu; and 'Search name' with a text input field. At the bottom left, there is a 'Search' button highlighted with a red box and a 'Clear all' button.

Incoming Microsoft 365 Backup Solutions

Introducing Microsoft 365 Backup

Microsoft 365 Backup



Microsoft Provided Application

An add-on service for enhanced restore coverage for Microsoft 365 Content



Platform for Partner Solution

An API Platform for third party ISV partners to build their solution

Key Capabilities



Content Backups

In-place backups of Microsoft 365 content at service defined frequencies



Browse or Search

Content discovery tools to select what to restore



Restore

Restore content from backups at desired granularity

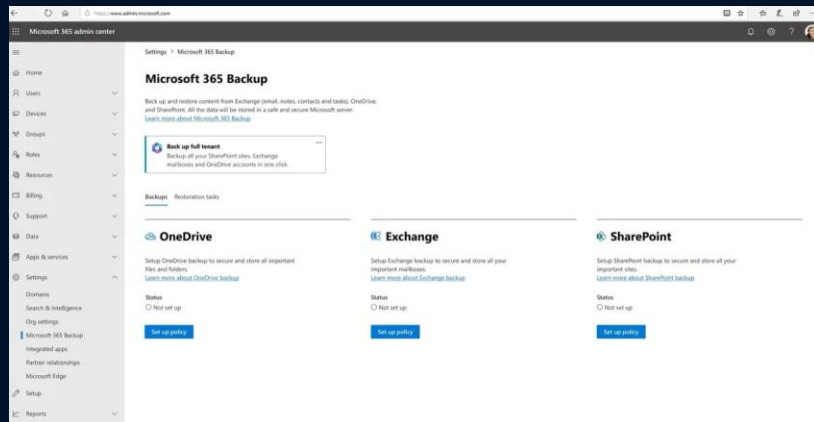


Monitoring

Audit changes and restores; control storage usage

Microsoft 365 Backup

- A new service that provides Backup & Recovery of all or selected SharePoint sites, OneDrive accounts, and Exchange mailboxes in your tenant.
- Restore files, sites, and mailbox items in your tenant in parallel to a prior point-in-time in a granular manner or at massive scale
- Search or filter content in your backups using key metadata such as item or site names, owners, or event types within specific restore point date ranges.



Demo

Microsoft 365 Backup



Microsoft 365

https://www.admin.microsoft.com

Microsoft 365 admin center

Home

Users

Devices

Groups

Roles

Resources

Billing

Support

Data

Apps & services

Settings

Domains

Search & intelligence

Org settings

Microsoft 365 Backup

Integrated apps

Partner relationships

Microsoft Edge

Setup

Reports

Health

Settings > Microsoft 365 Backup

Microsoft 365 Backup

Back up and restore content from Exchange (email, notes, contacts and tasks), OneDrive, and SharePoint. All the data will be stored in a safe and secure Microsoft server.
[Learn more about Microsoft 365 Backup](#)

Back up full tenant

Backup all your SharePoint sites, Exchange mailboxes and OneDrive accounts in one click.

Backups

Restoration tasks

OneDrive

Setup OneDrive backup to secure and store all important files and folders.
[Learn more about OneDrive backup](#)

Status

☐ Not set up

Set up policy

Exchange

Setup Exchange backup to secure and store all your important mailboxes.
[Learn more about Exchange backup](#)

Status

☐ Not set up

Set up policy

SharePoint

Setup SharePoint backup to secure and store all your important sites.
[Learn more about SharePoint backup](#)

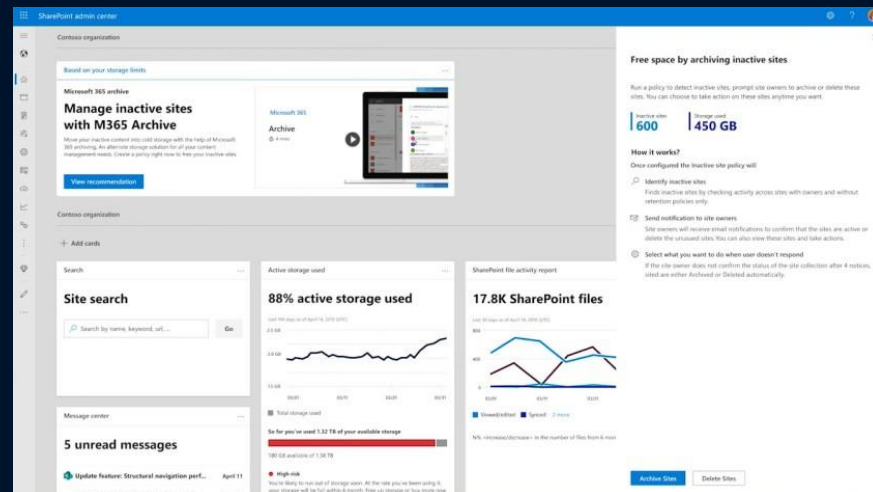
Status

☐ Not set up

Set up policy

Introducing Microsoft 365 Archive

- A New Archival Service in Microsoft 365 that will
- Select and archive or reactivate full sites in place without needing to migrate your data outside of Microsoft. File level archiving will be coming in the second half of 2024.
- Maintain full admin-level search, eDiscovery, access policy, sensitivity label, DLP (Data Loss Prevention), retention policy, access control settings, and other security and compliance functionality.
- Gain additional de-cluttering experiences and site lifecycle control capabilities.



Demo

Microsoft 365 Archive



Contoso organization

+ Add cards

Search

Site search

Search by name, keyword, url, ...

Go

Message center

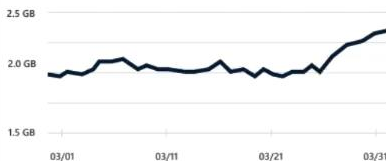
5 unread messages

- Update feature: Structural navigation perf...** April 11
- Updated feature: We're changing your de... April 10
- Status of your OneDrive and SharePoint O... April 10
- Status of your OneDrive and SharePoint O...** April 10
- New feature: audience targeting in Share... April 9
- New feature: Mail Flow Insights is coming th... April 7
- Updated feature: Versioning settings in Mic... April 7
- New feature: Mail Flow Insights is coming th...** April 6
- We're making some changes to translation o...** April 6
- New feature: Mail Flow Insights is coming th... May 20

Active storage used

30% active storage used

Last 180 days as of April 14, 2019 (UTC)



Total storage used

So far you've used .56 TB of your available storage

1.02 TB available of 1.58 TB

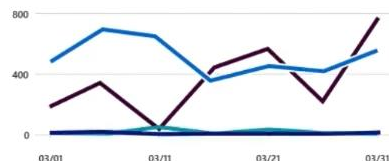
Free up storage

Buy more storage

SharePoint file activity report

17.8K SharePoint files

Last 30 days as of April 14, 2019 (UTC)



Viewed/edited Synced 2 more

N% <increase/decrease> in the number of files from 6 months ago

View sites with most files

OneDrive account usage

23% active accounts

Last 30 days as of April 16, 2019 (UTC)



Site creation sources

30% of sites are created from SharePoint admin center

Top 10 site creation sources in the last 30 days as of April 14, 2019 (UTC)



Anomalies

2 critical events identified

As of March 16, 2022 (UTC)

- Ransomware detection**
Detection: Today at 3:30 pm
- Sites with 'Top secret' labelled files overshared**
Detection: Yesterday at 3:30 pm
- User trying to access protected files**
Detection: 5 days ago
- Spike detected in App access site**
Detection: 5 days ago

Show all

SharePoint site usage

12.51% of sites are active

Last 30 days as of April 16, 2019 (UTC)



Conclusions

“Zero Trust Security Works”

Identity

Security

Compliance

Consequences!





NIC Cloud
Connect

Oslo Spektrum
November 7 - 9