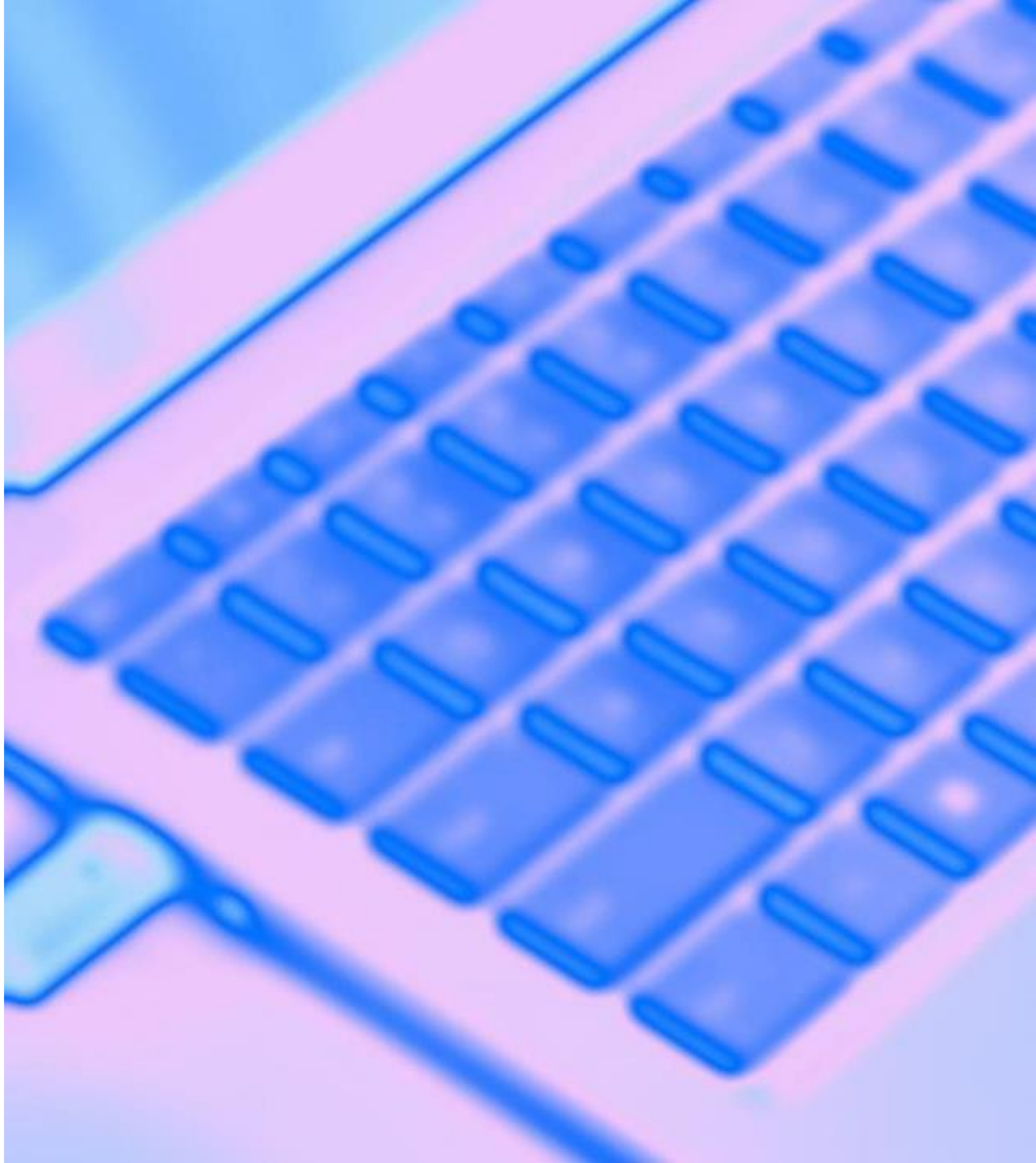
Microsoft Security

Endpoint Protection

Daniel Vodrážka
System4u



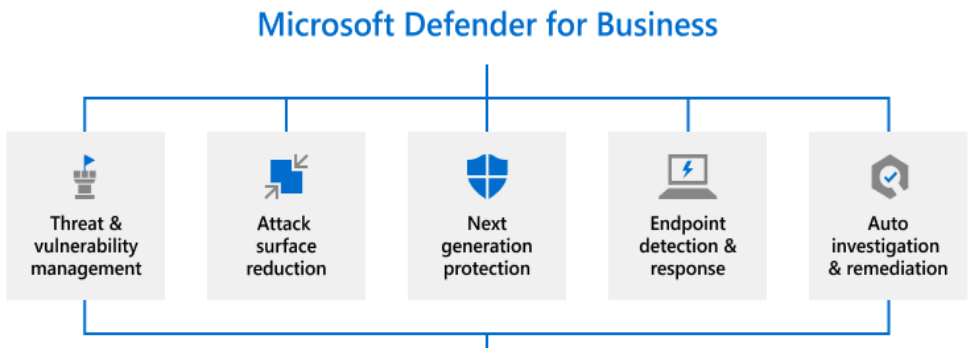
ALSO ARROW TD SYNNEX GOPAS Microsoft system4u

Defender for Business úvod

- → Co je Defender for Business?
  - → Defender for Endpoint pro menší firmy (SMBs)
  - → Do maximálně 300 uživatelů

Defender for Business vs Endpoint plan 1/2

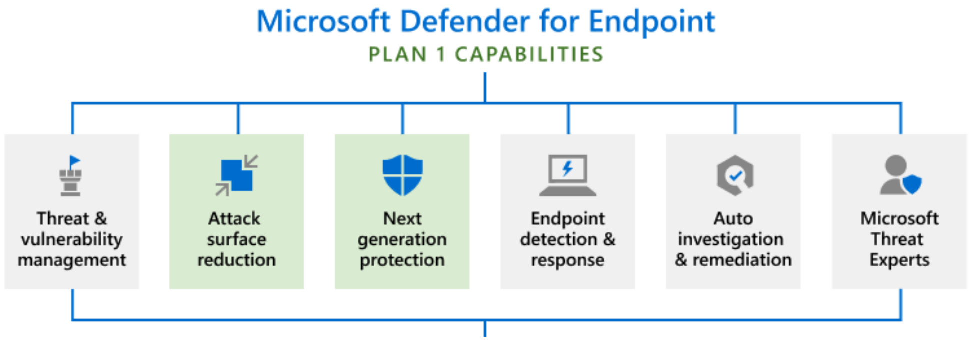
→ Defender for Business



Microsoft Defender for Business

- Threat & vulnerability management
- Attack surface reduction
- Next generation protection
- Endpoint detection & response
- Auto investigation & remediation

→ Defender for Endpoint Plan 1 / Plan 2



Microsoft Defender for Endpoint

PLAN 1 CAPABILITIES

- Threat & vulnerability management
- Attack surface reduction
- Next generation protection
- Endpoint detection & response
- Auto investigation & remediation
- Microsoft Threat Experts

Defender for Business overview

→ Možnosti nasazení

- Setup Wizzard
- Manual setup

→ Licencování

- Microsoft 365 Business Premium
- Defender for Business standalone

Defender for Business overview

→ Podporované platformy

- Windows, MacOS
- Android, iOS

→ Data locations: EU, UK, US, AU

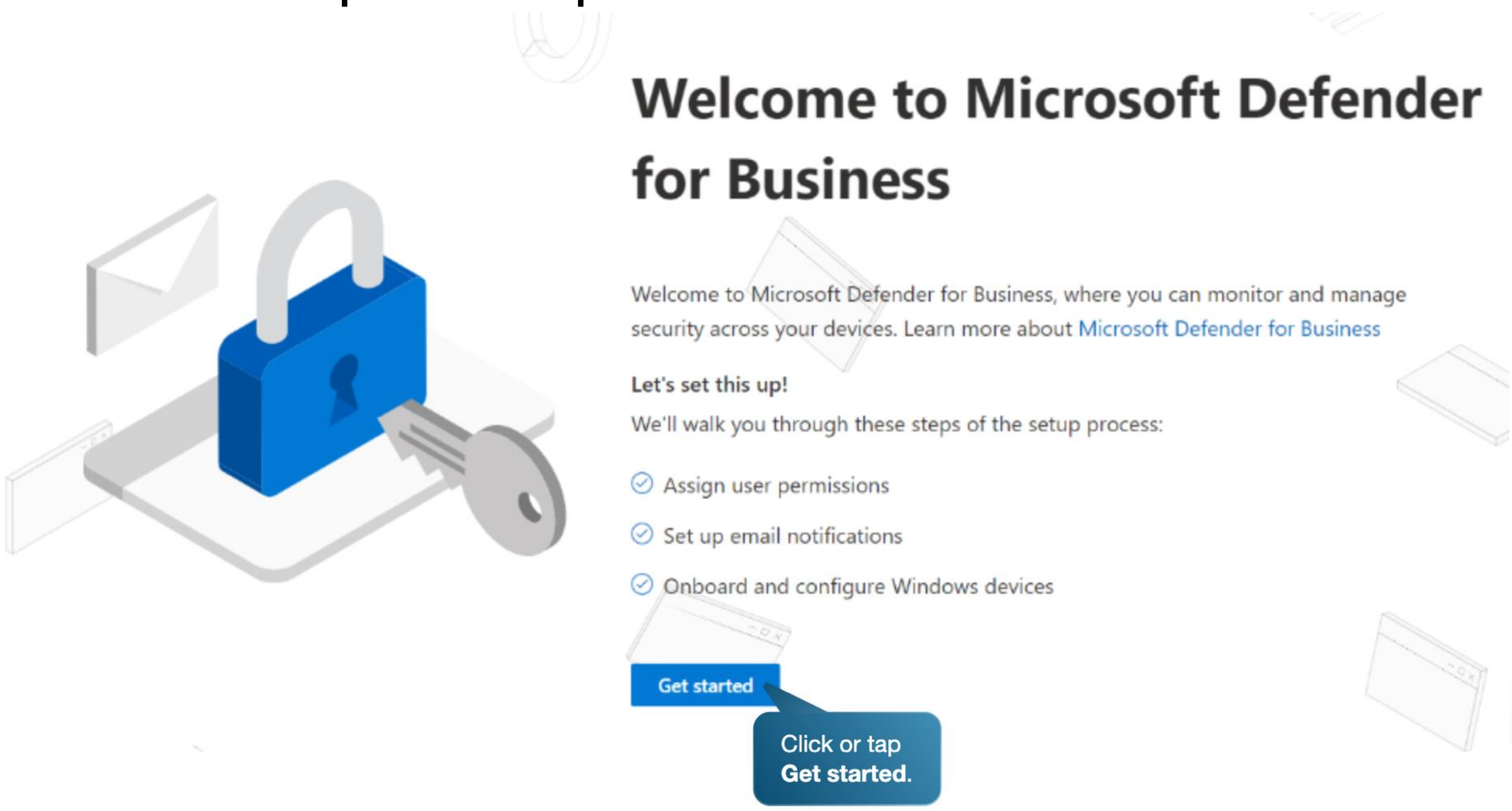
Defender for Business setup

→ Postup nasazení

1. Get Defender for Business
2. Add users and assign licenses
3. Assign security roles and permissions
4. Set up email notifications for your security team
5. Onboard devices
6. Set up and review your security policies

Defender for Business setup

→ Nasazení pomocí průvodce



Welcome to Microsoft Defender for Business

Welcome to Microsoft Defender for Business, where you can monitor and manage security across your devices. Learn more about Microsoft Defender for Business

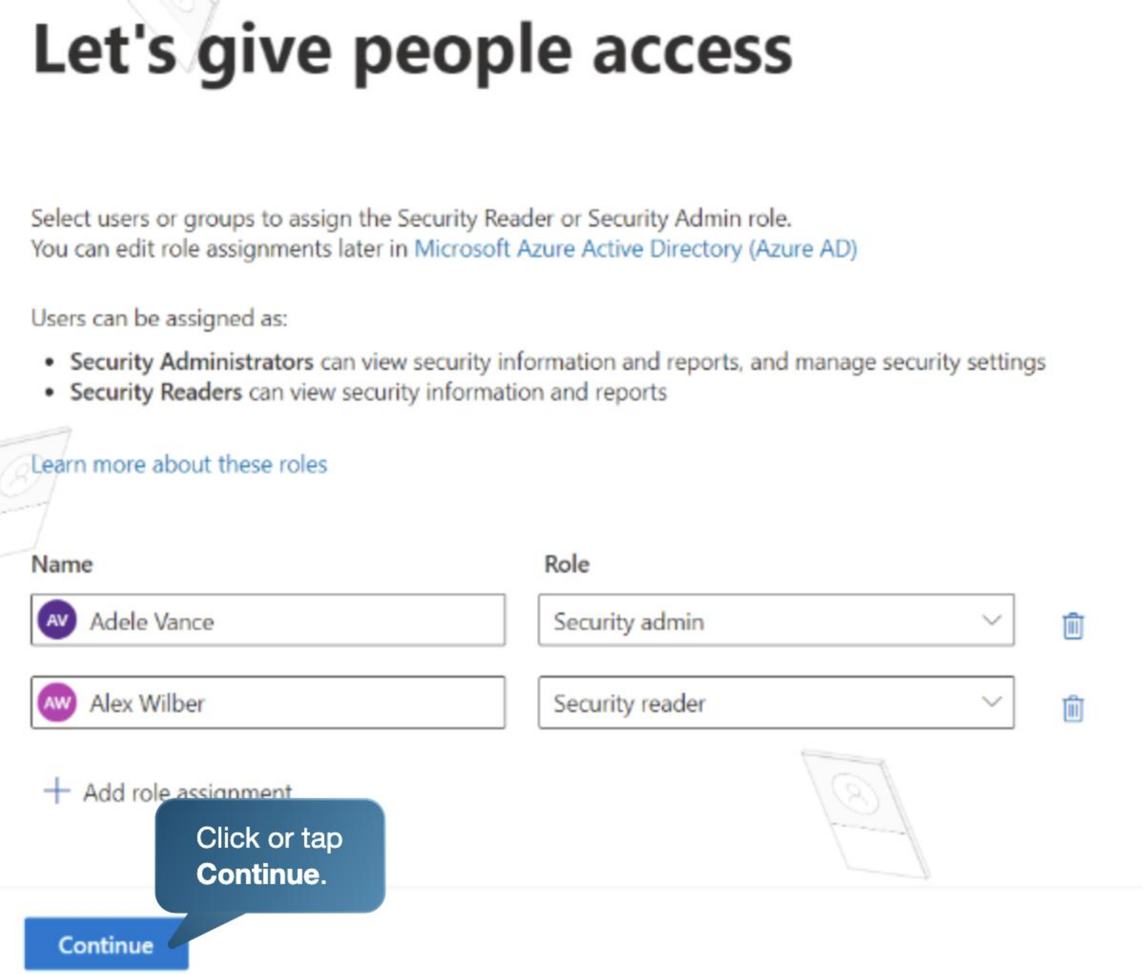
Let's set this up!

We'll walk you through these steps of the setup process:

- ✓ Assign user permissions
- ✓ Set up email notifications
- ✓ Onboard and configure Windows devices

Click or tap **Get started.**

Defender for Business setup



Let's give people access

Select users or groups to assign the Security Reader or Security Admin role.
You can edit role assignments later in Microsoft Azure Active Directory (Azure AD)

Users can be assigned as:

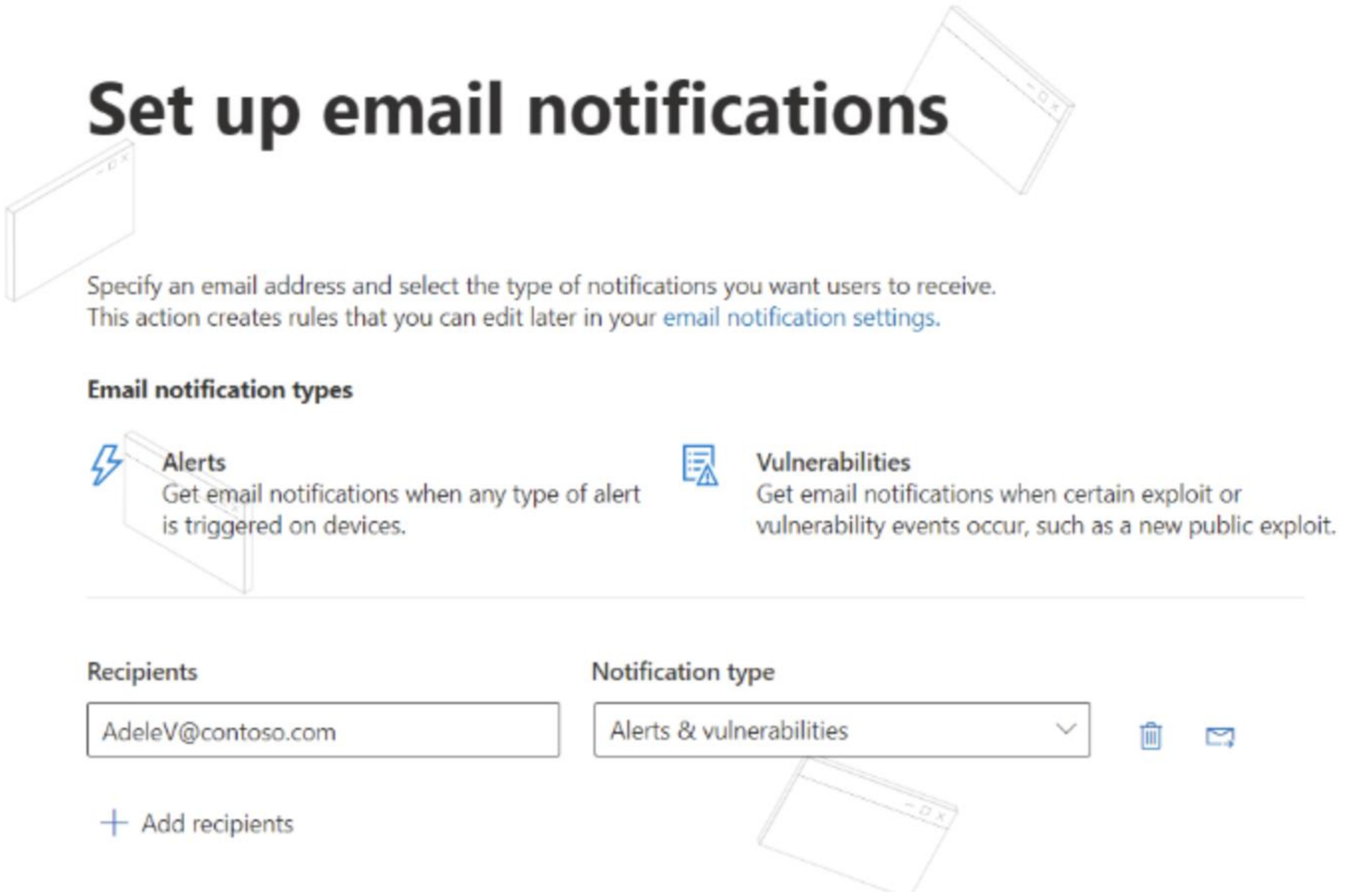
- **Security Administrators** can view security information and reports, and manage security settings
- **Security Readers** can view security information and reports

Learn more about these roles

Name	Role
AV Adele Vance	Security admin
AW Alex Wilber	Security reader

Click or tap **Continue.**

Defender for Business setup



Set up email notifications

Specify an email address and select the type of notifications you want users to receive. This action creates rules that you can edit later in your email notification settings.

Email notification types

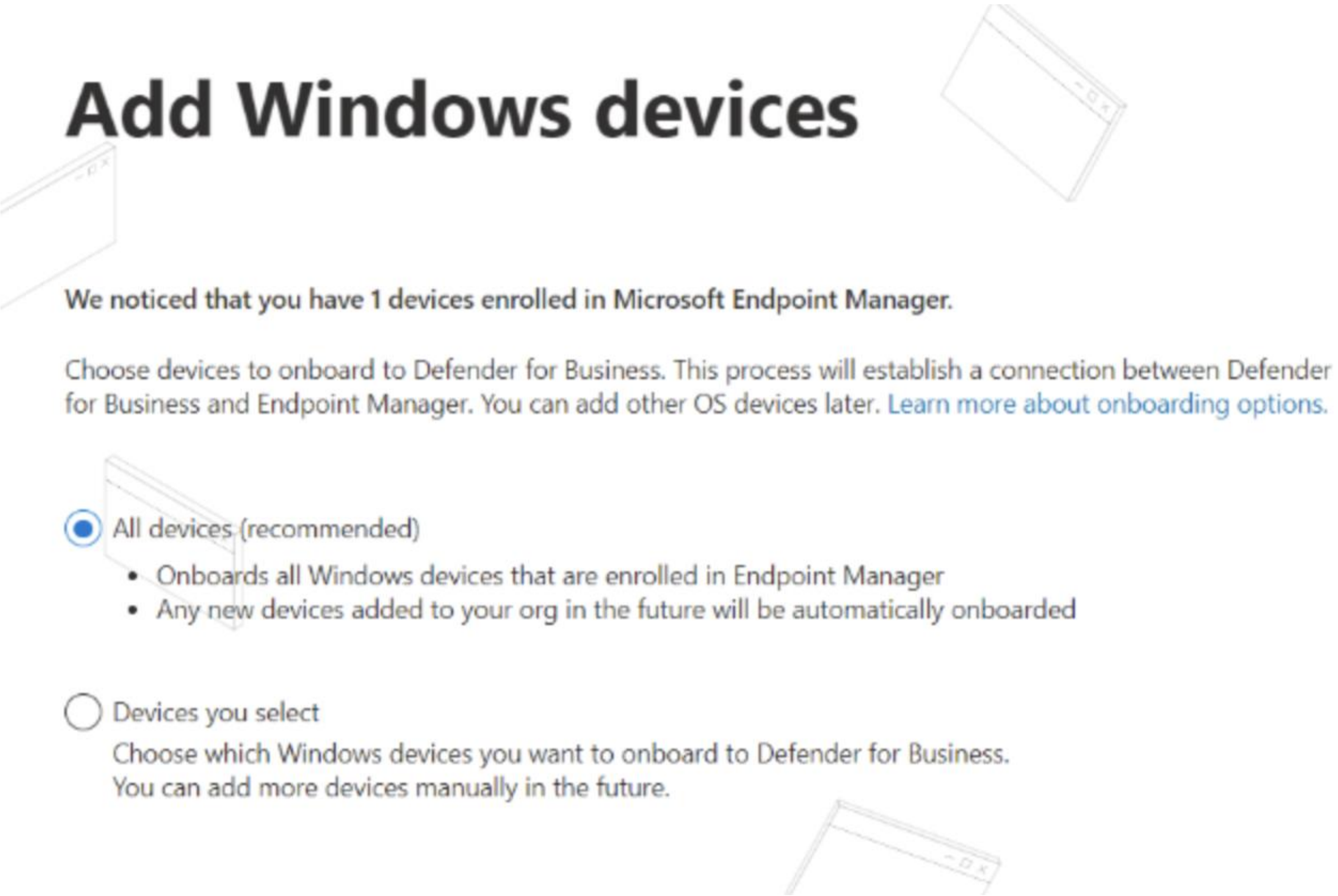
Alerts
Get email notifications when any type of alert is triggered on devices.

Vulnerabilities
Get email notifications when certain exploit or vulnerability events occur, such as a new public exploit.

Recipients	Notification type
AdeleV@contoso.com	Alerts & vulnerabilities

+ Add recipients

Defender for Business setup



Add Windows devices

We noticed that you have 1 devices enrolled in Microsoft Endpoint Manager.

Choose devices to onboard to Defender for Business. This process will establish a connection between Defender for Business and Endpoint Manager. You can add other OS devices later. Learn more about onboarding options.

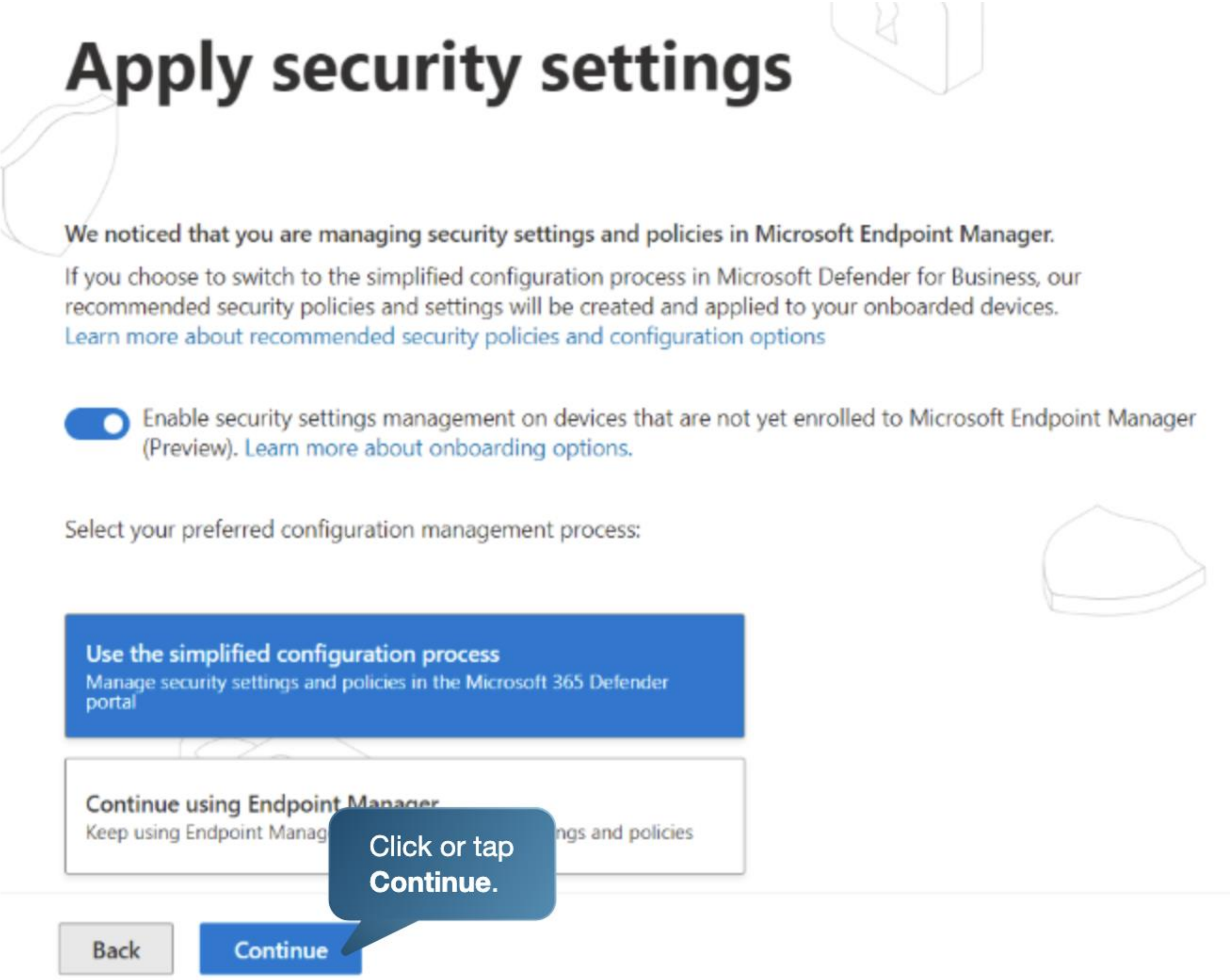
● All devices (recommended)

- Onboards all Windows devices that are enrolled in Endpoint Manager
- Any new devices added to your org in the future will be automatically onboarded

○ Devices you select

Choose which Windows devices you want to onboard to Defender for Business.
You can add more devices manually in the future.

Defender for Business setup



Apply security settings

We noticed that you are managing security settings and policies in Microsoft Endpoint Manager.

If you choose to switch to the simplified configuration process in Microsoft Defender for Business, our recommended security policies and settings will be created and applied to your onboarded devices.
Learn more about recommended security policies and configuration options

● Enable security settings management on devices that are not yet enrolled to Microsoft Endpoint Manager (Preview). Learn more about onboarding options.

Select your preferred configuration management process:

Use the simplified configuration process
Manage security settings and policies in the Microsoft 365 Defender portal

Continue using Endpoint Manager
Keep using Endpoint Manag ngs and policies

Click or tap **Continue.**

Defender for Business onboarding

→ Windows

- Local script
- GPO
- Intune

→ MacOS

- Local script
- Intune

→ Mobile (Android, iOS)

- Defender for Endpoint app
- Intune

Integrace Intune s Defender for Business

- Jednorázová akce umožňující propojit Defender a Intune

- Výhody:
  - Možnost onboardingu zařízení pomocí Intune
  - Sdílení Risk Level zařízení

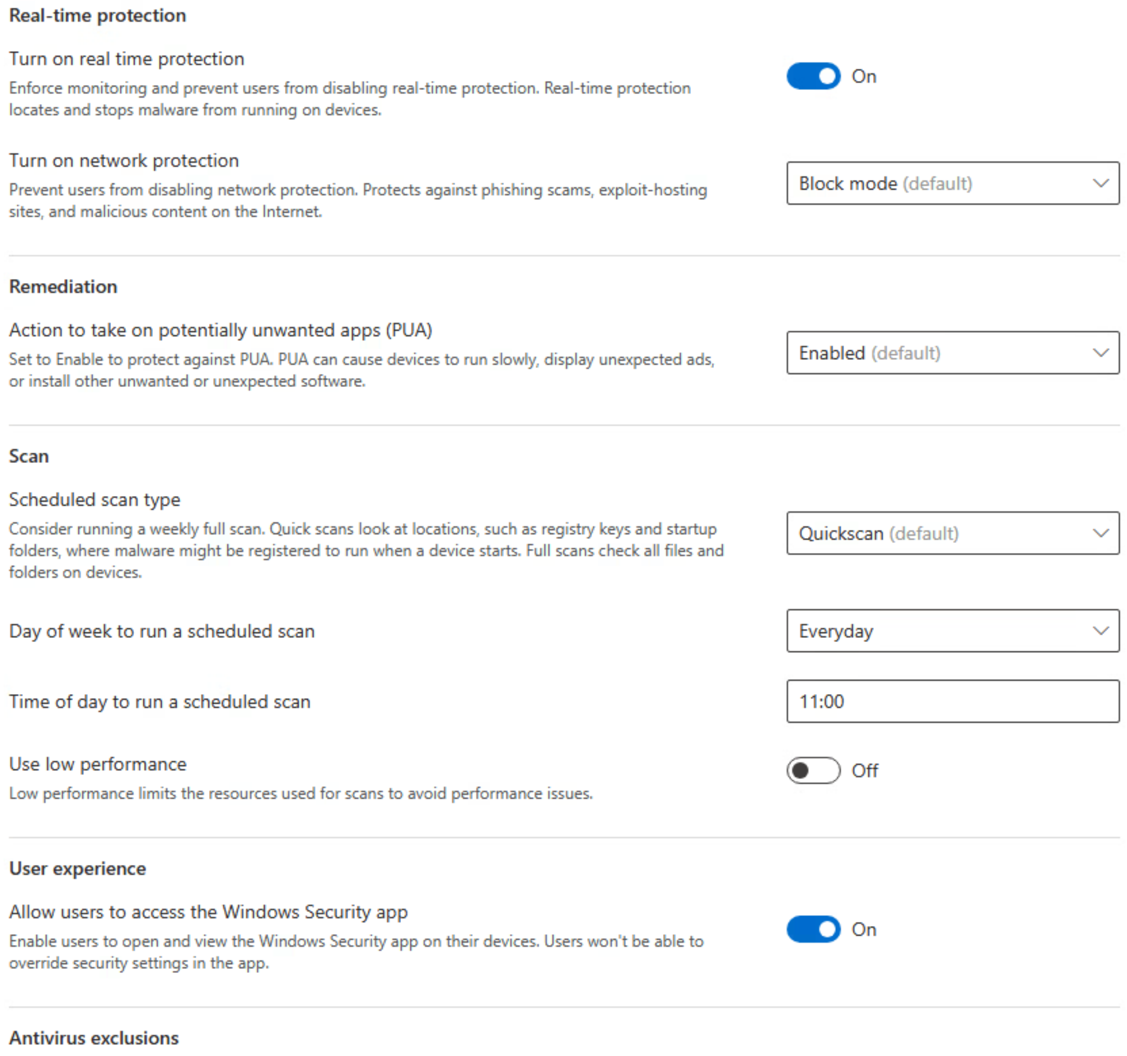
Defender for Business – Windows onboarding

→ Onboarding Windows zařízení pomocí MS Intune

Defender for Business – Windows politiky

- Existuje několik typů politiky:
  - **Next-generation Protection (AV)**
  - **Windows Security Experience**
  - **Windows Firewall**
  - **Attack surface reduction (ASR)**
  - Antivirus exclusions

Defender for Business – Windows Antivirus



Real-time protection

Turn on real time protection
Enforce monitoring and prevent users from disabling real-time protection. Real-time protection locates and stops malware from running on devices.
On

Turn on network protection
Prevent users from disabling network protection. Protects against phishing scams, exploit-hosting sites, and malicious content on the Internet.
Block mode (default)

Remediation

Action to take on potentially unwanted apps (PUA)
Set to Enable to protect against PUA. PUA can cause devices to run slowly, display unexpected ads, or install other unwanted or unexpected software.
Enabled (default)

Scan

Scheduled scan type
Consider running a weekly full scan. Quick scans look at locations, such as registry keys and startup folders, where malware might be registered to run when a device starts. Full scans check all files and folders on devices.
Quickscan (default)

Day of week to run a scheduled scan
Everyday

Time of day to run a scheduled scan
11:00

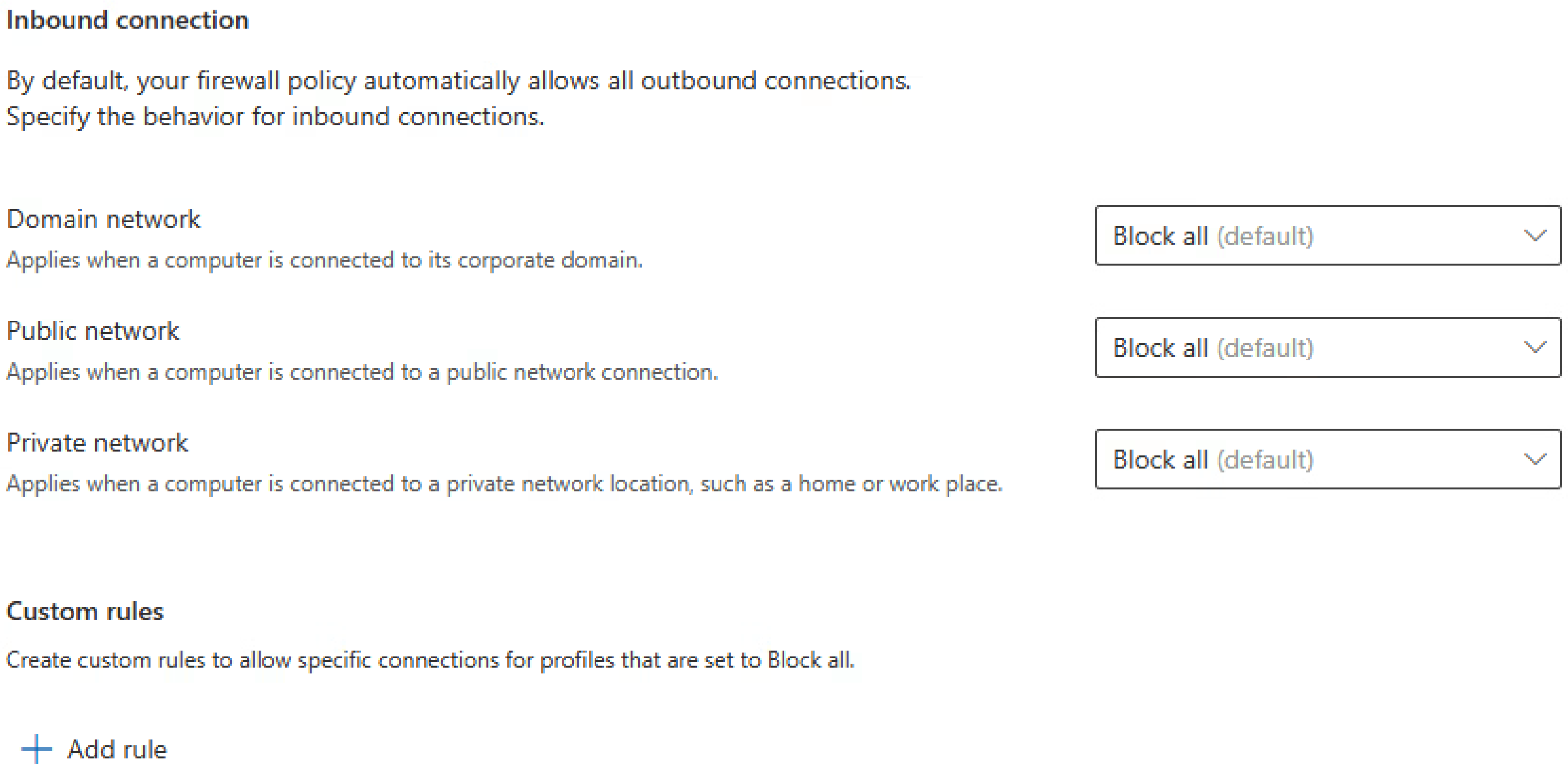
Use low performance
Low performance limits the resources used for scans to avoid performance issues.
Off

User experience

Allow users to access the Windows Security app
Enable users to open and view the Windows Security app on their devices. Users won't be able to override security settings in the app.
On

Antivirus exclusions

Defender for Business – Windows Firewall



Inbound connection

By default, your firewall policy automatically allows all outbound connections.
Specify the behavior for inbound connections.

Domain network
Applies when a computer is connected to its corporate domain.
Block all (default)

Public network
Applies when a computer is connected to a public network connection.
Block all (default)

Private network
Applies when a computer is connected to a private network location, such as a home or work place.
Block all (default)

Custom rules

Create custom rules to allow specific connections for profiles that are set to Block all.

Microsoft Intune – Endpoint security

→ Disk encryption (Bitlocker / FileVault)

→ Attack surface reduction (ASR)

→ Device compliance

→ Conditional access

Defender for Business – Windows onboarding

→ Otestování nasazení:

https://learn.microsoft.com/en-us/defender-endpoint/run-detection-test

https://learn.microsoft.com/en-us/defender-endpoint/defender-endpoint-demonstration-smartscreen-url-reputation

Defender for Business Servers

→Windows

- Local script

→Linux

- Local script
- další možnosti: Ansible, Chef, Puppet

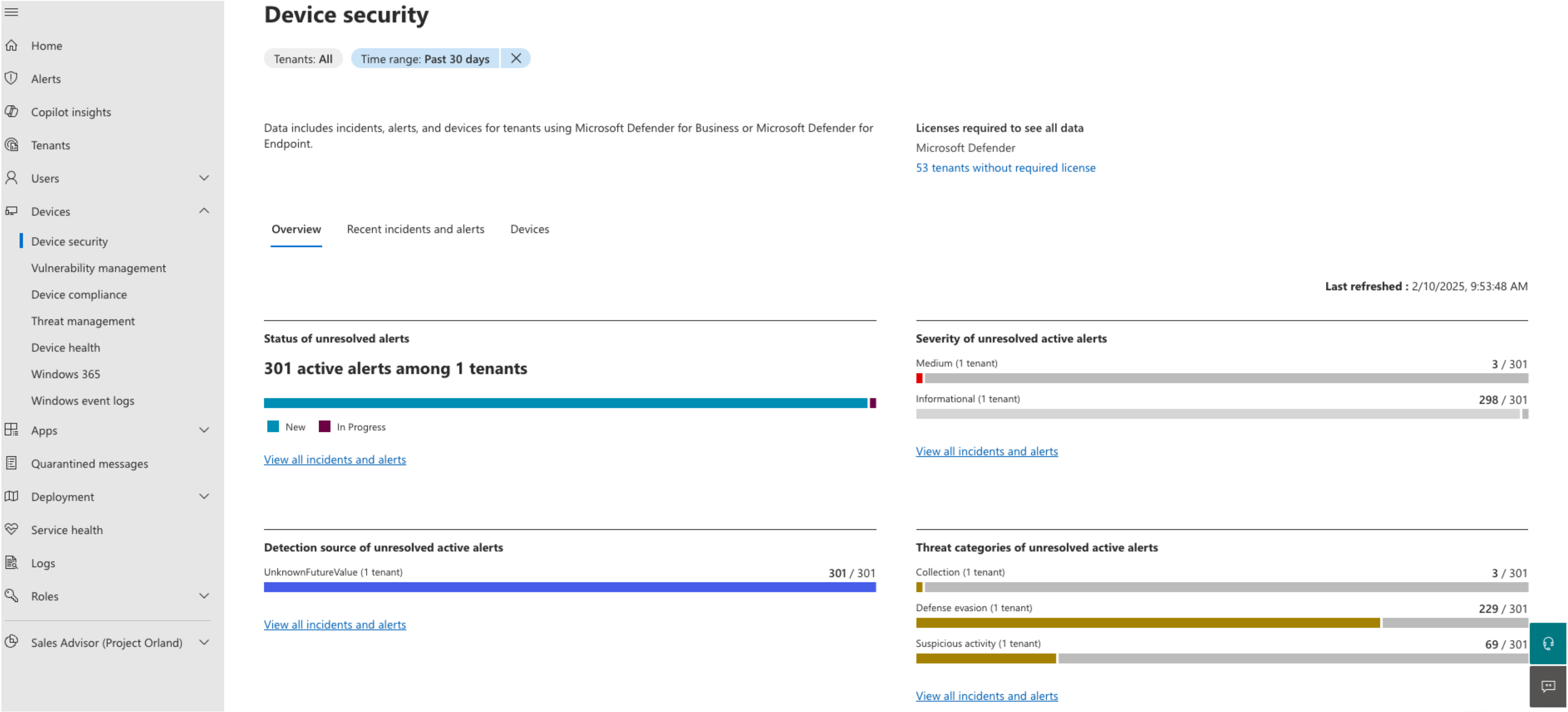
→Bezpečnostní politiky se nastavují pouze v konzoli Microsoft Defender

Defender for Business - Lighthouse

- Jedna konzole pro správu více tenantů
- Určeno pro Managed Service Providers (MSPs)

- Defender for Endpoint/Business:
  - Device Security
  - Vulnerability Management
  - Device Compliance
  - Threat Management

Defender for Business – Lighthouse / Device Security



Device security

Tenants: **All** Time range: **Past 30 days** ✕

Data includes incidents, alerts, and devices for tenants using Microsoft Defender for Business or Microsoft Defender for Endpoint.

Licenses required to see all data
Microsoft Defender
53 tenants without required license

Last refreshed : 2/10/2025, 9:53:48 AM

Status of unresolved alerts

301 active alerts among 1 tenants

🟦 New 🟪 In Progress

View all incidents and alerts

Severity of unresolved active alerts

Medium (1 tenant)	**3** / 301
Informational (1 tenant)	**298** / 301

View all incidents and alerts

Detection source of unresolved active alerts

UnknownFutureValue (1 tenant)	**301** / 301

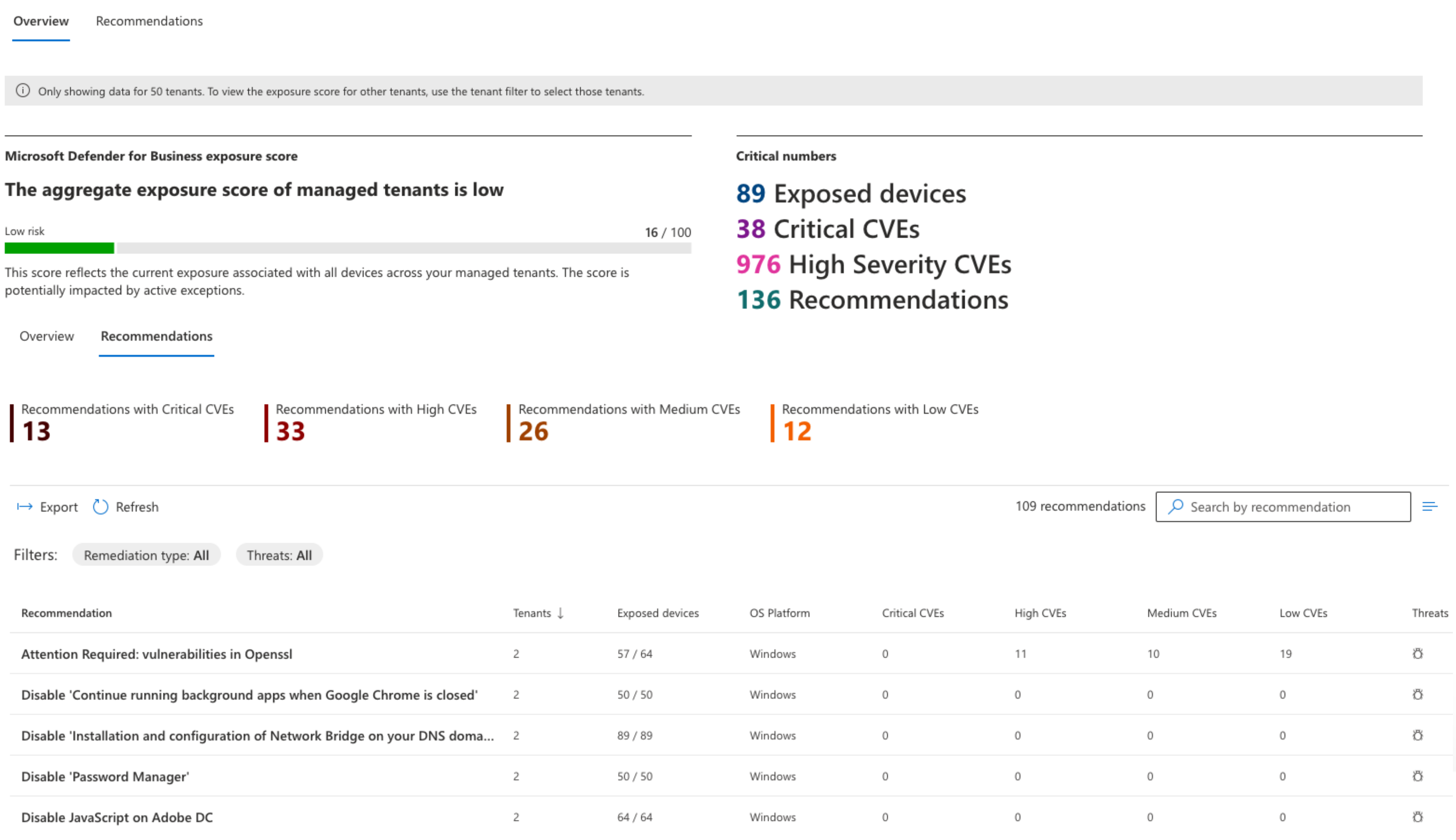
View all incidents and alerts

Threat categories of unresolved active alerts

Collection (1 tenant)	**3** / 301
Defense evasion (1 tenant)	**229** / 301
Suspicious activity (1 tenant)	**69** / 301

View all incidents and alerts

Defender for Business – Lighthouse / Vulnerability Management



Overview | Recommendations

ⓘ Only showing data for 50 tenants. To view the exposure score for other tenants, use the tenant filter to select those tenants.

Microsoft Defender for Business exposure score

The aggregate exposure score of managed tenants is low

Low risk 16 / 100

This score reflects the current exposure associated with all devices across your managed tenants. The score is potentially impacted by active exceptions.

Critical numbers

89 Exposed devices
38 Critical CVEs
976 High Severity CVEs
136 Recommendations

Overview | Recommendations

Recommendations with Critical CVEs 13

Recommendations with High CVEs 33

Recommendations with Medium CVEs 26

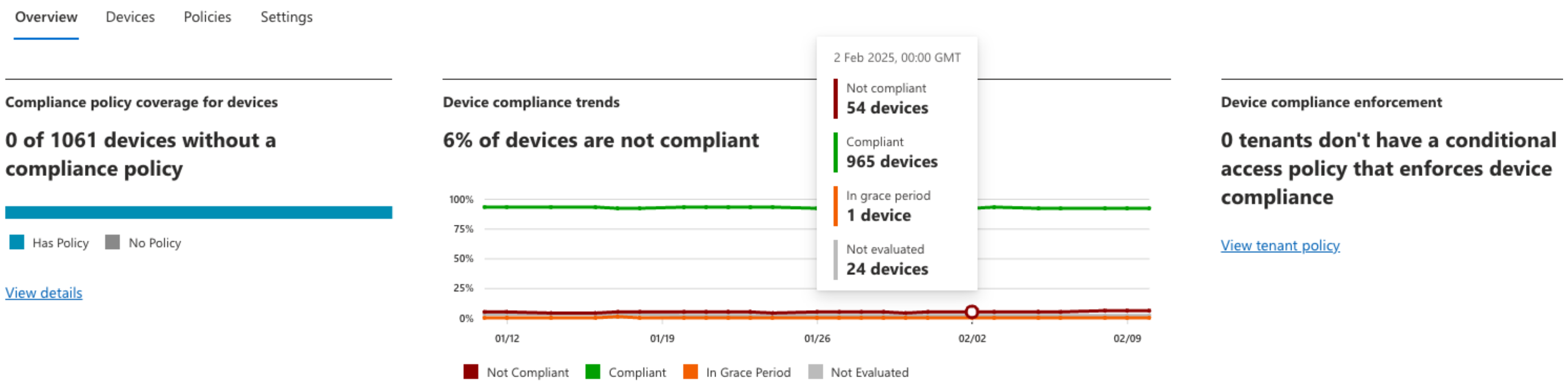
Recommendations with Low CVEs 12

Export | Refresh | 109 recommendations | Search by recommendation

Filters: Remediation type: All | Threats: All

Recommendation	Tenants ↓	Exposed devices	OS Platform	Critical CVEs	High CVEs	Medium CVEs	Low CVEs	Threats
Attention Required: vulnerabilities in Openssl	2	57 / 64	Windows	0	11	10	19	🐛
Disable 'Continue running background apps when Google Chrome is closed'	2	50 / 50	Windows	0	0	0	0	🐛
Disable 'Installation and configuration of Network Bridge on your DNS doma...	2	89 / 89	Windows	0	0	0	0	🐛
Disable 'Password Manager'	2	50 / 50	Windows	0	0	0	0	🐛
Disable JavaScript on Adobe DC	2	64 / 64	Windows	0	0	0	0	🐛

Defender for Business – Lighthouse / Device Compliance



Overview Devices Policies Settings

Compliance policy coverage for devices

0 of 1061 devices without a compliance policy

🟦 Has Policy ▨ No Policy

View details

Device compliance trends

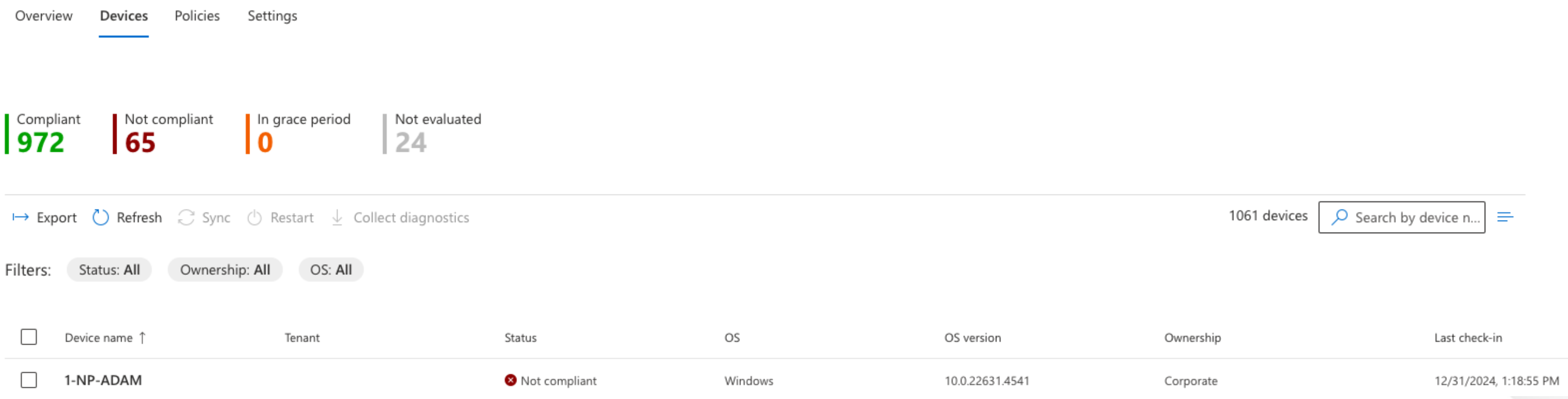
6% of devices are not compliant

🟥 Not Compliant 🟩 Compliant 🟧 In Grace Period ▨ Not Evaluated

Device compliance enforcement

0 tenants don't have a conditional access policy that enforces device compliance

View tenant policy



Overview Devices Policies Settings

Compliant 972 | Not compliant 65 | In grace period 0 | Not evaluated 24

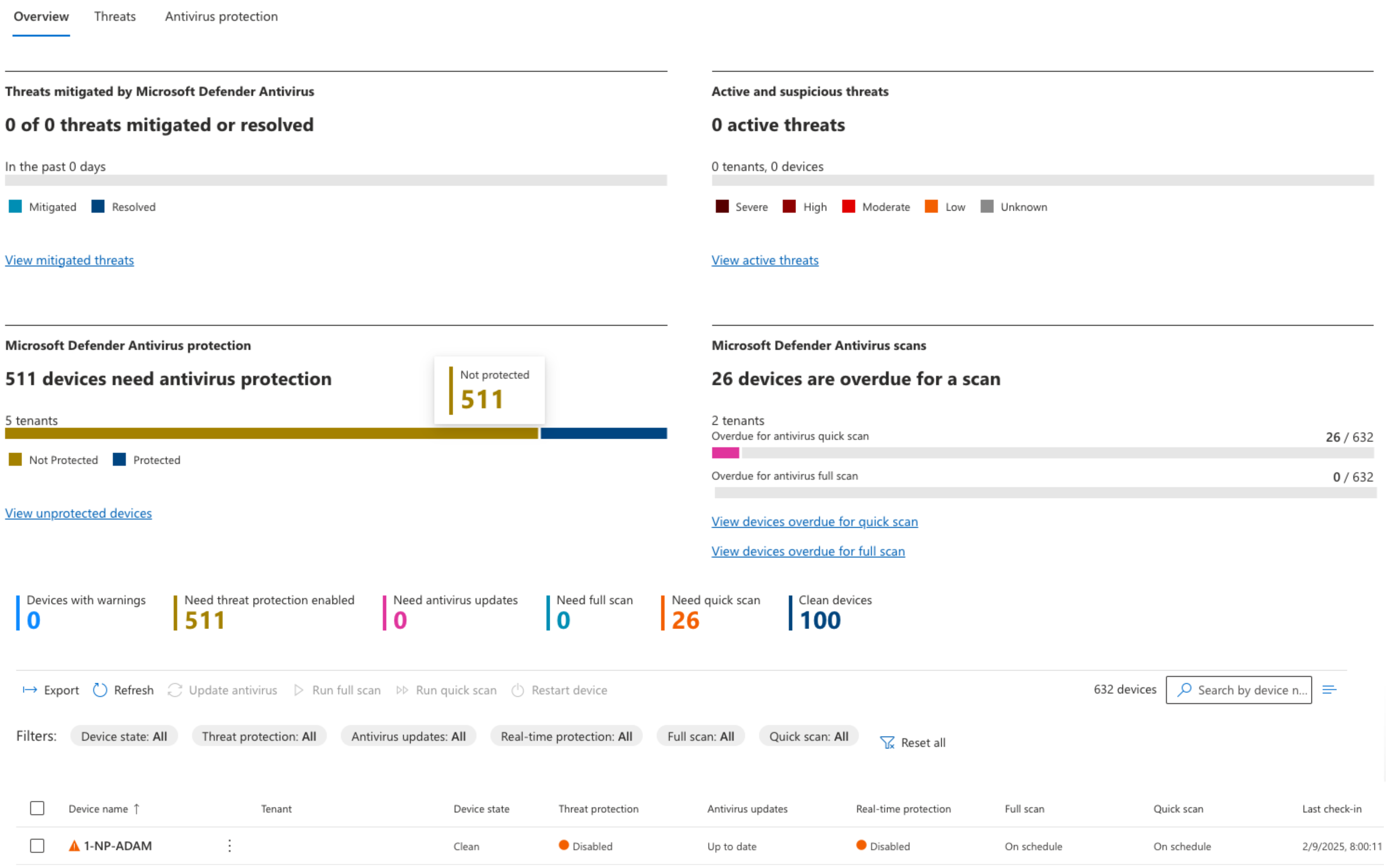
Export Refresh Sync Restart Collect diagnostics

1061 devices Search by device n...

Filters: Status: All Ownership: All OS: All

□	Device name ↑	Tenant	Status	OS	OS version	Ownership	Last check-in
□	1-NP-ADAM		☒ Not compliant	Windows	10.0.22631.4541	Corporate	12/31/2024, 1:18:55 PM

Defender for Business – Lighthouse / Threat Management



Overview | Threats | Antivirus protection

Threats mitigated by Microsoft Defender Antivirus

0 of 0 threats mitigated or resolved

In the past 0 days

■ Mitigated ■ Resolved

View mitigated threats

Active and suspicious threats

0 active threats

0 tenants, 0 devices

■ Severe ■ High ■ Moderate ■ Low ■ Unknown

View active threats

Microsoft Defender Antivirus protection

511 devices need antivirus protection

Not protected 511

5 tenants

■ Not Protected ■ Protected

View unprotected devices

Microsoft Defender Antivirus scans

26 devices are overdue for a scan

2 tenants

Overdue for antivirus quick scan 26 / 632

Overdue for antivirus full scan 0 / 632

View devices overdue for quick scan

View devices overdue for full scan

Devices with warnings	Need threat protection enabled	Need antivirus updates	Need full scan	Need quick scan	Clean devices
0	511	0	0	26	100

632 devices

Filters: Device state: All | Threat protection: All | Antivirus updates: All | Real-time protection: All | Full scan: All | Quick scan: All | Reset all

□	Device name ↑	Tenant	Device state	Threat protection	Antivirus updates	Real-time protection	Full scan	Quick scan	Last check-in
□	⚠ 1-NP-ADAM		Clean	● Disabled	Up to date	● Disabled	On schedule	On schedule	2/9/2025, 8:00:11

Microsoft Security

Microsoft Partner Security Day

Praha, 11. 2. 2025

ALSO ARROW TD SYNNEX GOPAS Microsoft system4u