

Saugi darbo vieta – IT saugumo pagrindas

Rimas Kareiva
Skaitmeninių darbo vietų kompetencijų centras
Grupės vadovas

MASLOW'S HIERARCHY OF NEEDS

SELF-ACTUALIZATION

creation, beauty, unity, aesthetics, exploration

ESTEEM

dignity, respect, achievement, purpose, recognition

SOCIAL

friendship, intimacy, community, sense of belonging

SAFETY

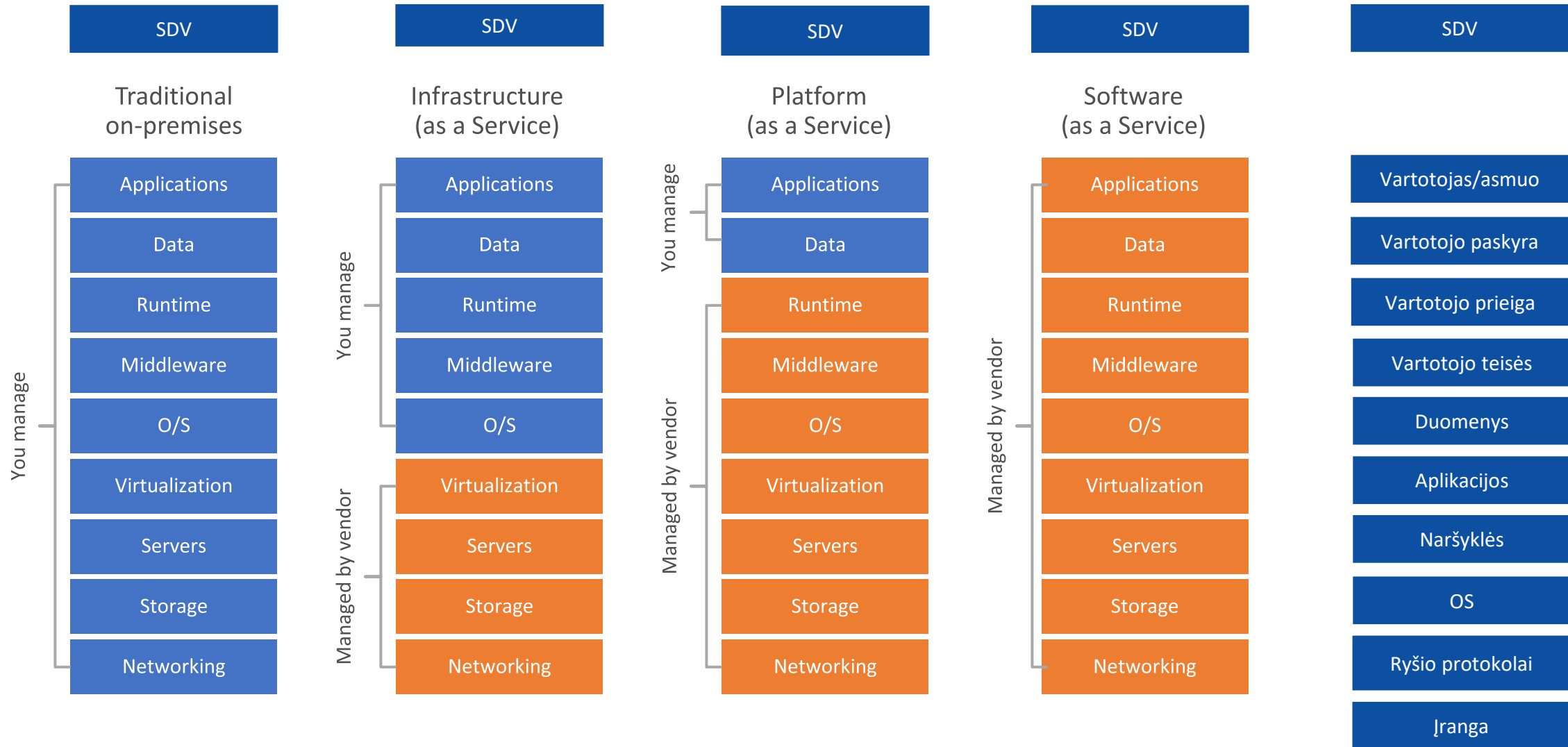
personal security, resources, source of income, structure, order

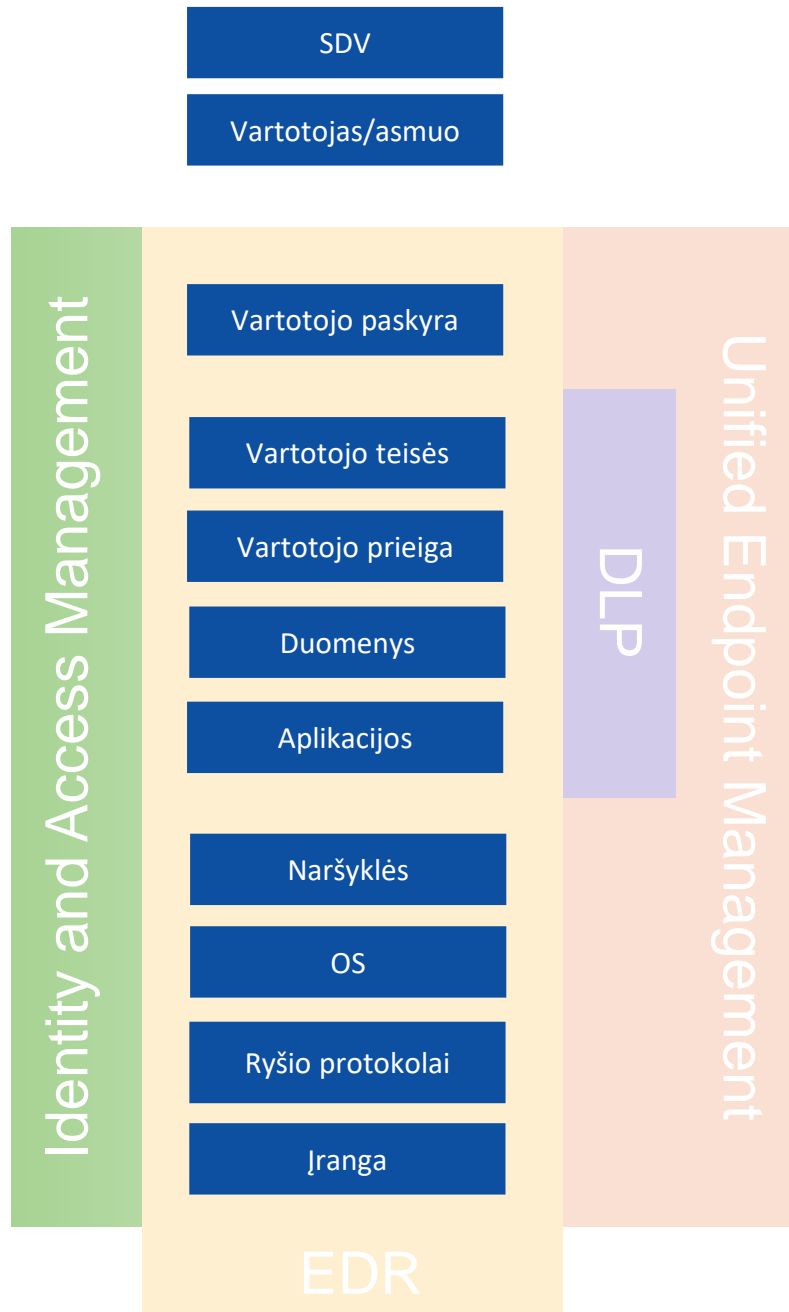
PHYSIOLOGICAL

water, food, shelter, bare necessities for human survival

Source: SimplyPsychology.org

Skaitmeninė darbo vieta





Identity and Access Management

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

Microsoft Azure

[Home](#) > [ATEA, UAB | Security](#) > [Security | Conditional Access](#) > [Conditional Access | Overview](#) >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on their network or physical location. [Learn more](#)

Configure

Yes No

Name *

Example: 'Device compliance app policy'

Include Exclude

Assignments

Users

0 users and groups selected

Any network or location

All trusted networks and locations

All Compliant Network locations

Selected networks and locations

Target resources

No target resources selected

Network **NEW**

Any network or location

To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. [Learn more on how to enable GSA Adaptive Access Signaling.](#)

Conditions

1 condition selected

'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure Access capability of 'All Compliant network locations'. No action required. [Learn more.](#)

Access controls

Grant

0 controls selected

Session

0 controls selected

ATEA

Identity and Access Management

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

Microsoft Azure

Home > ATEA, UAB | Security > Security | Conditional Access > Conditional Access | Overview >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Name *

Example: 'Device compliance app policy'

Device platforms

Not configured

Assignments

Locations

Any network or location

Users

0 users and groups selected

Client apps

Not configured

Target resources

No target resources selected

Filter for devices

Not configured

Network

Any network or location

Authentication flows (Preview)

Not configured

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

0 controls selected

ATEA

Identity and Access Management

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The breadcrumb navigation is: Home > ATEA, UAB | Security > Security | Conditional Access > Conditional Access | New. The page title is "New" and the subtitle is "Conditional Access policy".

The main content area describes the policy: "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)".

The configuration fields are as follows:

- Name ***: Example: 'Device compliance app policy'
- Assignments**
 - Users**: 0 users and groups selected
 - Target resources**: No target resources selected
 - Network**: NEW, Any network or location
 - Conditions**: 1 condition selected
 - Access controls**
 - Grant**: 0 controls selected
 - Session**: 0 controls selected

The right-hand pane is titled "Session" and contains the following options:

- Use app enforced restrictions
- Use Conditional Access App Control
- Sign-in frequency
- Persistent browser session
- Customize continuous access evaluation
- Disable resilience defaults
- Use Global Secure Access security profile

Informational messages:

- Blue box: "This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. [Learn more](#)"
- Blue box: "This option only works with 'Global Secure Access' as the targeted resource."

Identity and Access Management

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The breadcrumb navigation is: Home > ATEA, UAB | Security > Security | Conditional Access > Conditional Access | Grant. The page title is "New" with a dropdown arrow, and the subtitle is "Conditional Access policy".

The main content area is titled "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)".

The configuration fields are as follows:

- Name ***: A text input field containing "Example: 'Device compliance app policy'".
- Assignments**: A section header.
- Users**: 0 users and groups selected.
- Target resources**: No target resources selected.
- Network**: NEW (highlighted in green), Any network or location.
- Conditions**: 1 condition selected.
- Access controls**: Grant (selected), 0 controls selected.
- Session**: 0 controls selected.

The right-hand pane is titled "Grant" and contains the following options:

- Block access
- Grant access
- Require multifactor authentication
- Require authentication strength
- Require device to be marked as compliant
- Require Microsoft Entra hybrid joined device
- Require approved client app (See list of approved client apps)
- Require app protection policy (See list of policy protected client apps)
- iOS Terms of Use Demo

For multiple controls:

- Require all the selected controls
- Require one of the selected controls

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

Unified Endpoint Management

The screenshot shows the Microsoft Intune admin center interface. The top navigation bar is blue with the text "Microsoft Intune admin center". Below it, there is a "Home" link and a list of navigation items: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Devices | Overview" and features a search bar. The left sidebar is expanded to show "By platform" with sub-items: Windows, iOS/iPadOS, macOS, Android, and Linux. Other sections include "Device onboarding" (Windows 365, Enrollment), "Manage devices" (Configuration, Compliance, Conditional access, Scripts and remediations, Group Policy analytics, eSIM cellular profiles (preview), Policy sets, Device categories, Partner portals), "Manage updates" (Windows updates, Apple updates, Android FOTA deployments), and "Organize devices" (Device clean-up rules, Filters).

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

Unified Endpoint Management

The screenshot shows the Microsoft Intune admin center interface. The top navigation bar is blue with the text "Microsoft Intune admin center". Below it, there is a "Home" button and a list of navigation items: Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Apps | Overview" and includes a search bar. The "Overview" section is expanded, showing a list of categories: All apps, Monitor, By platform (Windows, iOS/iPadOS, macOS, Android), Policy (App protection policies, App configuration policies, iOS app provisioning profiles, S mode supplemental policies, Policies for Office apps, Policy sets, Quiet time), Other (App selective wipe, App categories, E-books, Filters), and Help and support (Help and support).

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

DLP

Naršyklės

OS

Ryšio protokolai

Įranga

Edit sensitivity label

- Label details
- Scope
- Items**
- Access control**
- Content marking
- Auto-labeling for files and emails
- Groups & sites
- Finish

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Only for a number of days

Users have offline access to the content for this many days

30

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

Edit sensitivity label

- Label details
- Scope
- Items
- Groups & sites**
- Finish

Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. [Learn more about these settings](#)

- Privacy and external user access**
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.
- External sharing and Conditional Access**
Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.
- Private teams discoverability and shared channel settings**
Decide whether private teams will be discoverable in searches and control the types of teams that can be invited to shared channels.

Apply a label to channel meetings

For Teams channels that have this label applied, you can also select a label to automatically apply to any meetings created from the channel. Users won't be able to change or remove the label. [Learn more about this setting](#)

None

Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ✓ Items
- **Groups & sites**
- **Privacy & external user access**
- External sharing & conditional access
- Private teams & shared channel settings
- Finish

Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

Privacy

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

- Public
Anyone in your organization can access the group or team (including content) and add members.
- Private
Only team owners and members can access the group or team, and only owners can add members.
- None
Team and group members can set the privacy settings themselves.

External user access

- Let Microsoft 365 Group owners add people outside your organization to the group as guests. [Learn about guest access](#)



Edit sensitivity label

- Label details
- Scope
- Items
- Groups & sites**
- Privacy & external user access
- External sharing & conditional access**
- Private teams & shared channel settings
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

- Anyone ⓘ
Users can share files and folders using links that don't require sign-in.
- New and existing guests ⓘ
Guests must sign in or provide a verification code.
- Existing guests ⓘ
Only guests in your organization's directory.
- Only people in your organization
No external sharing allowed.

Use Microsoft Entra Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

- Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [Microsoft Entra hybrid joined](#) or enrolled in Intune).

ⓘ For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

- Allow full access from desktop apps, mobile apps, and the web
- Allow limited, web-only access ⓘ
- Block access ⓘ
- Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)
No authentication contexts set up yet

Edit sensitivity label

- Label details
- Scope
- Items
- Groups & sites**
- Privacy & external user access
- External sharing & conditional access
- Private teams & shared channel settings**
- Finish

Private teams discoverability and shared channel controls

Decide whether labeled private teams will be discoverable in searches, and control how channels can be shared with other teams. [Learn more about this setting](#)

Private team discoverability

Allow users to discover private teams that have this label applied

When selected, any user assigned to a Teams policy that has 'Private teams discovery' turned on can search for and discover private teams that have this label applied. Clear this option to prevent those users from discovering these labeled private teams.

ⓘ If the 'Private teams discovery' setting turned off in a Teams policy, all users assigned to that policy won't be able to discover private teams, even if this option is selected and the label is applied.

Teams shared channels

Control the types of teams that can be invited to shared channels in labeled teams. These settings don't affect invitations to individual users.

Internal only

When selected, external teams can't be invited to shared channels. This setting doesn't affect teams that were invited to shared channels before the label was applied.

Same label only

When selected, only teams with this label applied can be invited to shared channels. This setting doesn't affect teams from other organizations or teams that were invited to shared channels before the label was applied.

Private teams only

When selected, public teams (including external public teams) can't be invited to shared channels. Any previously invited public teams are removed when the label is applied. If an invited team's privacy setting is changed from private to public, it's removed from the channel.

ⓘ The channel can always be shared with the parent team, even if the parent team is a public team.

Edit policy

- Labels to publish
- Admin units
- Users and groups
- Settings**
- Documents
- Emails
- Meetings
- Sites and Groups**
- Fabric and Power BI
- Name
- Finish

Default settings for sites and groups

Apply a default label to sites and groups

The label you choose will automatically be applied to new, unlabeled SharePoint sites and Microsoft Groups. Users can always change the default label before they create the site or group.

Default label

- Requires users to apply a label to their groups or sites

- Template or custom policy
- Name
- Admin units
- Locations**
- Policy settings
- Policy mode
- Finish

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. [Learn more about role group permissions.](#) ✕

[View role groups](#)

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

⚠ Some of your users devices are in not updated state. [See more details](#)

Location	Scope	Actions
<input checked="" type="checkbox"/> Exchange email	All groups	Edit
<input checked="" type="checkbox"/> SharePoint sites	All sites	Edit
<input checked="" type="checkbox"/> OneDrive accounts	All users & groups	Edit
<input checked="" type="checkbox"/> Teams chat and channel messages	All users & groups	Edit
<input type="checkbox"/> On-premises repositories	Turn on location to scope	
<input type="checkbox"/> Power BI workspaces	Turn on location to scope	

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

Įranga

EDR

ATEA

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security

Endpoint security | Endpoint detection and response

- Overview
 - Overview
 - All devices
 - Security baselines
 - Security tasks
- Manage
 - Antivirus
 - Disk encryption
 - Firewall
 - Endpoint Privilege Management
 - Endpoint detection and response**
 - App Control for Business (Preview)
 - Attack surface reduction
 - Account protection
 - Device compliance
 - Conditional access
- Monitor
 - Assignment failures
- Setup
 - Microsoft Defender for Endpoint
- Help and support
 - Help and support

Summary EDR Onboarding Status

Defender for Endpoint Connector Status

Defender for Endpoint connector unavailable

Windows devices onboarded to Defender for Endpoint


Refresh Report generated 9/17/2024, 6:13:10 AM

0 / 0



Endpoint detection and response (EDR) policies

Create policy Refresh Export Columns

Policy name	Policy type	Assigned	Platform
 No data found			

Create a profile

Platform: Windows

Profile: Endpoint detection and response

Endpoint detection and response

Microsoft Defender for Endpoint endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats

This policy applies to: Windows 10, Windows 11, and Windows Server

The settings in this policy can be targeted to: MDM, Microsoft Sense supported devices



Ačiū už kantrybę ir dėmesį!!!

Klausimai?