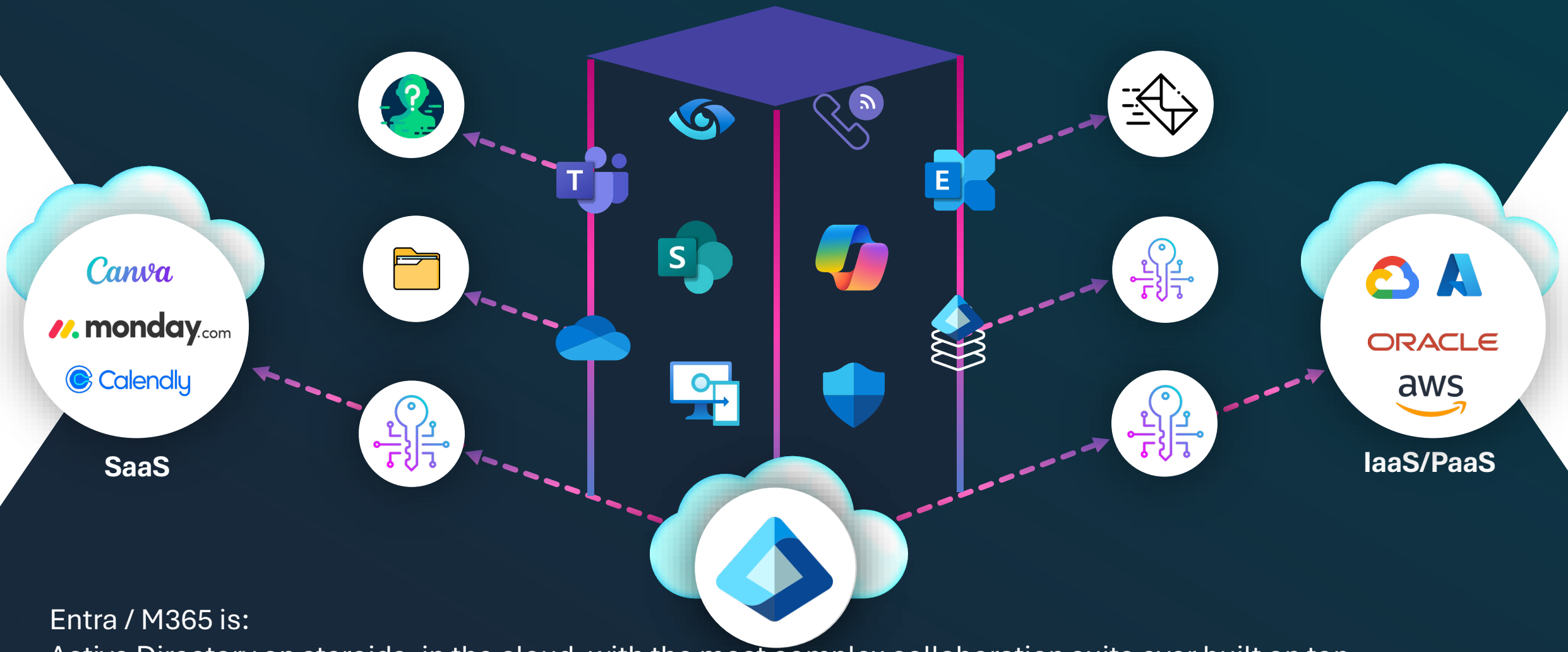
Cyber Resilience for Microsoft 365

Build layers of resilience into your Tenant

There has never been a security risk like Microsoft 365



Entra / M365 is:
Active Directory on steroids, in the cloud, with the most complex collaboration suite ever built on top, and then exposed to the internet

And Microsoft Tenants are exposed

71%

of Microsoft 365 tenants face 7 successful account takeover attacks per year

VECTRA®

79%

Increase in configuration tampering during attacks on Microsoft environments

Sophos X-Ops

63%

of M365 orgs are failing to implement the principle of least privilege

Microsoft

The Essential 8 (ASD)

The Australian Signals Directorate (equivalent of NSA in US) created the “Strategies to Mitigate Cyber Incidents” standard, which includes the “Essential 8”

The Essential 8 applies to:

Government Agencies in Australia and those doing business with Australian government Agencies

It is also best practice for all Australian organisations (private and public)

ASD AUSTRALIAN SIGNALS DIRECTORATE

CoreView

Impact for M365 Admins

The Essential 8 is very simple and clear. It includes:

- multi-factor authentication: must be configured and enforced
- restrict administrative privileges: this requires restriction of global and other admins, and also application privileges
- application control: many businesses will use Microsoft’s native endpoint/application control tech, requiring specific configurations
- patch applications & operating systems
- restrict Microsoft Office macros: requires very specific configurations to restrict Office macros
- user application hardening: requires office, internet explorer, and Microsoft suite configurations to be set very specifically
- **regular backups Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.**

AND THEY'RE NOT THE ONLY ONES…

Major Standards now have requirements for deployment and enforcement of configuration

NIST Special Publications 800-53
CM-3 Configuration Change Control

- Restrict configuration changes
- Document config changes
- Test & Validate changes before deploying them
- Identify when configurations occur without authorization

Gartner said there is no M365 backup without backing up and monitoring configurations:

> It's not just the documents and files stored in M365 that organizations are looking to back up. **If your main concern is around ransomware, or losing access to your tenant, you will want a solution that can monitor configuration drift**.
>
> Your first option is for your **solution to notify you that a configuration has been changed from your baseline**. Alternatively, you may want your solution to not just report and detect changes, but to **automatically revert them as well**.
>
> Unfortunately, **there aren't any native functions that can track and remediate this**, however Microsoft does provide an unsupported, open source solution with Microsoft365DSC.

Gartner ID – G00816401

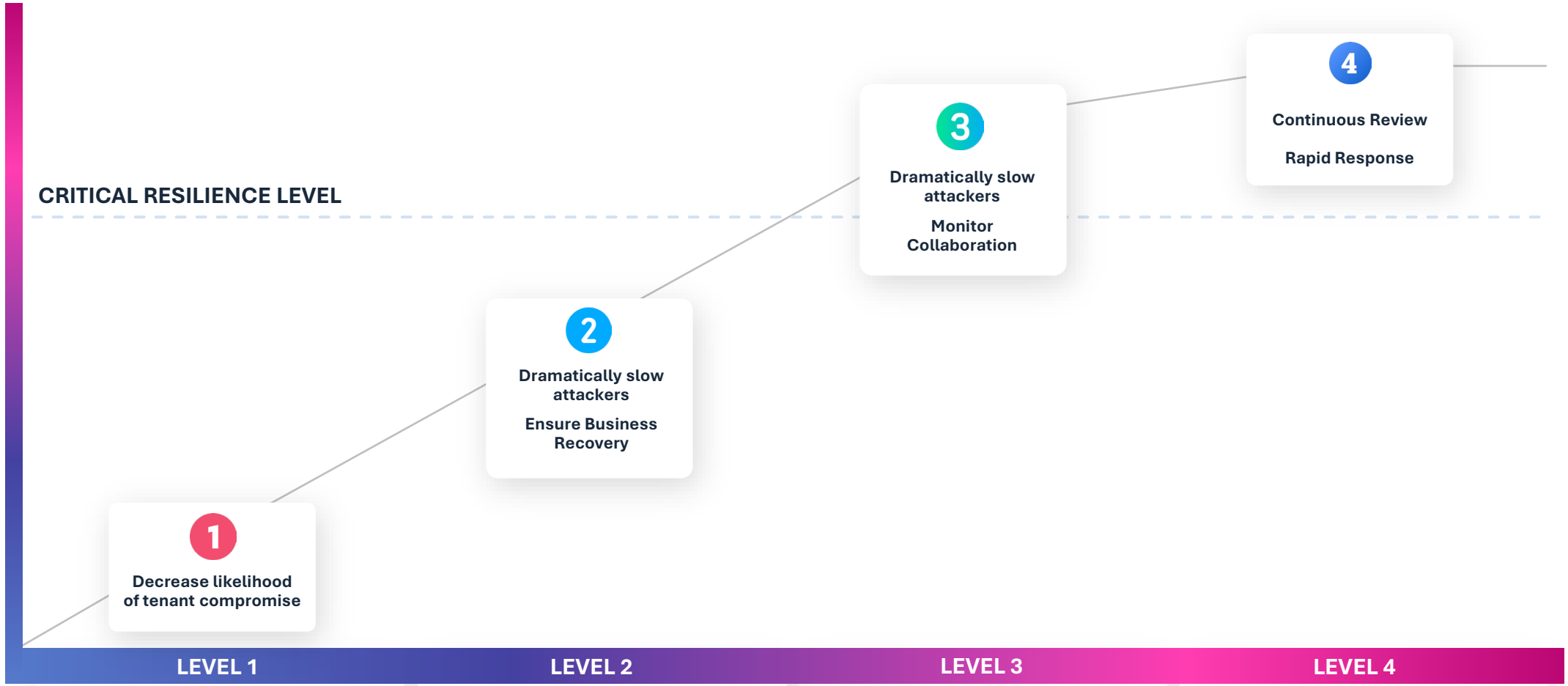
M365 Key Security Questions

What is the compliance state of your Microsoft 365?

How quickly could you restore to the last, verified backup of your M365 configuration?

Who has access to what? Are your admin rights segmented to minimize your exposure?

Microsoft 365 Cyber Resilience Maturity Model



ENFORCE ZERO TRUST ACCESS

- Detect users without MFA
- Enforce Conditional Access
- Detect weak passwords
- Detect access policies changes
- Detect guest/app access points

CONFIGURATION & BACKUP

- Configuration Backup
- Deploy Secure Configurations
- Detect Configuration Drift
- Enforce Change Management
- Detect & Test new M365 updates

LEAST PRIVILEGE & COLLABORATION

- Least Privilege Admin Roles
- Entra App Management
- External User Management
- Detect High Risk Files/Sharing
- Detect Suspicious Mailboxes

GOVERNANCE & AUTOMATION

- Sprawl & Lifecycle Management
- User Access Reviews
- Enhanced Admin UI/UX
- Secure Task Automation
- Rapid Extensibility

The Essential 8 (ASD)

The Australian Signals Directorate (equivalent of NSA in US) created the “Strategies to Mitigate Cyber Incidents” standard, which includes the “Essential 8”

The Essential 8 applies to:

Government Agencies in Australia and those doing business with Australian government Agencies

It is also best practice for all Australian organisations (private and public)

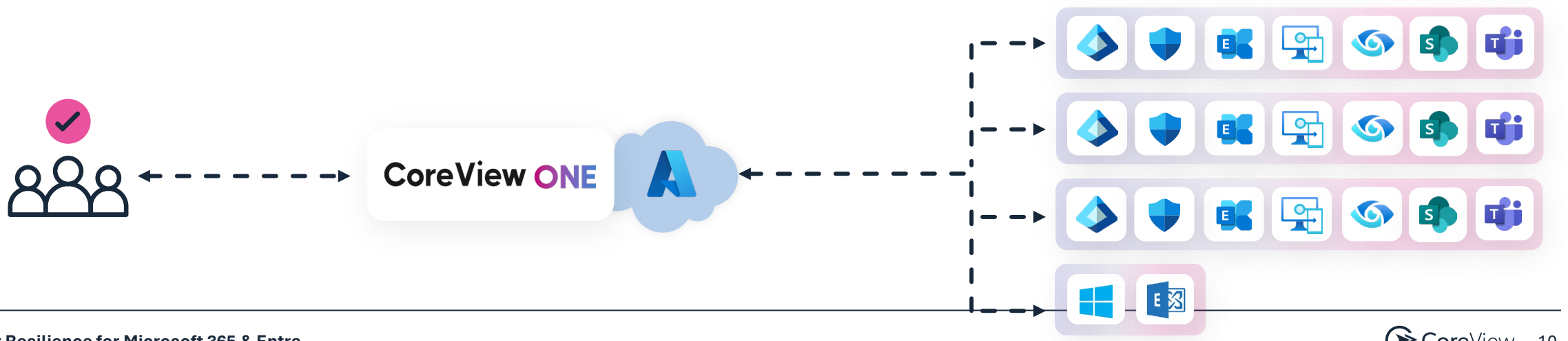
ASD AUSTRALIAN SIGNALS DIRECTORATE

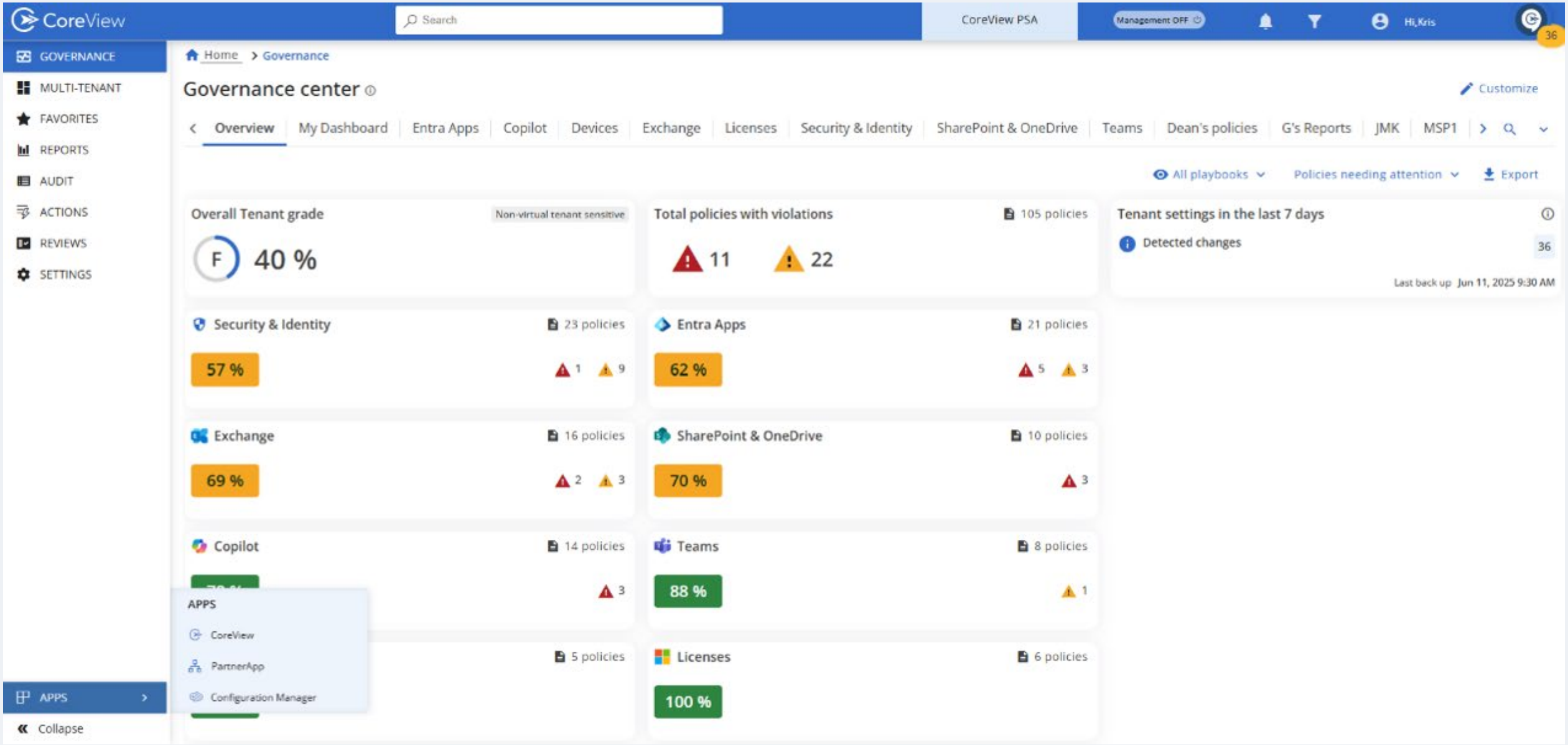
Essential Eight Strategy	CoreView Template Setting	Required for Maturity Level 1	Required for Maturity Level 2	Required for Maturity Level 3
Multi-factor Authentication (MFA)	Use FIDO2	✓	✓	✓
	Enable Temporary Access Path	✓	✓	✓
	Use X509 Certificate	✓	✓	✓
	Use Microsoft Authenticator (Number Match Only)	✓		
	Enforce Conditional Access: ACSC Essential Eight MFA Policy	✓	✓	✓
	Configure Entra ID Authentication Strength Settings	✓	✓	✓
Restrict Administrative Privileges	Define Granular Admin Roles and PIM	✓	✓	✓
Patch Operating Systems	Enforce Latest Version Windows Compliance Policy	✓	✓	✓
	Enforce Latest Version macOS Compliance Policy	✓	✓	✓
	Configure Windows Update Frequency (Test, Pilot, Fast, Broad, Critical)	✓	✓	✓
	Configure Windows Driver Updates	✓	✓	✓
Application Control	Enforce Attack Surface Reduction (ASR) Rules	✓	✓	✓
Configure Microsoft Office	All Macros Disabled	✓	✓	✓
	Macros Enabled for Trusted Publishers	✓	✓	✓
	Office Macro Hardening – Prevent Activation of OLE	✓	✓	✓
User Application Hardening	Apply ACSC Windows Hardening Guidelines	✓	✓	✓
	Apply ACSC Edge Hardening Guidelines		✓	✓
	Disable Internet Explorer	✓	✓	✓
	Remove Legacy Features (PowerShell 2.0, IE, .NET 3.5)	✓	✓	✓
Regular Backups / Data Retention	Enforce Tenant Backup Retention Policies (SharePoint, OneDrive, Exchange, Teams)	✓	✓	✓

CoreView Cyber Resilience for Microsoft 365 & Entra

Build resilience at each stage of the attack

1	2	3	4	5
Tenant Compromise	**Configuration tampering**	**Privilege Elevation & Lateral Movement**	**Incident Response & Recovery**	**Governance & Lifecycle**
CoreView **ENFORCES** zero trust access across your environment	CoreView **DETECTS** config changes and collaboration risks	CoreView **SEGMENTS** for least privilege in any environment	CoreView **REVEALS** changes, and **REWINDS** after an incident	CoreView **MINIMIZES** your attack surface and enforces governance




CoreView
Search
CoreView PSA
Management OFF
Hi,Kris
36
GOVERNANCE
MULTI-TENANT
FAVORITES
REPORTS
AUDIT
ACTIONS
REVIEWS
SETTINGS
Home > Governance
Governance center
Customize
Overview
My Dashboard
Entra Apps
Copilot
Devices
Exchange
Licenses
Security & Identity
SharePoint & OneDrive
Teams
Dean's policies
G's Reports
JMK
MSP1
All playbooks
Policies needing attention
Export
Overall Tenant grade
Non-virtual tenant sensitive
F
40 %
Total policies with violations
105 policies
11
22
Tenant settings in the last 7 days
Detected changes
36
Last back up Jun 11, 2025 9:30 AM
Security & Identity
23 policies
57 %
1
9
Entra Apps
21 policies
62 %
5
3
Exchange
16 policies
69 %
2
3
SharePoint & OneDrive
10 policies
70 %
3
Copilot
14 policies
3
Teams
8 policies
88 %
1
5 policies
Licenses
6 policies
100 %
APPS
CoreView
PartnerApp
Configuration Manager
APPS
Collapse

M365 Best practices

What you need to know and manage to stay secure

Discovery

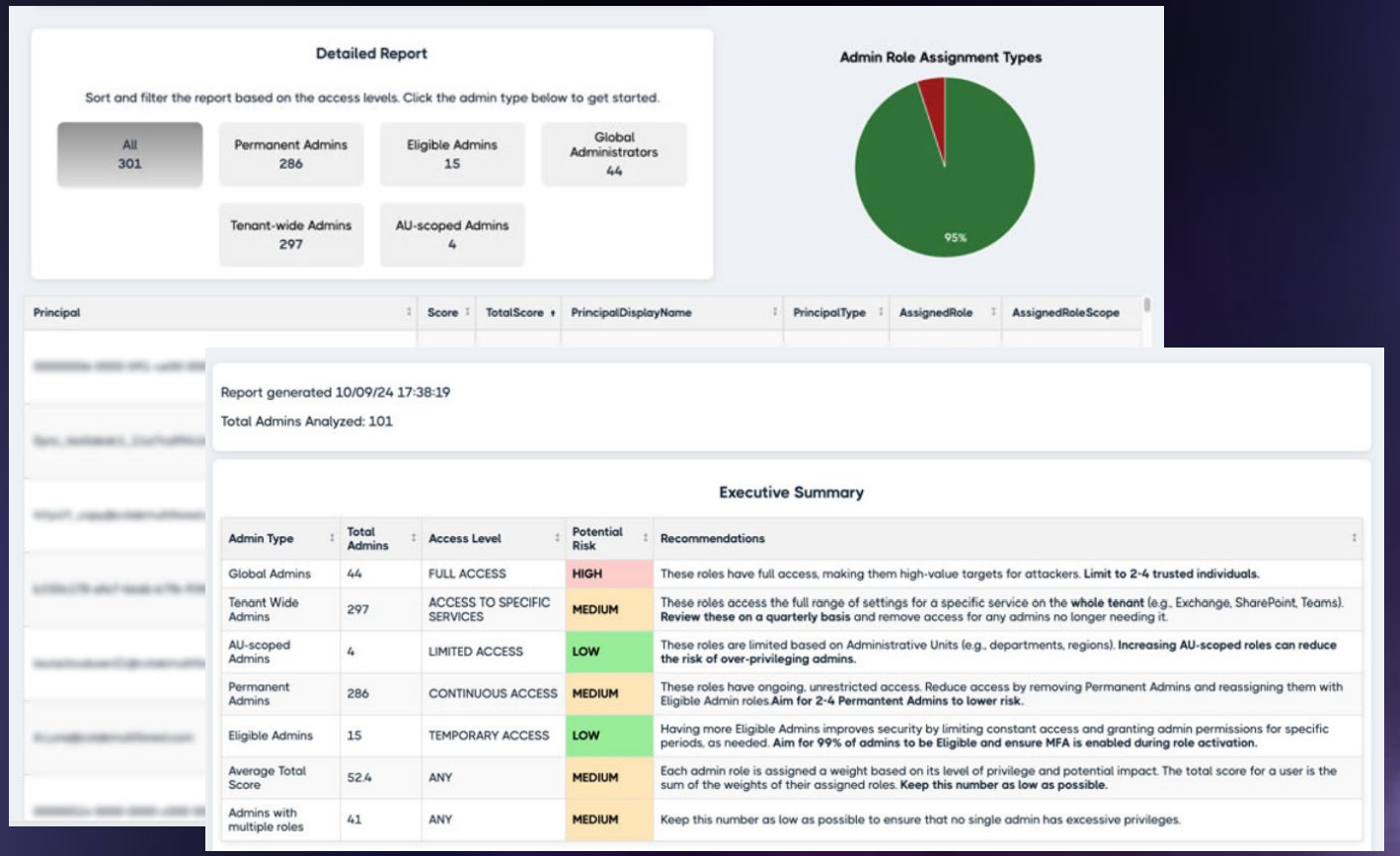
- Which Accounts Have Admin Access?
- What is my current tenant configuration?
- Do I have backups of my tenant configuration?
- Which Tasks Actually need Admin?
- Is my tenant in compliance?
- How quickly can I restore (DR)?

Response

- Least Privilege Audit, Grant Access by Task
- Report and compare against best practice
- Backup configuration to code

FREE Tool

M365 Admin Permissions Report



The tool generates:

- **A complete list of all admins with global, tenant-wide, and AU-scoped access**
- **Every app and service principal your admins can access, modify, or share**
- **Recommendations to grant least privileged access instead**

https://www.coreview.com/free-tool/admin-permissions-report