WEBINAR: IN VIER SCHRITTEN DIE SICHERHEIT UND RESILIENZ IHRES TENANTS ERHÖHEN.

first frame networkers

HERZLICH WILLKOMMEN

first frame networkers

Vielen Dank, dass Sie sich die Zeit für uns nehmen!

Was Sie heute erwartet:

Ein spannendes Referat über Massnahmen zur Verbesserung der Sicherheit von Microsoft 365-Tenants, inkl. Live-Demo und Praxisbeispiel.

Das Webinar wird in Schweizerdeutsch gehalten.

JÖRG KOCH
Leiter Marketing
first frame networkers ag

HERZLICH WILLKOMMEN

first frame networkers

PHILIPPE HIRZEL

Projektleiter Security Services
first frame networkers ag

- Seit insgesamt 8 Jahren bei der first frame networkers ag.
- Seine Aufgabe: Managed Services im Security-Bereich auf- und auszubauen.
- Aktuell studiert er am SANS Technology Institute für den Master of Science in Information Security Engineering.
- Neben der Arbeit kocht Philippe Hirzel gerne und ist Jugend- und Sport-Leiter (Ski).

AGENDA

first frame networkers

- 11:00 Begrüssung, Jörg Koch
- 11:05 M365 Security: In 4 Schritten die Sicherheit und Resilienz Ihres Tenants erhöhen, Philippe Hirzel
- 11:35 Fragen & Antworten
- 11:45 Schluss

Fragen können mit der Chatfunktion gestellt werden.

DIE VIER SCHRITTE

first frame networkers

1. Schritt 1: Notfall-Administratorenzugänge einrichten
2. Schritt 2: Wichtigste Security-Einstellungen vornehmen
3. Schritt 3: Authentifizierung und Access konfigurieren
4. Schritt 4: ~200 Best Practices-Einstellungen laufend prüfen

GRUNDLAGEN

Switzerland

Geography

Regions

1 Available

Highlights

Microsoft streng
digital future wi
investments in c

Read more

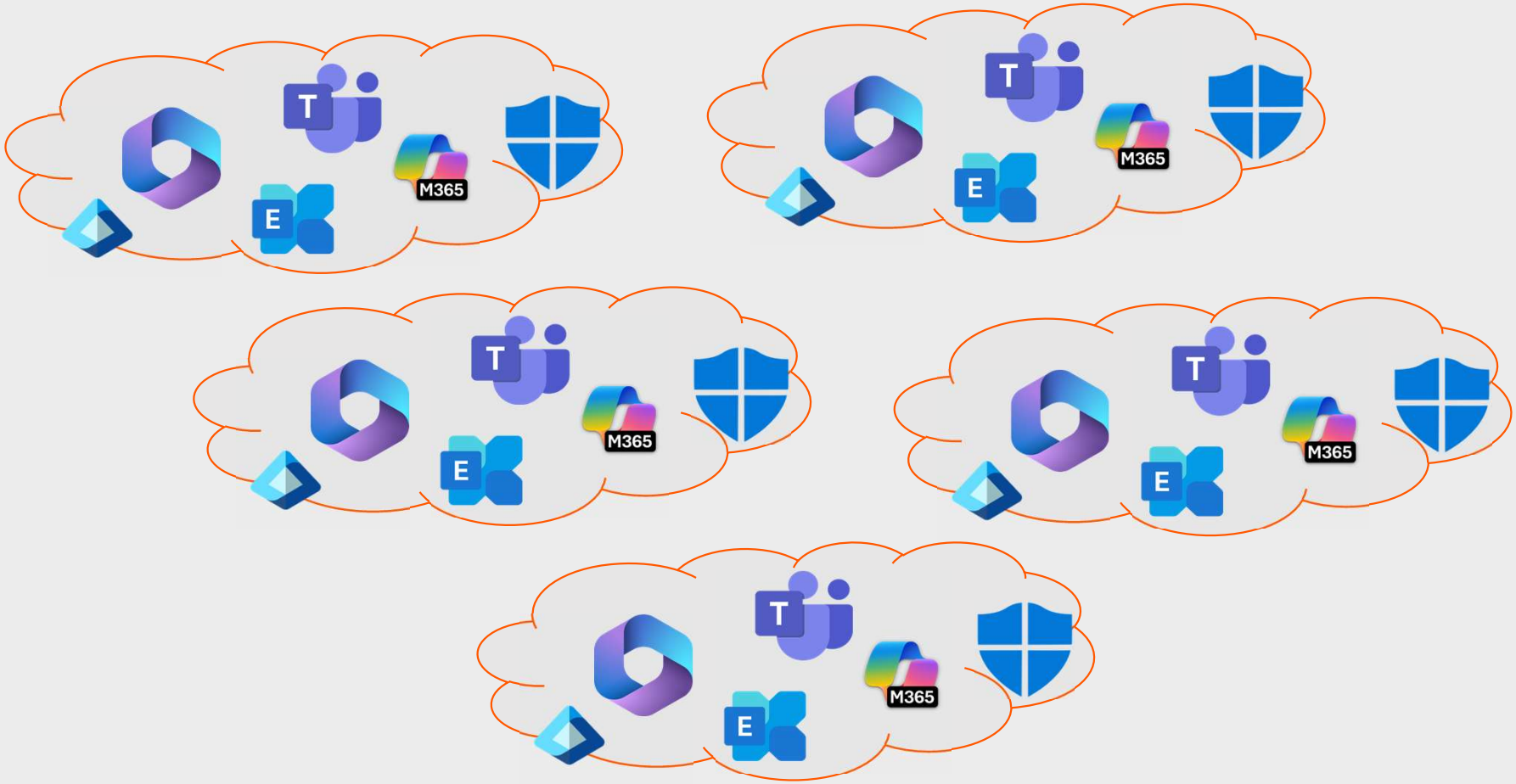
Microsoft Switze
local datacenter
Zones

Read more

Microsoft Switze
Dynamics 365, r
modules, and ad

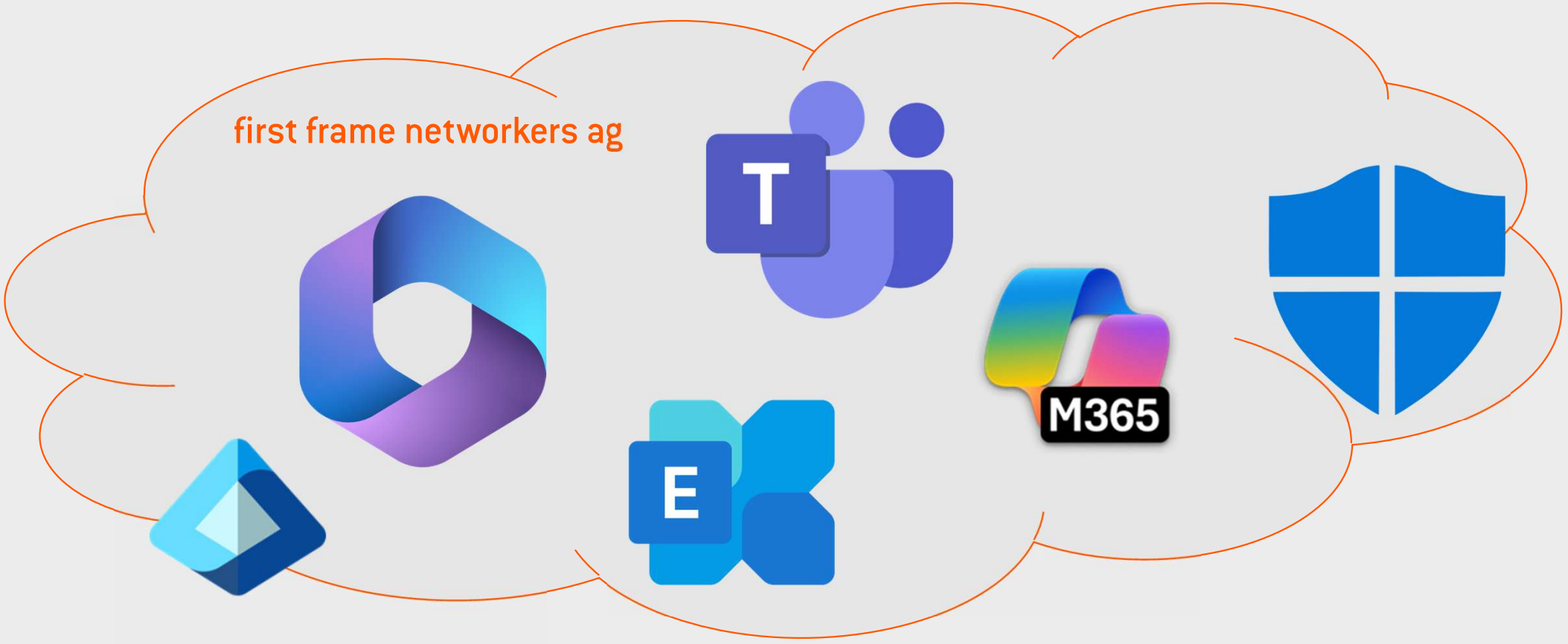
MICROSOFT 365

first frame networkers



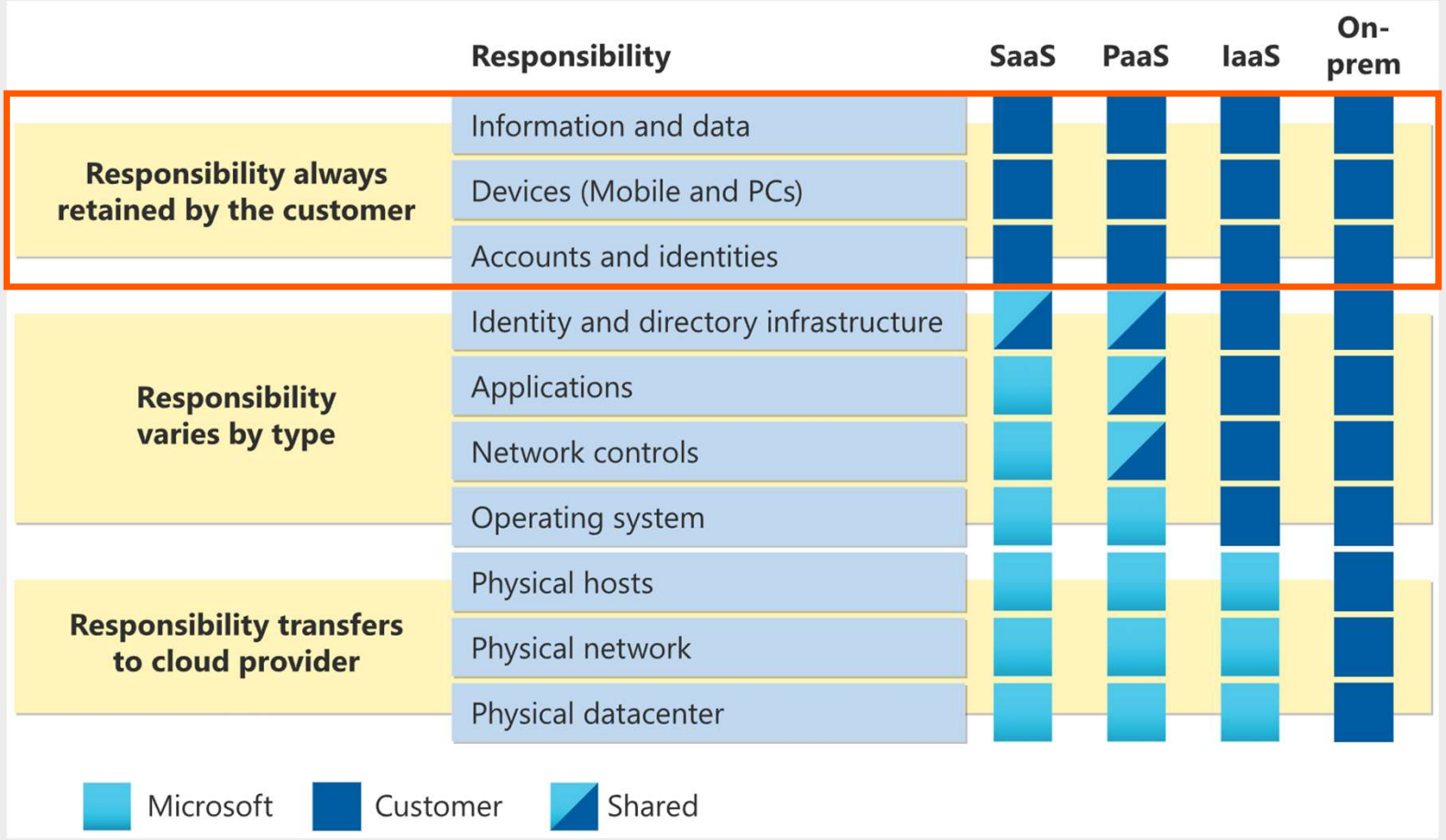
M365 TENANT

first frame networkers



SHARED RESPONSIBILITY

first frame networkers



WIESO DAS ALLES?

first frame networkers

- Tenant aktualisiert durch Microsoft
- Neue Einstellungen verfügbar
- Beispiele
  - Audit Log
  - App Registrieren
  - SMTP Basic Auth - https://admin.cloud.microsoft/?ref=MessageCenter/:/messages/MC786329
  - MFA Enforcement - https://admin.cloud.microsoft/?ref=MessageCenter/:/messages/MC1143999

EINSTELLUNGEN

UNIFIED AUDIT LOG

first frame networkers

- Wichtigstes Log im Tenant
- Weiterleiten für einfachere Arbeit
- Diverse Altlasten
  - In Exchange Online gespeichert
  - Bis zu 24h Verzögert
- Timeline
  - Aktiviert für neue Tenants seit Oktober 2021
  - Seit Oktober 2023 - 180 Tage statt 90 Tage Logaufbewahrung

PRÜFEN OB AKTIVIERT

first frame networkers

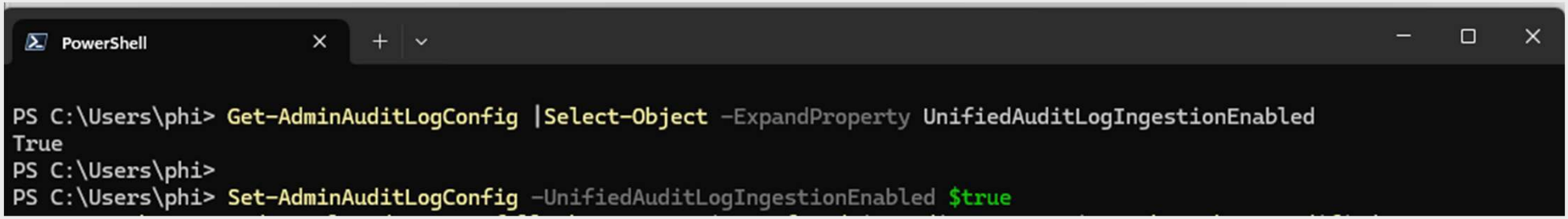
Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser

Import-Module ExchangeOnlineManagement

Connect-ExchangeOnline

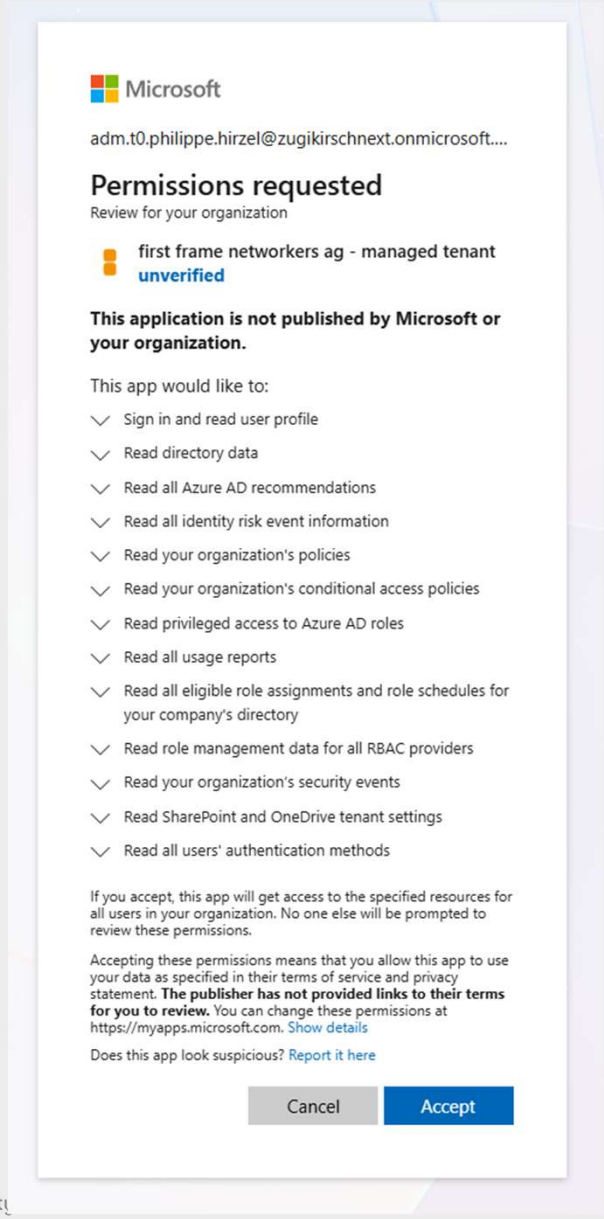
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

Get-AdminAuditLogConfig | Select-Object -ExpandProperty UnifiedAuditLogIngestionEnabled



APP REGISTRIEREN

- Jeder User kann Apps registrieren
- Missbrauch für Versand von SPAM
- Hintertüre für spätere Zugriffe



first frame networkers

SMTP BASIC AUTH

first frame networkers

- Basic Authentifizierung für E-Mail-Versand über Exchange Online wird deaktiviert am 01.03.2026
- Ursprünglich 01.09.2025
- Wie versendet Ihr Rechnungen, Newsletter etc?
- Alternativen vorhanden wie High Volume Email for Microsoft 365

FORCIERUNG VON MFA DURCH MICROSOFT

first frame networkers

Application Name	Enforcement starts
Azure portal	Second half of 2024
Microsoft Entra admin center	Second half of 2024
Microsoft Intune admin center	Second half of 2024
Azure command-line interface (Azure CLI)	October 1, 2025
Azure PowerShell	October 1, 2025
Azure mobile app	October 1, 2025
Infrastructure as Code (IaC) tools	October 1, 2025
REST API (Control Plane)	October 1, 2025
Azure SDK	October 1, 2025

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication?tabs=dotnet

CONDITIONAL ACCESS RICHTLINIEN

first frame networkers

Policy name	Created by	State	Alert
Multifactor authentication and reauthentication for risky sign-ins	MICROSOFT	On	
Multifactor authentication for admins accessing Microsoft Admin Portal	MICROSOFT	On	
CA - 011 Block access for unknown or unsupported device platform	USER	Report-only	
CA - 013 Require TAP for Device Registrations	USER	Report-only	
CA - Allowed Country List - 009	USER	Report-only	
CA - Block Legacy Authentication - 008	USER	Report-only	
CA - Block forbidden Countries - 009	USER	Report-only	
CA - Block high-risk sign-ins - 014	USER	Report-only	
CA - Require MAM Policy for Mobile - "000"	USER	Report-only	The policy uses the Client App grant control, which will retire in March 2026. Learn more

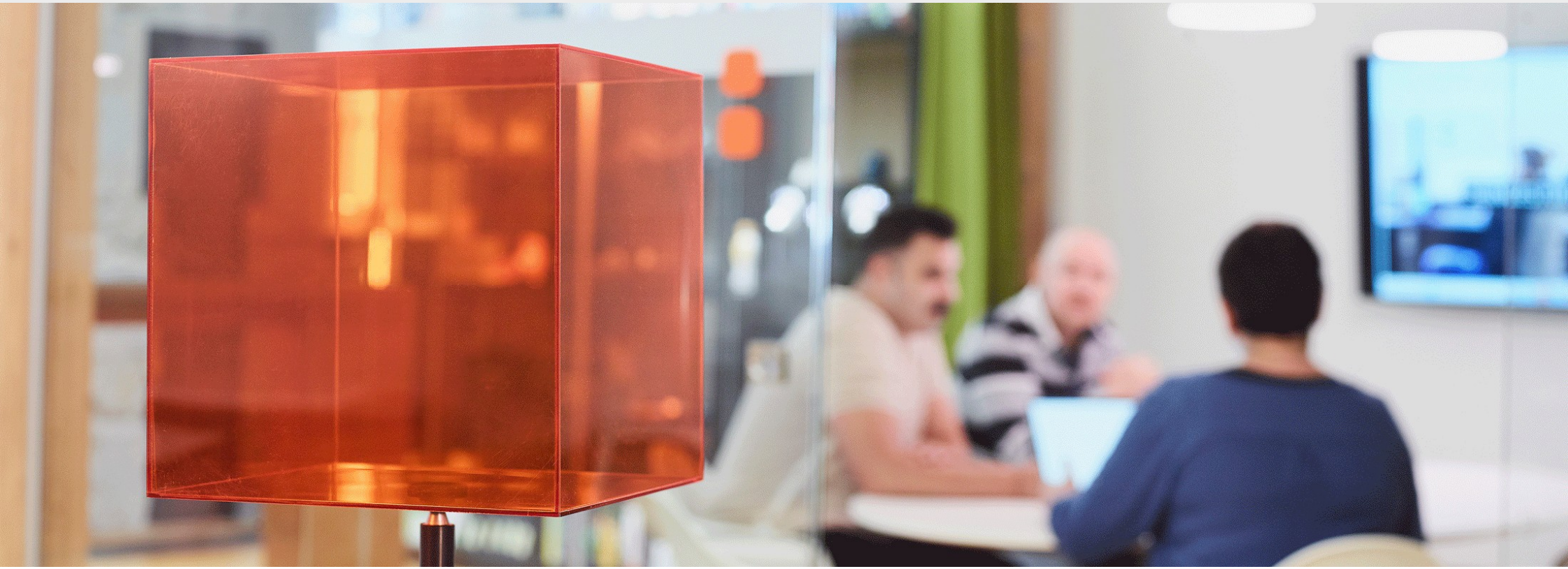
DEMO

LINKS AUS DER DEMO

first frame networkers

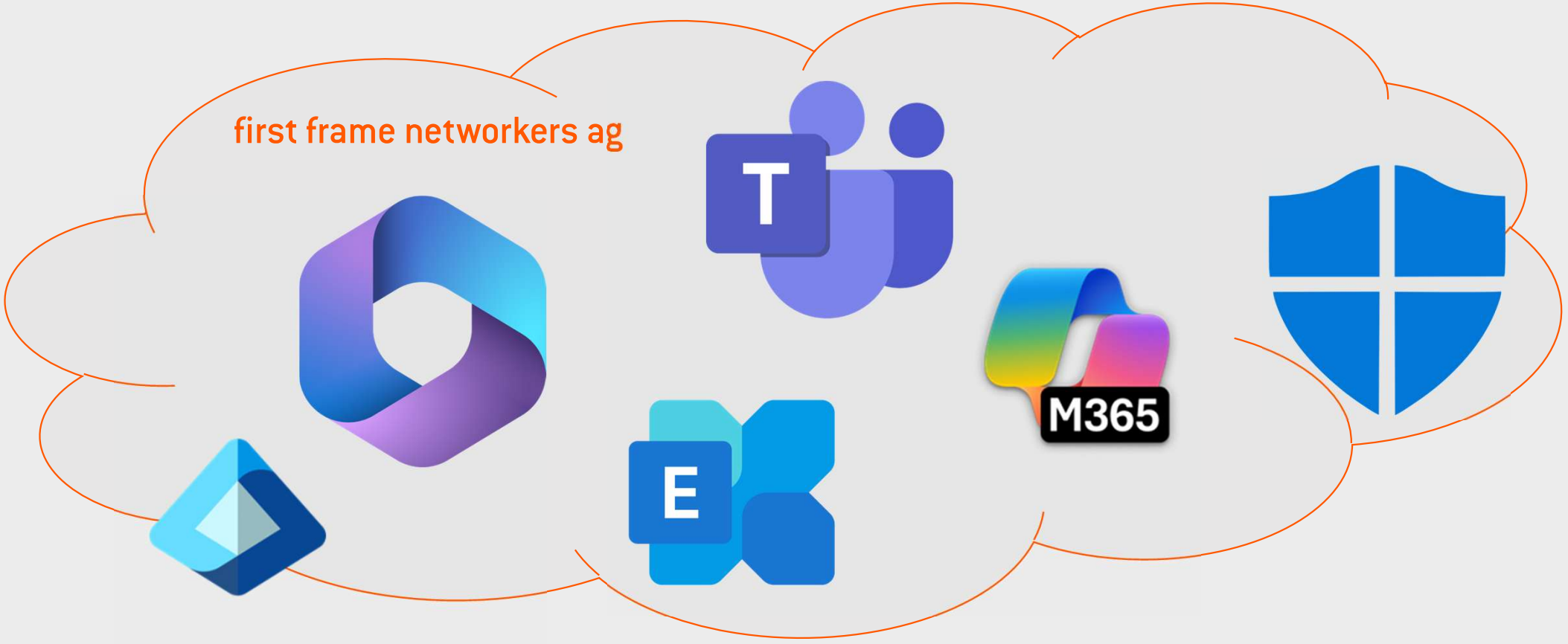
- App Registration
- SMTP Basic Auth Report
- UAL Suche

AUTHENTIFIZIERUNG

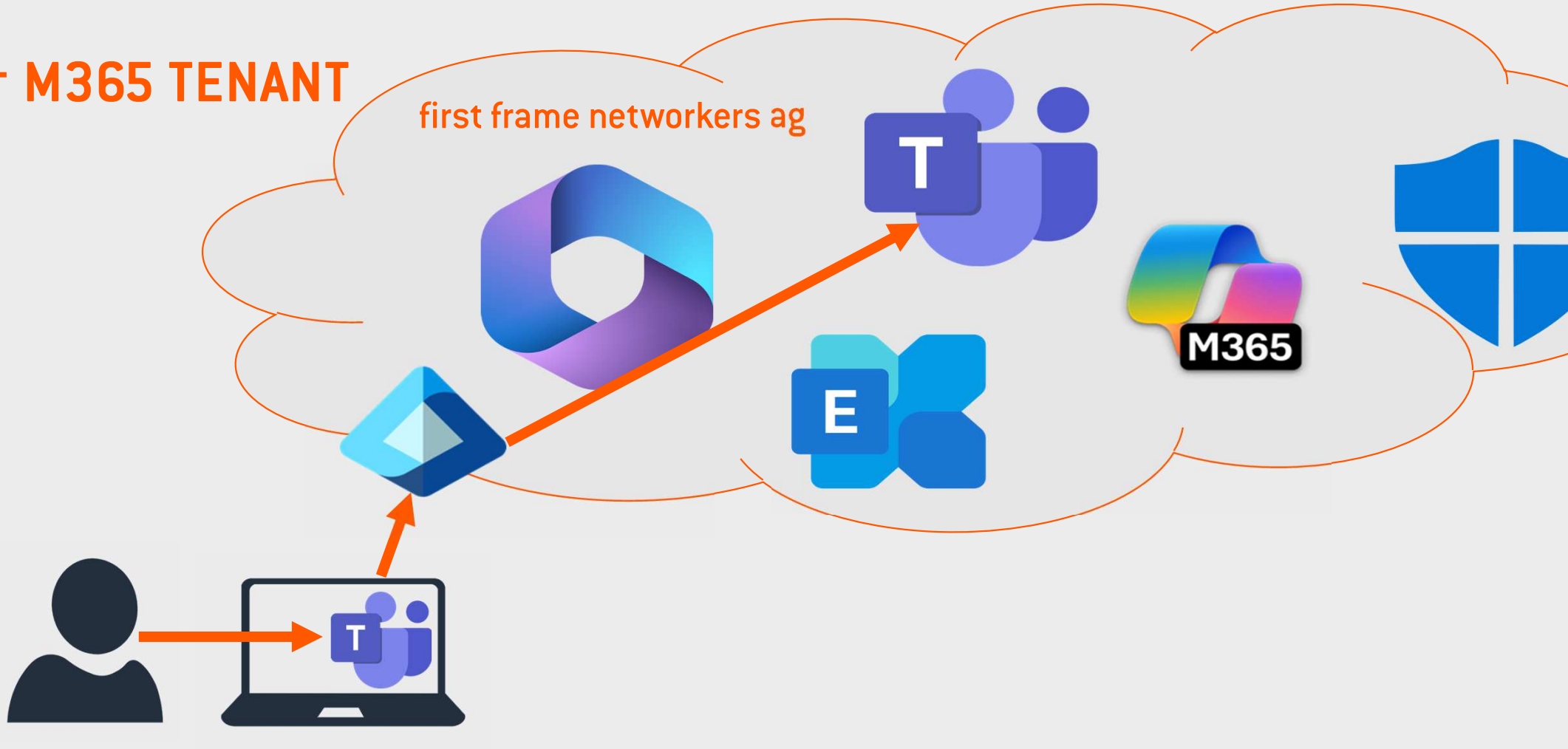


M365 TENANT

first frame networkers



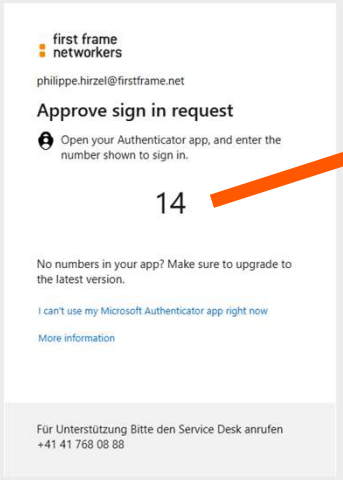
M365 TENANT

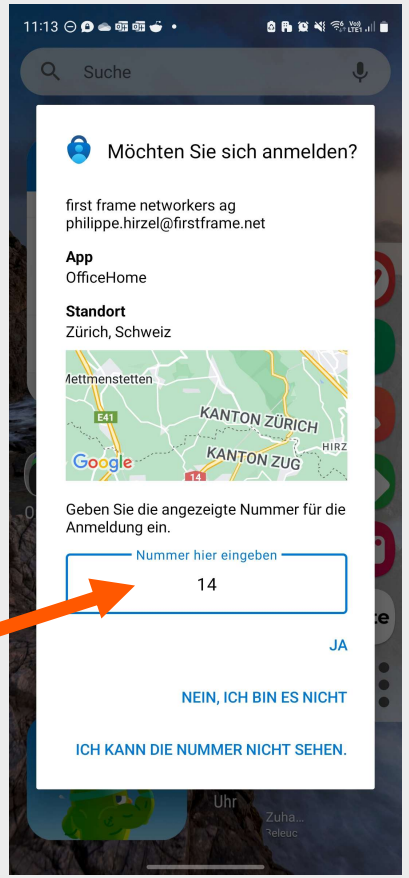


ENTRA ID

first frame networkers

- «Firewall» der Cloud
- Login für alle Microsoft Cloud-Dienste
- Multi-Faktor-Authentifizierung (MFA)
- Conditional Access für Steuerung vom Zugriff
  - MFA-Ausnahmen
  - Zugriff nur von Firmen-Geräten
  - Etc.

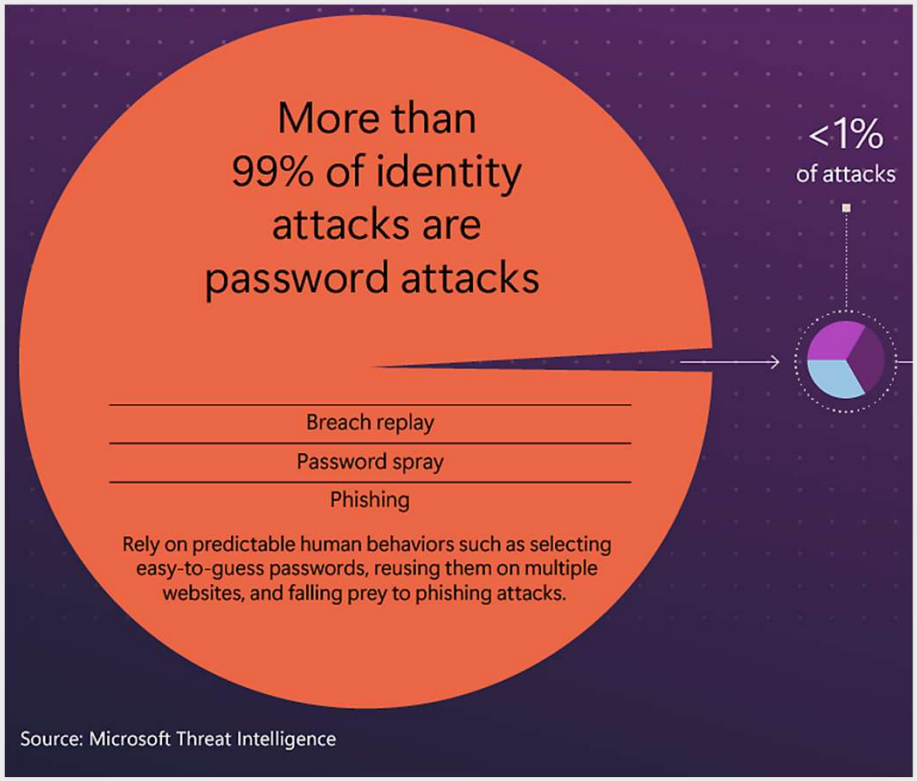




MFA IST ESSENZIELL

first frame networkers

- **99.2% Reduktion vom Risiko** einer Account-Kompromittierung



Microsoft Digital Defense Report 2024

ENTRA ID

first frame networkers

Entra ID Free

- Gratis für M/O365 Kunden
- 7 Tage Logs
- MFA an oder aus

Entra ID P1

- 30 Tage Logs
- MFA granular konfigurierbar
- Conditional Access, um granular den Zugriff auf Ressourcen zu steuern
- Optional: Überwachen von Notfall-Admins

Entra ID P2

- 30 Tage Logs
- MFA granular konfigurierbar
- Conditional Access, um granular den Zugriff auf Ressourcen zu steuern
- Optional: Überwachen von Notfall-Admins
- Risiko-Basierte Anmeldung
- Schutz vor Impossible Travel uvm.

Entra ID P1 ist die richtige Lösung für die meisten Kunden

NOTFALL ADMINISTRATOREN

first frame networkers

- Aussperren ist möglich!
- Ausnahmen in CA
- MFA trotzdem einrichten
- Anmeldung Überwachen
- Zwei erstellen

NOTFALL ADMINISTRATOREN

first frame networkers

Display Name	**Emergency Administrator Account**
UPN	**adm.emerg-24879@zugikirsch.onmicrosoft.com**
Passwort	**24-stelliges Passwort**
MFA	**MFA aus dem Passwortmanager**
Assignment	**Global Admin**

Hardware Key besser als MFA – für uns als Partner nicht handhabbar

KONTINUIERLICHE KONTROLLE

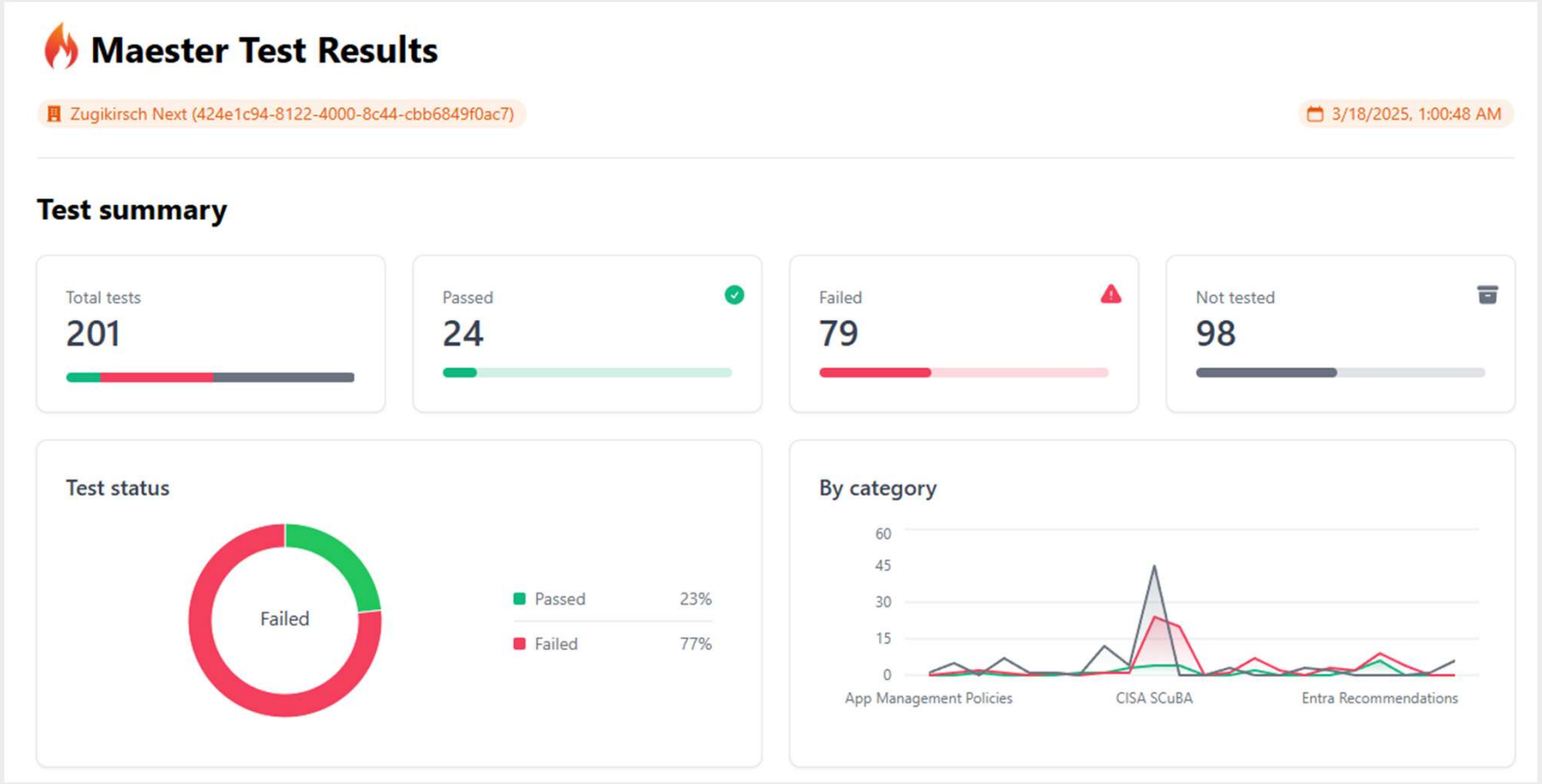
KONTINUIERLICHE KONTROLLE

first frame networkers

- Regelmässige Kontrolle von Einstellungen
- Tools wie Maester

KONTINUIERLICHE KONTROLLE

first frame networkers



ZUSAMMENFASSUNG

TIPPS

first frame networkers

Schützen Sie Ihren Zugang zur Cloud

Einstellungen ändern sich laufend

Überwachung nicht vergessen

MANAGED MICROSOFT TENANT

first frame networkers

CHF 49.90 / Monat / Tenant

Empfohlen: zusätzlich ~10.- pro Monat für Log Weiterleitung

Absichern Ihres „Zuhauses“ in der Cloud.

MANAGED MICROSOFT TENANT

first frame networkers

Service wird aufgeschaltet

MANAGED MICROSOFT TENANT

first frame networkers

Service wird aufgeschaltet

Wichtigste Sicherheitseinstellungen setzen:

- Registration von Apps unterbinden
- Passwörter laufen nicht aus
- Etc.

Regelmässige Prüfung von knapp 200 Einstellungen anhand Best Practises:

- CIS
- CISA SCUBA
- Etc.

Notfall Zugänge werden erstellt und bei uns abgelegt. Optional Ablage beim Kunden mit FIDO-Token.

Wichtigste Conditional Access Richtlinien:

- MFA für User & Admins
- Block Legacy Authentication

Zustellen von Quartalsreport

*Wichtigste Sicherheitseinstellungen gem. ffn best practises

KUNDENSTATEMENT

first frame networkers

«Als Energieversorger ist die Cybersicherheit von zentraler Bedeutung. Mit der first frame networkers ag haben wir einen zuverlässigen Partner, der uns mit den Managed Protected-Services proaktiv unterstützt. Gemeinsam schützen und sichern wir die ICT-Systeme des EWN optimal.»

Björn Gosswiler
Leiter ICT + Digitalisierung
Kantonales Elektrizitätswerk Nidwalden

Q & A

first frame networkers

NEXT STEPS

first frame networkers

Let's Talk!

- Mit Ihrem Account Manager
- Mit Philippe Hirzel: philippe.hirzel@firstframe.net oder +41 41 768 08 60

Weitere Infos

- Detaillierte Information Managed Microsoft Tenant-Service
- Verschiedene Blog-Artikel zum Thema IT-Security

FEEDBACK-FORMULAR

first frame networkers

- Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- Ihre Meinung ist uns sehr wichtig.
- Daher bitten wir Sie um eine Minute Ihrer wertvollen Zeit für die Feedbackumfrage.
- Unter allen ausgefüllten Fragebögen verlosen wir drei FFN-Rucksäcke.

- Den Link finden Sie auch im Chat:
- https://forms.office.com/e/uKFbgb6g37

Herzlichen Dank

first frame networkers