

— WEBINAR: MICROSOFT DEFENDER BOOTCAMP

 first frame
networkers



HERZLICH WILLKOMMEN



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

Was Sie heute erwartet:

Ein spannendes Referat über Funktionalitäten &
Einsatz von Microsoft Defender, dazu Praxisbeispiele
und Tipps.

Das Webinar wird in Schweizerdeutsch gehalten.



JÖRG KOCH

Leiter Marketing

first frame networkers ag

HERZLICH WILLKOMMEN



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

- ⇒ 11:00 Begrüssung, Jörg Koch
- ⇒ 11:05 Microsoft Defender Bootcamp, Philippe Hirzel
- ⇒ 11:35 Fragen & Antworten
- ⇒ 11:45 Schluss

Fragen können mit der Chatfunktion gestellt werden.

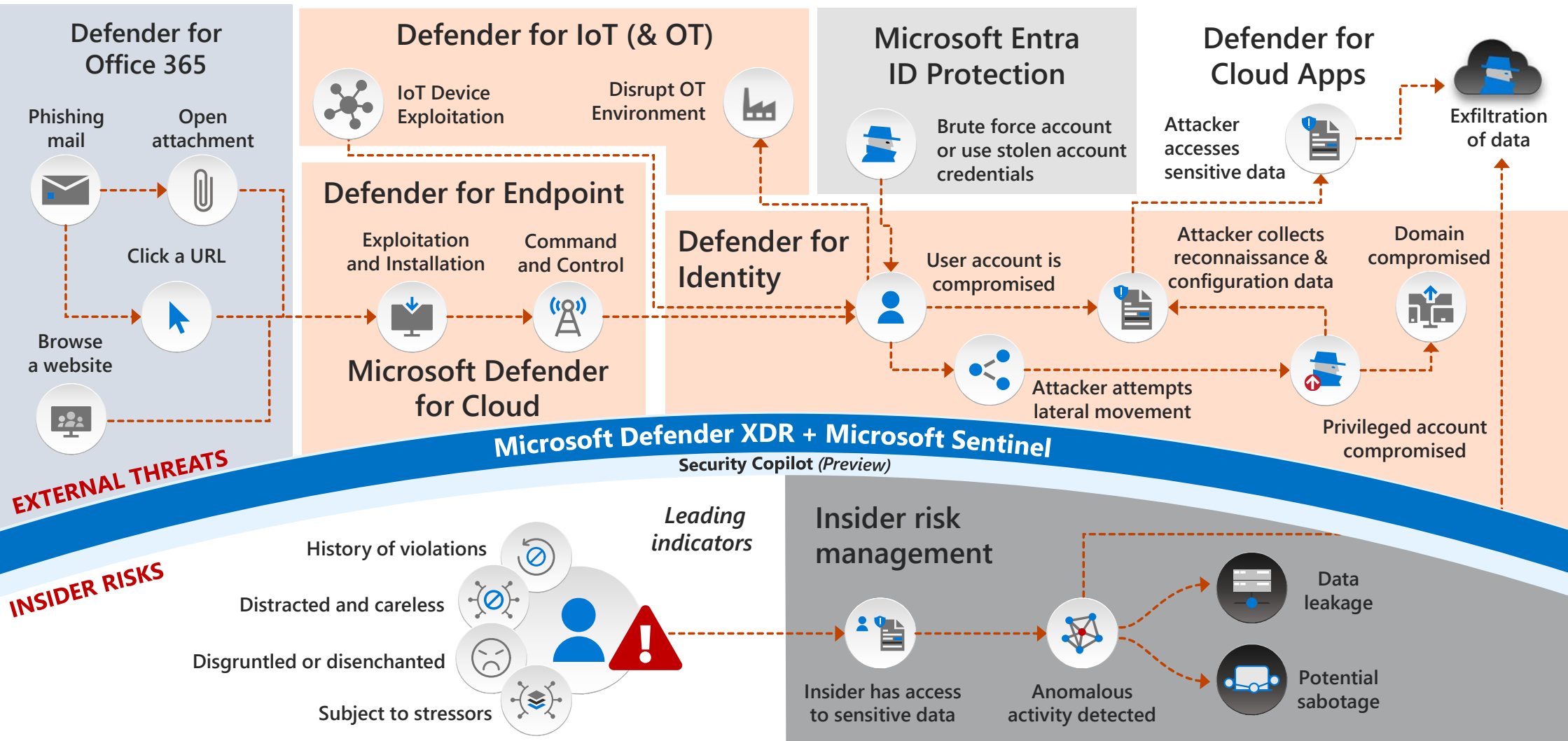


Defend across attack chains

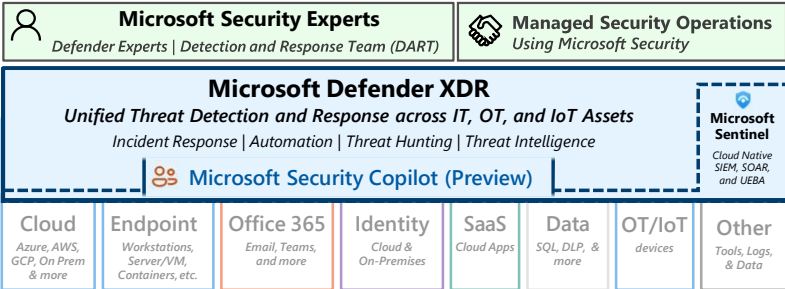
Insider and external threats



December 2023 – <https://aka.ms/MCRA>



Security Operations / SOC



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2023 – aka.ms/MCRA

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Adoption Framework](#)
2. [Security Documentation](#)
3. Cloud Security [Benchmarks](#)

Software as a Service (SaaS)



Microsoft Entra Internet Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Unified Endpoint Management (UEM)

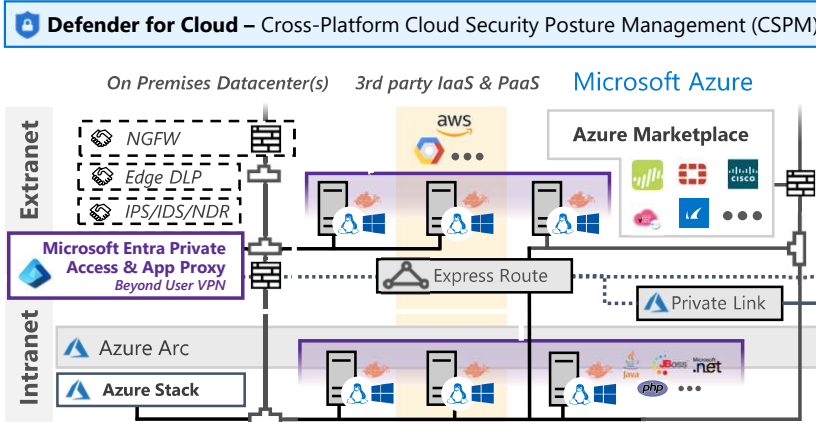
Intune Configuration Manager



Microsoft Defender for Endpoint
Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

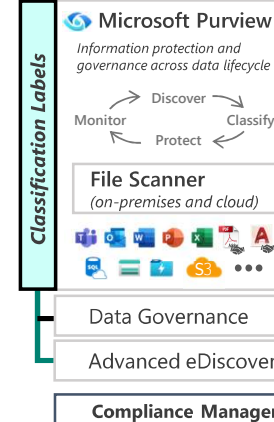
Hybrid Infrastructure – IaaS, PaaS, On-Premises



Secure Score
Compliance Dashboard

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- ... Security & Other Services

Information Protection



- Passwordless & MFA
 - Hello for Business
 - Authenticator App
 - FIDO2 Keys
 - Entra ID Protection
 - Leaked cred protection
 - Behavioral Analytics
 - ID Governance
 - Microsoft Entra PIM
 - External Identities
- Defender for Identity**
- Active Directory**

Securing Privileged Access – aka.ms/SPA

Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 Security

- Network protection
- Credential protection
- Full Disk Encryption
- Attack surface reduction
- App control
- Exploit protection
- Behavior monitoring
- Next-generation protection

IoT and Operational Technology (OT)



Microsoft Defender for IoT (and OT)

- ICS, SCADA, OT
- Asset & Vulnerability management
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Threat Detection & Response

Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises



Defender for APIs (preview)

People Security

- Attack Simulator
- Insider Risk Management
- Communication Compliance

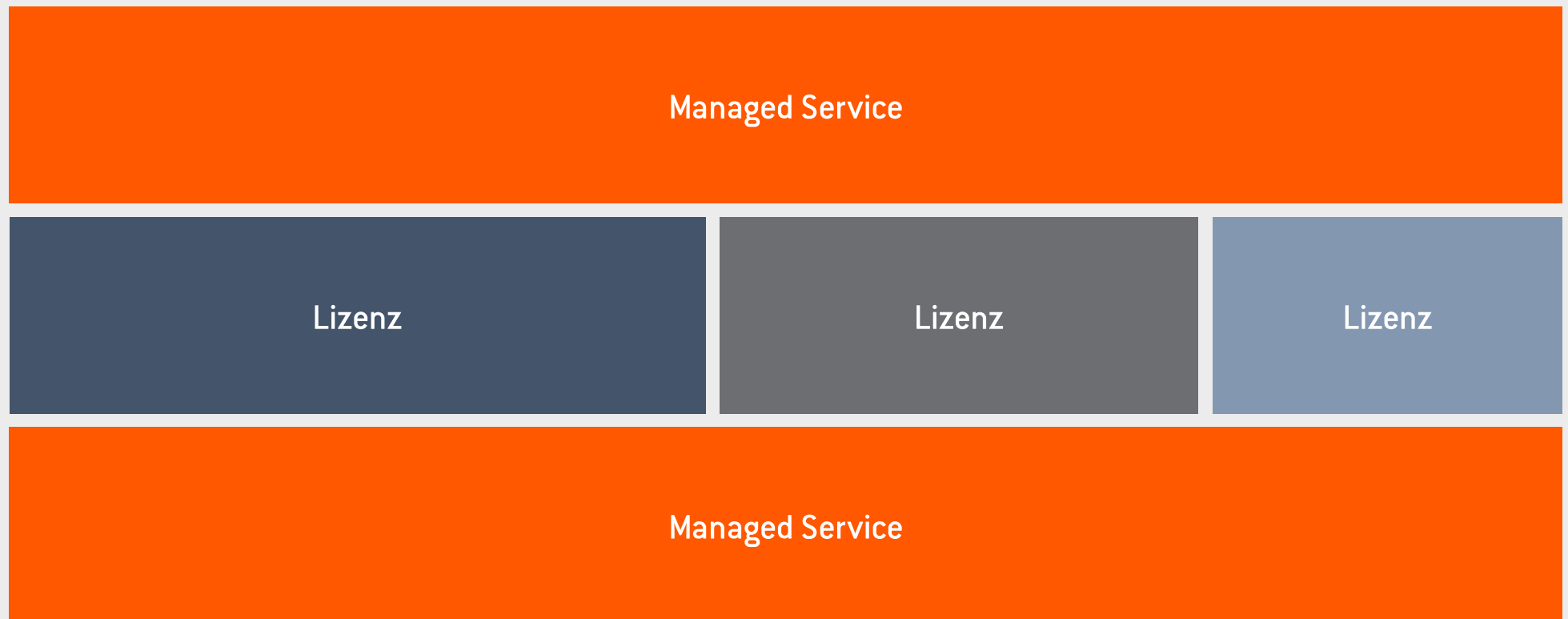
GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain

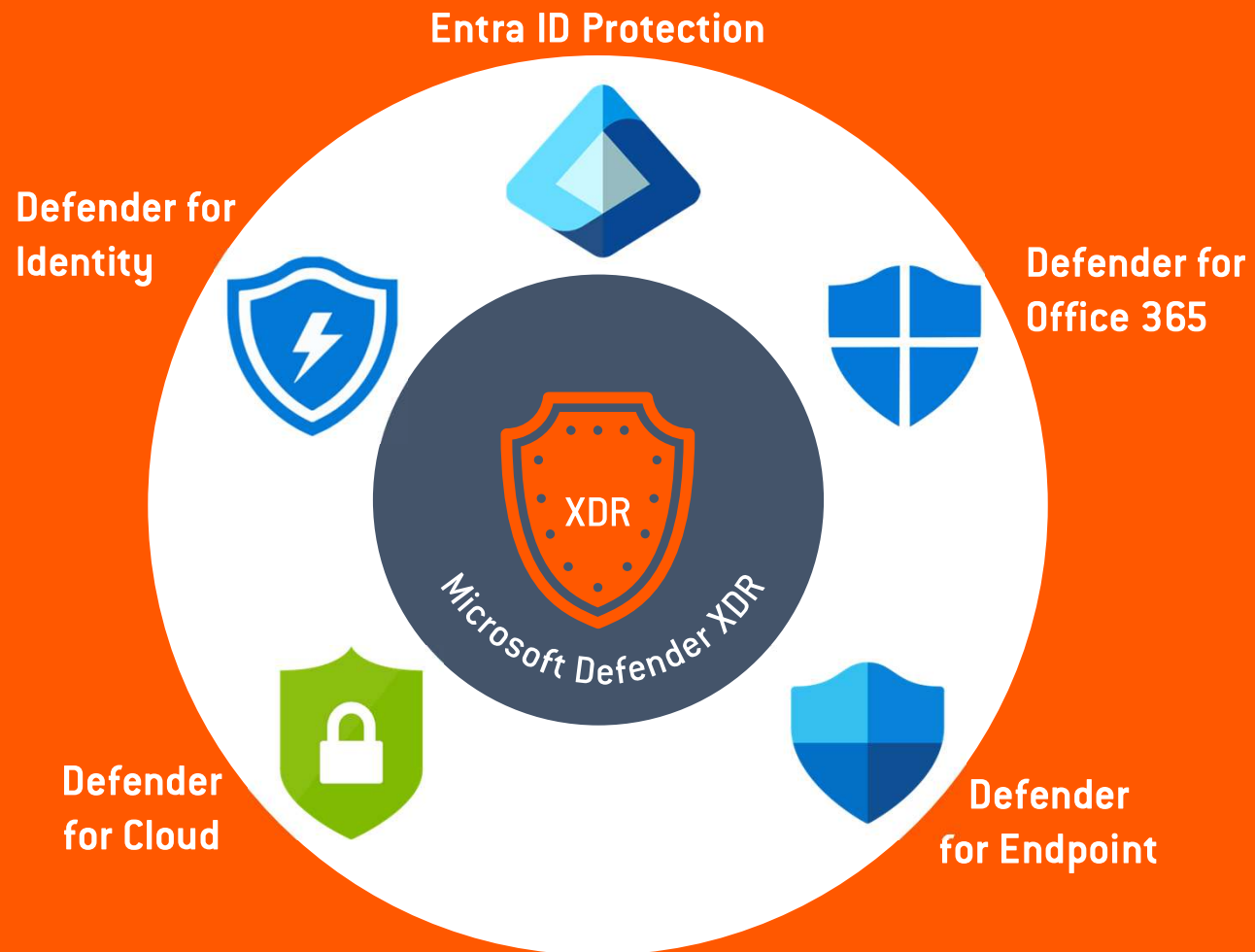
Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

MÖGLICHER AUFBAU FÜR KMU



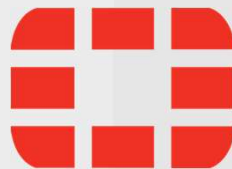




Remote Work



Office



AD-Server



Fileserver

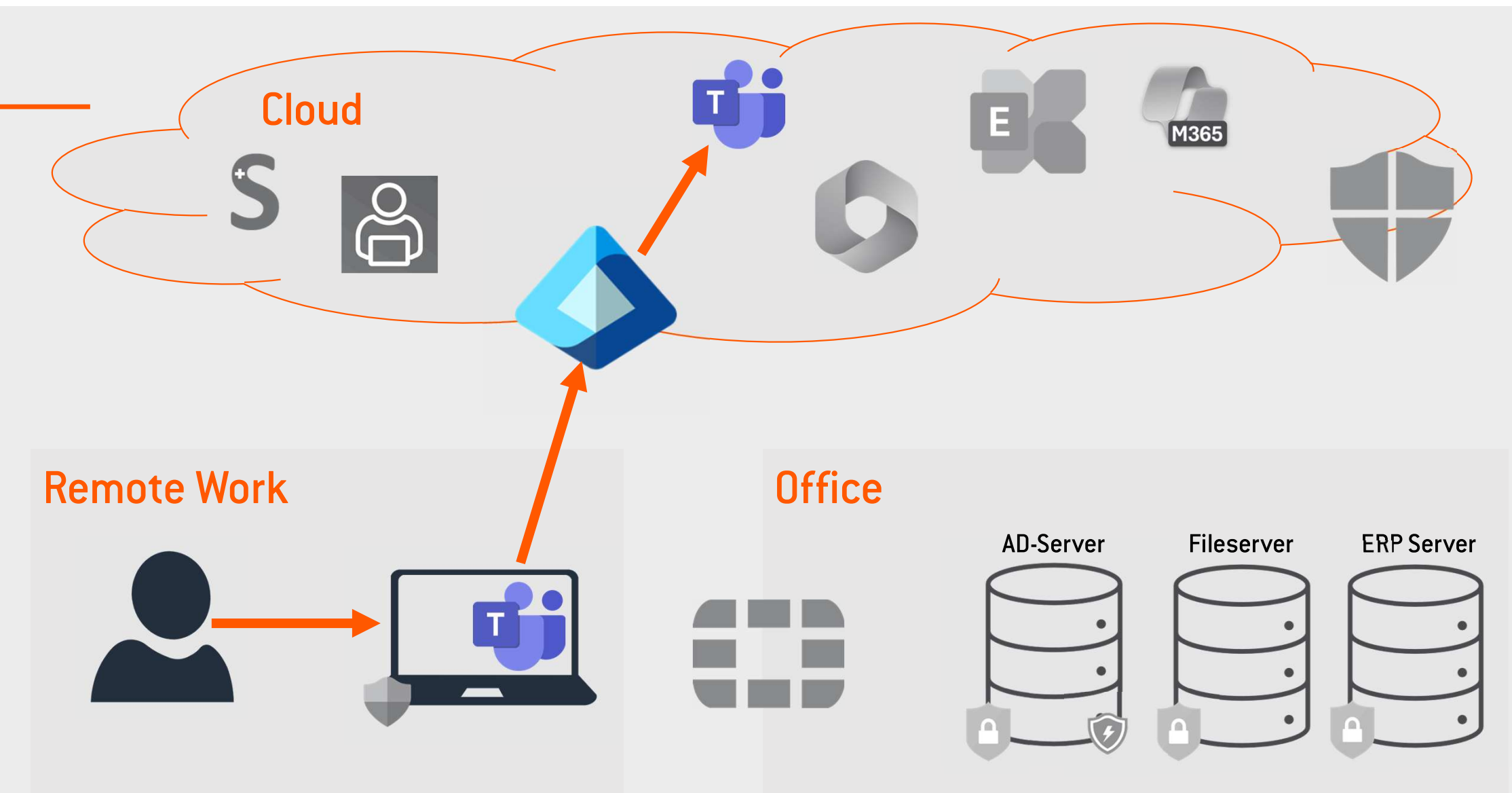


ERP Server



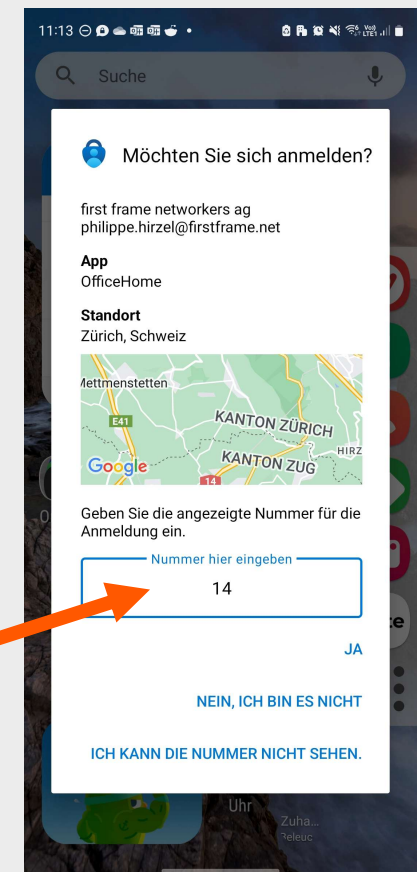
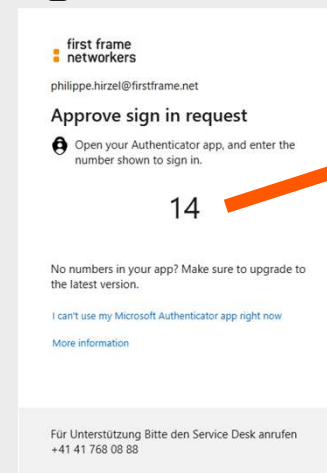
— ENTRA ID PROTECTION





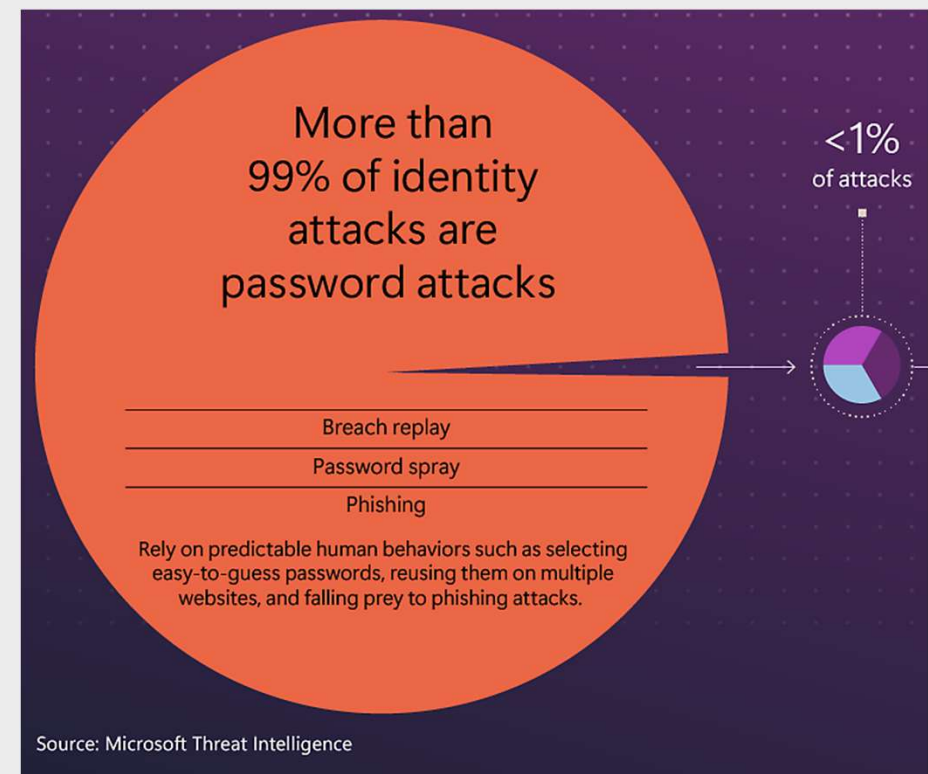
ENTRA ID PROTECTION

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



MFA IST ESSENZIELL

- ⇒ **99.2% Reduktion vom Risiko** einer Account-Kompromittierung
- ⇒ Conditional Access für Steuerung vom Zugriff



Microsoft Digital Defense Report 2024

ENTRA ID PROTECTION

Entra ID Free

- Gratis für M/0365 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

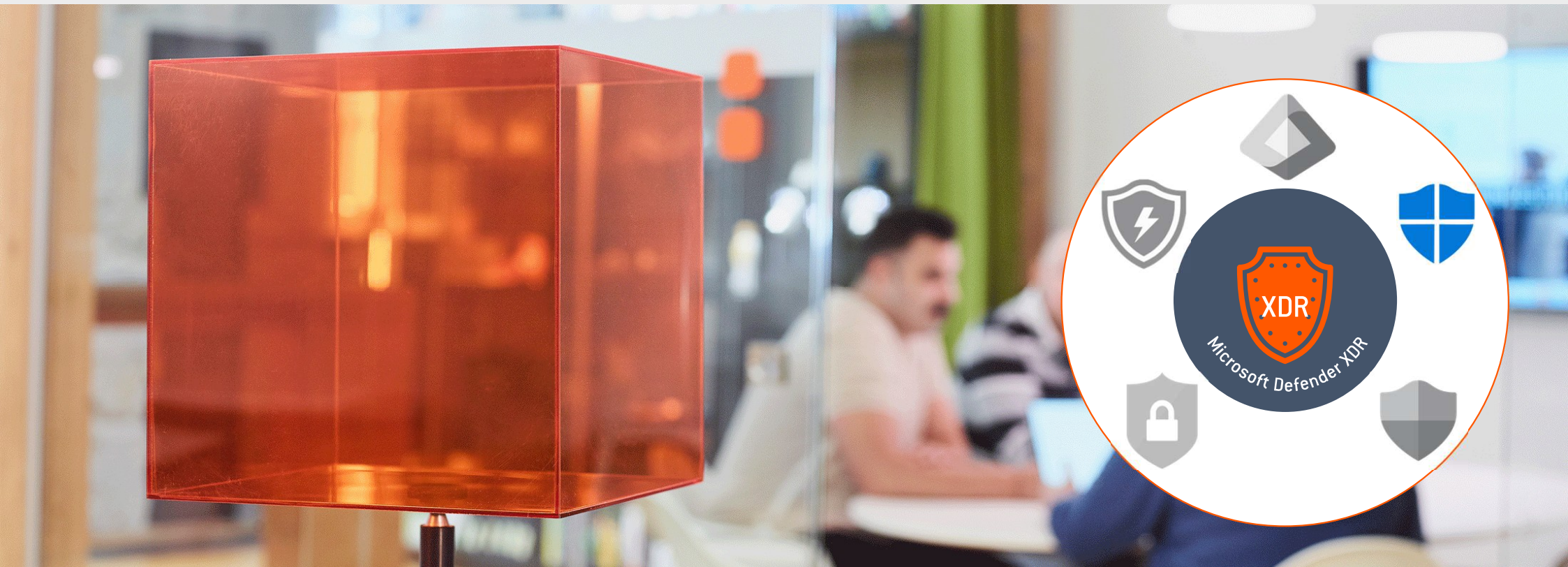
Entra ID P2

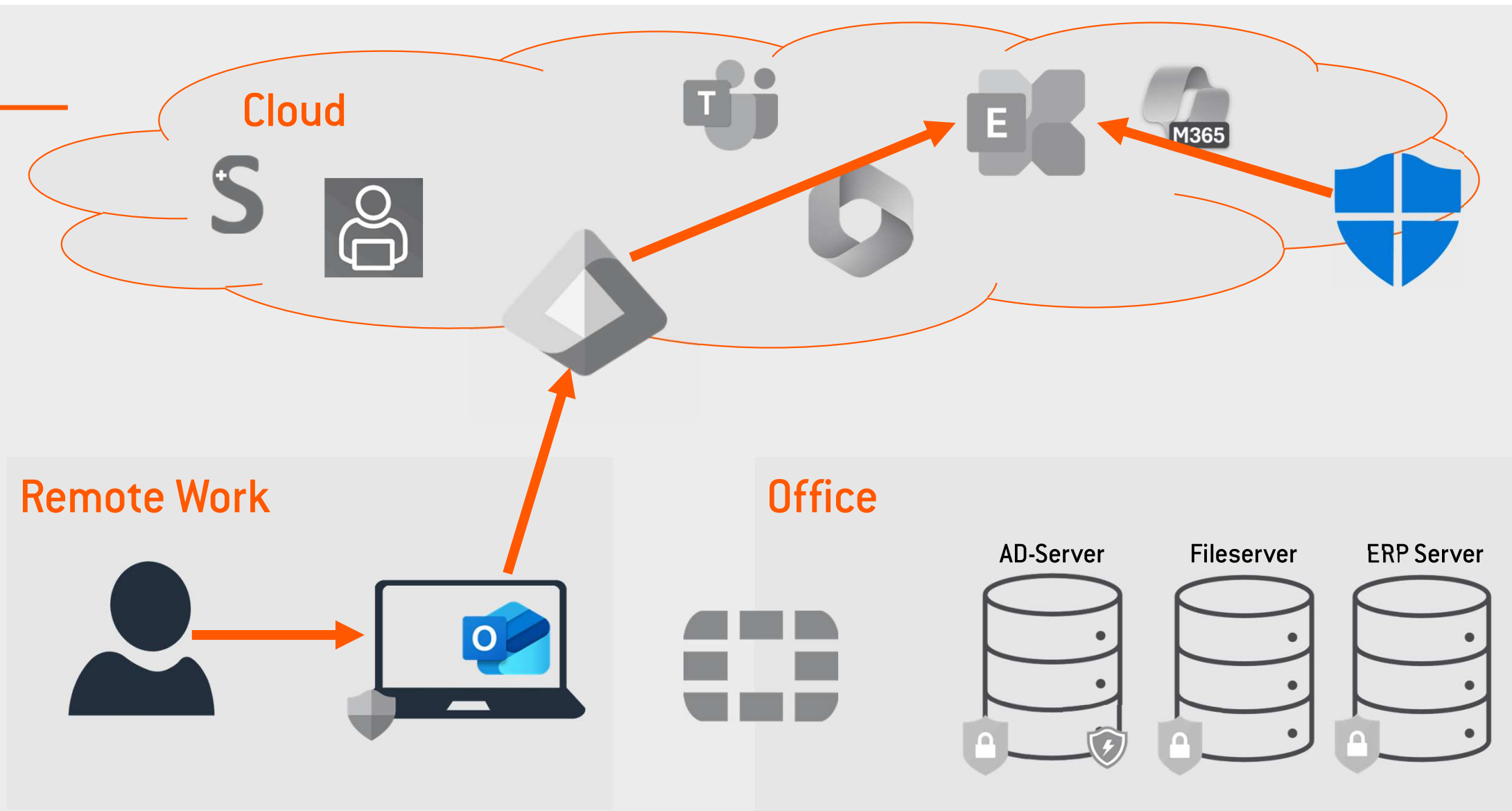
- 30 Tage Logs
- MFA granular konfigurierbar
- Conditional Access, um granular den Zugriff auf Ressourcen zu steuern
- Optional: Überwachen von Notfall-Admins
- Risiko-Basierte Anmeldung
- Schutz vor Impossible Travel [uvm.](#)

Entra ID P1 ist die richtige Lösung für die meisten Kunden

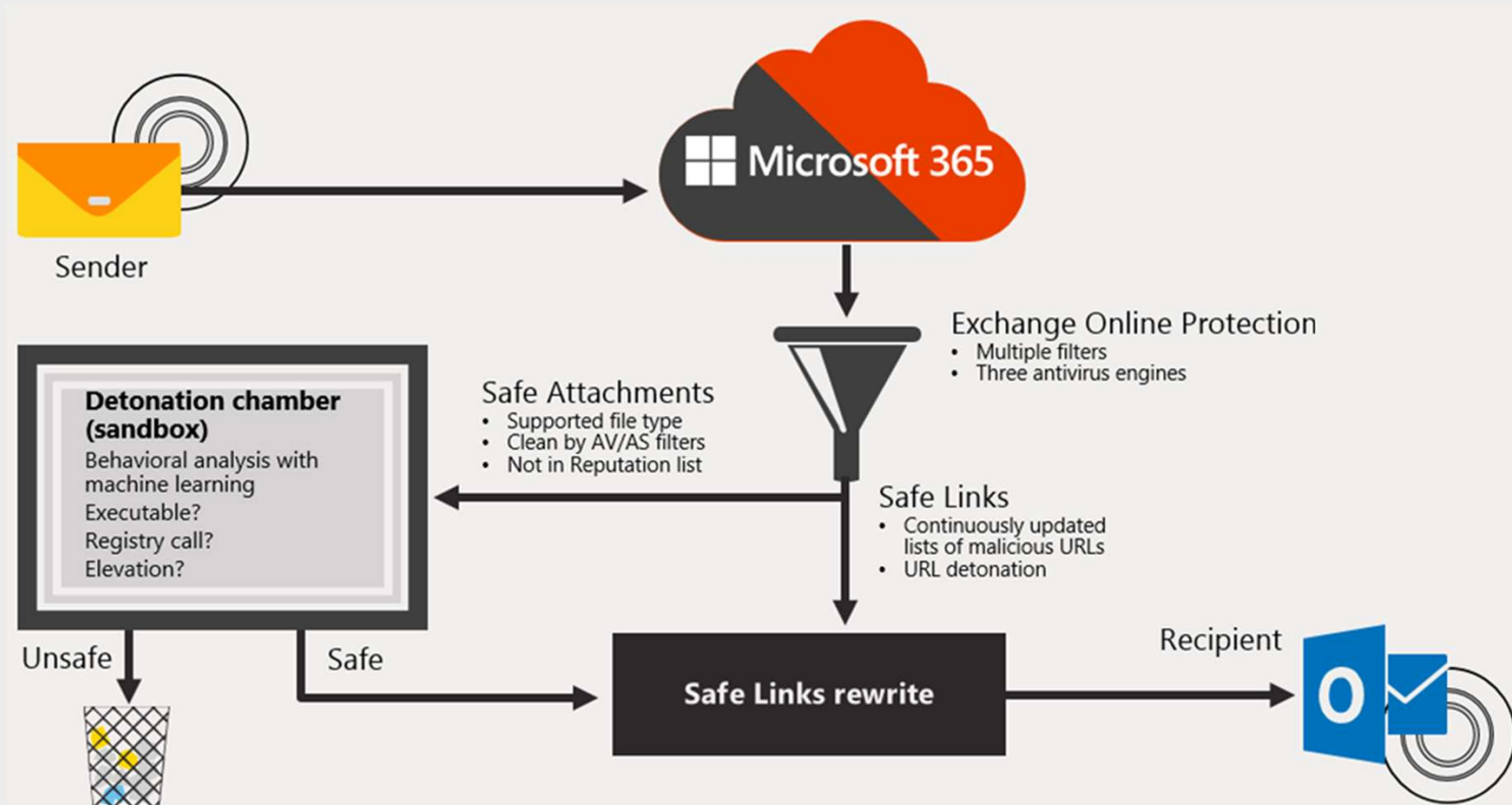


— DEFENDER FOR OFFICE 365





DEFENDER FOR OFFICE 365



DEFENDER FOR OFFICE 365

Exchange Online Protection

- Anti-Spam
- Anti-Malware
- Einfaches Anti-Phishing

Defender for Office 365 P1

- Anti-Spam
- Anti-Malware
- Anti-Phishing
- Safe-Links für E-Mail & Teams
- Safe-Attachments für E-Mail, Teams, Sharepoint & OneDrive

Defender for Office 365 P2

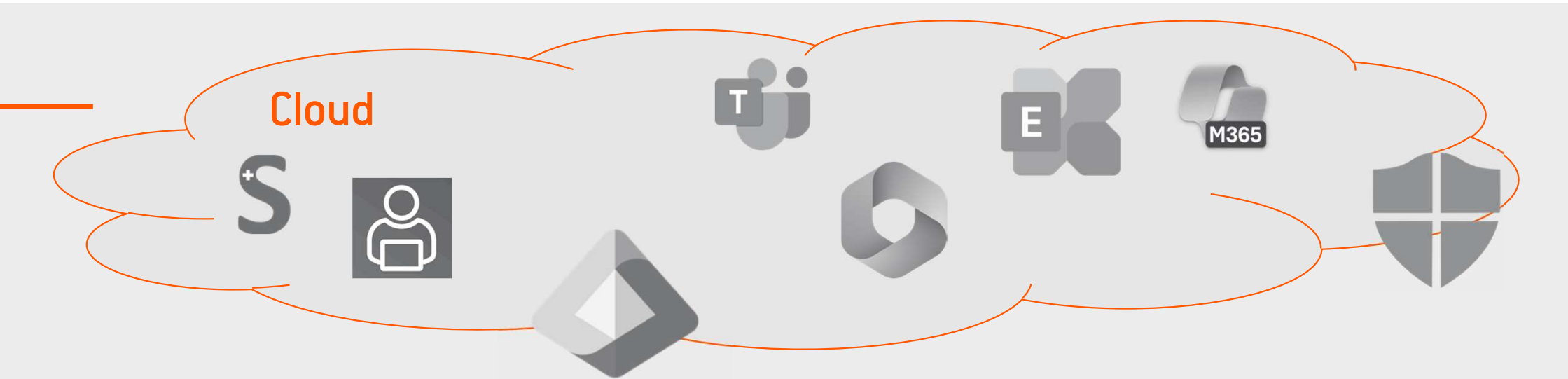
- Anti-Spam
- Anti-Malware
- Anti-Phishing
- Safe-Links für E-Mail & Teams
- Safe-Attachments für E-Mail, Teams, Sharepoint & OneDrive
- Automated Investigation and Response (AIR)
- Attack Simulation Training

Defender for Office 365 P1 ist die richtige Lösung für die meisten Kunden

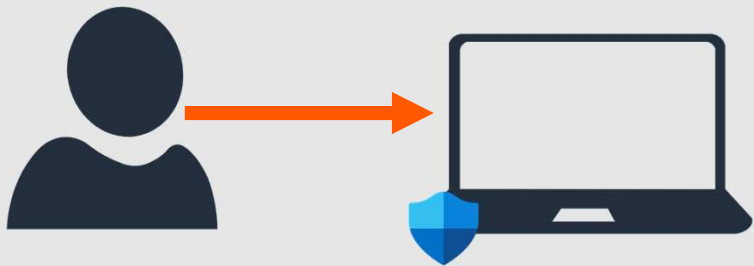


— DEFENDER FOR ENDPOINT

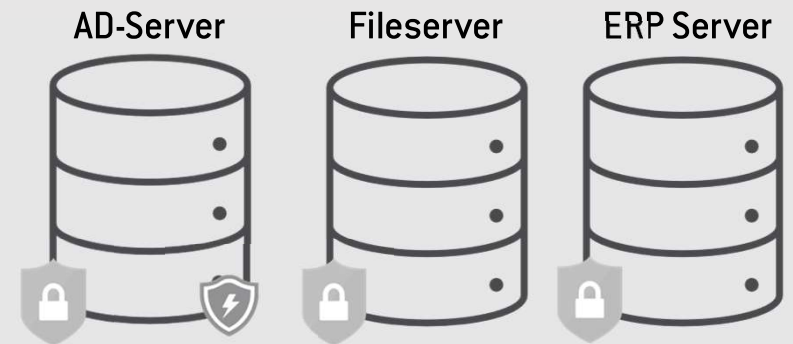




Remote Work



Office



DEFENDER FOR ENDPOINT

Defender for Business

- Threat and Vulnerability Management
- Attack Surface Reduction
- Next-Gen Protection
- Endpoint Detection and Response *
- Automated Investigation and Response *

* optimiert für KMU

Defender for Endpoint P1

- Attack Surface Reduction
- Next-Gen Protection

Defender for Endpoint P2

- Threat and Vulnerability Management
- Attack Surface Reduction
- Next-Gen Protection
- Endpoint Detection and Response
- Automated Investigation and Response
- Threat Hunting and 6-months data retention

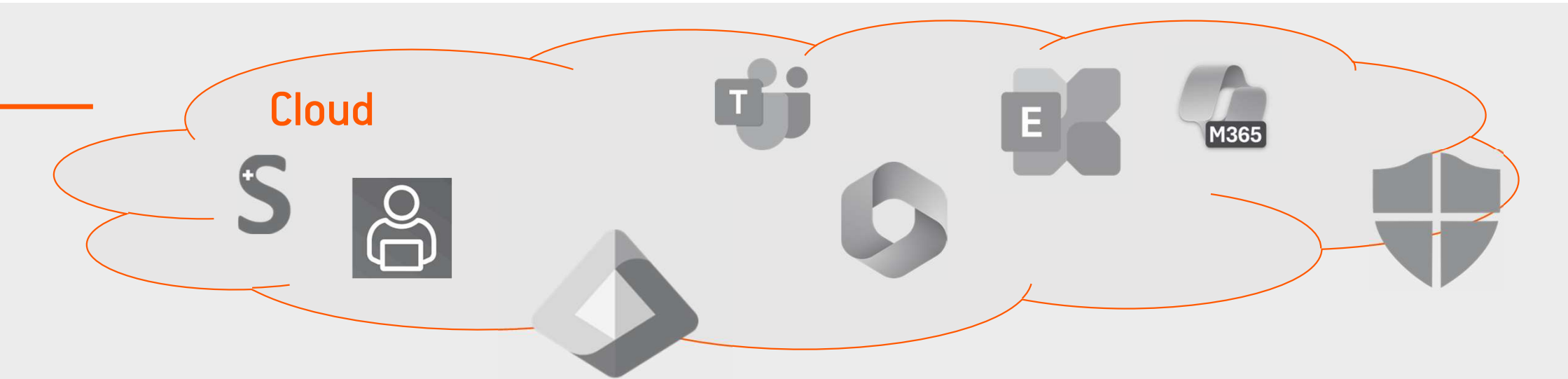
Defender for Business oder **Defender for Endpoint P2** sind die richtige Lösung für die meisten Kunden



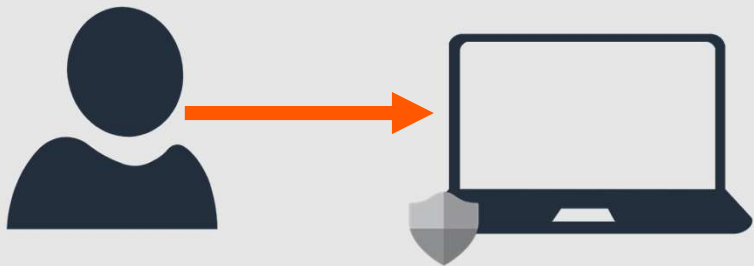
[Vergleich der Defender Versionen](#)

— DEFENDER FOR CLOUD



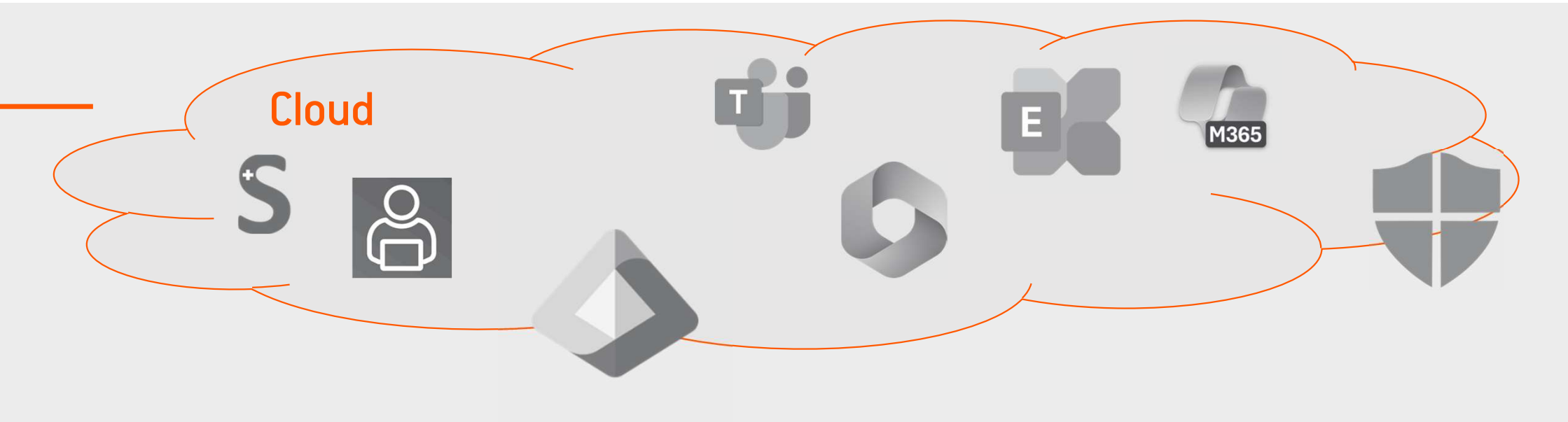


Remote Work

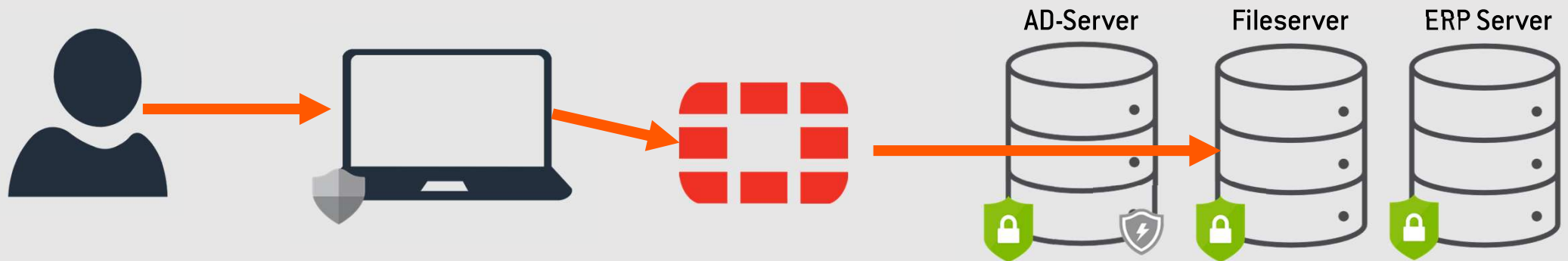


Office

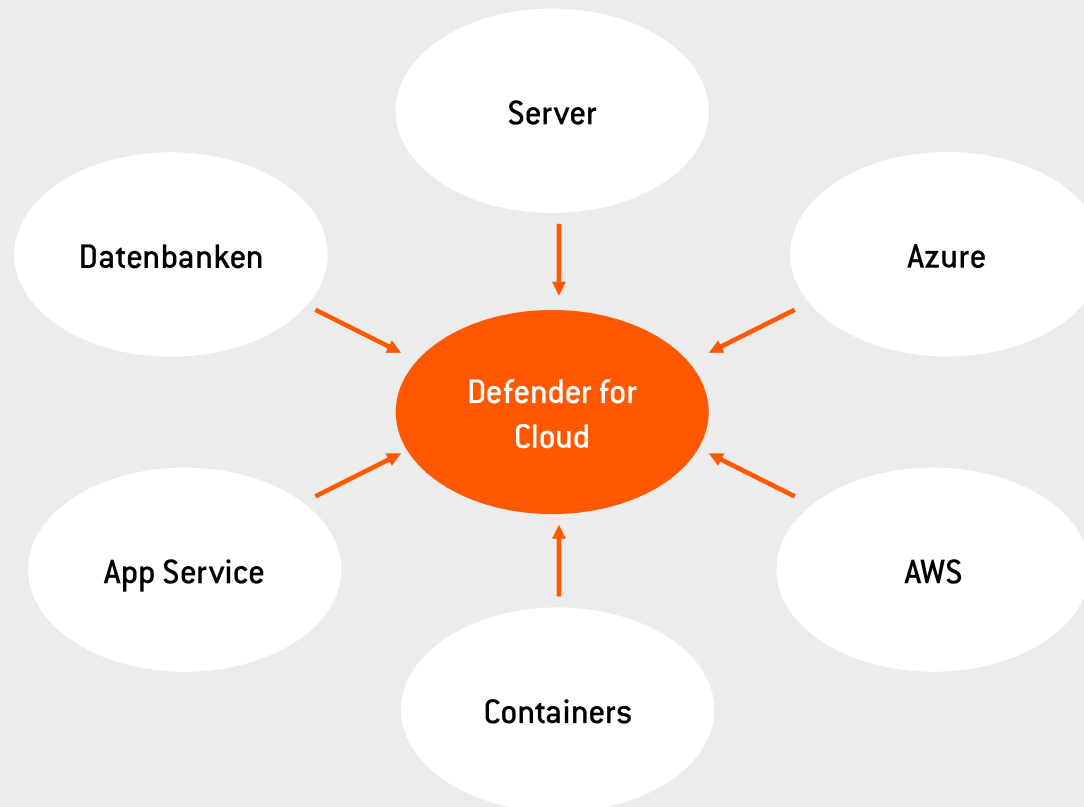




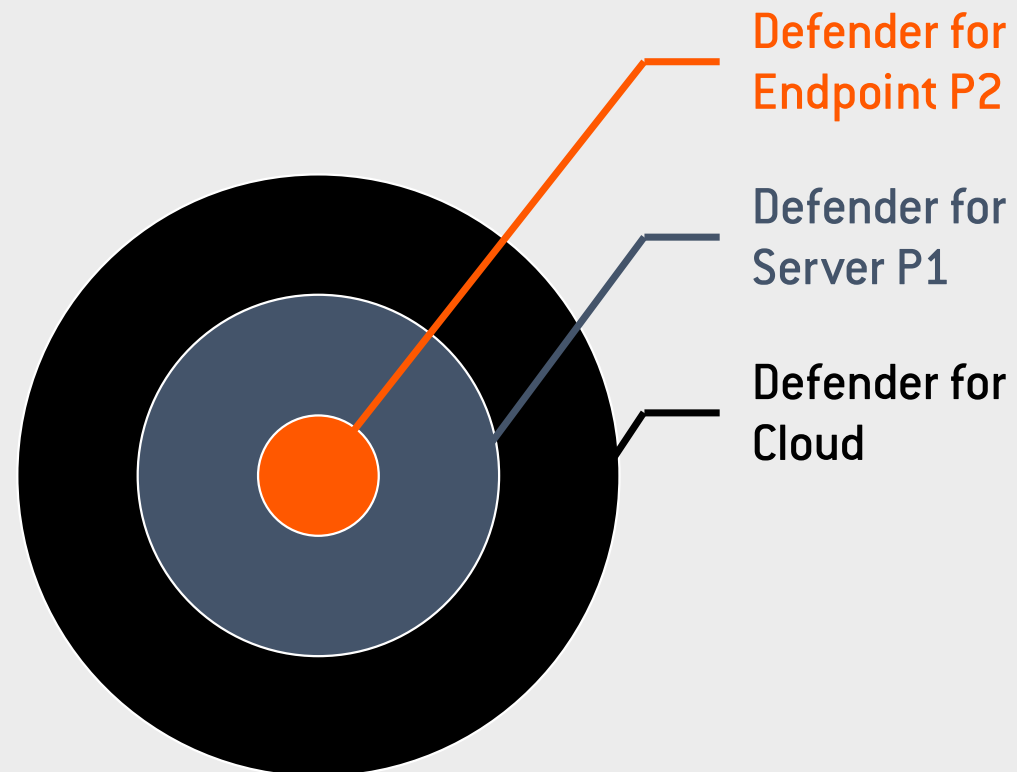
Office



DEFENDER FOR CLOUD



DEFENDER FOR CLOUD



DEFENDER FOR CLOUD

Defender for Business Servers

- Ergänzung zu Defender for Business
- Threat and Vulnerability Management
- Attack Surface Reduction
- Next-Gen Protection
- Endpoint Detection and Response *
- Automated Investigation and Response *

* optimiert für KMU

Defender for Server P1

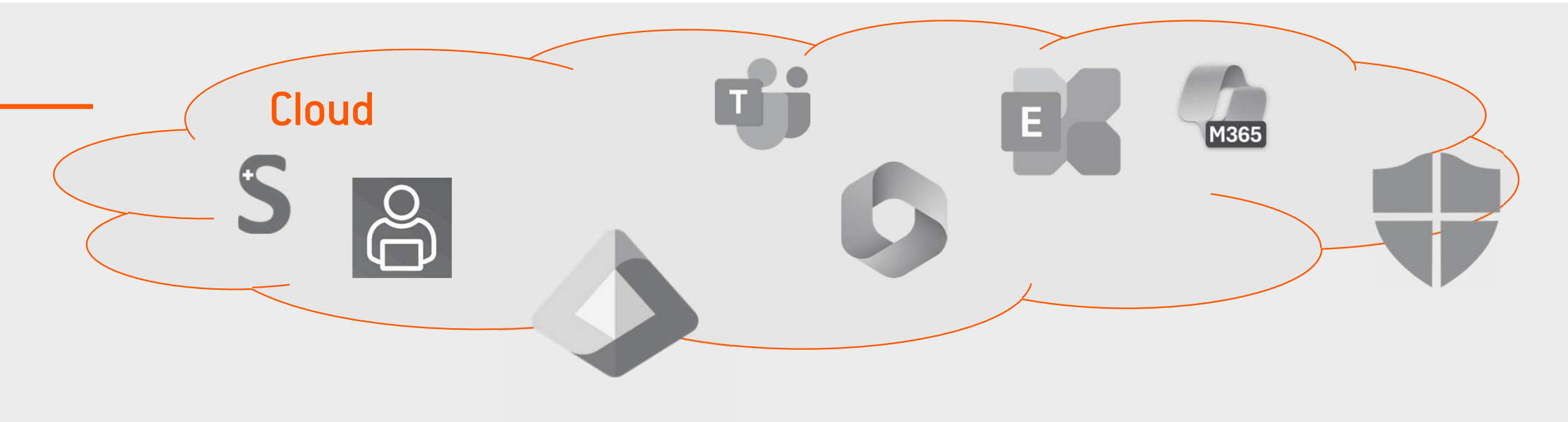
- Ergänzung zu Defender for Endpoint P2
- Threat and Vulnerability Management
- Attack Surface Reduction
- Next-Gen Protection
- Endpoint Detection and Response
- Automated Investigation and Response
- Threat Hunting and 6-months data retention

Je nach Defender auf dem Endpoint können beide die richtige Lösung sein

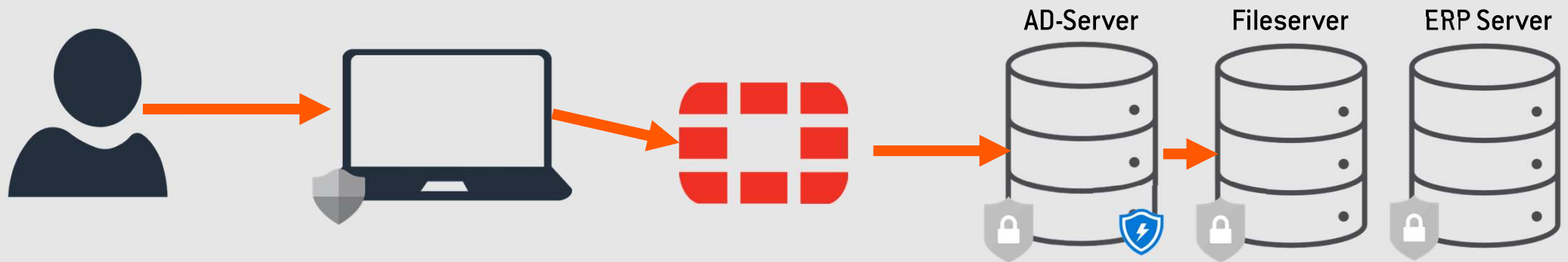


— DEFENDER FOR IDENTITY





Office



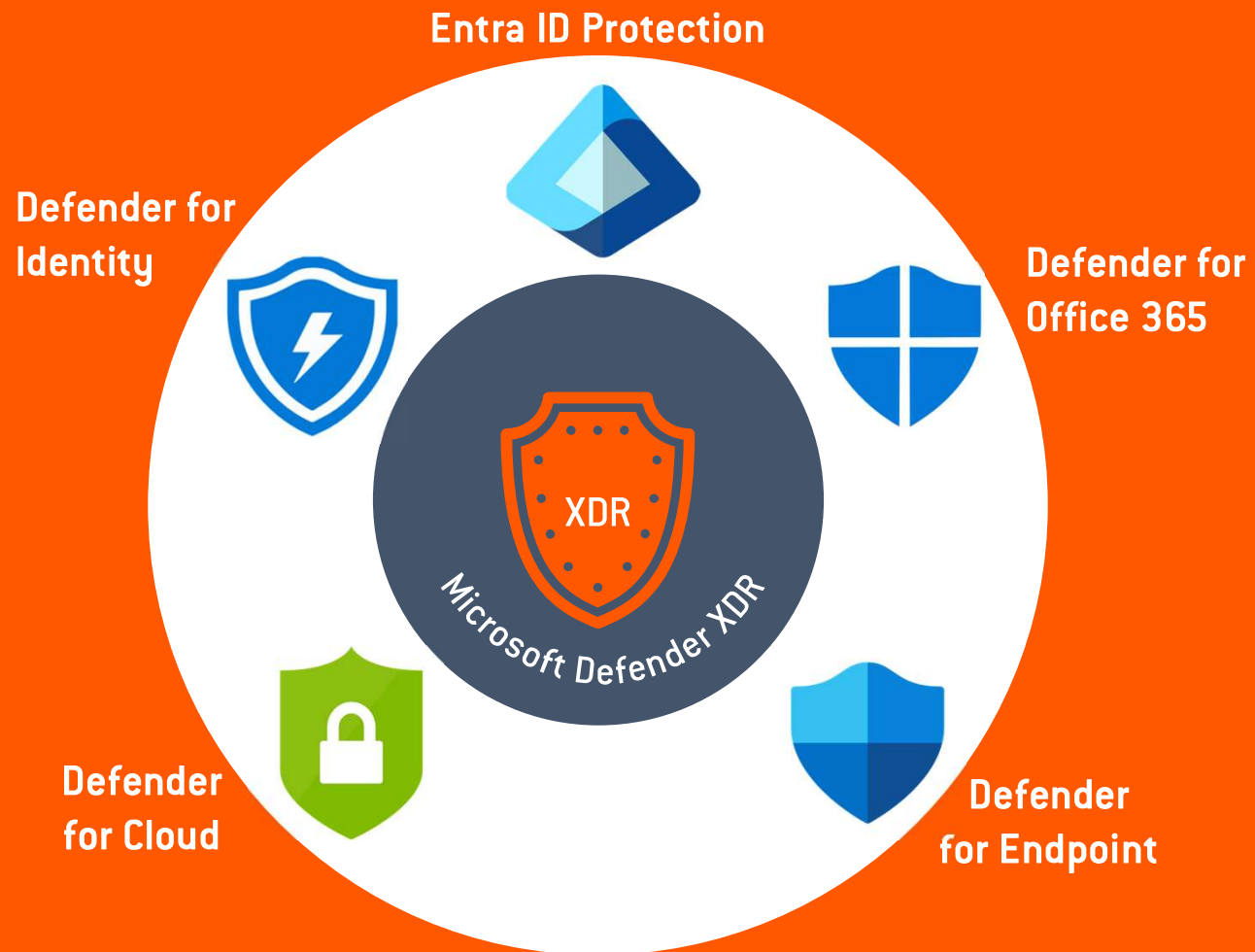
DEFENDER FOR IDENTITY

Defender for Identity






- Schutz der „Kronjuwelen“
- Schützt On-Prem Umgebungen
- Cloud Logins über Entra ID geschützt

Defender for Identity ist für alle Kunden welche längerfristig noch Active-Directory einsetzen werden





WELCHE LIZENZEN BRAUCHE ICH?

	Produkt	KMU	Internationale, regulierte oder sicherheitsbewusste Kunden
	Entra ID Protection	Entra ID P1	Entra ID P2
	Defender for Office 365	Defender for Office 365 P1	Defender for Office 365 P2
	Defender for Endpoint	Defender for Business	Defender for Endpoint P2
	Defender for Cloud	Defender for Business Servers	Defender for Servers P1
	Defender for Identity	Defender for Identity	Defender for Identity

— DEMO



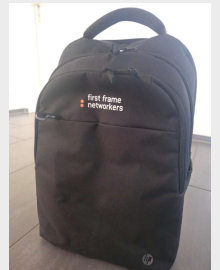
— WAS MUSS ICH JETZT UNTERNEHMEN?



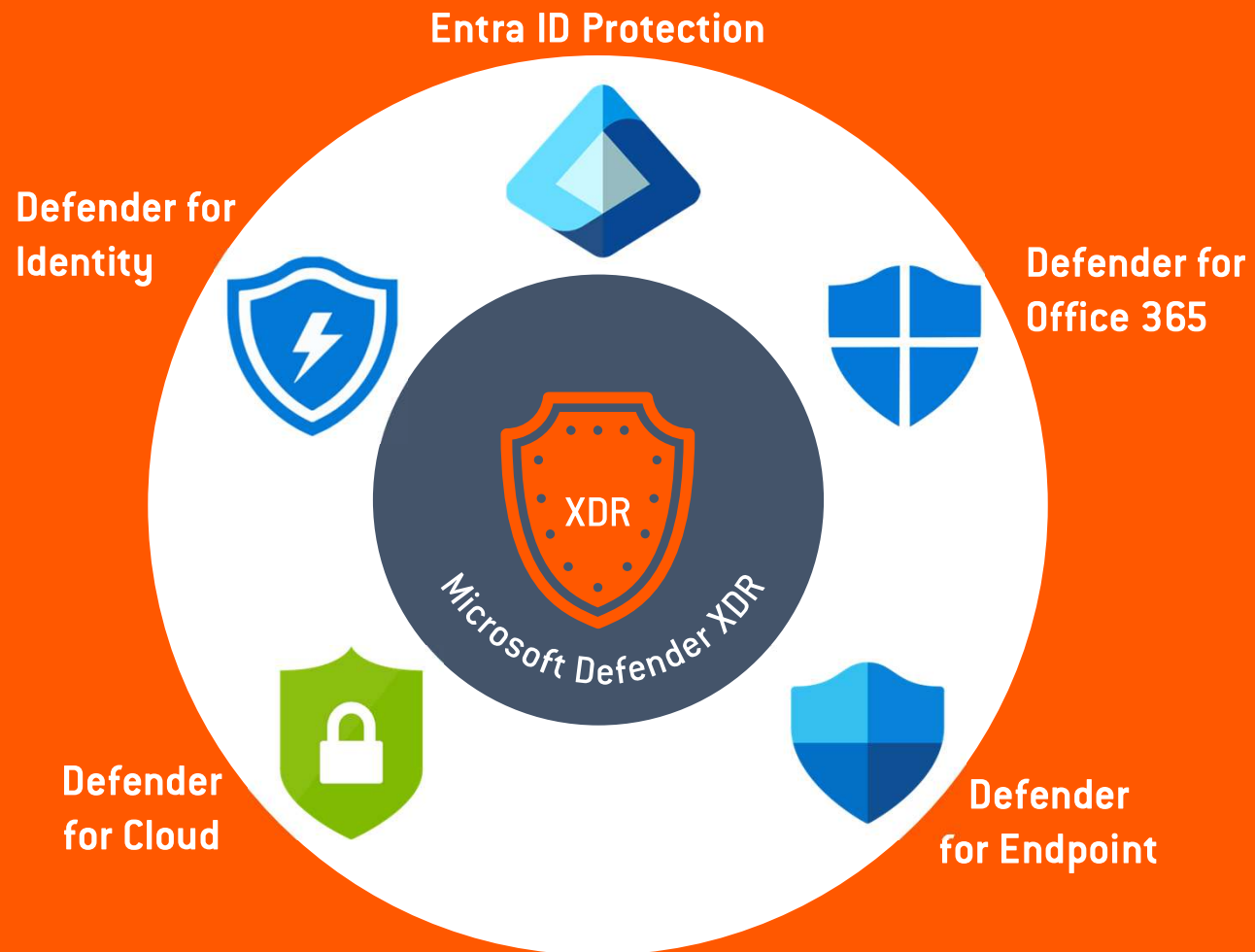
FEEDBACK-FORMULAR








- ⇒ Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- ⇒ Ihre Meinung ist uns 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/WPaYhqdpux>



WELCHE LIZENZEN BRAUCHE ICH?

	Produkt	KMU	Internationale, regulierte oder sicherheitsbewusste Kunden
	Entra ID Protection	Entra ID P1	Entra ID P2
	Defender for Office 365	Defender for Office 365 P1	Defender for Office 365 P2
	Defender for Endpoint	Defender for Business	Defender for Endpoint P2
	Defender for Cloud	Defender for Business Servers	Defender for Servers P1
	Defender for Identity	Defender for Identity	Defender for Identity

IN WELCHER REIHENFOLGE KAUFEN DIE LIZENZEN?



WELCHE LIZENZEN BRAUCHE ICH?

KMU-Kunden

- Entra ID P1
- Defender for Business
- Defender for Office 365 P1
- Defender for Business for Server



- Microsoft 365 Business Premium
- Defender for Business Servers

Sicherheitsbewusste KMU-Kunden

- Entra ID P2
- Defender for Endpoint P2
- Defender for Office 365 P2
- Defender for Server P1
- Defender for Identity



- Microsoft 365 Business Premium + Microsoft 365 E5 Security
- Defender for Server P1

Internationale, regulierte oder sicherheitsbewusste Kunden

- Entra ID P2
- Defender for Endpoint P2
- Defender for Office 365 P2
- Defender for Server P1
- Defender for Identity



- Microsoft M365 E3 + Microsoft 365 E5 Security
- Defender for Server P1

WELCHE LIZENZEN BRAUCHE ICH?

KMU-Kunden	Sicherheitsbewusste KMU-Kunden	Internationale, regulierte oder sicherheitsbewusste Kunden
<ul style="list-style-type: none">– Microsoft 365 Business Premium	<ul style="list-style-type: none">– Microsoft 365 Business Premium + Microsoft 365 E5 Security	<ul style="list-style-type: none">– Microsoft M365 E3 + Microsoft 365 E5 Security
<ul style="list-style-type: none">– Defender for Business Servers	<ul style="list-style-type: none">– Defender for Server P1	<ul style="list-style-type: none">– Defender for Server P1
		<ul style="list-style-type: none">– User– Server

Neu ab März 2025

AUFBAU FÜR KMU



AUFBAU FÜR KMU

Managed Protected Essentials
12.90 CHF pro User & Monat

Microsoft 365 Business Premium
~19.70 CHF pro User & Monat

Defender for Business Servers
~3.- CHF pro User & Monat

Azure Consumption
< 10.- CHF pro Monat

Managed Microsoft Tenant
49.90 CHF pro Monat

AUFBAU FÜR SICHERHEITSBEWUSSTE KUNDEN

Managed Protected Services Staffelung nach Anzahl Benutzer:innen

Microsoft 365 E3 + E5 Security
~ 48.70 CHF pro User & Monat

Defender for Server P1
~5.- CHF pro User & Monat

Azure Consumption
< 10.- CHF pro Monat

Managed Microsoft Tenant
49.90 CHF pro Monat

KUNDENSTATEMENT



«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 Gossweiler
Leiter ICT + Digitalisierung
Kantones Elektricitätswerk Nidwalden

TIPPS

Schützen Sie Ihren Zugang zur Cloud

Geräte absichern – auch im Cloud-
Zeitalter

Überwachung nicht vergessen

Q & A

NEXT STEPS



⇒ Let's Talk!

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

⇒ Weitere Infos

- ⇒ [Security Operations Center als Services - first frame networkers ag](#)
- ⇒ <https://blog.firstframe.net/tag/security>

**Herzlichen
Dank**