



all for one
Group

MITTELSTANDSFORUM 2020

Microsoft Cybersecurity-Roadmap umsetzen –
gibt Ihr Microsoft-Vertragskonstrukt das auch her?

Mario Krukow - Senior Cybersecurity Architect & Head of Information Protection
Riana-Yvonne Schimanski - Senior Consultant Licensing & Compliance

HERZLICHEN DANK, dass Sie dabei sind!

Referent

Mario Krukow

Senior Cybersecurity Architect &
Head of Information Protection



All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen
all-for-one.com

T: +49 2301 94 49 21
M: +49 151 617 20 395
E: mario.krukow@all-for-one.com

Referentin

Riana-Yvonne Schimanski

Senior Consultant Licensing & Compliance



All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen
all-for-one.com

T: +49 89 149 022 666
M: +49 170 877 49 19
E: riana.schimanski@all-for-one.com

Moderator

Michael Bauer

Transformation Architect



All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen
all-for-one.com

T: +49 211 550 26 315
M: +49 151 571 68 636
E: michael.bauer@all-for-one.com



Kurzvorstellung

Thementag 1 **Cybersecurity & Compliance**

- » Während der Präsentation sind die Mikrofone stumm geschaltet
- » Bitte stellen Sie Ihre Fragen im Chat, die Fragen werden am Ende der Session beantwortet
- » Nach dem Vortrag auf der Bühne besteht die Möglichkeit sich mit dem Experten auszutauschen – siehe **Meet the Expert**
- » Gerne bieten wir Ihnen auch individuelle Folgegespräche an

Cybersecurity & Compliance

Unser Wertversprechen

Wir befreien Unternehmen in einer digitalen, vernetzten Welt von der Sorge um Cyberangriffe und Datenverlust und unterstützen bei der Einhaltung von Compliance-Anforderungen.“

Unsere Leistungen

- » Ganzheitliche Sicherheit über alle Ebenen einer Unternehmensorganisation
- » Trusted Security Partner für Governance & Technologie sowie Single-Point of Contact
- » Beratung und Implementierung moderner Cloud-First und Cybersecurity-Design-Grundlagen



Technologische Partner

ConSecur
[security and consulting]

gemalto
a Thales company

Lookout

SEC Consult

Omada
DO MORE WITH IDENTITY

ITing
quality

SECUDE



Strategische Partner

Microsoft

SAP



Agenda

01

Cybersecurity-
Architektur

02

Suboptimale Beispiele
aus der Praxis

03

Optimale Beispiele
aus der Praxis

04

Key
Take-Aways

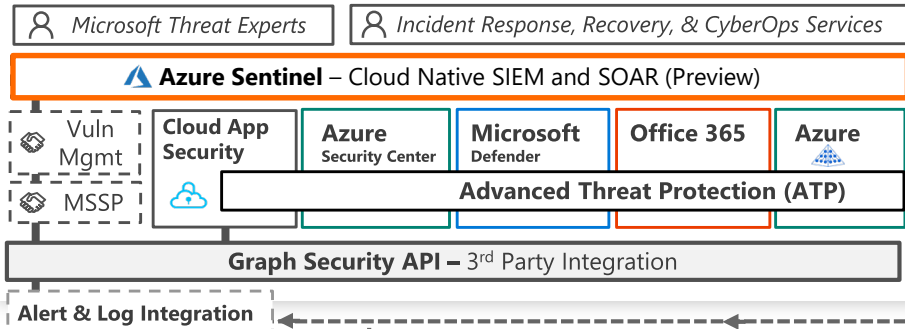


01

Cybersecurity-Architektur

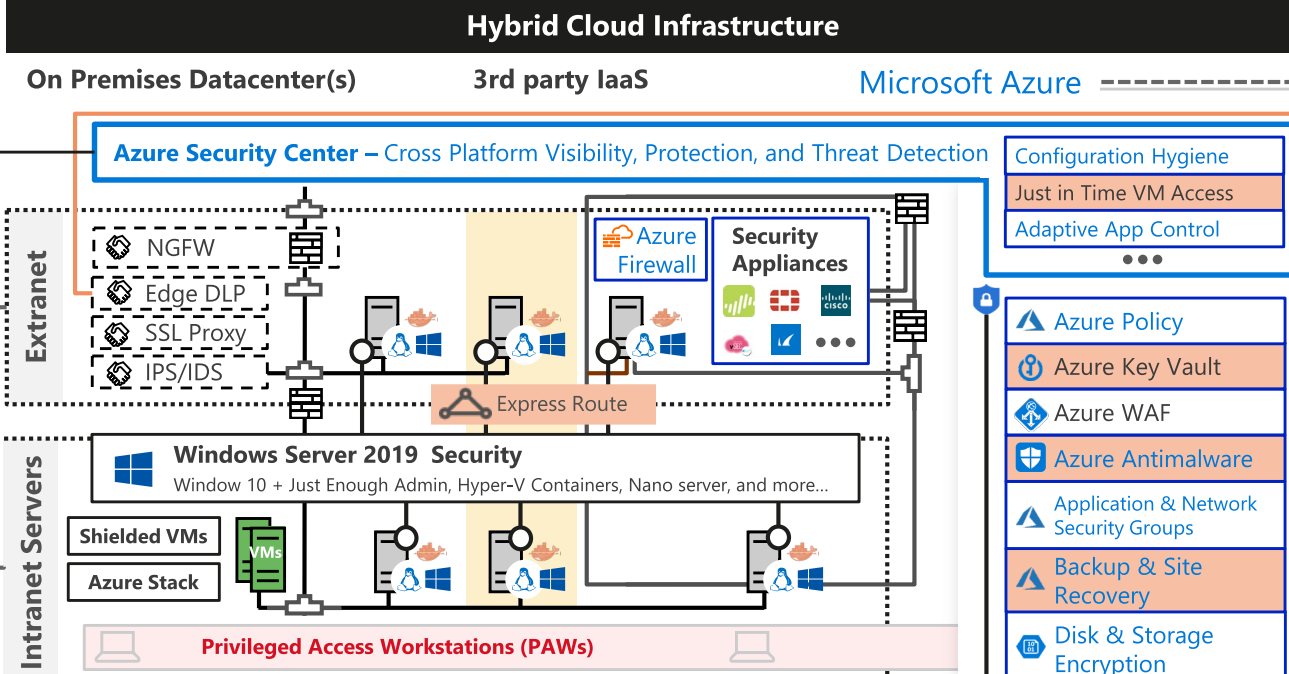
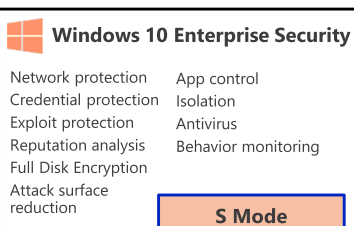
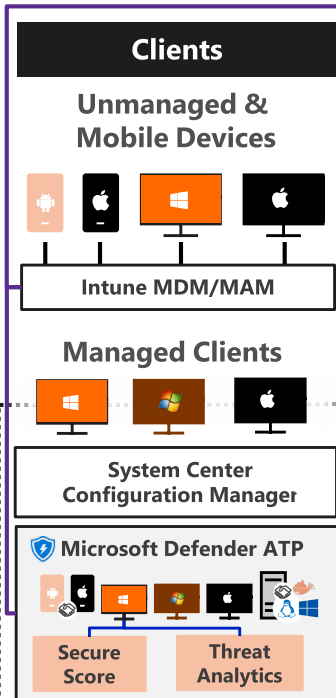
Die Basis für die Roadmap

Security Operations Center (SOC)



Cybersecurity

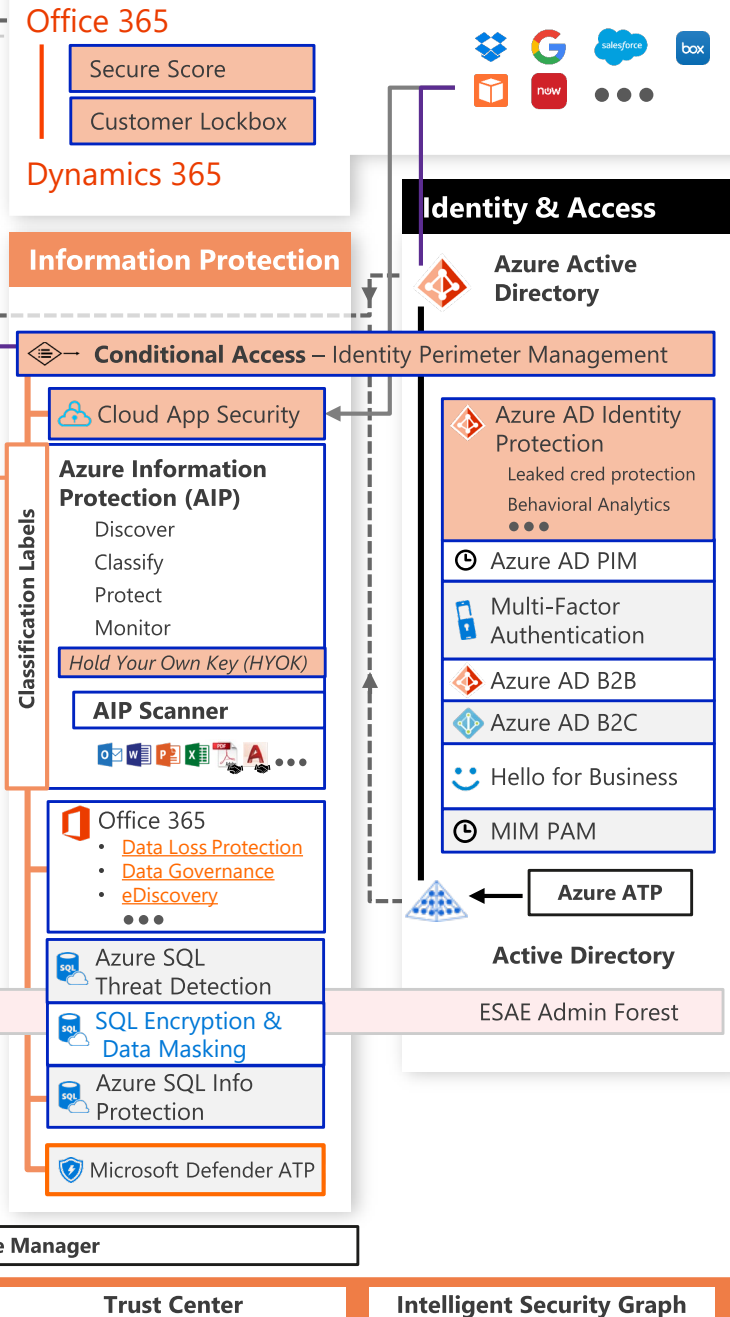
Referenz-Architektur



Included with Azure (VMs/etc.) Premium Security Feature

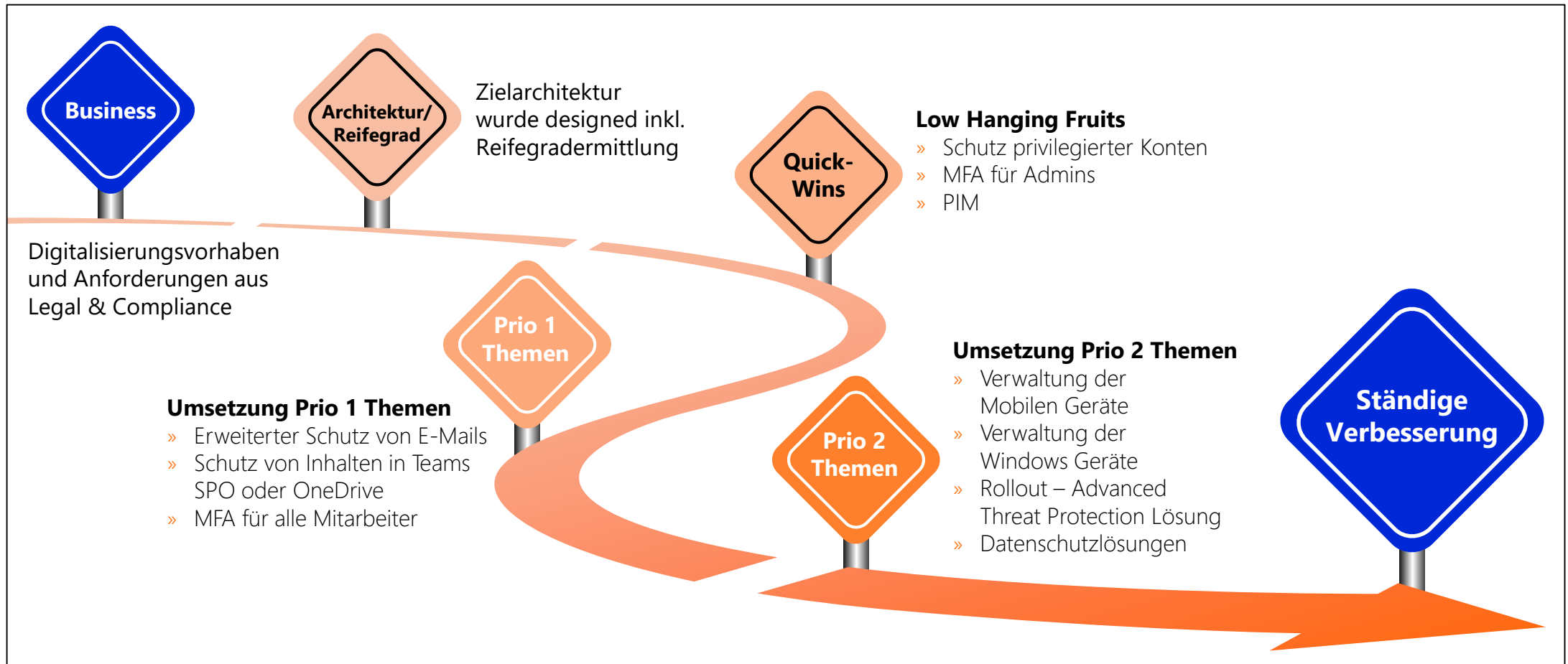
Security Development Lifecycle (SDL)

Software as a Service



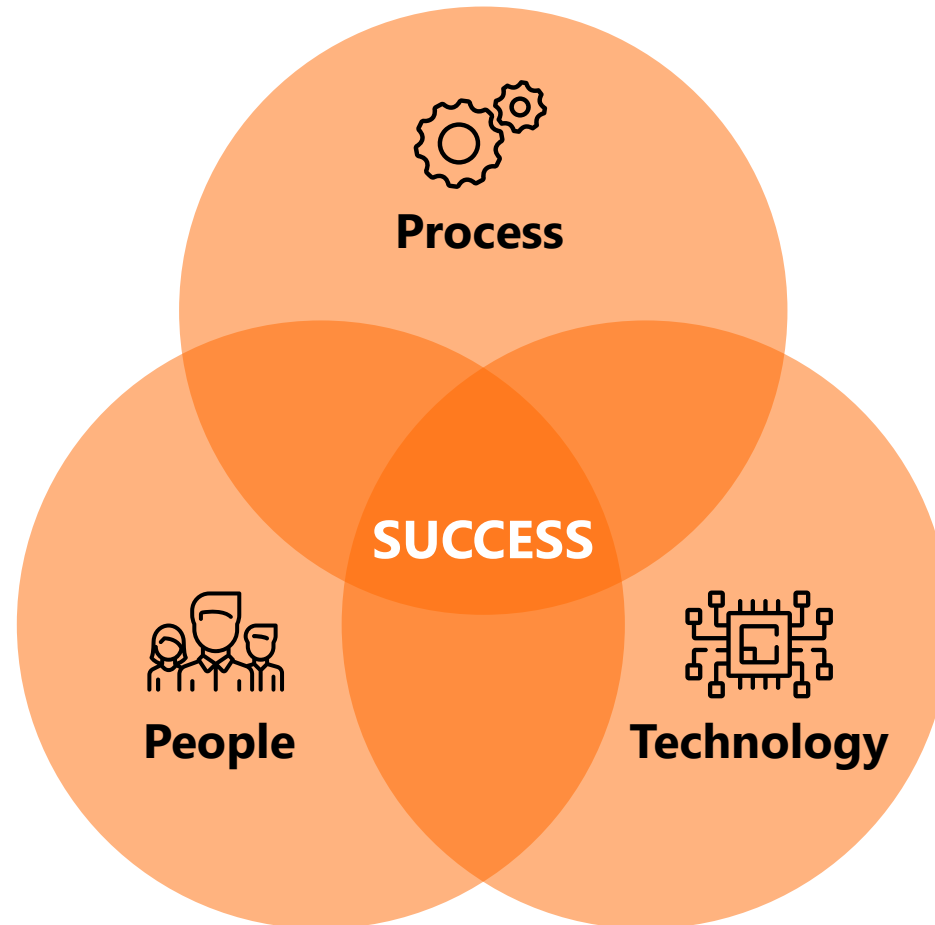


Ihre Security-Roadmap könnte so aussehen:





Ganzheitliche Security-Architekturen sind nicht nur Technologie



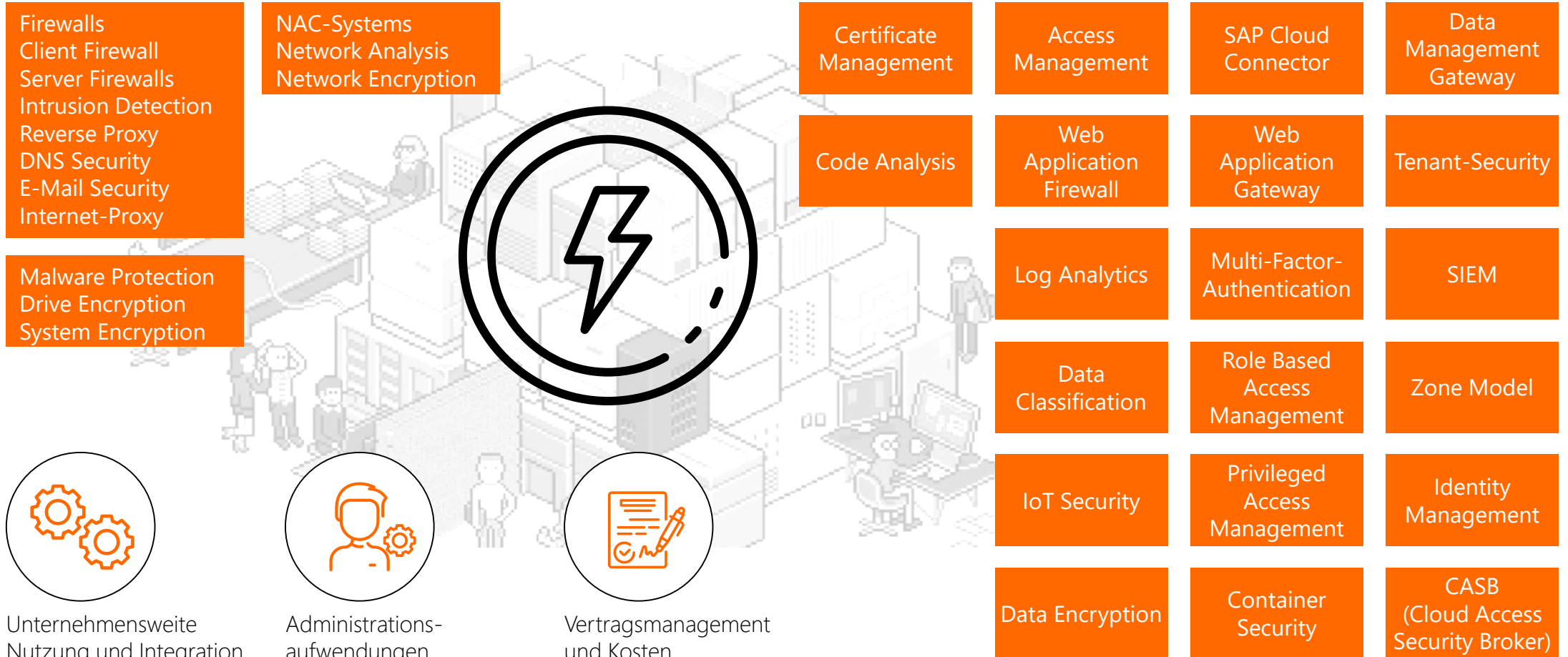


02

Suboptimale Beispiele aus der Praxis



Dezentral + viele Lösungen + keine übergeordnete Steuerung = „Flickenteppich“



Office 365 E3

Microsoft 365 Apps for Enterprise	Exchange Online Plan 2	SharePoint Online Plan 2	OneDrive for Business Plan 2
Office Web & Mobile Apps	E-Mail DLP planned Exchange Online Protection	Yammer Enterprise	Insights by MyAnalytics
Information Protection (Office 365)	Client DLP planned Data Loss Prevention	Power Apps for Office 365	Power Automate for Office 365
Sway	eDiscovery	Retention Policy	Stream for Office 365
Skype for Business Plan 2 (retiring)	Microsoft Teams	Microsoft Forms	Delve
Live Events	Planner	Audit Logging & Alerting	Kaizala Pro (retiring)

Office 365 E3

Enterprise Mobility + Security E3 (EMS E3)

Mobile Iron	Data Integrity planned		
Intune MDM & MAM	Azure Information Protection Plan 1	Advanced Threat Analytics implemented	Azure RMS
Microsoft Endpoint Config Manager	System Center Endpoint Protection	Windows Server CAL Rights	Active Directory RMS implemented McAfee
Conditional Access	LinOTP Multi-Factor Auth (MFA)	Microsoft Identity Manager	Azure AD B2B 5 guests per user
McAfee Web Gateway	App Proxy, including PingAccess	Cloud App Discovery	3rd Party MFA Integration
	Advanced Security Reports & Alerts	Single-Sign-On to other SaaS	Azure AD Connect Health
	Shared Account Password Roll-Over	Self-Service Password Reset in AD	Self-Service Group Management
			Enterprise State Roaming
			Group-Based Access Management

Azure AD Premium Plan 1 already available

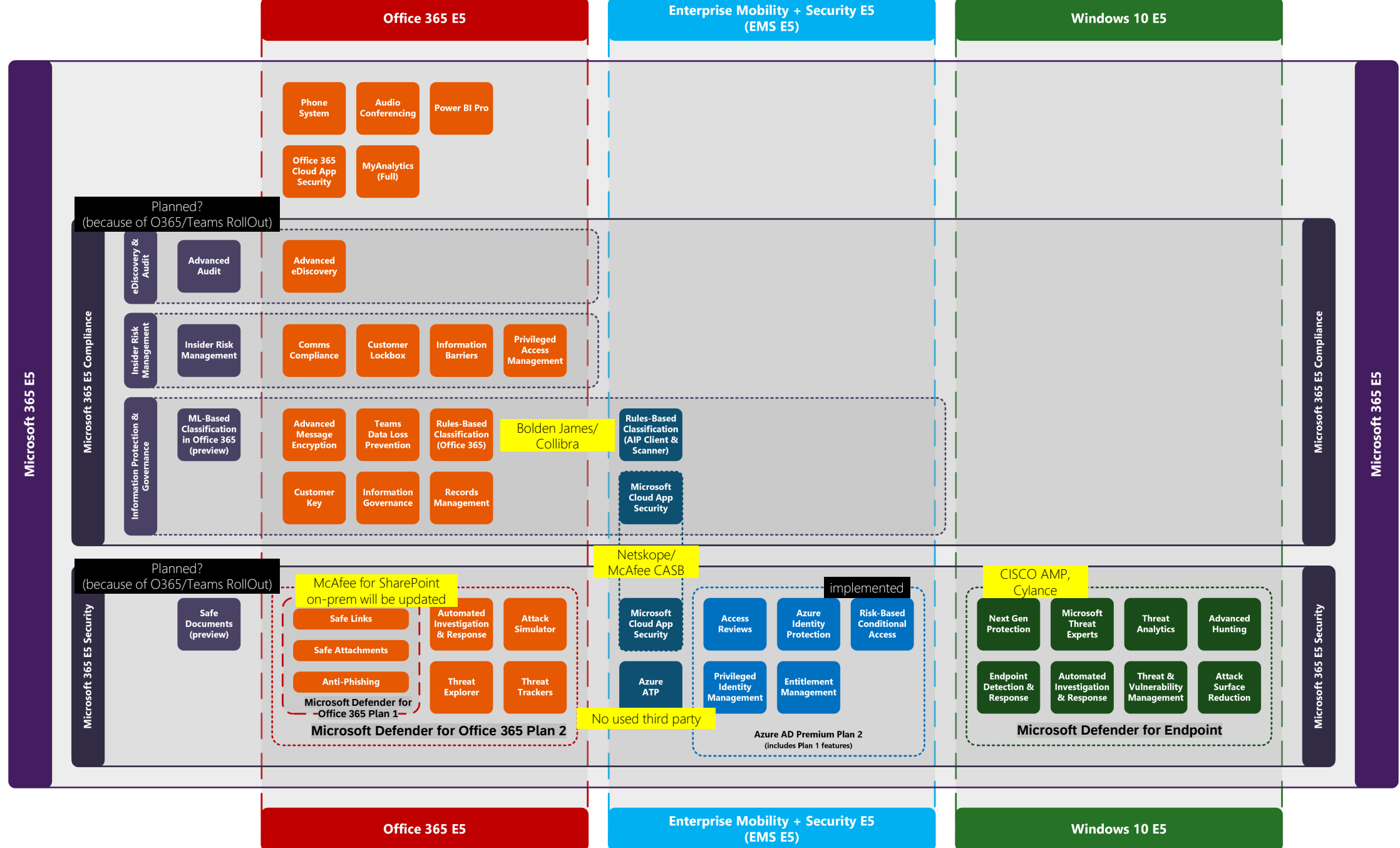
Enterprise Mobility + Security E3 (EMS E3)

Windows 10 E3

Windows 10 Enterprise Security planned

App-V	Application Guard	AppLocker	Azure AD & Domain Join
BitLocker & BitLocker to Go	BranchCache	Conditional Access	Cortana Management
Credential Guard	Device Guard	Direct Access	Long Term Servicing Channel
Mobile Iron	MDM & MAM	MDOP	Microsoft Store for Business
			User Experience Virtualisation
Voice, Pen, Touch, Ink, and Gesture	Windows Analytics	Windows Defender Antivirus	Windows Hello Management
Windows Information Protection	Windows to Go	Windows Update for Business	Windows Virtual Desktop

Windows 10 E3





Kundenszenario aus der Praxis

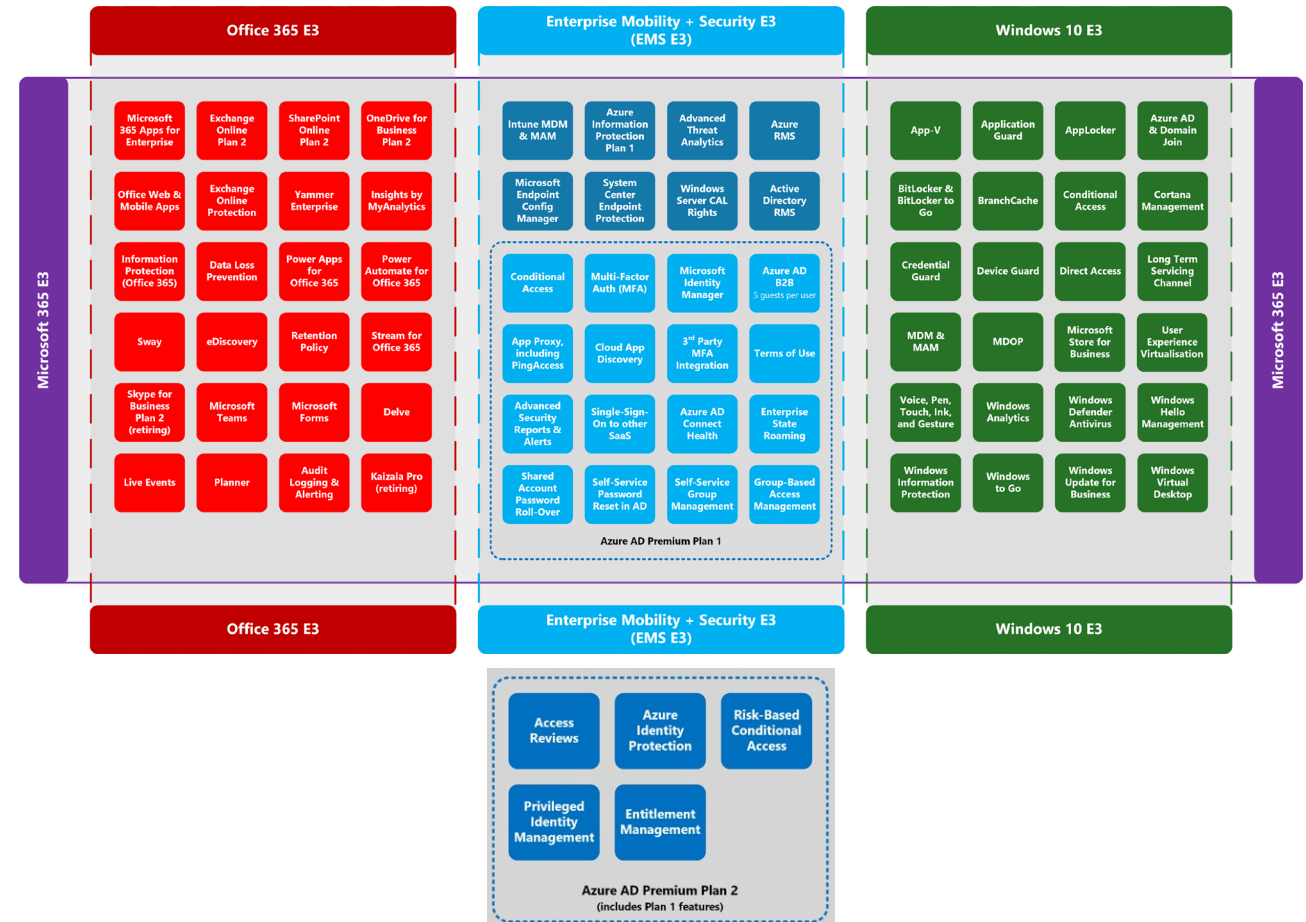
- » Kunde hat ein Enterprise Agreement, welches bereits 1 Jahr läuft
- » Die Microsoft 365 E3 Suite und zusätzlich für alle Mitarbeiter Azure Active Directory Premium Plan 2 lizenziert

Zielsetzung:

Microsoft Defender for Endpoint und evtl. Microsoft Defender for Office 365 Plan 1 und Azure ATP einführen

Problem:

Anrechnung der lizenzierten Azure Active Directory Premium Plan 2 Lizenzen an eine Microsoft 365 E5 Security Suite nur mit Zustimmung der Microsoft möglich





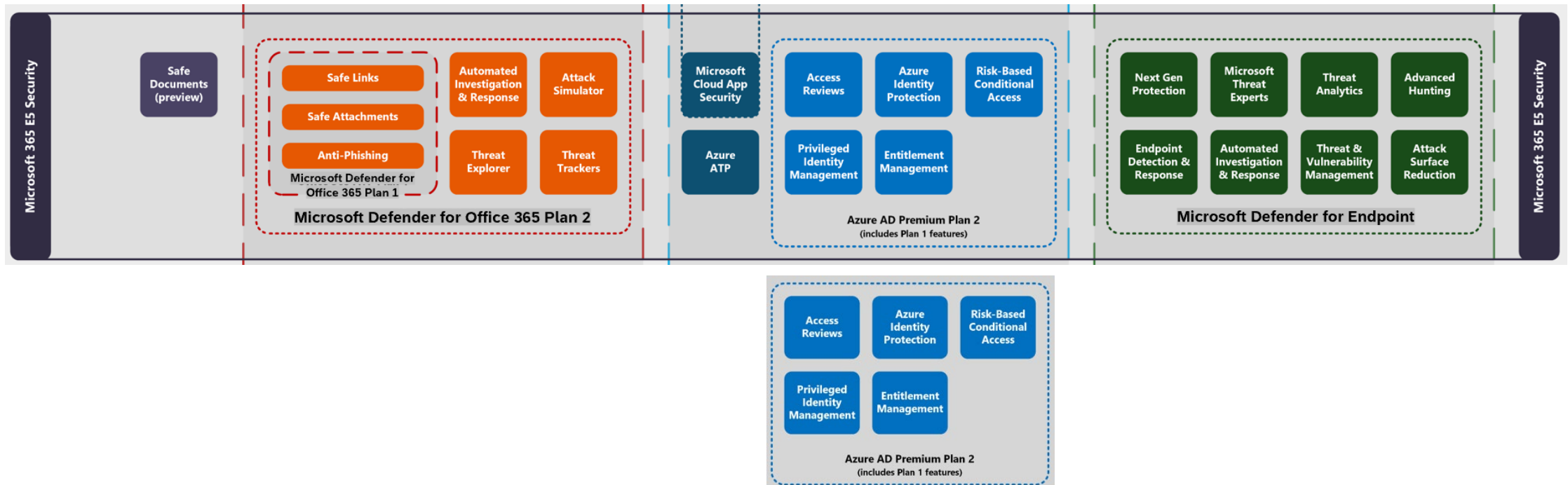
Kundenszenario aus der Praxis

Problem:

- » Die Vertragsverlängerung und die Architektur-planung erfolgten nicht aufeinander abgestimmt

Auswirkungen:

- » Es entstehen doppelte Kosten für nachträglich definierte Anforderungen
- » 3rd Party Produkte werden lizenziert obwohl diese in Microsoft Produkten bereits vorhanden sind
- » Eine Kündigung der 3rd Party Verträge ist unter Umständen nicht mehr möglich
- » Keine strategische IT-Ausrichtung auf Herstellerebene, daher entsteht ein „Flickenteppich“





03

Optimale Beispiele aus der Praxis

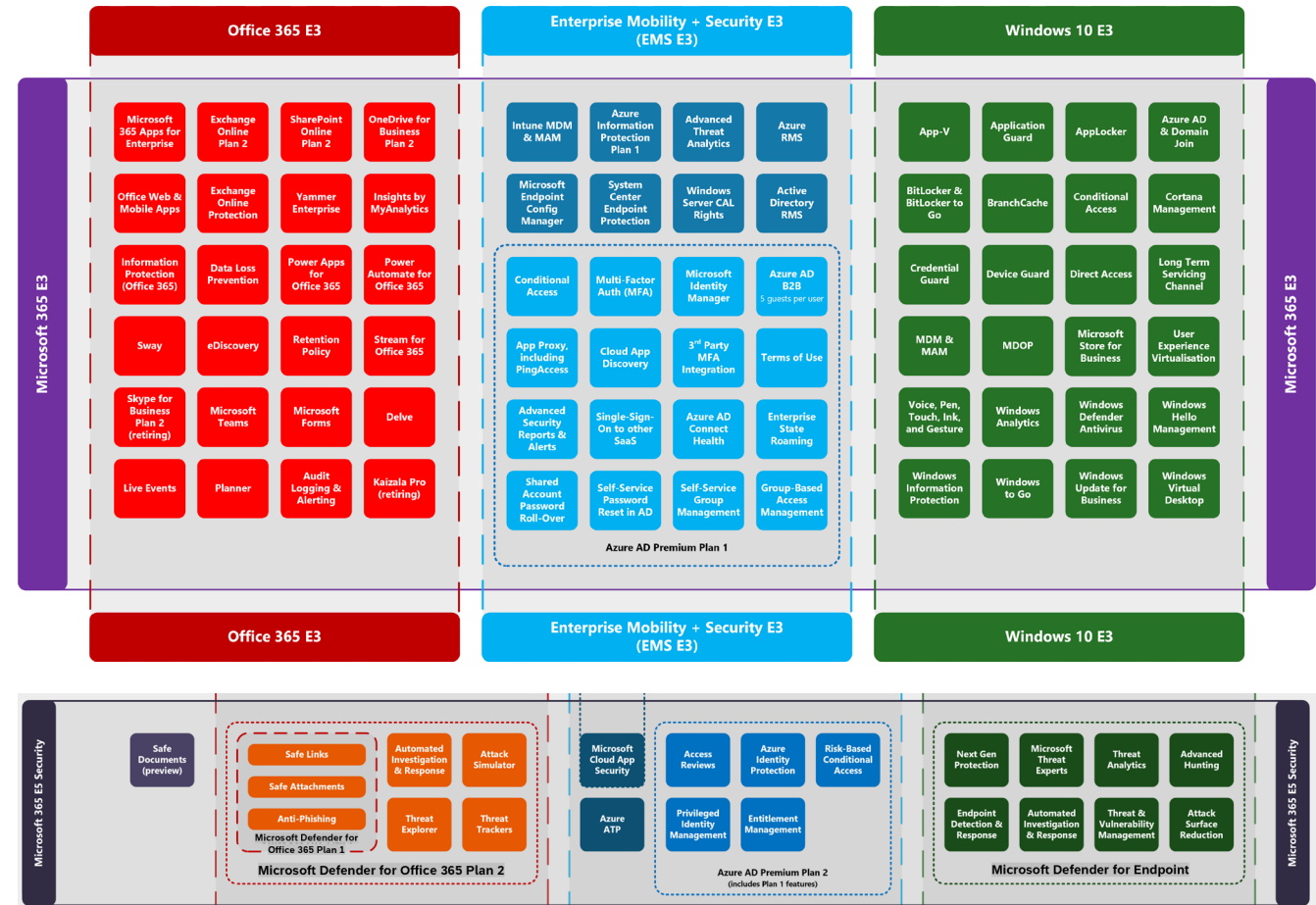


Kundenszenario aus der Praxis

- » Das Enterprise Agreement des Kunden läuft aus und er beginnt 1 Jahr vorher mit unseren Architekten die Anforderungen für zukünftige Security-Maßnahmen zu definieren
- » Er hat heute bereits in seinem noch laufenden Enterprise Agreement die Microsoft 365 E3 Suite lizenziert

Zielsetzung:

Anhand der gesetzten Prioritäten und der Security Roadmap, ermittelt durch unsere Architekten, erst Microsoft Defender for Office 365 Plan 1, dann Microsoft Defender for Endpoint und anschließend Azure Active Directory Premium P2 einführen





Wissen über Mitarbeiter und ihre Anforderungen

Die Durchführung einer Mitarbeiter-Profilanalyse ist unabdingbar:

- » Wer braucht was, wann und wie in welcher Ausprägung?
- » Welche Produktnutzungsbestimmungen gelten in welchem Vertrag für Produkte die ich benötige?
- » Welches Vertragskonstrukt bietet die Möglichkeiten die ich benötige?
- » Wie kann ich die Anforderungen bedienen anhand meiner Roadmap?

Fachbereich	Mobile User	Office User	Shop Floor User	Besprechungsräume
	• 300 Mitarbeiter	• 500 Mitarbeiter	• 200 Mitarbeiter	• 50 Räume
Anforderungen	• Mobiles Arbeiten an jedem Standort • Home Office • Office Pro Plus Installation • E-Mail von allen Geräten • Endgeräte und pro Mitarbeiter (Surface, iPad, Smartphone) • Verarbeiten von unternehmenskritischen Daten • Verschlüsselung der Daten • Teams für Video- und Telefonkonferenzen und Telefonie • SharePoint Online Intranet und für Dateiablage • Yammer • PowerApps für Reiseantrag und Urlaubsantrag • Mikros • Intune • PIM in der Anzahl wie Lizenzen heute • DevOps User in der Anzahl wie Lizenzen heute • Visual Studio in der Anzahl wie Lizenzen heute	• Office Pro Plus Installation • E-Mail • 1 Gerät pro Mitarbeiter • Verarbeiten von unternehmenskritischen Daten • Verschlüsselung der Daten • Teams für Video- und Telefonkonferenzen und Telefonie in Phase 2 • SharePoint Online Intranet und für Dateiablage • Yammer • PowerApps für Reiseantrag und Urlaubsantrag • Mikros • Intune • Windows 10 Enterprise	• Nur Office Online Apps über Browser • E-Mail über Browser • 1 Gerät pro Mitarbeiter • Teams für Video- und Telefonkonferenzen über Web • SharePoint Online Intranet • Yammer • PowerApps für Reiseantrag und Urlaubsantrag • Mikros • Windows 10 Enterprise	• Office Pro Plus Installation – Lizenzierung prüfen • Teams für Video- und Telefonkonferenzen und Telefonie • Intune • Windows 10 Enterprise
Anforderungen				

Profil 1	Microsoft 365
Mobile User	E32
	Install client apps on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user3
	Office Mobile Apps – Create/edit rights for commercial use of Office Mobile apps4
	Exchange Online Plan 2 (100 GB)
	SharePoint Online Plan 2
	Skype for Business Online Plan 2
	Microsoft Teams
	OneDrive for business 1-5+ TB7
	Yammer Enterprise
	Power Apps for Office 36511
	Microsoft Intune
	Phone System, Audio Conferencing
	Azure Information Protection Premium Plan 1
	Email archiving
	Basic Office Message Encryption
	Office 365 Advanced Threat Protection (ATP) Plan 1
	Windows 10 Desktop Operating System Upgrade Enterprise
	Microsoft Defender ATP
Plan 2 für Admins zusätzlich	Azure Active Directory Premium Plan 1



Klare Nutzungsszenarien

Die Analyse von klaren Nutzungsszenarien im Vorhinein ermöglichen eine genaue Zuordnung der Subscription-Pläne je Mitarbeiter:

Microsoft Defender for Office 365 Plan 1



Microsoft Defender for Endpoint



Azure Active Directory Premium Plan 2





Key Take-Aways

04



Key Take-Aways



Fokus auf die Business Needs, die Menschen und interne Prozesse. Es sind die wichtigsten Einflüsse auf die Sicherheitsstrategie. Prioritäten setzen.



Denken Sie unternehmensweit, ganzheitlich und langfristig.



Leben Sie die Abhängigkeiten zwischen Security Architektur, Wirtschaftlichkeit und Machbarkeit.



Definieren Sie klare Nutzungsszenarien gemeinsam mit ihrem Fachbereichen.





Steigen Sie ein: „Microsoft 365 Security Assessment“

DIE UMFASSENDE M365 SECURITY-ANALYSE

Stellen Sie die richtigen Stellschrauben um die Systemsicherheit Ihrer Office 365 / Microsoft 365 Umgebung zu erhöhen.

Mehr erfahren und nächste Schritte planen:

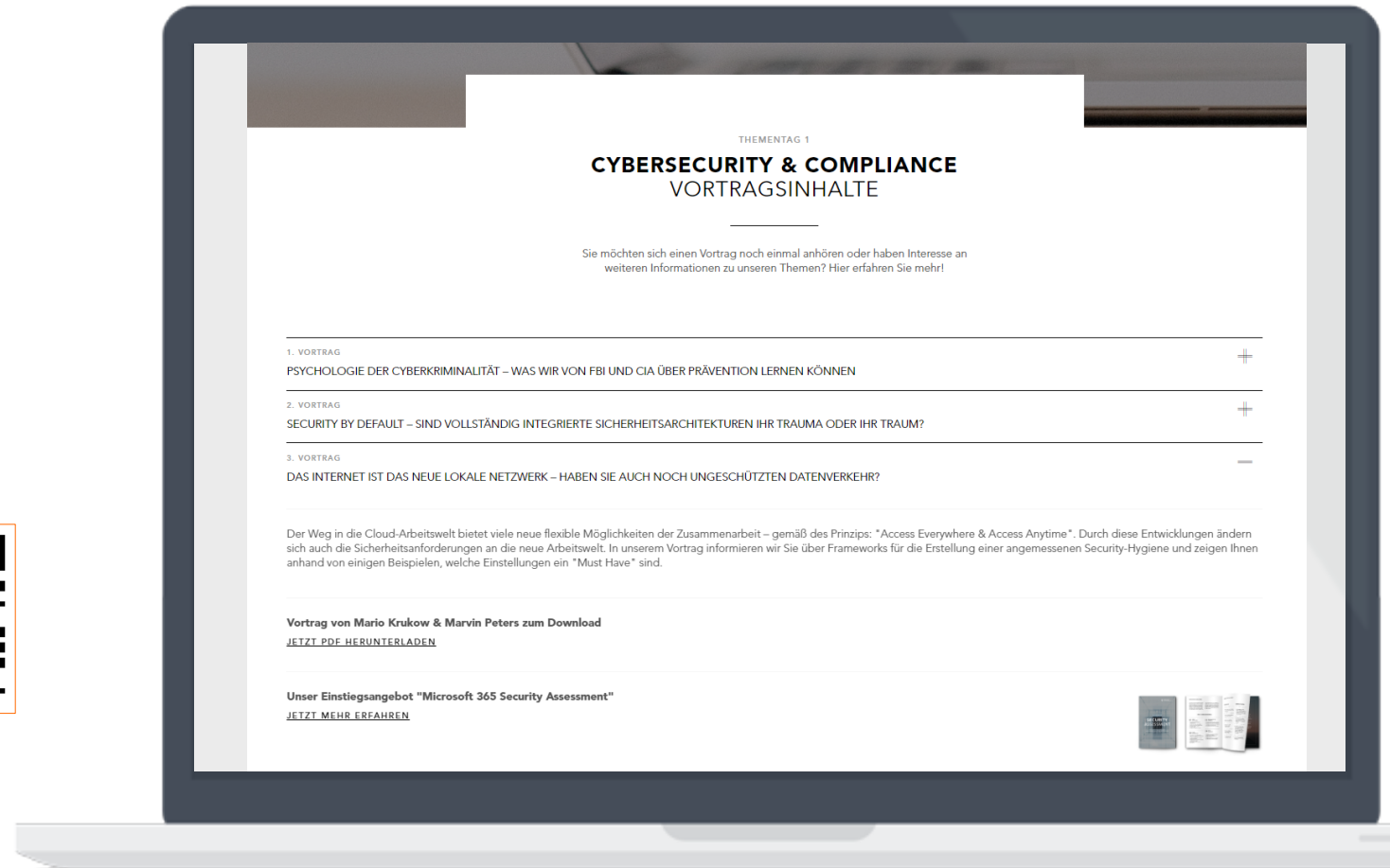
info.all-for-one.com/mifo2020-cybersecurity

**Jetzt QR-Code scannen
oder auf Link im Chat klicken!**



Sie finden dort auf unserer Website:

- Diesen Vortrag zum Download
- Informationen zum o.g. Workshop





**Jetzt QR-Code scannen
oder auf Link im Chat klicken!**

Sie finden dort auf unserer Website:

- Diesen Vortrag zum Download
- Informationen zum Workshop



HABEN SIE FRAGEN?



Ihre Ansprechpartner bei Cybersecurity & Compliance



Mario Krukow

Senior Cybersecurity Architect &
Head of Information Protection

+49 151 617 20 395

mario.krukow@all-for-one.com



Willi Prosen

Head of Sales Microsoft

+49 175 48 176 71

willi.prosen@all-for-one.com



Roland Dühning

Senior Sales Manager

+49 151 526 42 338

roland.duehring@all-for-one.com



one idea ahead



Disclaimer

Die Informationen in diesen Unterlagen sind vertraulich und dürfen nicht ohne vorherige schriftliche Genehmigung durch All for One Group SE bekannt gegeben werden. Alle Texte, Bilder und Grafiken unterliegen dem Urheberrecht und anderen Gesetzen zum Schutz des geistigen Eigentums. Alle Rechte an diesen Unterlagen sind der All for One Group SE vorbehalten.

All for One Group SE stellt diese Unterlagen ohne jegliche Verpflichtung, Gewährleistung oder Garantie, weder ausdrücklich noch stillschweigend, zur Verfügung. All for One Group SE übernimmt keine Verantwortung für Fehler oder Irrtümer in diesem Dokument, es sei denn, derartige Schäden beruhen auf Vorsatz oder grober Fahrlässigkeit. Der Inhalt dieser Unterlagen kann von All for One Group SE jederzeit geändert werden. Diese Unterlagen dienen ausschließlich informativen Zwecken und dürfen in keinen Vertrag aufgenommen, für Handelszwecke weiterverwendet oder an Dritte weitergegeben werden, soweit sie nicht für eine solche Verwendung gekennzeichnet sind oder eine vorherige schriftliche Genehmigung von All for One Group SE vorliegt.