ÖBB HOLDING

Lessons Learned in the Cloud

ENISA/ERA Conference
08.11.2023, Athens

Best of Lessons learned „Cloud“

Cloud Network

1 **Bridging On-Premise Infrastructure and Cloud Environments.**

2 **Allowing Bridging and Connections within Cloud.**

3 **Confidentiality in the Cloud.**

M365

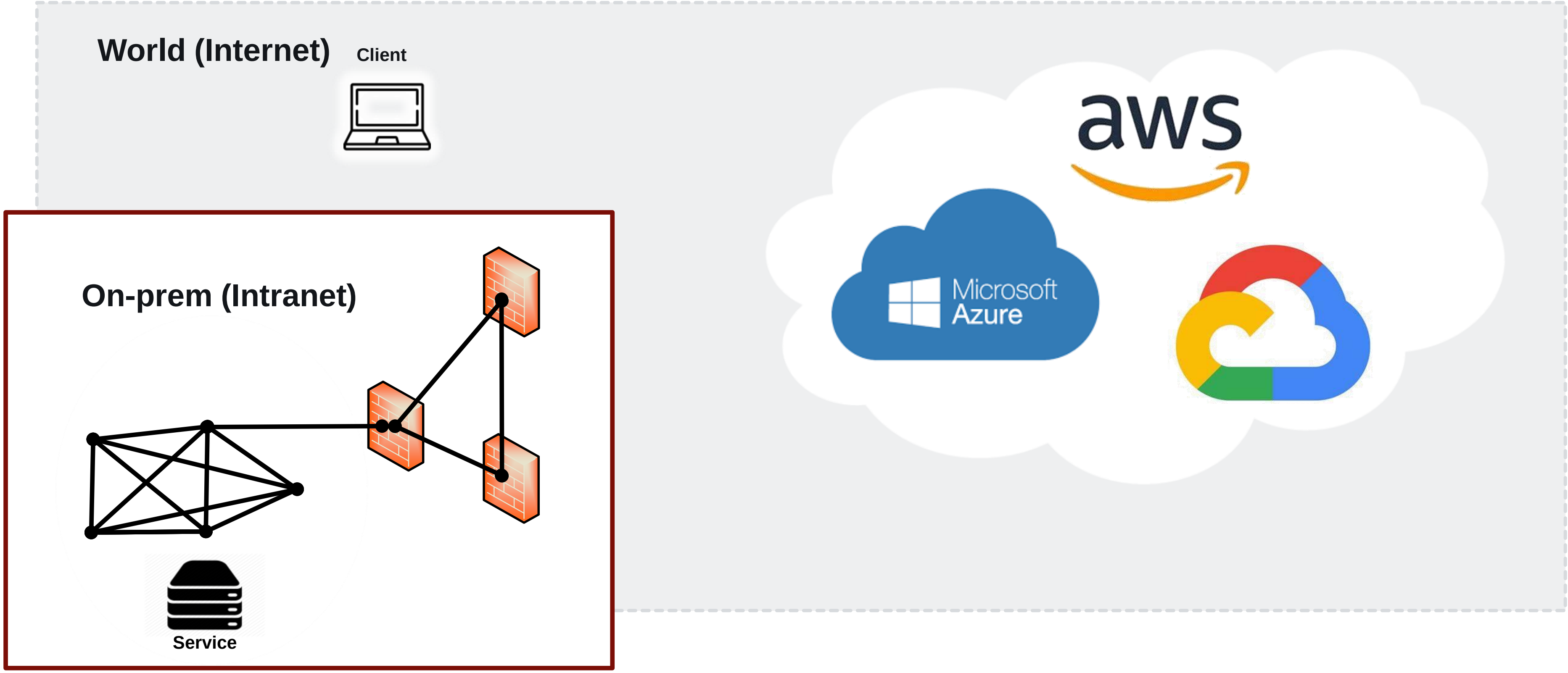
4 **Compare Features used by Users with the Microsoft License.**

Defenders

5 **Every Defender needs its own resources**

1 Bridging On-Premise Infrastructure and Cloud Environments

ÖBB HOLDING



How to connect to the cloud?

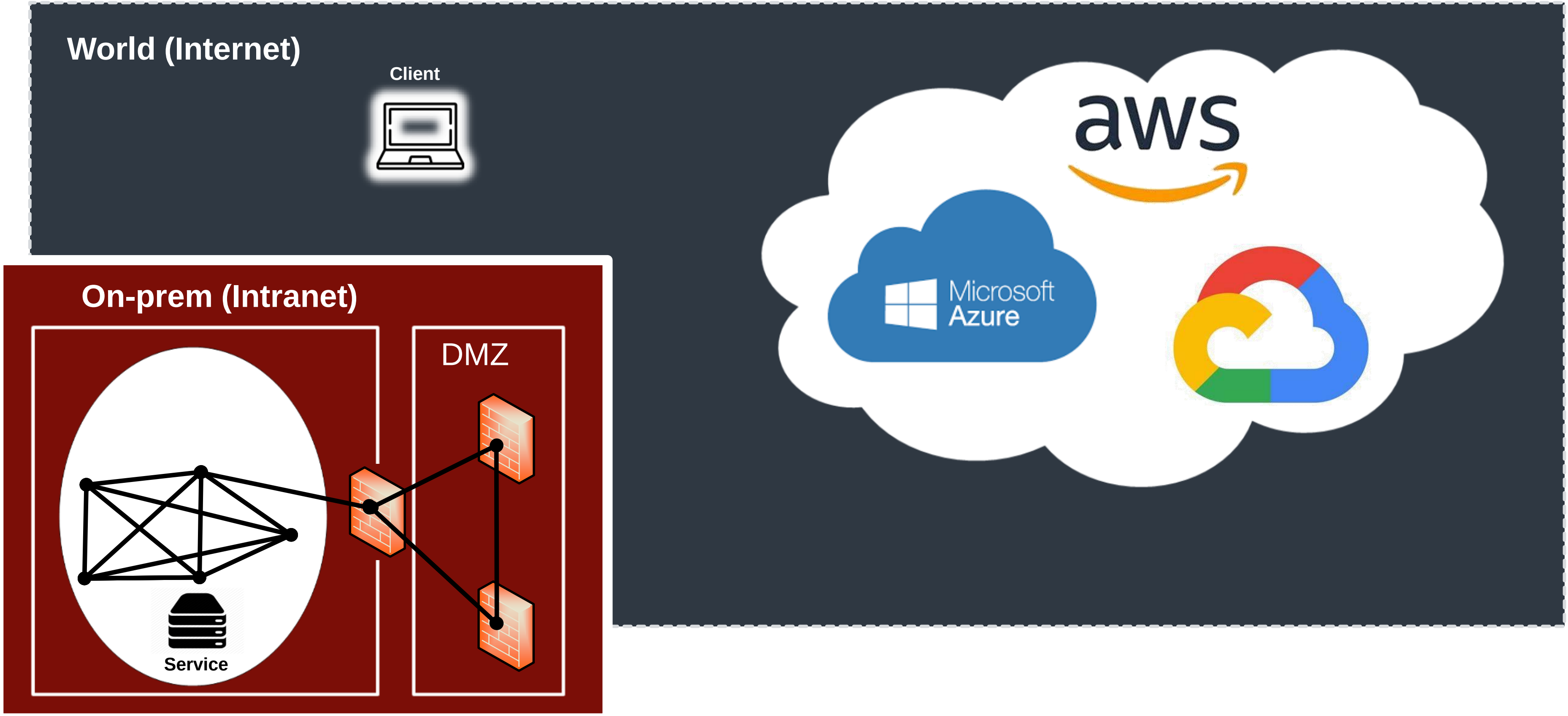
HTTPS, VPN, dedicated cable (ExpressRoute, Direct Link, Dedicated Interconnect)?

Comparison

	HTTPS	S2S VPN (Non-Azure native)	S2S VPN (Azure native)	Express Route (incl. IPSec)
Security (logical)	+	+	+	+
Security (physical)	-/+	-/+	-/+	**++**
Latency	-/+	-	-	**++**
Bandwidth	+	-/+	-/+	-/+
Complexity of operations (lower better)	+	-	+	-/+
Vendor lock-in	++	**+**	-	-
HTTP lock-in	**--**	+	+	+
Interoperability with legacy/proprietary protocols and applications	-	**++**	+	+
Deployment time	**++**	-	**++**	--
Elasticity (Scalability)	++	-	+	-
Interoperability with Azure native services	+	-	+	+
Transparency over endpoints	+	+	-	-
Capex (lower better)	**++**	**-**	**+/-**	**-**
Opex (lower better)	**+**	**-**	**-**	**--**

Lesson learned: *Do not limit the customer. Answer the needs!*

2 Allowing Bridging



Which connections are allowed?

“Lessons Learned | Obvious” Procedure to Cloud Adoption

Cloud should be the enabler in your company. Alignt to IT-Strategy:

- Cloud only
- Cloud first
- Cloud too

Be fair and not only black white.

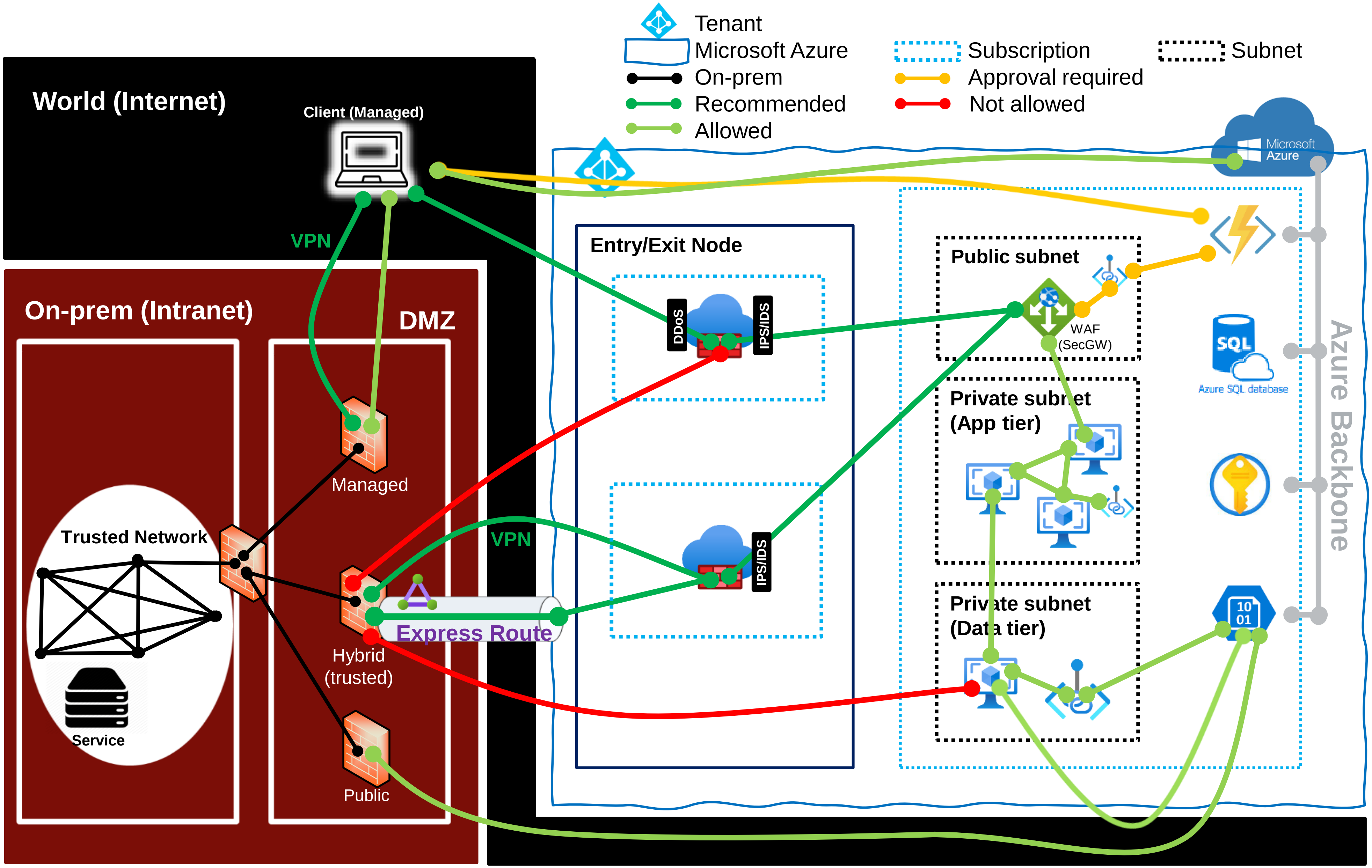
Apply policies and assessments to all cloud providers and services in the same manner.

Start with Use Cases and clearly define connection matrices within the company
(include enterprise architects, network architects, cloud developers, information security & data protection officers, product owners)

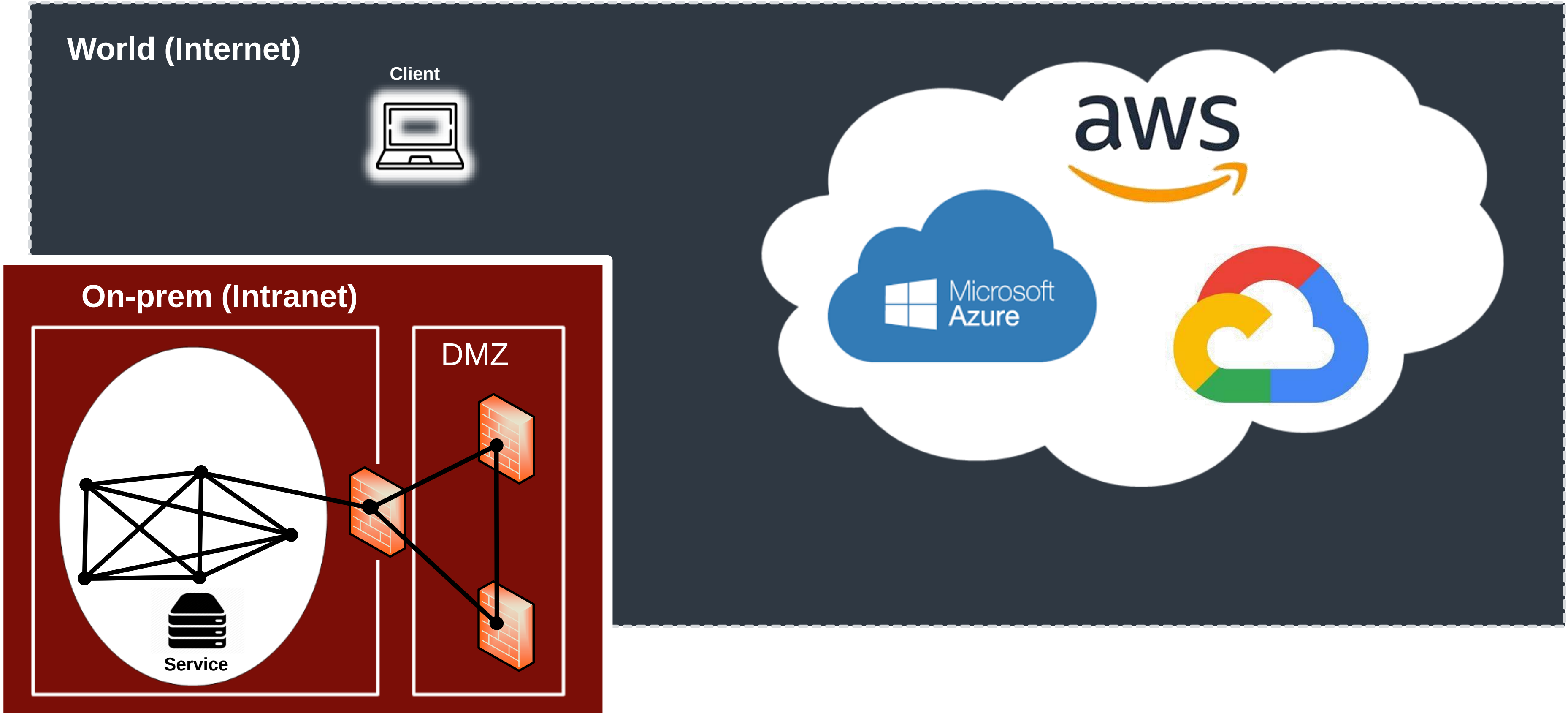
Make the connection matrix transparent and visualize it

Find time for lessons learned

Example of Visualization



3 Confidentiality in the Cloud



How do I handle confidential data in the cloud?

“Lessons Learned | Handle Confidential data in the cloud

- Learn to trust (but verify).
- Understand shared responsiblity model and how it applies to you.
- Learn your risk apetite. Remember, cloud environments are not your on-prem infrastructure. You are usually one of many customers.
- Let stakeholder (business owner, data owner, legal, data privacy officers, management,…) classify their data.
- Define security protection measures according to classification levels, not cloud providers or services. Prioritize data classification over service classification.

Start with beeing more strict, the business will overrule you.

Example of a Decision Table – Data at Rest

ÖBB HOLDING

Confidentiality

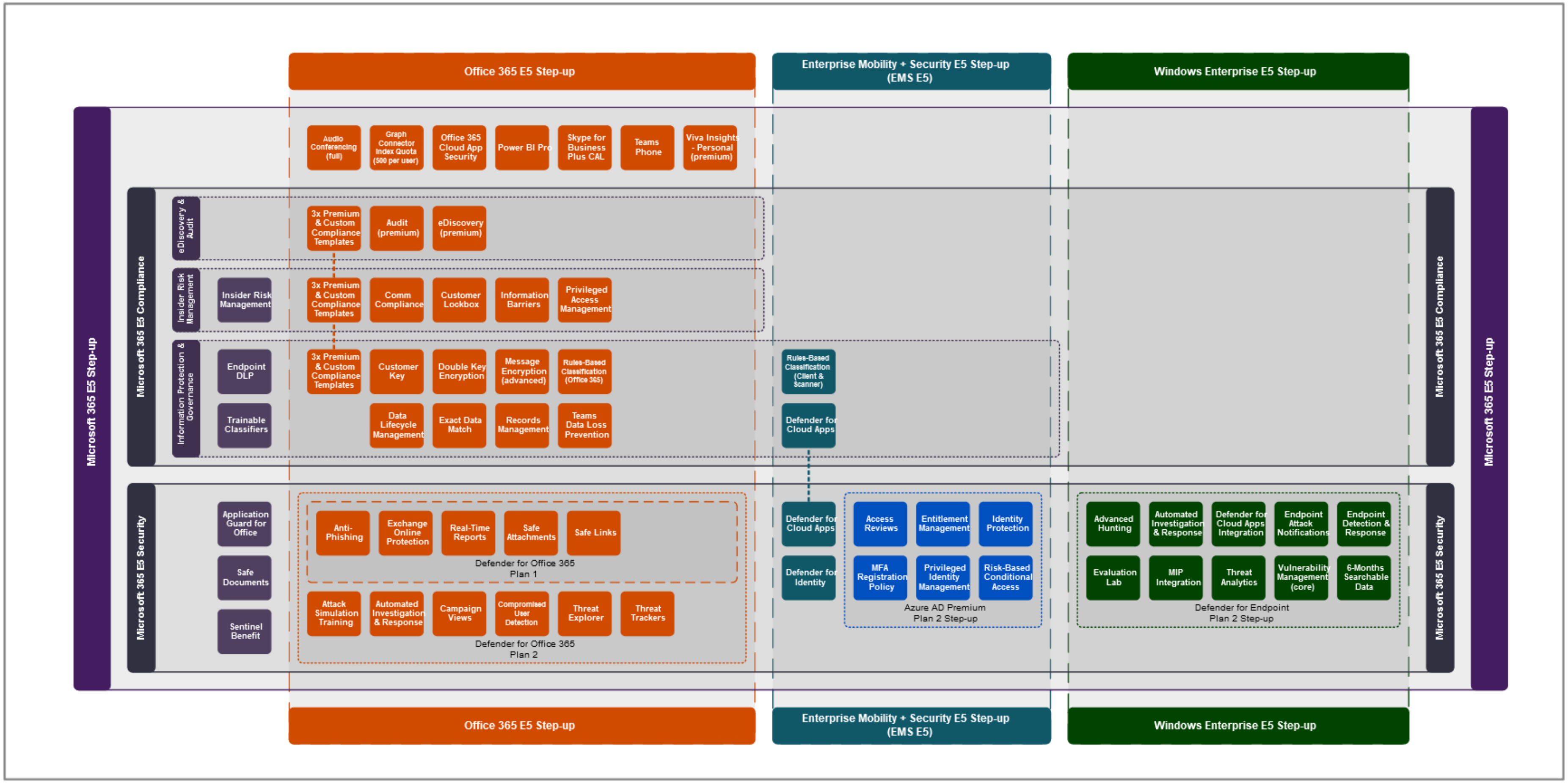
	Public	Internal	Confidential	Strictly confidential
Native credentials & encryption	○	☑	☑	🚫
BYOK credentials & encryption	○	☑	☑	👁
Long term archiving of **BYOK** credentials in the Cloud	○	☑	👁	👁
HYOK credentials & encryption	○	☑	☑	☑

Legende: ○ Optional ☑ Mandatory 👁 Additional approval 🚫 Not allowed

How confortable are you with your on-prem key management? HYOK is best, but complex to handle it. BYOK seems to be a „Kompromiss“.

4 Compare Features used by Users with the Microsoft License.

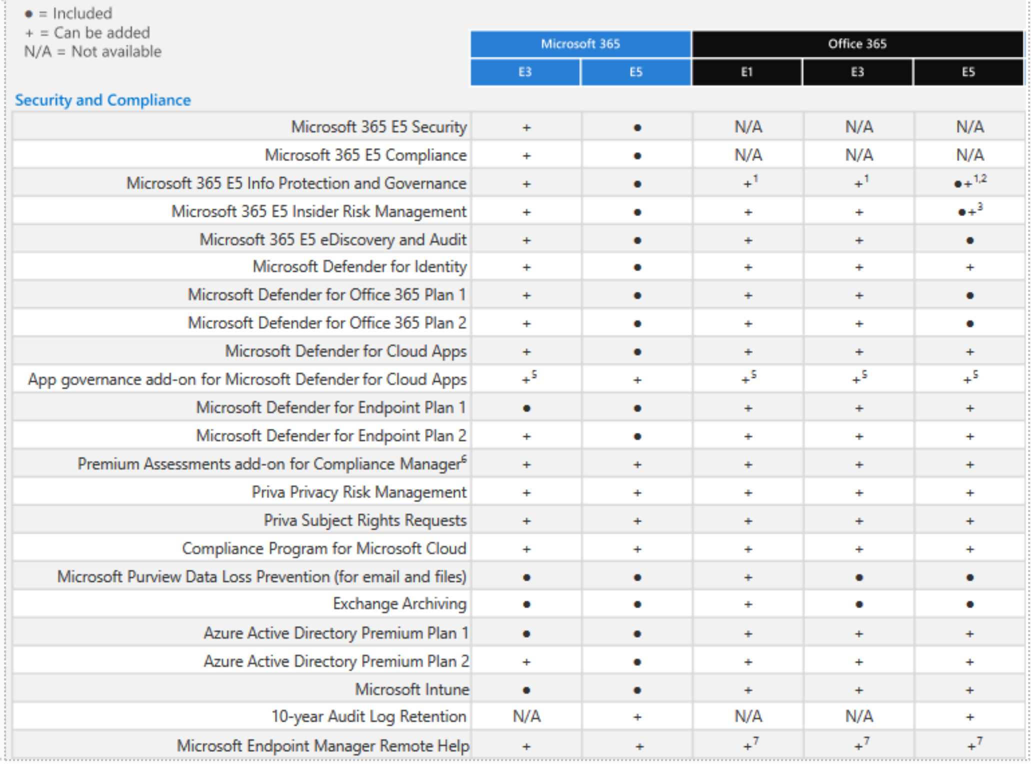
ÖBB HOLDING


Office 365 E5 Step-up
Enterprise Mobility + Security E5 Step-up (EMS E5)
Windows Enterprise E5 Step-up
Microsoft 365 E5 Step-up
Microsoft 365 E5 Compliance
Microsoft 365 E5 Security
eDiscovery & Audit
Insider Risk Management
Information Protection & Governance
Audio Conferencing (full)
Graph Connector Index Quota (500 per user)
Office 365 Cloud App Security
Power BI Pro
Skype for Business Plus CAL
Teams Phone
Viva Insights - Personal (premium)
3x Premium & Custom Compliance Templates
Audit (premium)
eDiscovery (premium)
Insider Risk Management
3x Premium & Custom Compliance Templates
Comm Compliance
Customer Lockbox
Information Barriers
Privileged Access Management
Endpoint DLP
Trainable Classifiers
3x Premium & Custom Compliance Templates
Customer Key
Double Key Encryption
Message Encryption (advanced)
Rules-Based Classification (Office 365)
Data Lifecycle Management
Exact Data Match
Records Management
Teams Data Loss Prevention
Rules-Based Classification (Client & Scanner)
Defender for Cloud Apps
Application Guard for Office
Safe Documents
Sentinel Benefit
Anti-Phishing
Exchange Online Protection
Real-Time Reports
Safe Attachments
Safe Links
Defender for Office 365 Plan 1
Attack Simulation Training
Automated Investigation & Response
Campaign Views
Compromised User Detection
Threat Explorer
Threat Trackers
Defender for Office 365 Plan 2
Defender for Cloud Apps
Defender for Identity
Access Reviews
Entitlement Management
Identity Protection
MFA Registration Policy
Privileged Identity Management
Risk-Based Conditional Access
Azure AD Premium Plan 2 Step-up
Advanced Hunting
Automated Investigation & Response
Defender for Cloud Apps Integration
Endpoint Attack Notifications
Endpoint Detection & Response
Evaluation Lab
MIP Integration
Threat Analytics
Vulnerability Management (core)
6-Months Searchable Data
Defender for Endpoint Plan 2 Step-up

https://m365maps.com/files/Microsoft-365-E5.htm

Compare Features used by Users with the Microsoft License.

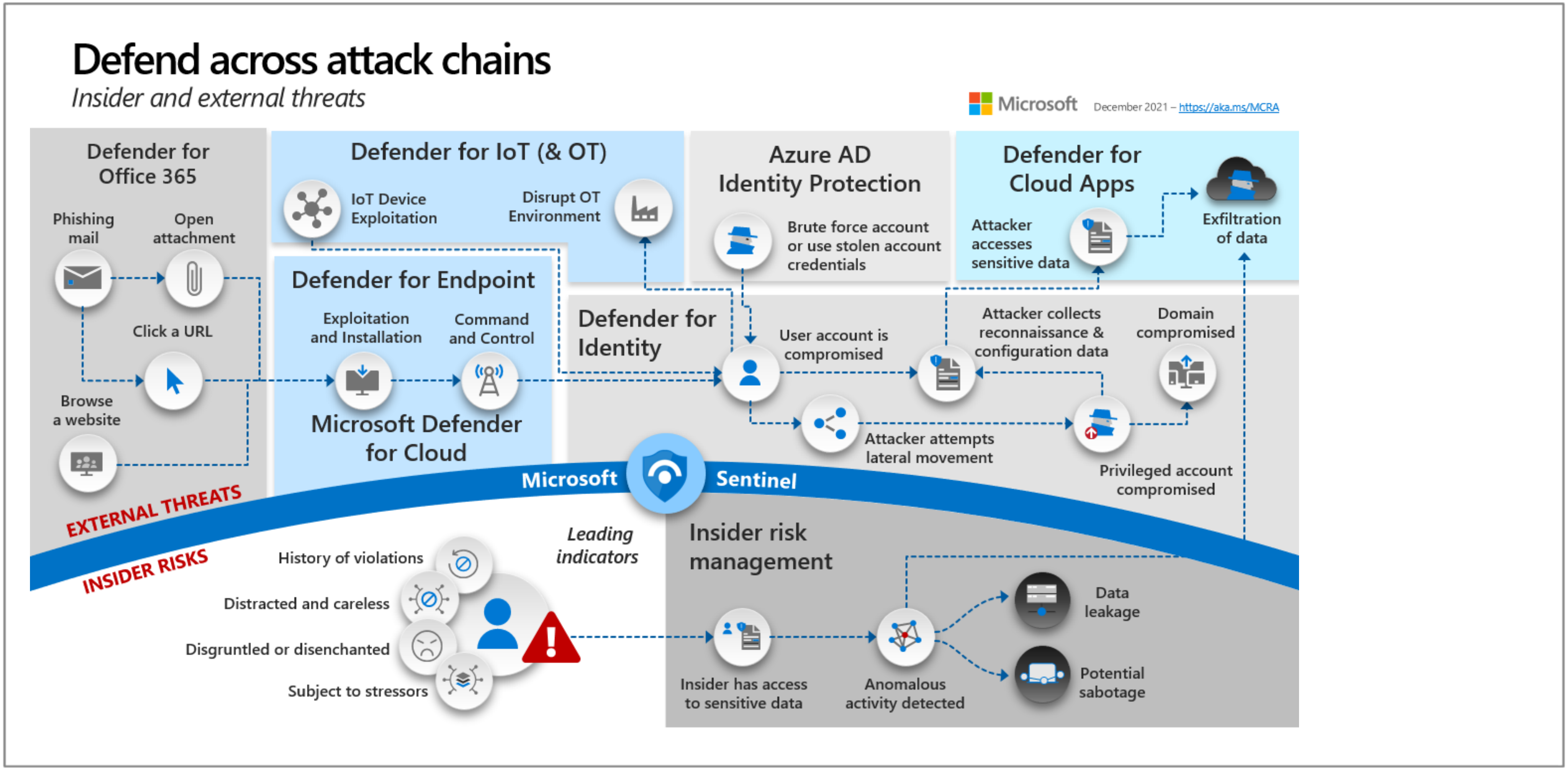
- Define functionality you need before deep-diving into E3 or E5 features.
  It is not X-mas yet!
- You will virtually always find a new „useful“ add-in.
- Compare licensed features with deployed ones.
- Check if all licensed features are well configured or only default configuration is set.
- Check the status of the feature (GA / public preview)



● = Included
+ = Can be added
N/A = Not available

	Microsoft 365		Office 365		
	E3	E5	E1	E3	E5
Security and Compliance					
Microsoft 365 E5 Security	+	●	N/A	N/A	N/A
Microsoft 365 E5 Compliance	+	●	N/A	N/A	N/A
Microsoft 365 E5 Info Protection and Governance	+	●	+[1]	+[1]	●+[1,2]
Microsoft 365 E5 Insider Risk Management	+	●	+	+	●+[3]
Microsoft 365 E5 eDiscovery and Audit	+	●	+	+	●
Microsoft Defender for Identity	+	●	+	+	+
Microsoft Defender for Office 365 Plan 1	+	●	+	+	●
Microsoft Defender for Office 365 Plan 2	+	●	+	+	●
Microsoft Defender for Cloud Apps	+	●	+	+	+
App governance add-on for Microsoft Defender for Cloud Apps	+[5]	+	+[5]	+[5]	+[5]
Microsoft Defender for Endpoint Plan 1	●	●	+	+	+
Microsoft Defender for Endpoint Plan 2	+	●	+	+	+
Premium Assessments add-on for Compliance Manager[6]	+	+	+	+	+
Priva Privacy Risk Management	+	+	+	+	+
Priva Subject Rights Requests	+	+	+	+	+
Compliance Program for Microsoft Cloud	+	+	+	+	+
Microsoft Purview Data Loss Prevention (for email and files)	●	●	+	●	●
Exchange Archiving	●	●	+	●	●
Azure Active Directory Premium Plan 1	●	●	+	+	+
Azure Active Directory Premium Plan 2	+	●	+	+	+
Microsoft Intune	●	●	+	+	+
10-year Audit Log Retention	N/A	+	N/A	N/A	+
Microsoft Endpoint Manager Remote Help	+	+	+[7]	+[7]	+[7]

5 Every Defender needs its own 24x7 resources – do you have it?


Defend across attack chains
Insider and external threats
Microsoft
December 2021 – https://aka.ms/MCRA
Defender for Office 365
Phishing mail
Open attachment
Click a URL
Browse a website
Defender for IoT (& OT)
IoT Device Exploitation
Disrupt OT Environment
Defender for Endpoint
Exploitation and Installation
Command and Control
Microsoft Defender for Cloud
Azure AD Identity Protection
Brute force account or use stolen account credentials
Defender for Identity
User account is compromised
Attacker attempts lateral movement
Attacker collects reconnaissance & configuration data
Domain compromised
Privileged account compromised
Defender for Cloud Apps
Attacker accesses sensitive data
Exfiltration of data
Microsoft Sentinel
EXTERNAL THREATS
INSIDER RISKS
History of violations
Distracted and careless
Disgruntled or disenchanted
Subject to stressors
Leading indicators
Insider risk management
Insider has access to sensitive data
Anomalous activity detected
Data leakage
Potential sabotage

Thank you, any Questions & Feedback?

ÖBB HOLDING

Marian Kühnel
Information Security Architect
Business-IT & Cloud

ÖBB Group
+43 664 886 77170
Marian.kuehnel@oebb.at

Helmut Klarer
Chief Information Security Architect

ÖBB Group
+43 664 617 8807
Helmut.klarer@oebb.at

Source: https://www.dell.com/en-us/blog/cloud-adoption-strategy-vs-reality/

TLP green (ÖBB company-internal)

ÖBB HOLDING

Thank you