WEBINAR: CASE STUDY EWN -
NETZWERKVERKEHR IN ECHTZEIT ÜBERPRÜFEN

first frame networkers

HERZLICH WILLKOMMEN

first frame networkers

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

Was Sie heute erwartet:

Case Study: Wie das Kantonale Elektrizitätswerk Nidwalden EWN den Netzwerkverkehr in Echtzeit überprüft.

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 9 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).

KURZVORSTELLUNG FIRST FRAME NETWORKERS AG

first frame networkers

- Gründung 1997 in Zug, heute Hauptsitz in Baar
- 85 Mitarbeitende, davon 5 Lernende
- Inhabergeführt
- ISO 9001 & ISO 27001 für alle Geschäftsprozesse des ganzen Unternehmens.
- IT-Infrastrukturen und IT-Services für Unternehmen
- Branchenunabhängig
- Gesamte Deutschschweiz

UNSER FOKUS: IT-SERVICES

first frame networkers

Workplace Services

Wir schützen Ihre Endpoints und steigern die Effizienz und Zufriedenheit der IT-Nutzenden.

Security Services

Unser Security Services erkennt Cyberangriffe frühzeitig und unterstützt Sie bei Sicherheits-Vorfällen.

Network Services

Abgestimmt auf Ihre die Bedürfnisse sorgen wir für eine sichere Netzwerk-umgebung.

Cloud Services

Unsere «first 365» Cloud Lösungen sind ideal für eine überwachte und geschützte IT-Infrastruktur.

KURZVORSTELLUNG EWN

first frame networkers

Kantonales Elektrizitätswerk Nidwalden

128	298.18	8
Mitarbeitende	Mio. kWh Stromabsatz 2025	Eigene Wasserkraftwerke

AUSGANGSLAGE EWN

first frame networkers

IST

- Kritische Infrastruktur mit hohem Schutzbedarf
- EDR, Firewall, PAM – alles im Einsatz
- OT und IT-Netzwerke

Soll

- Logs von Drittquellen anbinden
- Verbessern der Bereitschaft für Forensik
- Zentrale Aufbewahrung der Logs

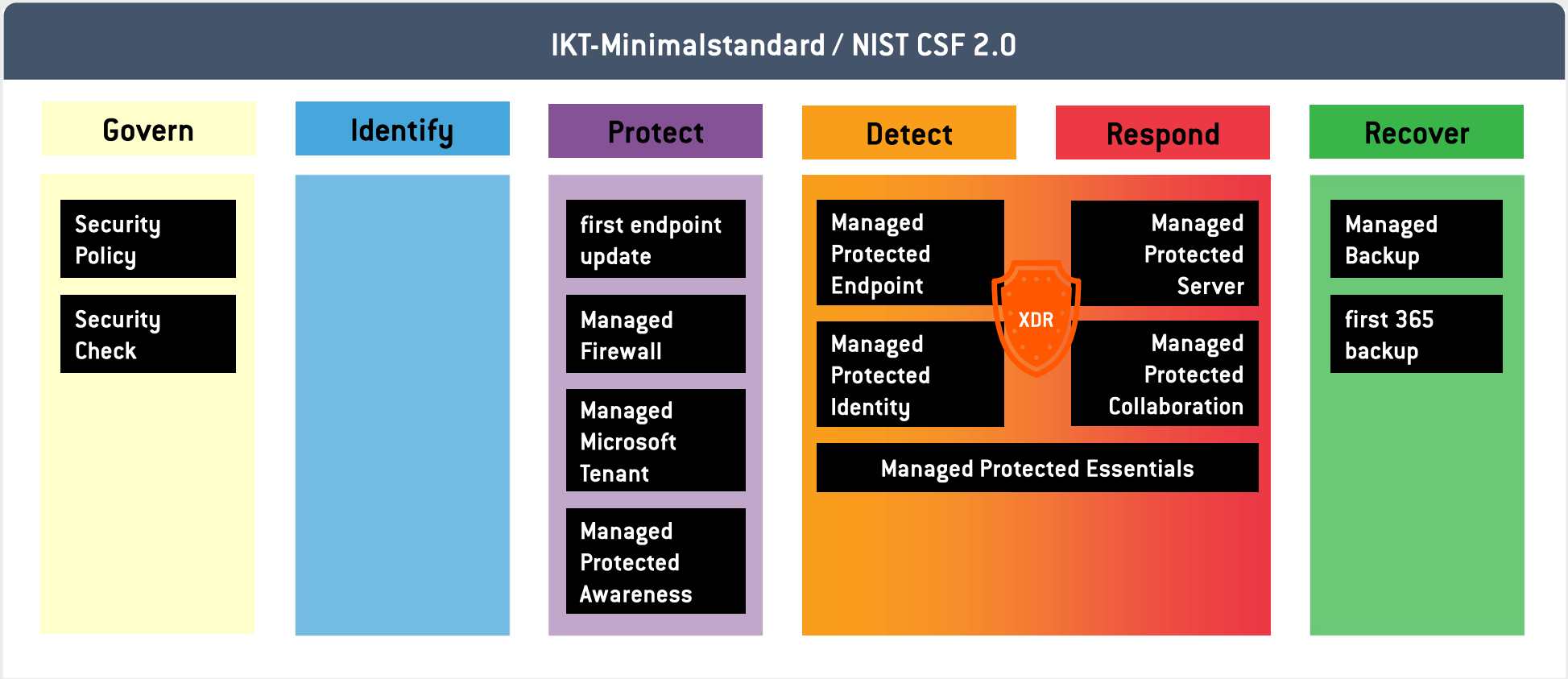
DISCLAIMER OT

first frame networkers

- OT können wir nicht zeigen
- Gezeigte Produkte unterstützen OT Protokolle wie :
- IEC 60870-5-104, Modbus TCP und Profinet
- BACnet, BSAP, CIP, COTP, DNP3, ECAT, ENIP, Modbus, OPC UA, S7

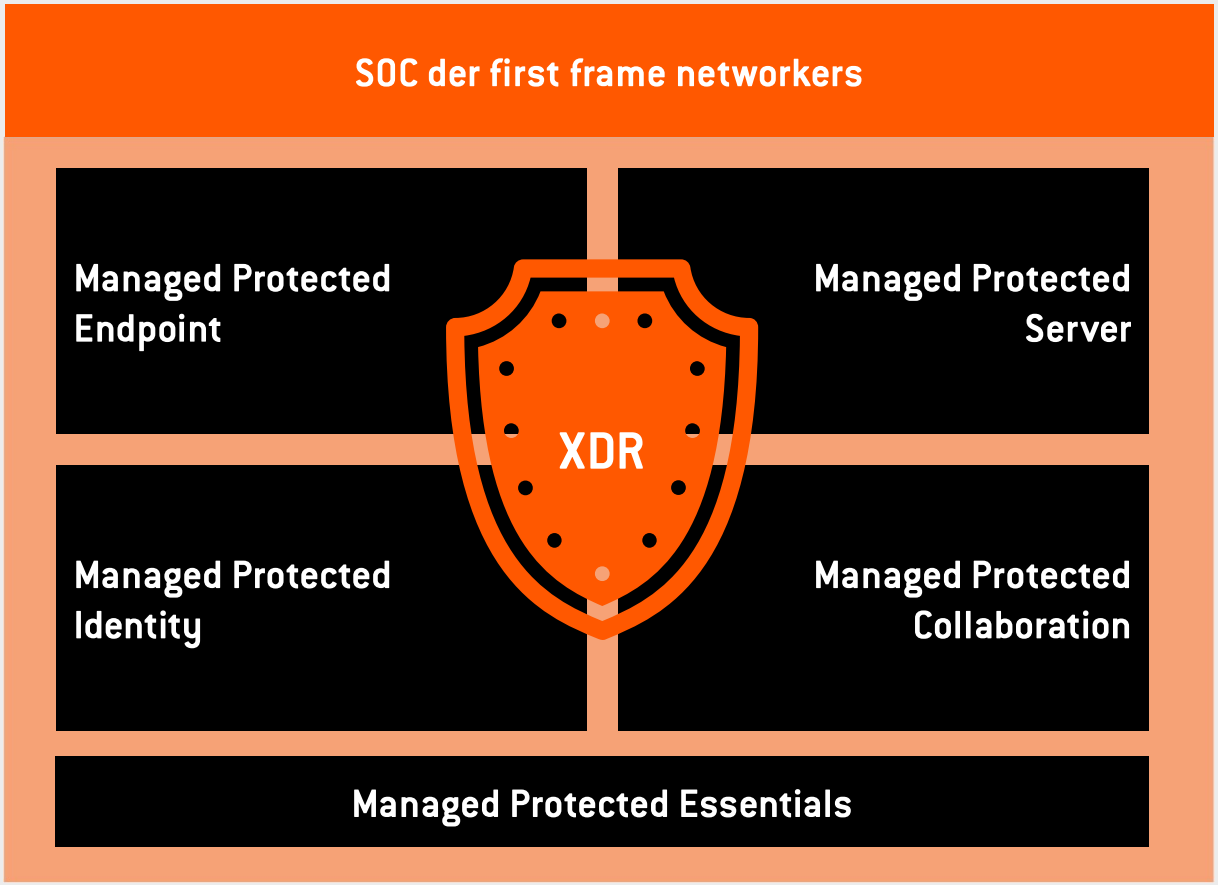
GESAMTES SECURITY PORTFOLIO

first frame networkers



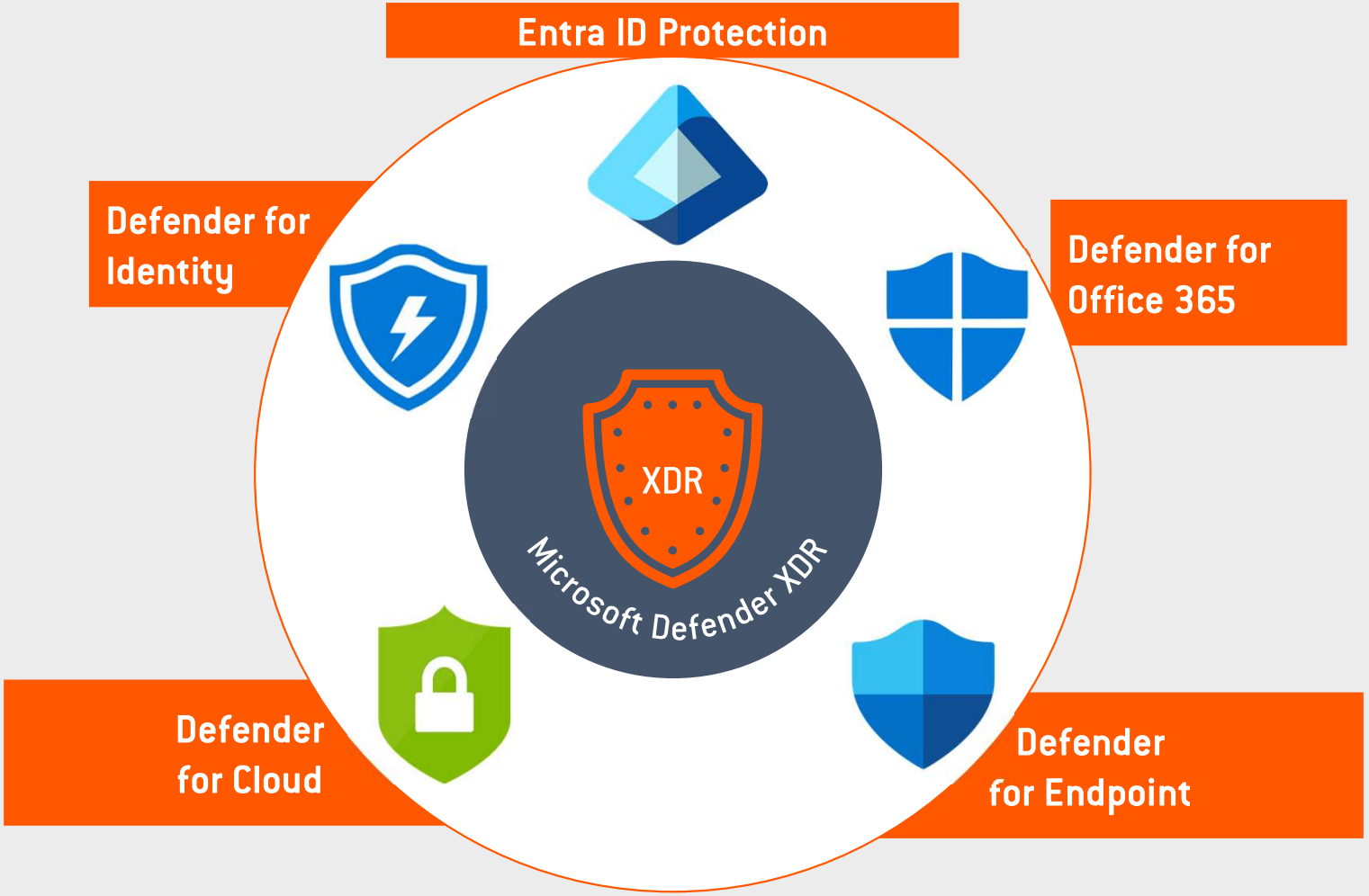
WIE SIEHT DAS FÜR MICH ALS KUNDEN AUS?

first frame networkers



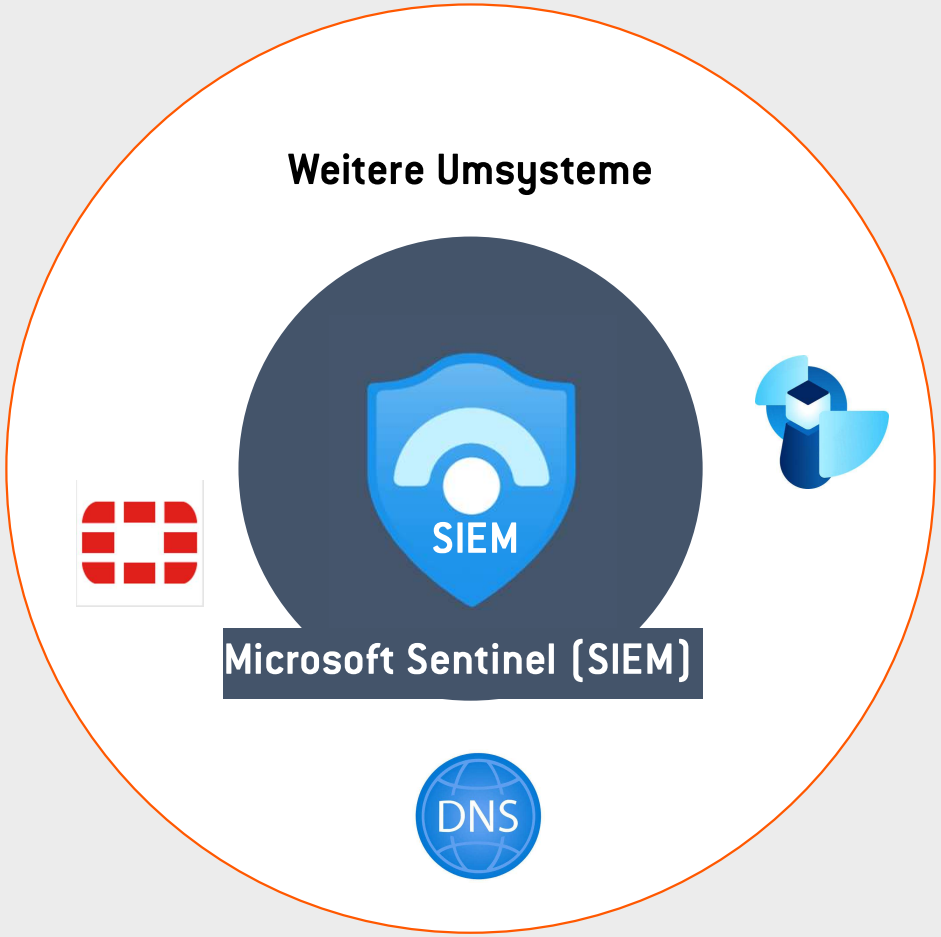
WIR HABEN DOCH MICROSOFT DEFENDER XDR

first frame networkers



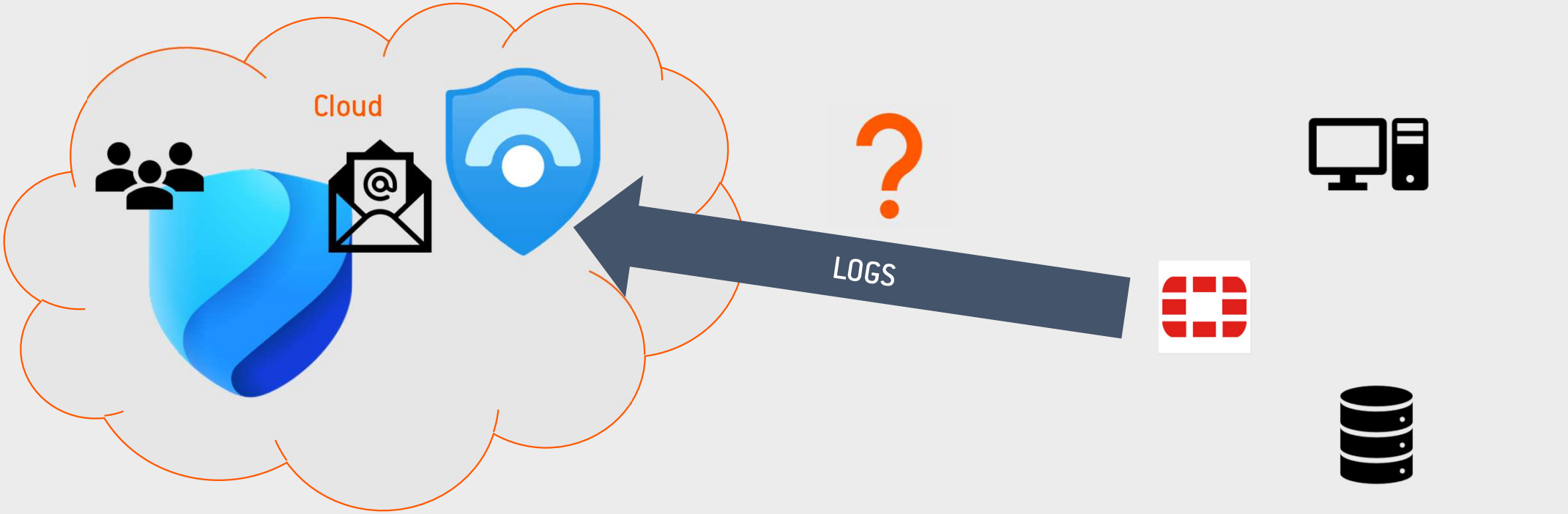
INTEGRATION MIT SIEM

first frame networkers



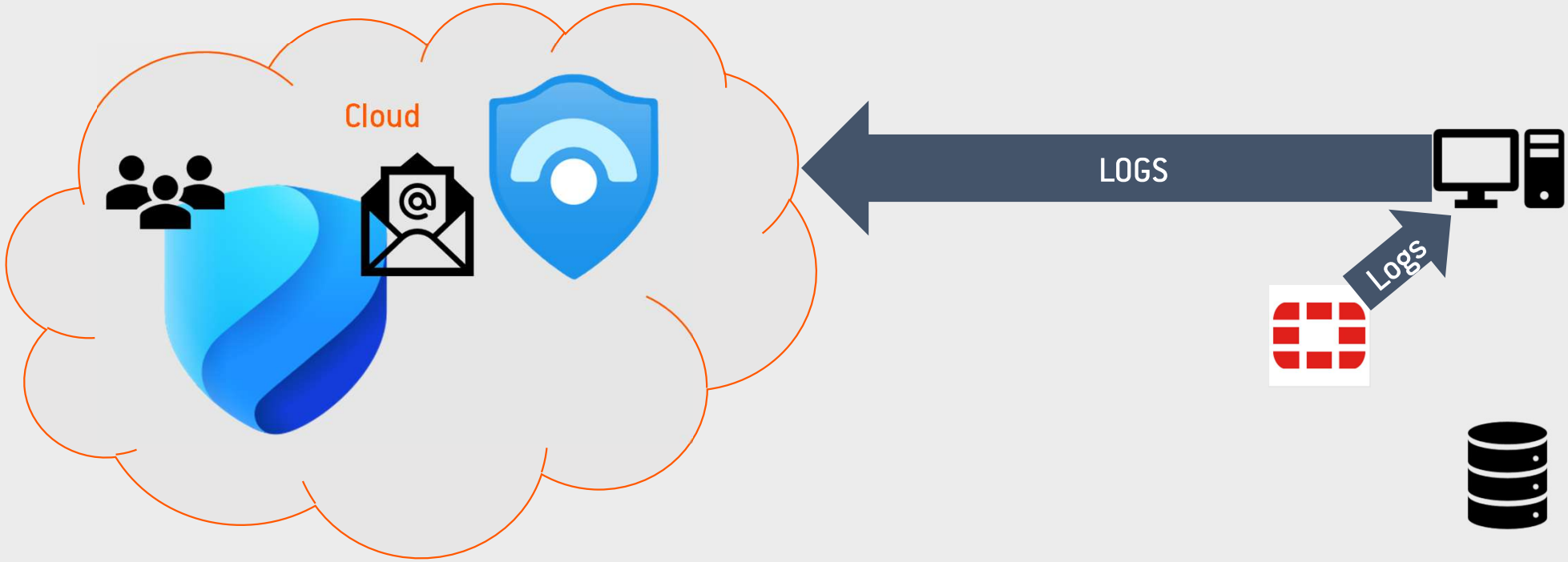
INTEGRATION MIT SIEM

first frame networkers



WIE KOMMEN LOGS ZU SENTINEL

first frame networkers



DIE FRAGE

first frame networkers

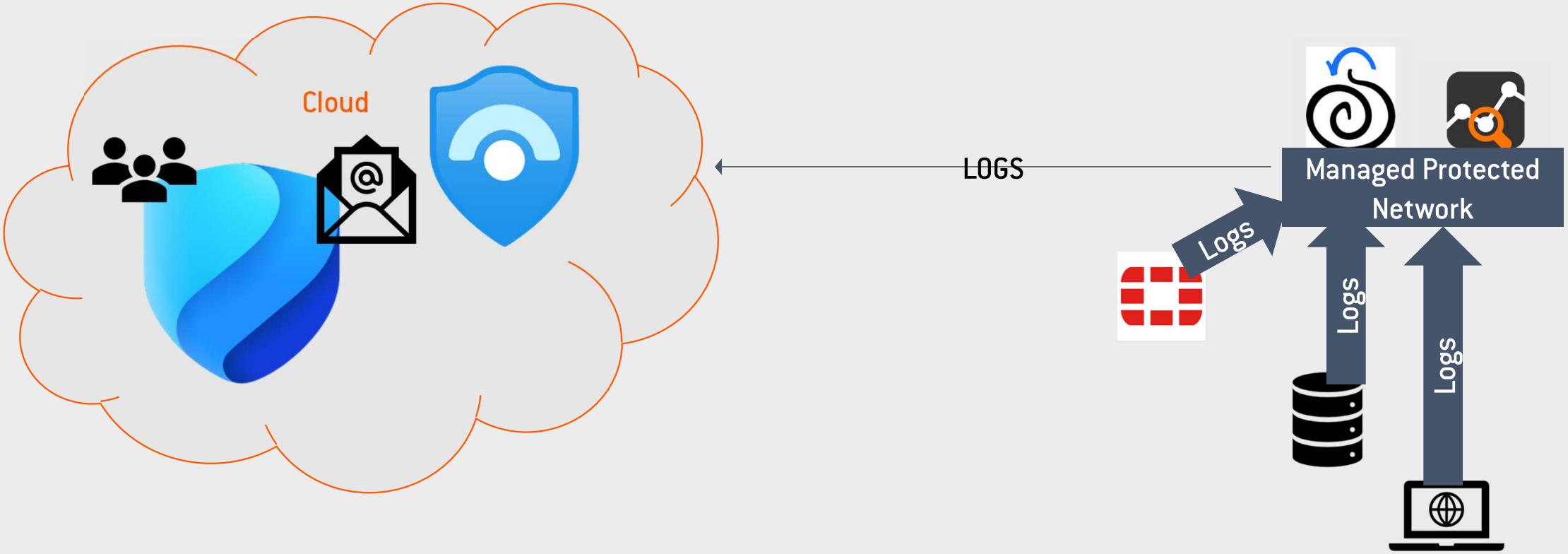
- **Wieso dieser VM kein GUI + zusätzliche Aufgaben geben?**

ZUSÄTZLICHE AUFGABEN

first frame networkers

- Echtzeit-Analyse
- Historische Analyse
- Anbinden weiterer Quellen
- Sicherheits Checks

INTEGRATION MIT SIEM



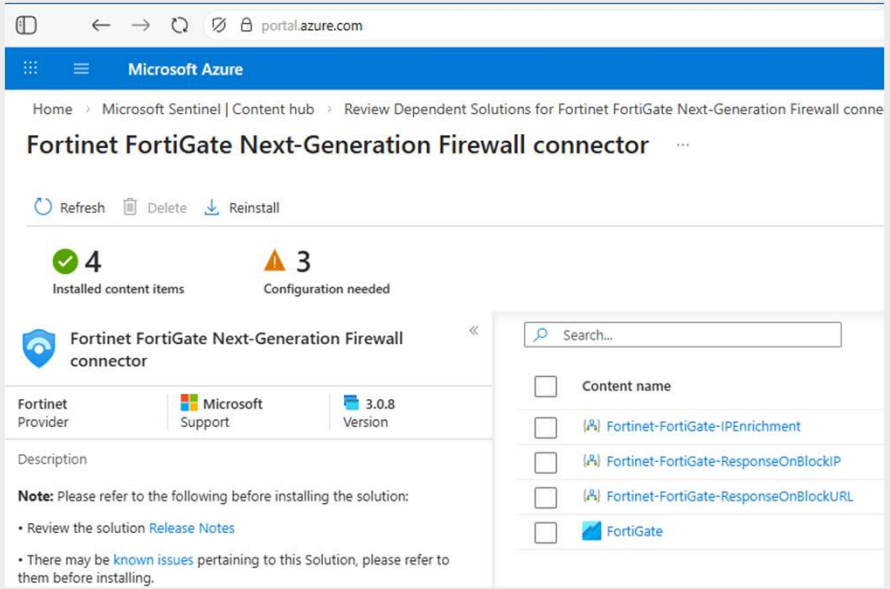
WIESO NICHT NUR SENTINEL

first frame networkers

Kosten

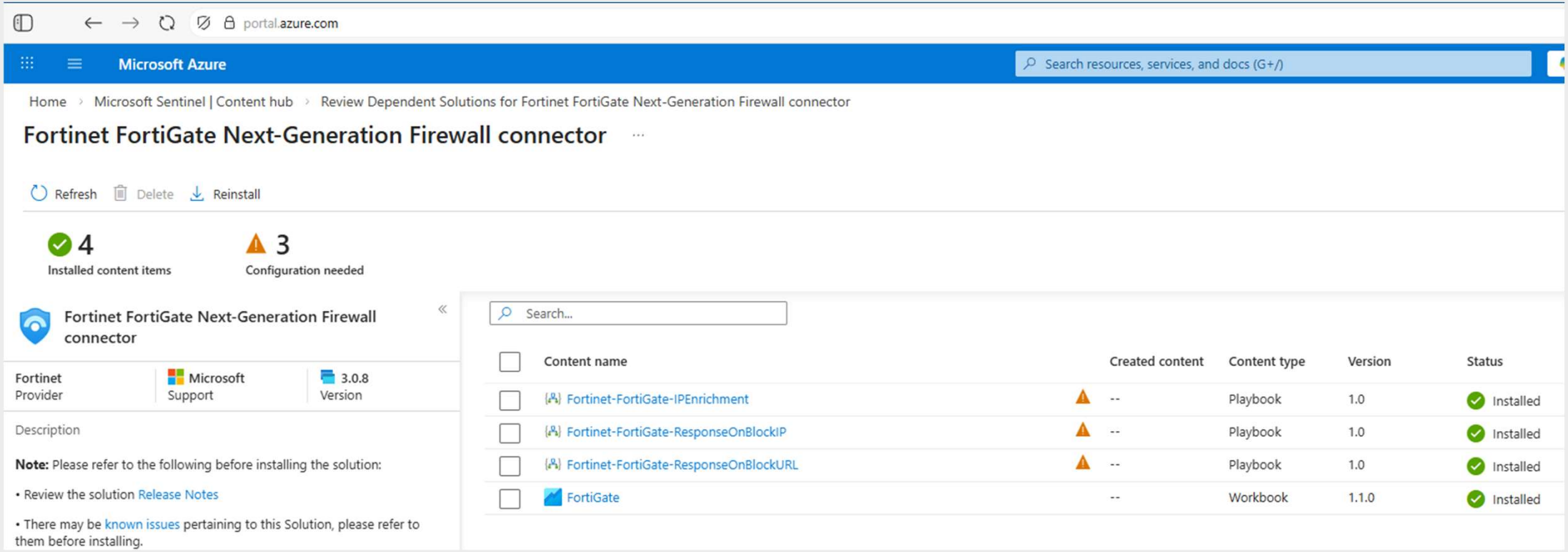
- 5.- CHF pro GB
- 0.15 CHF pro GB (Abfragen kosten separat)

Funktionalität



NUTZEN - SENTINEL & FORTIGATE BUILT-IN «RULES»

first frame networkers

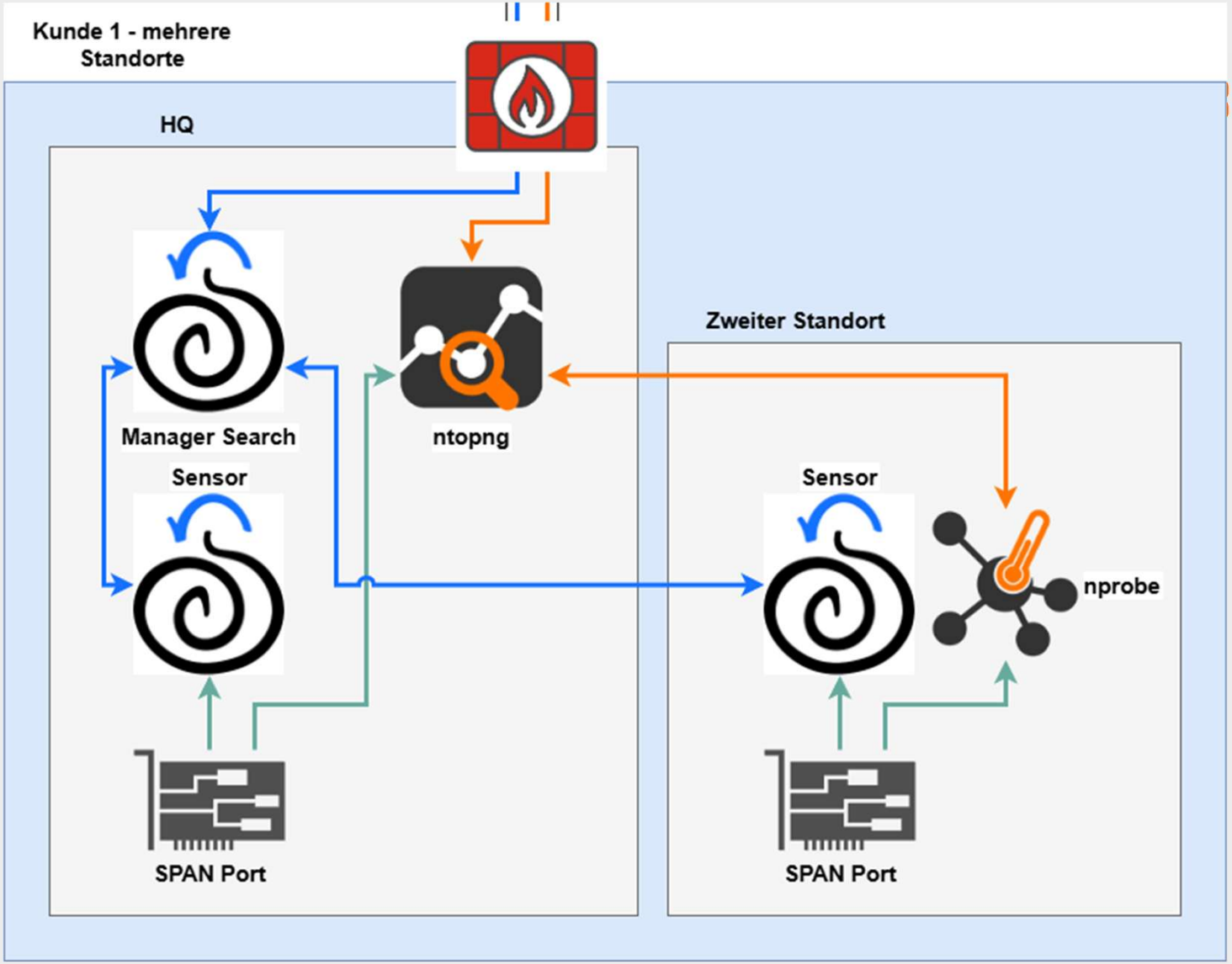


KOSTEN AM BEISPIEL EWN

first frame networkers

- Analyse von ~ 2000 GB Traffic pro Tag
- Ergibt ~ 50 GB Logs pro Tag
- Empfohlen >90 Tage Aufbewahrung
- Sentinel 90 Tage à 5 CHF / GB -> ~ 22’500 CHF

first frame networkers



VORTEILE

first frame networkers

- Echtzeit Ansicht vom eigenen Netzwerk
- Zusätzliche Sicherheits-Prüfungen neben Firewall
- Historische Auswertungen vom eigenen Netzwerk
- Von Alert bis zu Packet komplette Sichtbarkeit
- Lokale AI für Analysen möglich

DEMO

VORTEILE

first frame networkers

- Echtzeit Ansicht vom eigenen Netzwerk
- Zusätzliche Sicherheits-Prüfungen neben Firewall
- Historische Auswertungen vom eigenen Netzwerk
- Von Alert bis zu Packet komplette Sichtbarkeit
- Lokale AI für Analysen möglich

SERVICE - MANAGED PROTECTED NETWORK

first frame networkers

- Kritische Alerts gelangen aktiv zu uns -> wir greifen ein
- Wöchentliche Huntings und Bereinigungen von aktiven Alerts
- Diverse Erkennungsregeln von Community & FFN (>60k)
- Monatlicher Report
- Kunde kann so viel Daten speichern, wie er Platz hat -> keine Limitierung
- Empfohlen sind 90 Tage oder mehr

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 Security Operations Center
  - Verschiedene Blog-Artikel zum Thema IT-Security
  - www.firstframe.net

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 einen Bontique-Gutschein im Wert von CHF 75.—.
- Den Link finden Sie auch im Chat: https://forms.cloud.microsoft/e/M0mjuqFZwB

Herzlichen Dank

first frame networkers