# KUPPER
# IT-Impulse

KUPPER

IT. innovativ. effizient. sicher.

# VPN als Sicherheitsrisiko?

## WatchGuard FireCloud zeigt den Ausweg.

Kupper IT-Impulse | Webinar | 03. Juni 2026

KUPPER | WatchGuard™

IHR HEUTIGER REFERENT

# Thomas Runte

Senior Sales Engineer bei WatchGuard und technischer Partnerbetreuer der Kupper IT.

In dieser Rolle unterstützt er Partner und Kunden bei Proofs of Concept, technischen Fragen zu Security Designs sowie bei der Bewertung und Umsetzung passender IT-Sicherheitslösungen.

# VPN als Sicherheitsrisiko

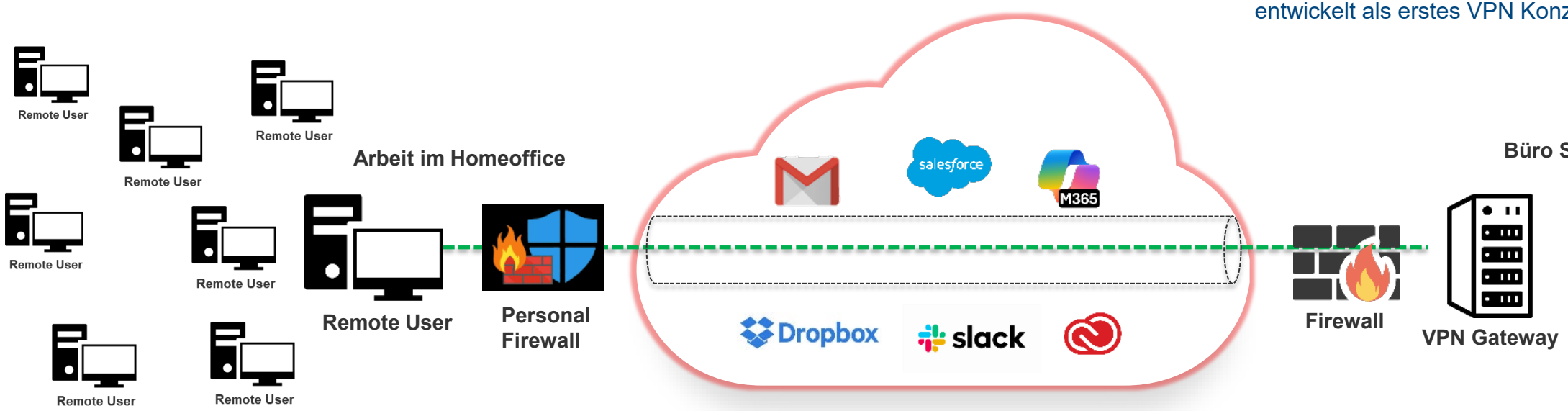
- VPN Rückblick
- Die VPN Falle
- Was bedeutet Zero Trust?
- Kritische Einsatz-Szenarien
- Der Übergang zu Zero Trust

# Managed Detection & Response (MDR)

- Überblick
- Erläuterung des Schutzniveaus
- Reaktionsgeschwindigkeiten
- Bi-direktionale Kommunikation
- Der Start mit MDR

# Rückblick: Remote User VPNs

1996 wurde von Microsoft Mitarbeitern das Peer-to-Peer Tunneling Protocol (PPTP) entwickelt als erstes VPN Konzept.




VPNs boten ausgewählten Mitarbeiter*innen einen “Tunnel” ins Unternehmens-Netzwerk.

Einfache Logik: Wer zugreifen darf, ist vertrauenswürdig.

Umfangreicher Zugriff auf
- Fileserver oder Dateien
- Datenbanken
- Interne Applikationen

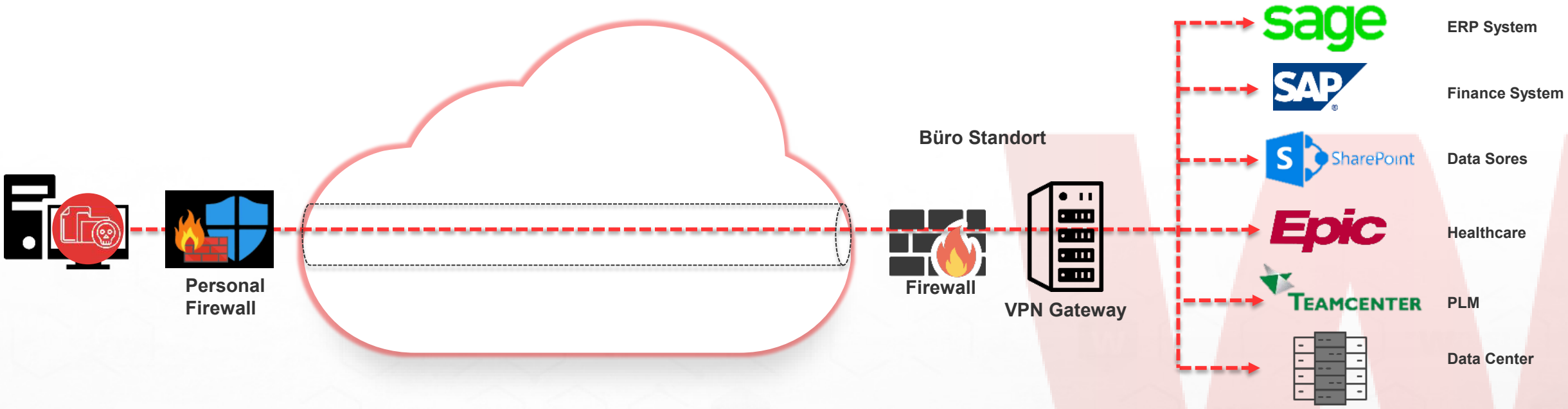
Heute: Hunderte Personen arbeiten außerhalb der Standorte, SaaS Anwendungen und Cloud-Infrastruktur werden intensiv genutzt und hybride Umgebungen sind die Normalität.

Die sichere Verbindung entwickelt sich hierbei zu einem **höheren Risiko**.

## Und so entsteht die Falle!

# Die VPN Falle: 5 Herausforderungen

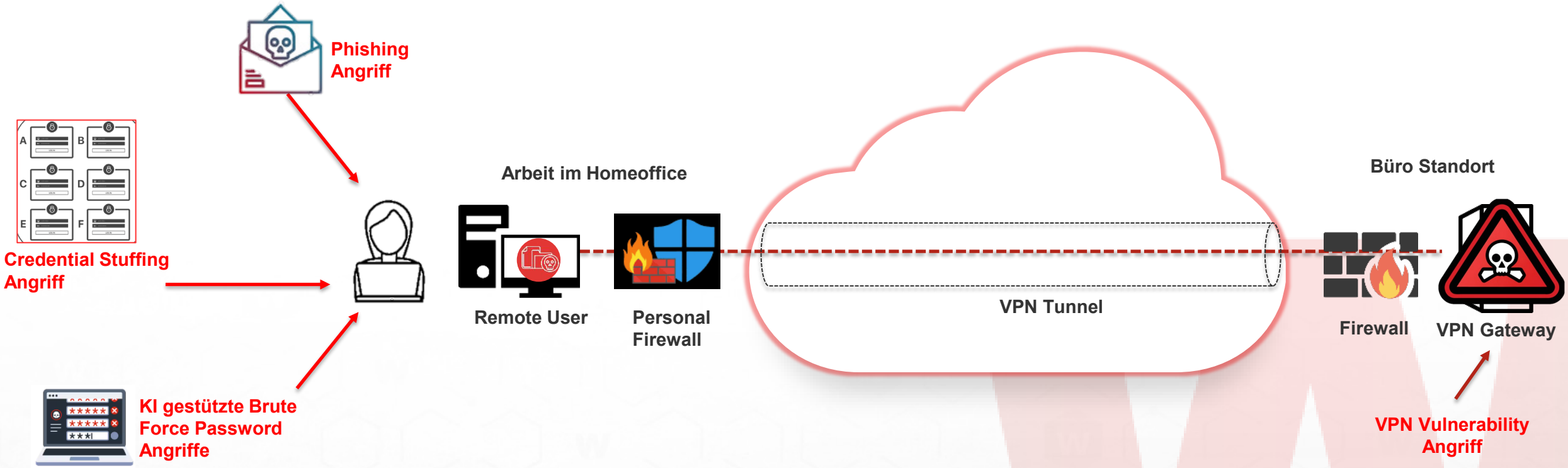
## 1. Uneingeschränkte Zugriffe auf Netzwerke




**Laterale Bewegung, zu leichter Zugriff bei Ransomware Angriffen und Datendiebstahl**

# Die VPN Falle: 5 Herausforderungen

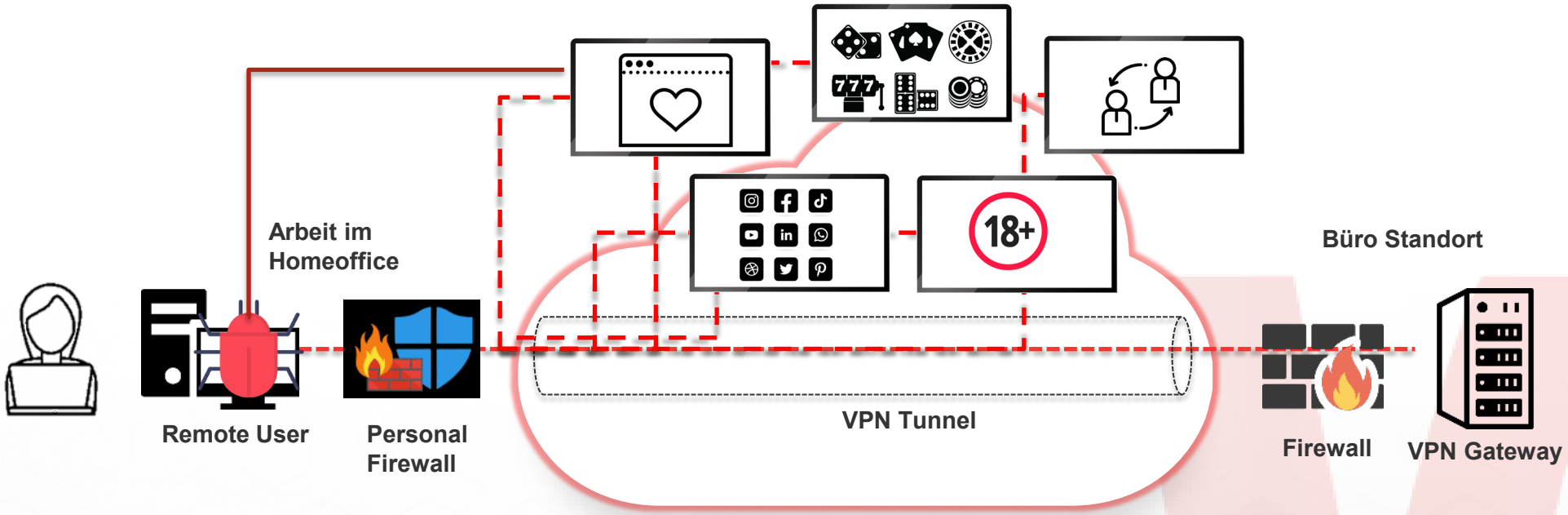
## 2. Identitäten als Risiko: Passwort + VPN = Angriffsmöglichkeit




**Kompromittierte Zugangsdaten → VPN Anmeldung → Zugriff → Ransomware Infektion**

# Die VPN Falle: 5 Herausforderungen

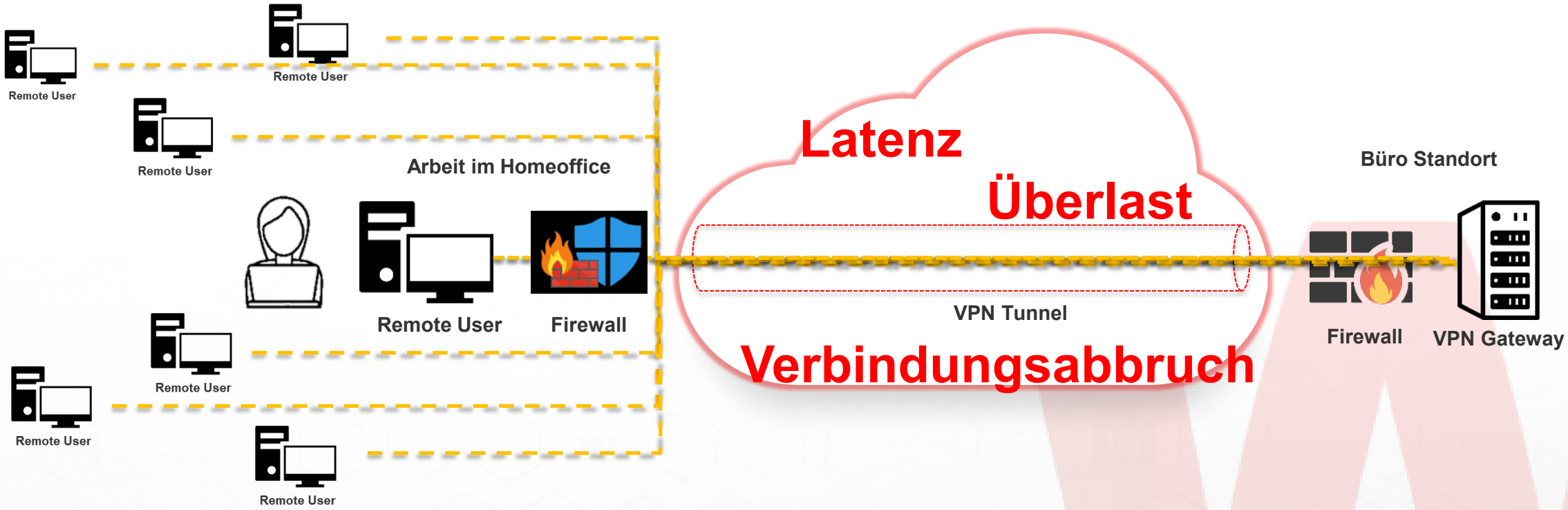
## 3. Im Blindflug – Gerätesicherheit bleibt unklar




**Verschlüsselte Kommunikation verbirgt Aktivitäten.**

# Die VPN Falle: 5 Herausforderungen

## 4. Geschwindigkeitseinbuße verringern Produktivität




**Optimierung der Produktivität führt oft zu höherem Risiko.**

# Die VPN Falle: 5 Herausforderungen

## 5. Ein teurer Verwaltungs-Albtraum

Average number of VPN-related support tickets per month

10

Average IT cost per ticket (USD)

100

Hours/month managing VPN tunnels / firewall rules

10

Average IT hourly cost (USD)

90

Average time lost per user/week due to VPN (minutes)

20

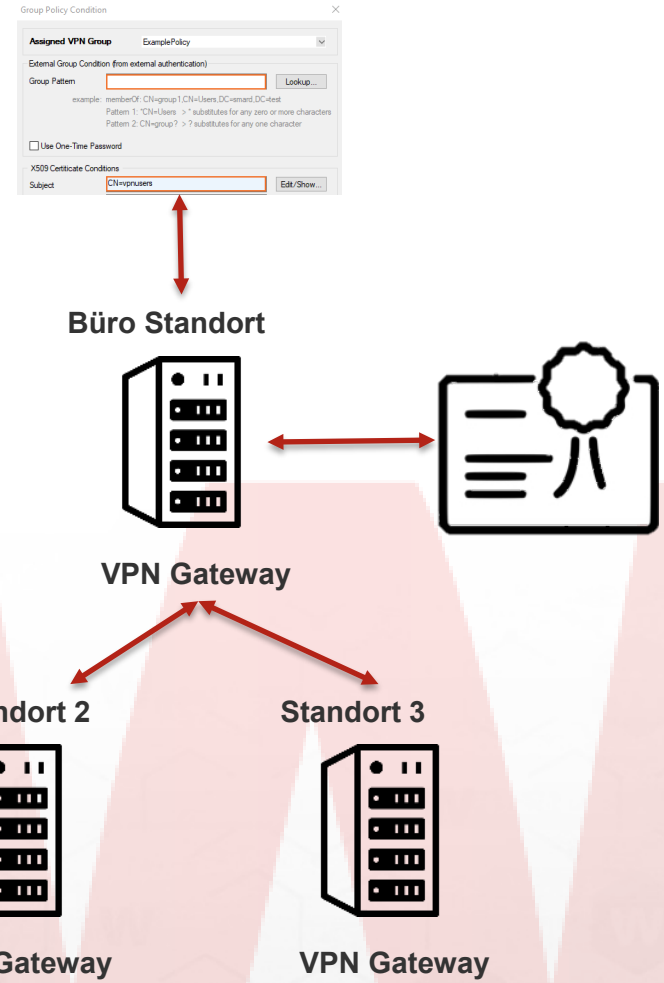
Number of remote users

150

Average employee hourly cost (USD)

30

| | |
|---|---|
| **Annual cost savings** | **$64,800** |
| Total VPN annual cost | $100,800 |
| FireCloud annual cost | $36,000 |
| Annual support cost | $12,000 |
| Annual management cost | $10,800 |
| Annual productivity loss | $78,000 |




**VPNs erzeugen versteckte Kosten bei zeitgleich steigendem Risiko.**

# Gefahrenlage: Die Falle schnappt zu

ThreatLabz: 56% der Organisationen waren 2024 von einem VPN Angriff betroffen

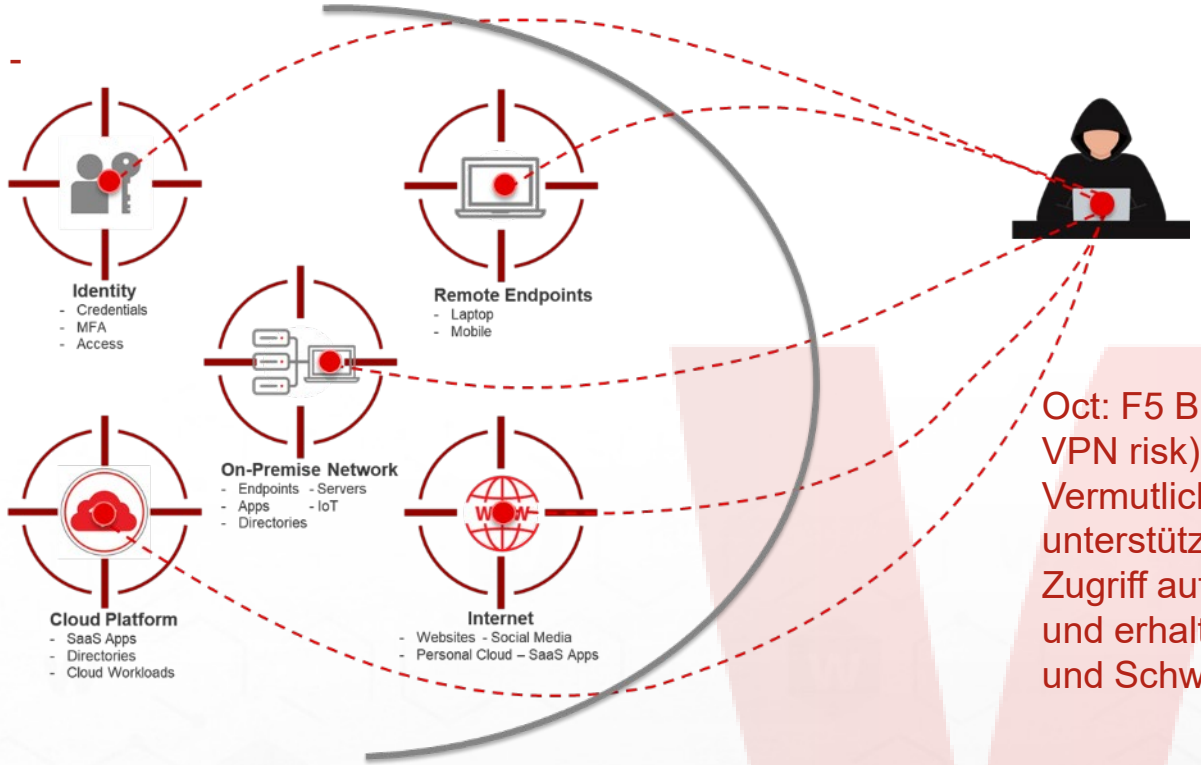
Jan: Ivanti Connect Secure / Policy Secure / ZTA
Zwei Schwachstellen gemeldet (CVE-2025-0282, -0283); eine davon wurde seit Dezember 2024 als Zero Day ausgenutzt.

Apr: Ivanti Connect Secure. ein kritischer Buffer Overflow (CVE-2025-22457) wird auf VPN Gateways ausgenutzt um nicht autorisierten Code auszuführen.

Apr: Fortinet FortiGate SSL-VPN. Angreifer verwenden bei vorheriger Ausnutzung von Schwachstellen/Bugs implementierte Tools für Angriffe. CISA gibt eine Warnung heraus.

Jul: SonicWall SMA 100 series (Remote Access VPN)
Ausnutzung des OVERSTEP Backdoors zur Kompromittierung und dem Diebstahl von Anmeldeinformationen und anderen Daten.

Sep: Cisco ASA/FTD (VPN Web Server)
Zwei Zero-Day Exploits (CVE-2025-20333, -20362) ermöglichen unautorisierten Zugang und werden intensiv ausgenutzt.




Oct: F5 Breach (BIG-IP / APM VPN risk)
Vermutlich durch eine Nation unterstützte Angreifer erlangen Zugriff auf interne Systeme bei F5 und erhalten Einsicht in Quellcode und Schwachstellen.

Oct: SonicWall SSL-VPN Account Kompromittierungen
Huntress identifiziert >100 VPN Accounts bei 16 Kunden, die von einer einzelnen IP bei einem Angriff am 4. Oktober genutzt werden.

# Grundlegende Technologien für das Zero Trust Prinzip

Integrieren von Identitäts-, Endgeräte- und Netzwerk-Sicherheit zur kontinuierlichen Überprüfung.

## Essentielle Technologien:

- **Identity Management:** Zentralisierung von Anmeldungen, MFA, SSO und Zugriffsrichtlinien.
- **Endpoint Security:** Kontinuierliche Überprüfung der Geräte-Sicherheit.
- **Remote User Network Security**: Visualisierung und Umsetzung von Richtlinien bei Verbindungen
  - Firewall as a Service
  - Secure Web Gateway
- **Zero Trust Network Access**: Stellt die sichere Nutzung von Applikationen und Daten sicher.

**Hybrid Network Security**

## Unterstützende Möglichkeiten:

- **Cloud Policy Automation & Orchestration:** Dynamische Richtlinienanwendung basierend auf Risiko und Verhalten.
- **Threat Detection & Response:** Aktivitäten werden über verschiedene Ebenen korreliert und schnelle Eindämmungs-Möglichkeiten stehen zur Verfügung.
- **Cloud Access Security Broker:** Ermöglicht eine sichere und den Richtlinien entsprechende Nutzung von Cloud-Applikationen.

# Zero Trust Architektur

**Connection Manager**: Ein schlanker Agent, der

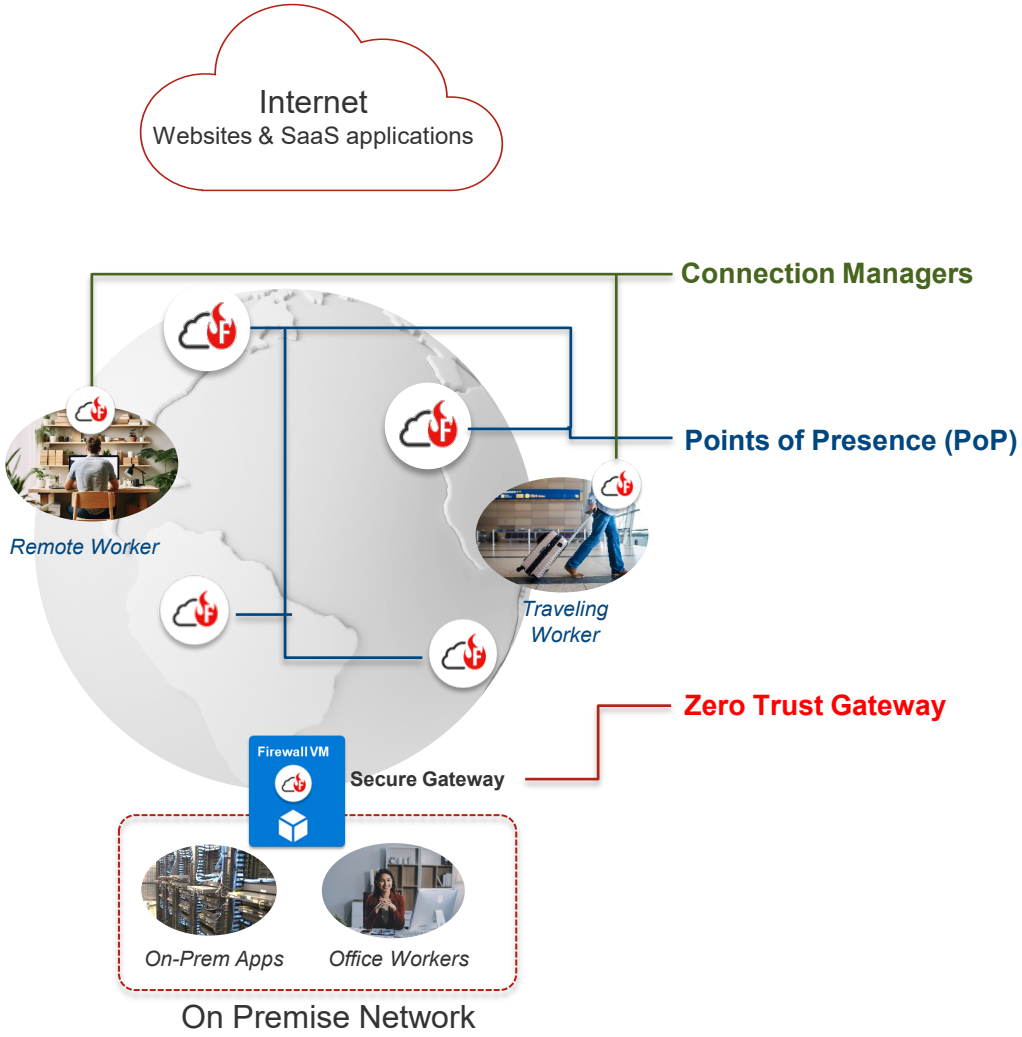
- die Authentifizierung verwaltet,
- den Datenverkehr an PoPs weiterleitet,
- Richtlinien gemeinsam nutzt und die Kommunikation sichert.

**Point of Presence (PoP) Infrastruktur**:
Ein globales Netzwerk von Cloud-basierten Durchsetzungspunkten, die

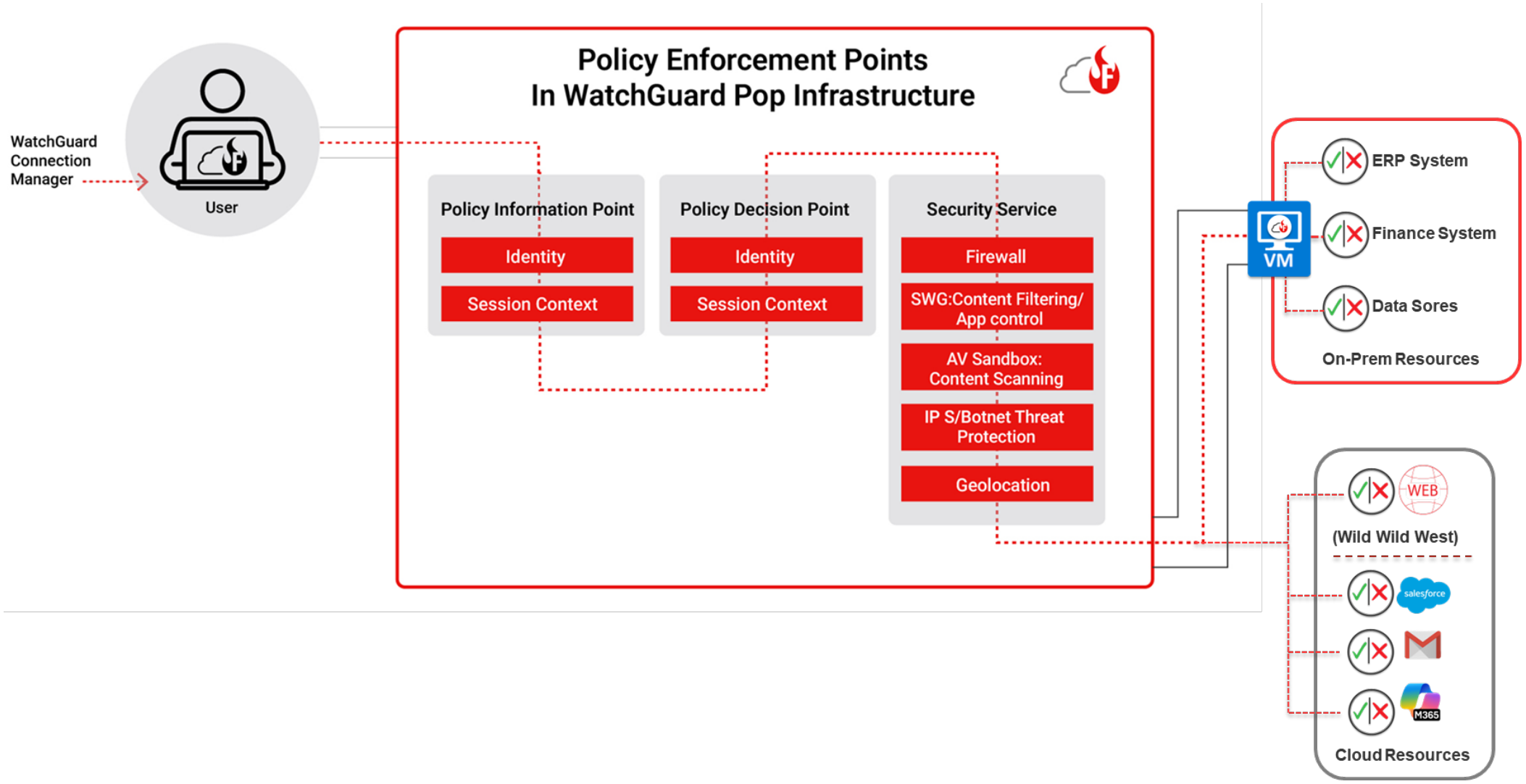
- verschlüsseln, optimieren und Verbindungen kontrollieren
- als Durchsetzungspunkte für Richtlinien und Zero Trust fungieren
- die Leistung optimieren und für Skalierbarkeit und Redundanz sorgen.

**Zero Trust Gateways**: Eine virtuelle Appliance, die bereitgestellt wird, und

- sichere, verschlüsselte Verbindungen zwischen FireCloud-PoPs und privaten Anwendungen bereitstellt.
- Zero Trust Network Access (ZTNA) für lokale Anwendungen ohne offene Ports ermöglicht.
- identitätsbasierte Richtlinien für Benutzerzugriffe durchsetzt.



# FireCloud Total Access



[Live Demo]

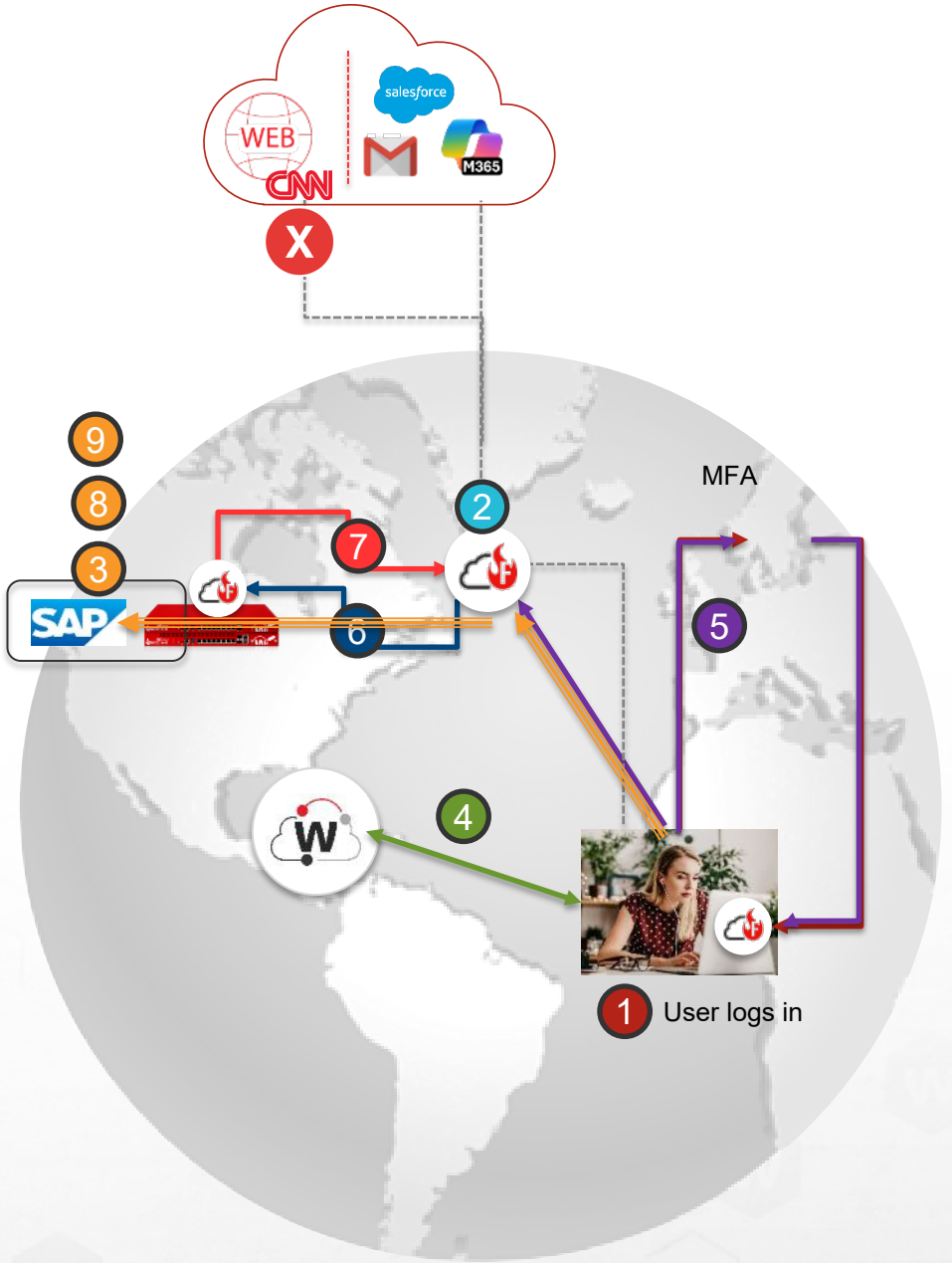
# Neugierig geworden?

**Fragen Sie doch einfach gleich ein unverbindliches Beratungsgespräch inkl. FireCloud Live Demo an**

# Zero Trust Prozess

1. Benutzer*in authentifiziert sich per MFA am Gerät. EDR, Identitäts- und hybride Netzwerk-Sicherheitsrichtlinien werden umgesetzt.
2. Öffnen von Nachrichtenseiten, Abrufen von E-Mails - PoP nutzt FWaaS und SWG zur sicheren Verbindung
3. Zugriffsversuch auf Anwendung im eigenen Rechenzentrum (on-premise)
4. ZTNA überprüft über Cloud-Infrastruktur die Identität, Gruppe und anzuwendenden Richtlinien.
5. ZTNA validiert Zugangsdaten und Parameter.
   - ZTNA validiert das Geräte-Risiko und blockiert ggf. den Zugriff.
   - ZTNA übermittelt die Information an PoP.
6. Der PoP setzt die gesammelten Sicherheitsrichtlinien um
   - Informationen über Zugriffsrechte werden an das Gateway gesendet.
   - Kontrolle des Internet-Zugriffs bei aktiver Verbindung zur internen Applikation.
   - Weiterleitung der Verbindung vom PoP zum Gateway und in das on-prem Rechenzentrum.
7. Überprüfung der Zugriffsberechtigung (Benutzer*in, Standort, etc.) durch das Gateway und den PoP.
8. Die sichere Verbindung wird nach Validierung ermöglicht
9. Der Zugriff auf die interne Anwendung ist möglich.

   Wird im Zuge der laufenden Verbindung ein Risiko erkannt, kann jederzeit die Verbindung geschlossen werden und weitere Maßnahmen zur Eindämmung können erfolgen.




**Remote Worker Accessing on-premise Application**

# Kritische Einsatz-Szenarien – Remote Work und Hybrid Work

*Remote Work*
*Zugriffe auf öffentliche Dienste*

Verbindung zu:
- Öffentliche Wi-Fi Netze
- Unsichere Netzwerke im Homeoffice
- Jegliche Webseiten im Internet
- Private Cloud Applikationen
- Cloud Applikationen der Firma (M365, Salesforce, Google)

Risiken
- Kompromittierung der Zugangsdaten
- Kompromittierung der Geräte
- Daten-Diebstahl

**Identity Management (MFA)**

**Endpoint Security (EDR)**

**Hybrid Network Security**
- **FWaaS**
- **SWG**

*Remote Work*
*Zugriff auf private Dienste*

Verbindung zu:
- Dienste und Daten des Unternehmens
- Applikationen und Daten im Rechenzentrum (on-premise)

Risiken
- Kompromittierung der Zugangsdaten
- VPN-Schwachstellen
- Brute Force Angriffe
- Dienste und Daten im Internet erreichbar
- Gefahr lateraler Bewegung

**Identity Management (MFA)**

**Endpoint Security (EDR)**

**Hybrid Network Security**
- **FWaaS**
- **SWG**

**Zero Trust Network Access (ZTNA)**

# Kritische Einsatz-Szenarien: Compliance

| Framework | Control / Article | What It Requires | How FireCloud Total Access Helps |
|---|---|---|---|
| **HIPAA (164.312 – Technical Safeguards)** | Access Control, Audit Controls, Integrity Controls | Limit access to PHI, log all activity, and protect against improper alteration. | FireCloud enforces identity-based, per-user/per-app Zero Trust access, generates centralized audit logs, and blocks unapproved traffic at the PoP. |
| **PCI DSS 4.0 (Req. 7, 8, 10)** | Restrict access to cardholder data; identify/authenticate users; log activity | Least-privilege access, MFA, and per-user accountability. | FireCloud integrates with AuthPoint MFA/SAML, enforces least-privilege access to only required apps, and provides user-level logging of all remote access sessions. |
| **GDPR (Articles 25, 32)** | Data Protection by Design; Security of Processing | Ensure access is limited, encrypted, and logged with appropriate safeguards. | FireCloud delivers identity-based access controls, TLS-encrypted tunnels, contextual policies (location, device, time), and full reporting for audits. |
| **NIS2 Directive (EU Critical Infrastructure)** | Article 21 – Cybersecurity Risk Management Measures | Mandates measures like access control, authentication, encryption, monitoring, and incident response. | FireCloud provides Zero Trust access enforcement, no exposed VPN ports, encrypted traffic via WatchGuard PoPs, and continuous monitoring through Cloud reports. |
| **SOX (Section 404 IT Controls)** | Internal Controls for Financial Systems | Demonstrate user accountability and protect financial data. | FireCloud ensures only authenticated users can access finance/ERP apps, logs per-user access, and enforces role-based restrictions. |
| **ISO/IEC 27001:2022 (Annex A 5.15, 5.18, 8.16, 8.20)** | Access Control, Identity Management, Secure Authentication, Monitoring Activities | Strong authentication, restricted access, monitoring and review. | FireCloud enforces authentication, identity-based app-level access, continuous monitoring, and centralized reporting via WatchGuard Cloud. |
| **CMMC 2.0 (AC.1.003, AC.2.007, AU.2.041)** | Limit access to authorized users; enforce MFA; log system use | Access must be controlled, logged, and limited to “need-to-know.” | FireCloud provides Zero Trust per-app access, integrated MFA, and audit-ready logs to support CMMC compliance. |
| **Cyber Insurance Underwriting** | Control Requirements (MFA, Zero Trust, VPN replacement) | Many policies now require MFA, Zero Trust, and proof of VPN phase-out. | FireCloud replaces VPNs with Zero Trust access, integrates MFA, and provides reporting that insurers accept as proof of controls. |

# Der Übergang zu Zero Trust

## Risiko identifizieren

Wo werden VPNs genutzt?
Welche Personen / Geräte?
Welche Anwendungen?

Aufzeigen der externen Erreichbarkeit – RDP, SSH, private SaaS Dienste, etc. Kalkulation der Kosten.

## Schutz der Remote Mitarbeitenden

Bereitstellung des Schutzes durch FWaaS und SWG für Remote Mitarbeitende.

Visualisierung und Kontrollmöglichkeiten

## MFA und Geräte-Sicherheit

Bereitstellung von MFA

Sicherstellen, dass eine EDR Lösung alle Geräte schützt.

Verwendung einer Lösung zur einheitlichen Nutzung von Zero Trust Richtlinien

## Zugriffe für Applikationen gesichert bereitstellen

Fokus auf kritische interne Applikationen (HR, Finanzen, Dev Tools)

Verwendung von Cloud-basierten Zero Trust Network Access Lösungen zur Ablöse von VPNs

## Session Level Monitoring & Korrelation

Nutzungs- und Zugriffs-Daten fließen in eine umfassende Erkennungs-Plattform ein.

Korrelation von Identitäten, Geräte und Netzwerk-Telemetrie um selbst verborgene Angriffe aufzudecken.

# Zusammenfassung

## Einschränkungen traditioneller VPNs

VPNs stützen sich auf eine betagte Architektur und implizites Vertrauen. Großes Risiko durch gestohlene Anmeldeinformationen und Herausforderungen bei Netzwerk-Segmentierung.

## Moderne Sicherheits Prinzipien

Überprüfung der Identitäten, des Geräte-Zustands, Anwendung des Prinzips der geringsten Zugriffsrechte und kontinuierliche Überwachung sind erforderlich für eine robuste, moderne Sicherheits-Strategie.


## Übergang zu Zero Trust

Vermeidung von VPNs reduziert Risiken und unterstützt die digitale Transformation. Hierbei wird die Notwendigkeit einer schnellen Entwicklung zu Zero Trust deutlich.

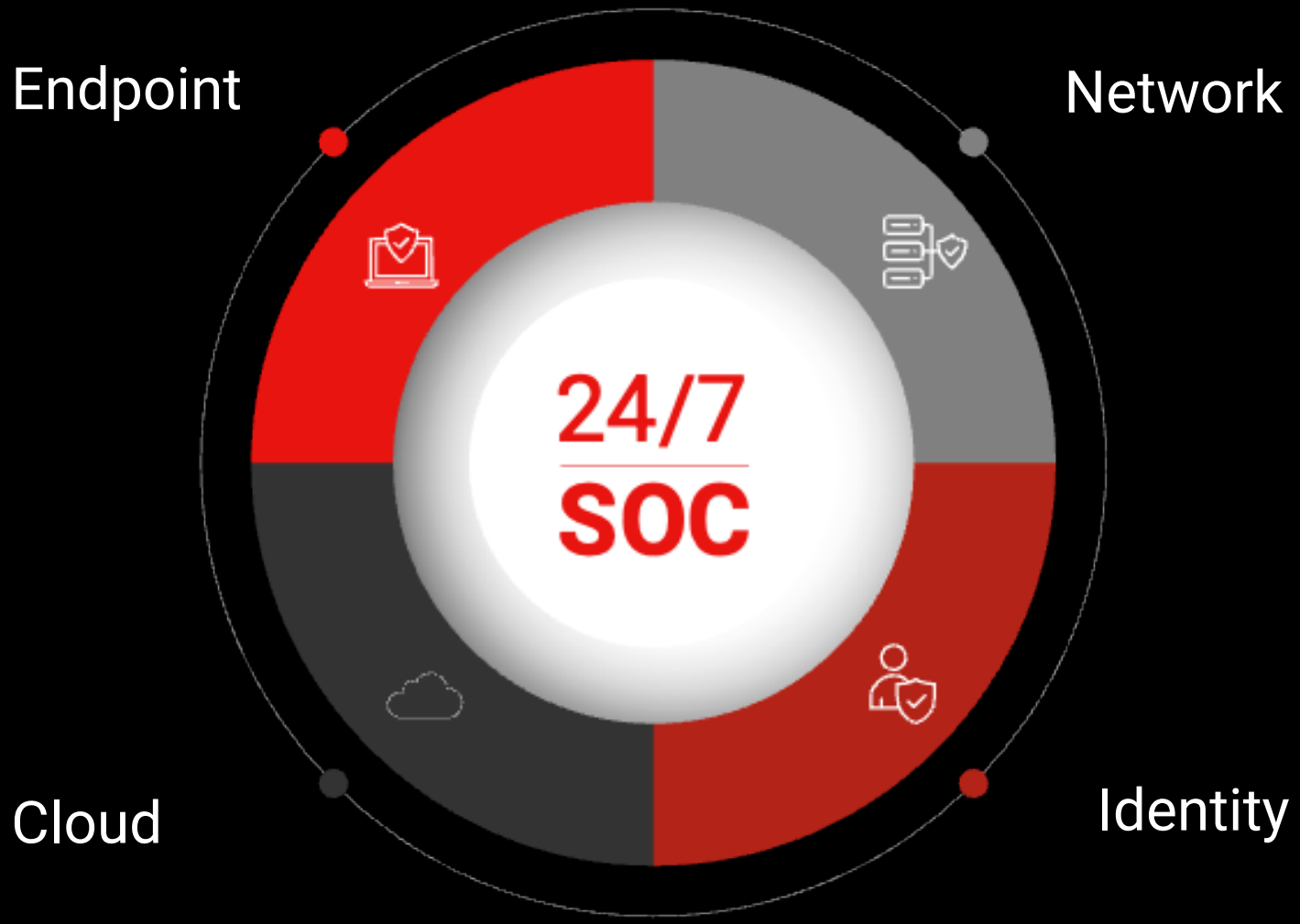
# Managed Detection & Response

**Monitoren und reagieren Sie aktiv darauf und zwar weit über Ihre Endgeräte hinaus!**

# MDR ein Gamechanger

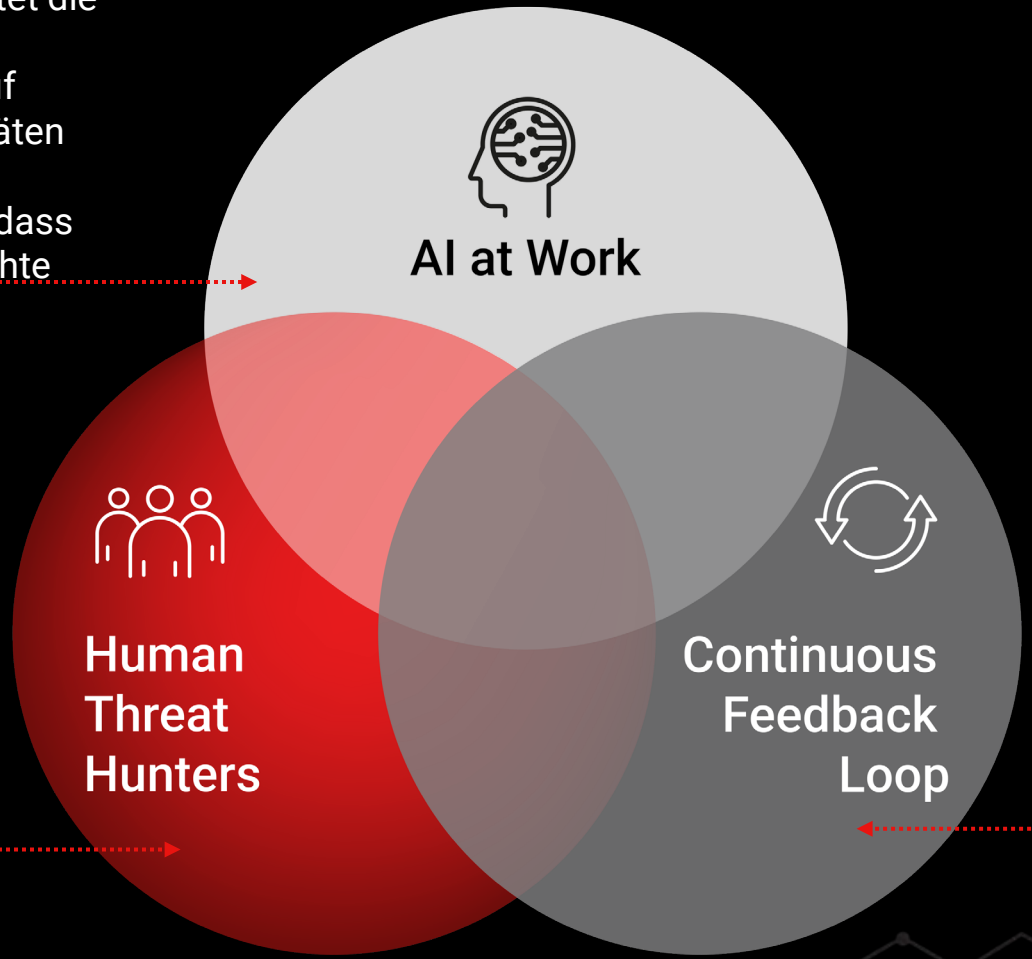
## Von Tools zu 24/7 Schutz

- Kombiniert Endpunkt-, Netzwerk-, Identitäts- und Cloud-Schutz in einem einzigen Service.
- Bietet rund um die Uhr kontinuierliche Erkennung und Reaktionen in Echtzeit.
- Unterstützt durch KI, Automatisierung und ein Team aus erfahrenen Analysten.



# KI + Menschen: Wie das SOC zusammenarbeitet

- Filtert Störsignale heraus und bewertet die Wahrscheinlichkeit einer Bedrohung
- Erkennt Verhaltensabweichungen auf Endgeräten, im Netzwerk, bei Identitäten und in der Cloud
- Automatisiert die Klassifizierung, sodass sich Analysten ausschließlich auf echte Bedrohungen konzentrieren können




- Untersuchen. Überprüfen. Eindämmen.
- Ergreifen Sie Sofortmaßnahmen – Endgeräte isolieren, IP-Adressen sperren, Konten deaktivieren.
- Ergänzung der KI-Entscheidungen durch menschliche Einschätzungen.

- Die Ergebnisse der Analysten dienen dazu, die KI für eine intelligentere Erkennung zu trainieren.
- TAMs teilen Erkenntnisse und Trends mit den Partnern.
- Die Partner passen ihre Abwehrmaßnahmen anhand der SOC-Empfehlungen an.

# Wie schnell können wir unsere Kunden schützen?

## 1 Warnung erhalten & Case eröffnen

Der Analyst prüft die Warnmeldung, stellt fest, dass es sich nicht um einen Fehlalarm handelt, und weist ihr eine Priorität zu. Er legt einen Vorfallseintrag im Fallmanagementsystem an und dokumentiert die ersten Details.

## 2 Kontextsuche

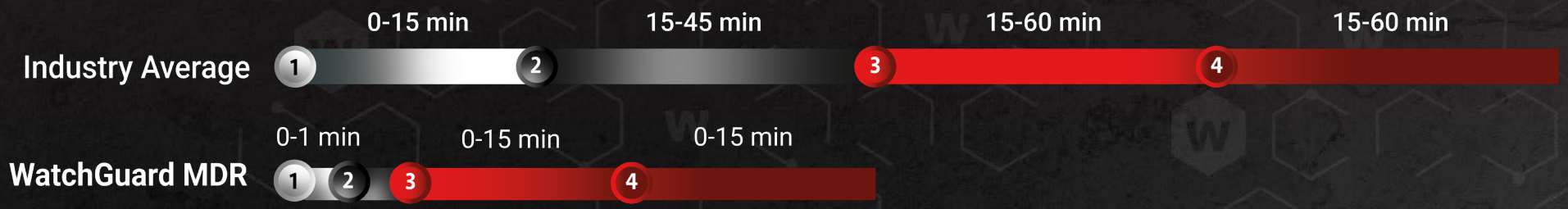
Abfrage von SIEM-, EDR-, Firewall- und Bedrohungsdaten zu entsprechenden Ereignissen, Ressourcen und Benutzern.

## 3 Untersuchen

Analysieren Sie Protokolle, Endpunkte und Netzwerkdaten eingehend, um den Umfang und die Schwere des Vorfalls zu ermitteln.

## 4 Bedrohung eindämmen

Endpunkte isolieren, bösartige Konten oder Datenverkehr blockieren, vorübergehende Maßnahmen ergreifen.



# Geschwindigkeit und Präzision

## Präzision

- Unwichtige Nachrichten werden herausgefiltert, bevor sie in Ihrem Posteingang landen.
- Die Analysten konzentrieren sich ausschließlich auf bestätigte Bedrohungen.


## Geschwindigkeit

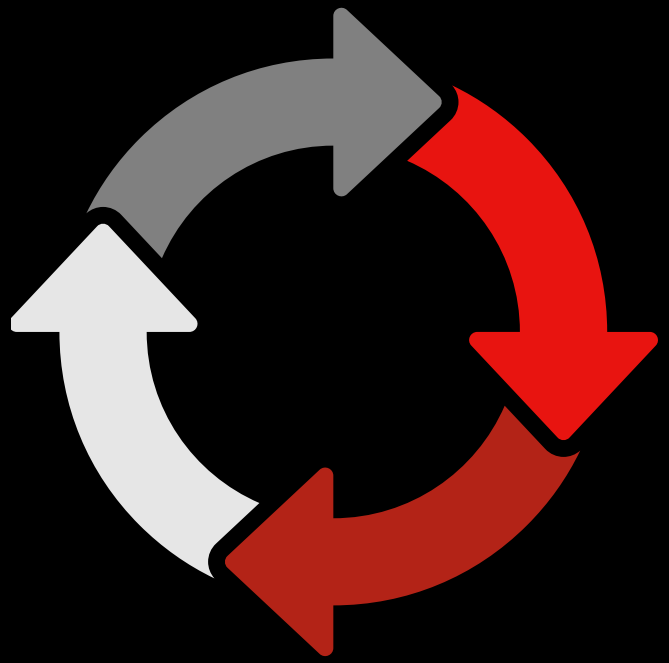
- Erkennung → Reaktion → Behebung: <6 Minuten bei kritischen Bedrohungen
- Phishing-Versuch gestoppt, bevor Anmeldedaten wiederverwendet wurden.
- Verdächtige Anmeldung erkannt, Konto automatisch gesperrt.

**90%** Auto-blocked

**<1** false positive pro Monat

# Wie unser Team mit Ihnen kommuniziert

## Erkennung und Reaktion
Kontinuierliche Überwachung 24/7.



## Benachrichtigungen
Alle Erkennungen und Reaktionen werden in Echtzeit im MDR-Portal protokolliert. Das SOC benachrichtigt Sie umgehend bei kritischen Warnmeldungen.
Es werden wöchentliche und monatliche Berichte versendet.

## TAM Review
Interprets SOC findings, explains what happened, and recommends next steps.

## Rückmeldung an das SOC
Die TAMs leiten ihre Empfehlungen an das SOC weiter, um eine kontinuierliche Verbesserung zu gewährleisten.

# Wie unser Team mit Ihnen kommuniziert

## Wann Sie von uns hören werden:

**Sofort:** Kritische oder bestätigte Bedrohung, die Maßnahmen seitens des Partners/Kunden erfordert.

**Täglich / wöchentlich:** Zusammenfassung der Erkennungen und ergriffenen Maßnahmen (über das Portal und per E-Mail).

**Monatlich / vierteljährlich:** Trend- und Sicherheitsstatus-Überprüfungen mit Ihrem TAM.

## So erreichen Sie das SOC

**MDR-Portal:** Tickets eröffnen oder einsehen, Erkennungen anzeigen, Nachverfolgung anfordern.

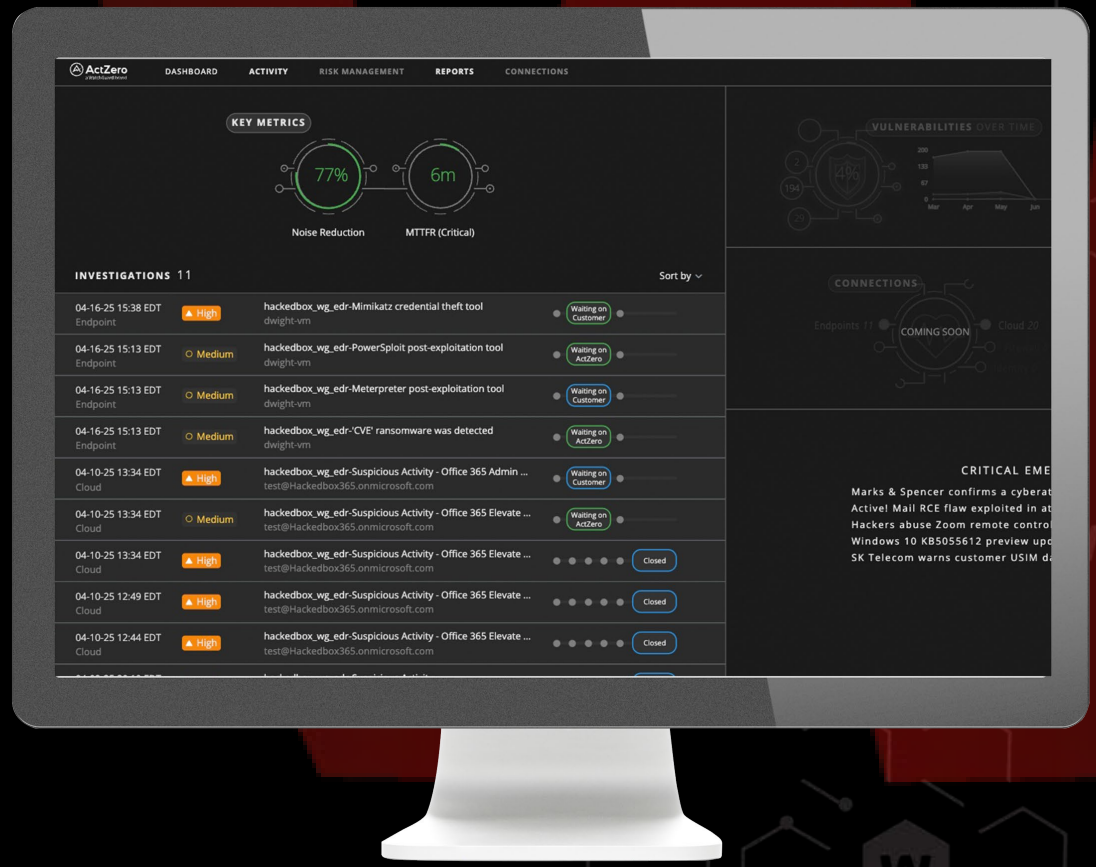
**E-Mail-Benachrichtigungen:** Direkte Eskalation bei kritischen Vorfällen.

**TAM-Support:** Ihr persönlicher Ansprechpartner für eingehendere Untersuchungen, Beratung und Serviceüberprüfungen.

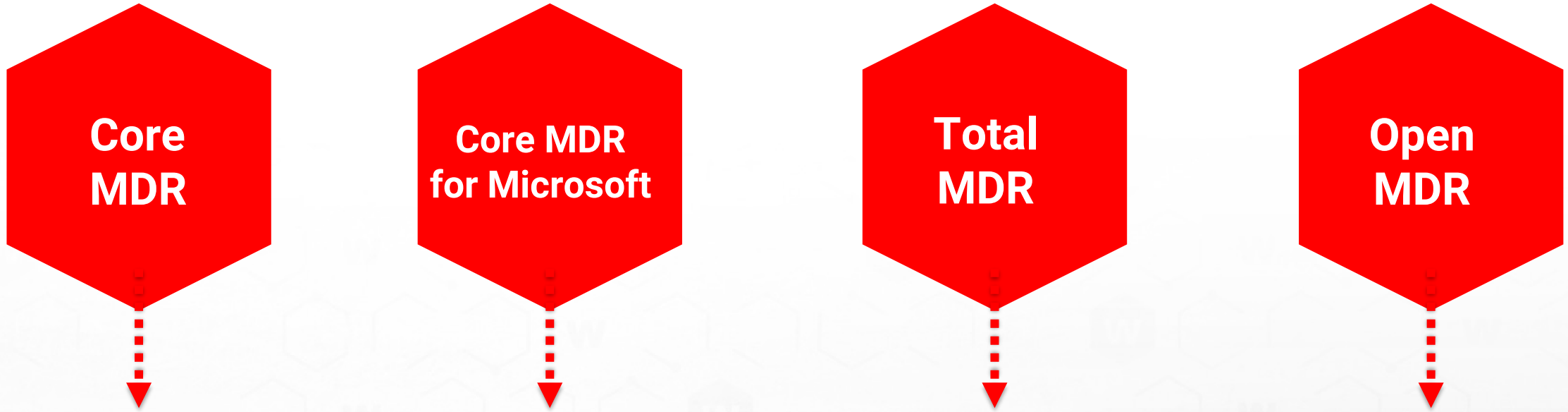
Real Security for the Real World

# Wie viel Sichtbarkeit erhalten Sie?

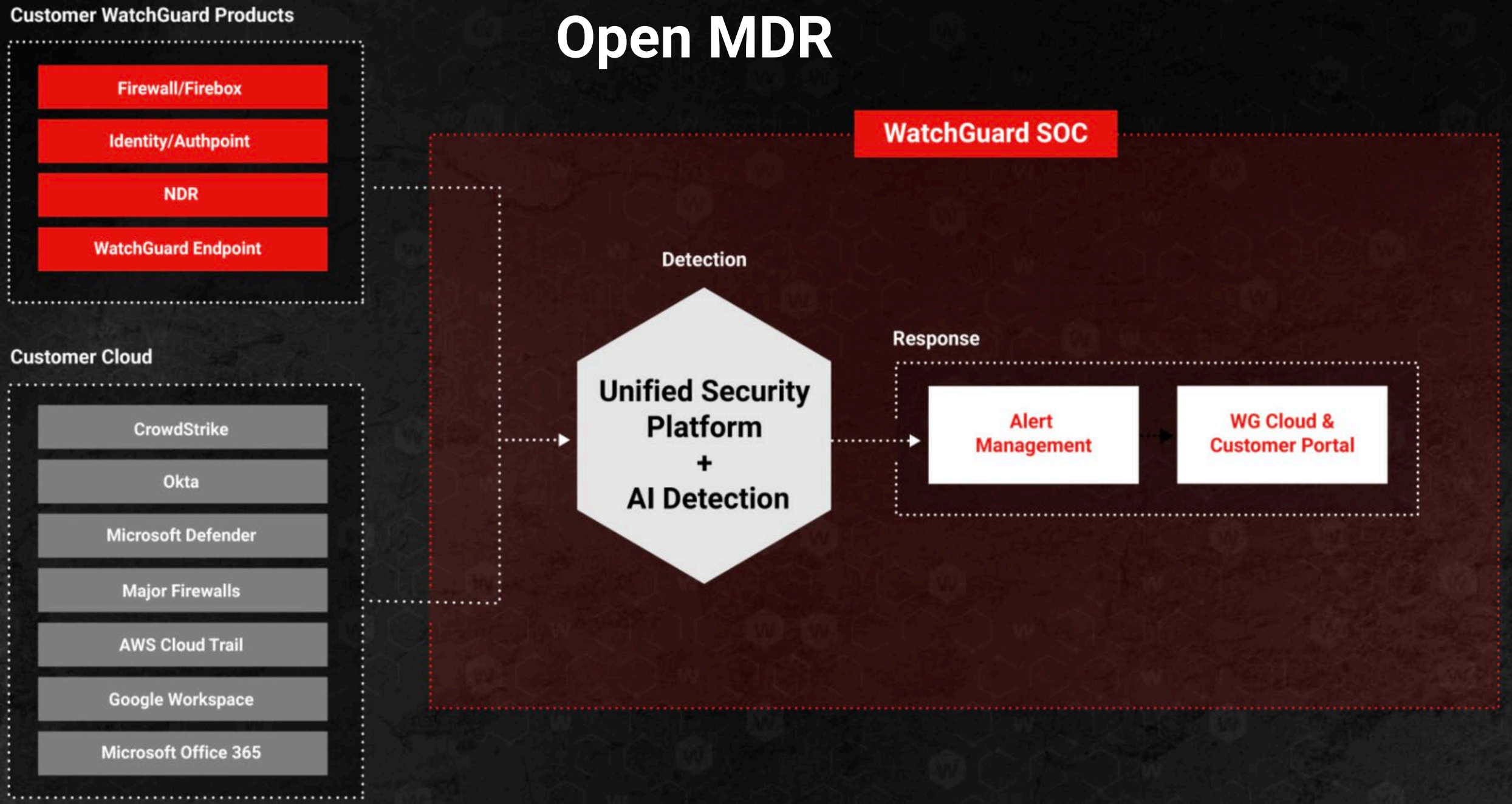
- Durchschnittliche Zeit bis zur ersten Reaktion auf kritische Warnmeldungen
- Rauschunterdrückung
- Untersuchungen
- Vom SOC ergriffene Maßnahmen
- Erkennungen



# MDR Service Levels

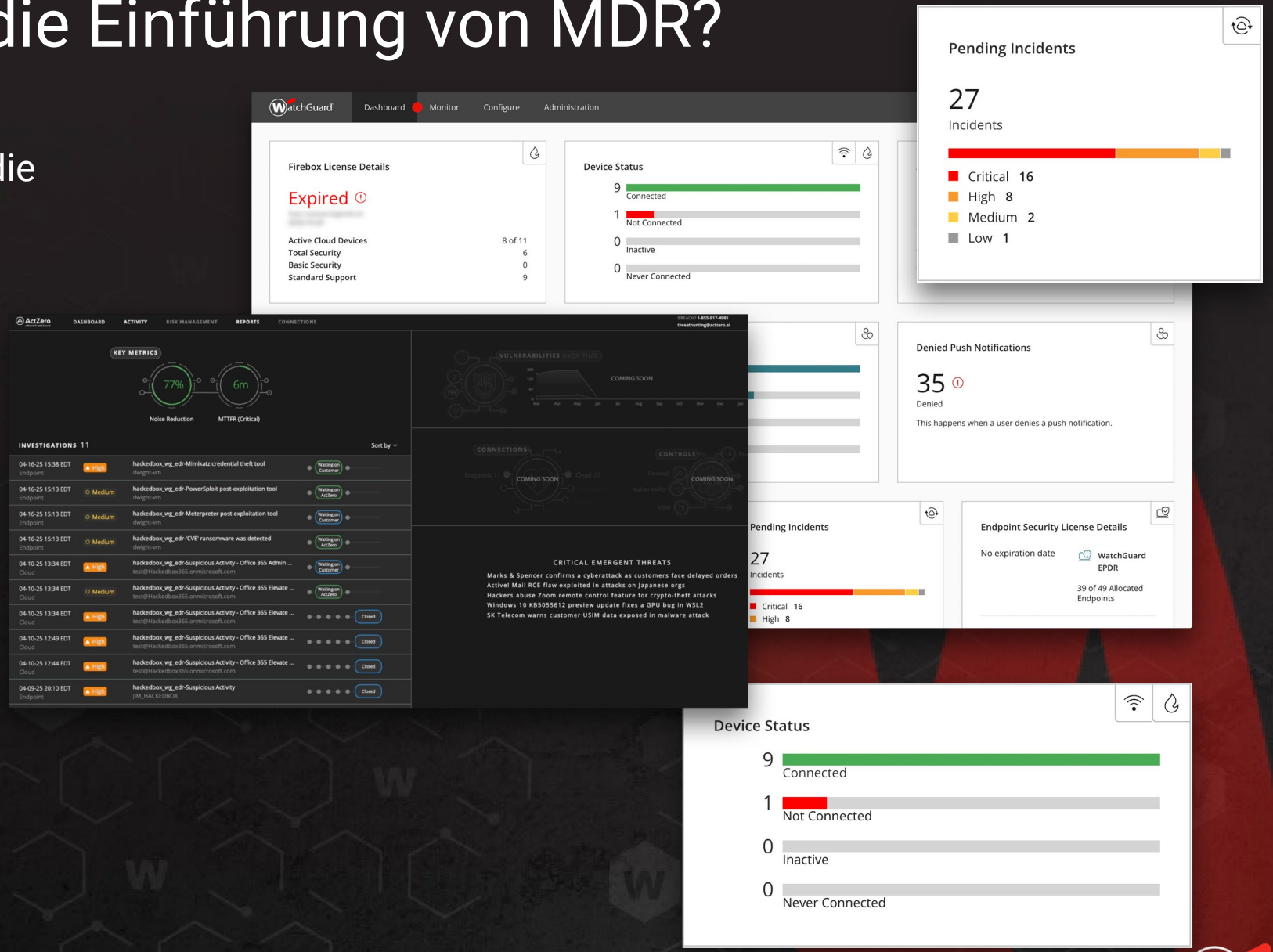


# Open MDR


Customer WatchGuard Products
Firewall/Firebox
Identity/Authpoint
NDR
WatchGuard Endpoint
Customer Cloud
CrowdStrike
Okta
Microsoft Defender
Major Firewalls
AWS Cloud Trail
Google Workspace
Microsoft Office 365
WatchGuard SOC
Detection
Unified Security Platform + AI Detection
Response
Alert Management
WG Cloud & Customer Portal

# Wie einfach ist die Einführung von MDR?

1. Verbinden Sie sich über die **WatchGuard Cloud**
2. MDR Lizenz aktivieren
3. “Spielregeln” definieren
4. Schutz start in Stunden



# Vielen Dank!


WatchGuard

**Real Security**
for the **Real World**

# Fragen und Antworten

Frage:

**Wie sieht das denn aus beim Aufbrechen von https bei https strikt und zum Beispiel bei Bankseiten aus?**

Antwort:

Einige Anwendungen und Webseiten nutzen Sicherheitsmechanismen wie HSTS, Certificate Pinning oder clientseitige Zertifikate (z. B. im Bankenumfeld), um Manipulationen an der TLS/HTTPS-Verbindung zu erkennen. In diesen Fällen kann der HTTPS-Datenverkehr nicht durch das FireCloud HTTPS-Scanning entschlüsselt werden. Solche Ziele können daher gezielt vom HTTPS-Scanning ausgenommen werden. Die Freigabe erfolgt flexibel über einzelne IP-Adressen, Netzbereiche oder komplette Domänen – ähnlich wie bei klassischen Firewall-Ausnahmen.

# Fragen und Antworten

Frage:

**Sollte ein regionaler PoP ausgelastet sein, wird dann automatisch über einen entfernten PoP geroutet?**

Antwort:

Fällt ein regionaler PoP aufgrund einer Störung oder eines Ausfalls der zugrunde liegenden Infrastruktur aus, wird der Datenverkehr automatisch über den nächstgelegenen verfügbaren PoP geleitet. Eine Umleitung aufgrund von Auslastung ist hingegen nicht vorgesehen, da die PoPs mit einer Scale-Out-Architektur arbeiten. Dabei werden Ressourcen dynamisch entsprechend dem aktuellen Bedarf bereitgestellt. Dadurch soll sichergestellt werden, dass ein PoP nicht an seine Kapazitätsgrenzen stößt und die Performance jederzeit gewährleistet bleibt.

# Fragen und Antworten

Frage:

**Wird die FireCloud-Verbindung auch verwendet, wenn ich mich bereits im Firmennetzwerk befinde?**

Antwort:

Aktuell versucht der FireCloud Connection Manager standardmäßig auch dann eine Verbindung zur FireCloud aufzubauen, wenn sich das Endgerät bereits im Unternehmensnetzwerk befindet. Soll dies verhindert werden, kann dies derzeit über entsprechende Firewall-Regeln im Firmennetz umgesetzt werden.Für die Zukunft ist jedoch eine Funktion zur Erkennung sogenannter Safe Locations bzw. Safe Networks geplant. Damit kann definiert werden, dass innerhalb vertrauenswürdiger Netzwerke – beispielsweise im Unternehmensnetz – keine FireCloud-Verbindung aufgebaut wird. Die Funktion befindet sich bereits auf der Produkt-Roadmap und wird zukünftig zur Verfügung stehen.

# Ihr Feedback ist uns wichtig!

IHR IT-VERSORGUNGSUNTERNEHMEN

# Wir sind für Sie da.

Mit über 100 Experten an 5 Standorten
in Mitteldeutschland.

**Leipzig** | Berlin | Chemnitz | Dresden | Görlitz


+ 49 341 30536-0

vertrieb@kupper-it.com

Prager Str. 15, 04103 Leipzig