Herzlich willkommen zum Admin-Frühstück

Schwachstelle VPN:

Die aktuelle Bedrohungslage im Fokus

Die VPN Falle: Warum klassischer Remote Access heute versagt

Thomas Runte
Senior Sales Engineer

Die VPN Falle: Warum klassischer Remote Access heute versagt

- Allgemein Übersicht der Bedrohungslage
- VPN Rückblick
- Die VPN Falle
- Was bedeutet Zero Trust?
- Kritische Einsatz-Szenarien
- Der Übergang zu Zero Trust
- Zusammenfassung
- Frage & Antwort

Allgemeine Übersicht der Bedrohungslage

Cyberangriffe der letzten Tage

Hackerangriff auf Romina Mineralbrunnen

News
4. Feb. 2026 • 1 Minuten

Ein Cyberangriff hat den Mineralwasser-Abfüller Romina lahmgelegt. Das Unternehmen ist aktuell nicht erreichbar.

Der Getränke-Abfüller Romina mit Sitz in Reutlingen-Rommelsbach wurde kürzlich von einer Cyberattacke getroffen. Wie das Unternehmen auf seiner **Website** erklärt, sei man deshalb weder telefonisch noch per E-Mail erreichbar. Laut einem Bericht des **Reutlinger General-Anzeiger** steht auch die Produktion aktuell still.

Weitere Details zu dem Vorfall gibt es bisher nicht. Daher ist unklar, wie der Angriff genau abgelaufen ist. Ebenfalls ist nicht bekannt, ob Daten gestohlen wurden. Der Regionalzeitung **Südwest Presse** zufolge ermittelt die Polizei Reutlingen bereits in dem Fall.

Romina Mineralbrunnen beschäftigt nach eigenen Angaben 130 Mitarbeiterinnen und Mitarbeiter. 2024 hatte das Unternehmen 180,7 Millionen Füllungen verzeichnet und einen Umsatz von mehr als 40 Millionen Euro erwirtschaftet.

Quelle:
https://www.csoonline.com/article/4127094/hackerangriff-auf-romina-mineralbrunnen.html

Cyberangriffe der letzten Tage

AOK-Datenpanne: 6.400 elektronische Patientenakten gesperrt

Seit vergangenem Jahr ist die elektronische Patientenakte Standard. Gegen ihre Verwendung kann man Einspruch einlegen. Mit solchen Widersprüchen ist bei der AOK Bayern jetzt etwas schief gegangen. Tausende Patientenakten sind plötzlich gesperrt.

Von BR24 BR24 Redaktion

Über dieses Thema berichtet: BR24 am 10.02.2026 um 22:00 Uhr.

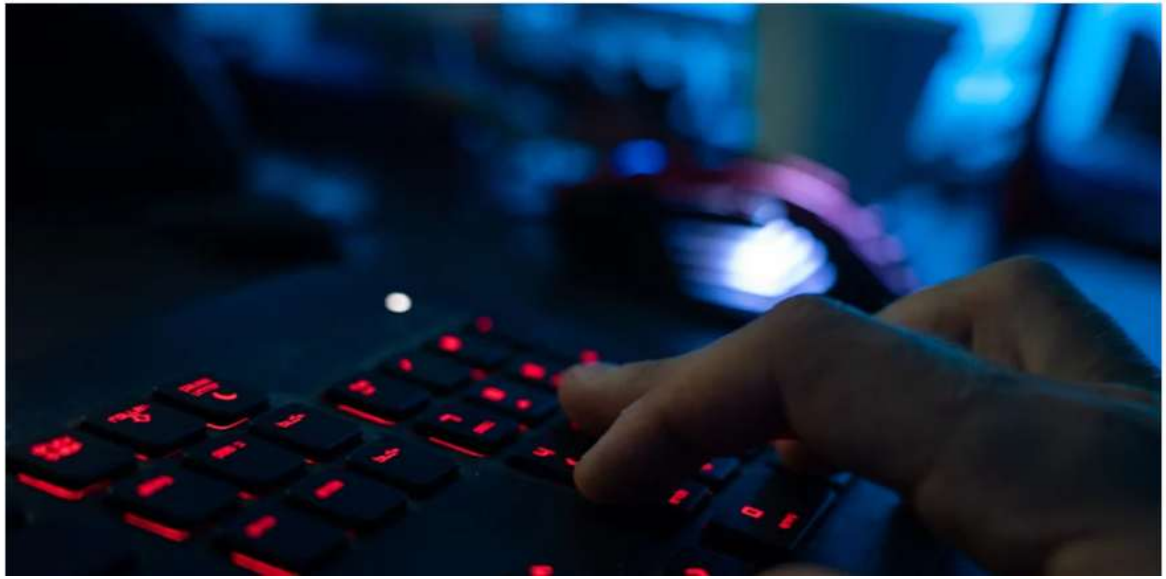
Eine Softwarepanne bei der AOK Bayern hat für 6.400 Versicherte unerfreuliche Folgen: Bei einer System-Umstellung wurden die elektronischen Patientenakten (ePA) gesperrt, die darin abgespeicherten Daten waren anschließend nicht mehr zugänglich, wie die Krankenkasse mitteilte. Ursache war ein Fehler bei einem geplanten Software-Update, das IT-Dienstleister durchführen sollten. "Es war kein Hackerangriff, es sind keine Daten abgeflossen", sagte ein Sprecher. Mittlerweile steht nach Angaben der Kasse fest, dass die gesperrten Dateien wiederhergestellt werden können.

Quelle:
https://www.br.de/nachrichten/bayern/aok-datenpanne-6-400-elektronische-patientenakten-gesperrt,VArKt9B

Cyberangriffe der letzten Tage

Hackerangriff betrifft IT der Beweisstückstelle der Polizei

Stand: 04.02.2026 | Lesedauer: 2 Minuten



Auswirkungen des Angriffs sind unklar

Welche Folgen der Angriff konkret hat, war zunächst unklar. «Das müssen wir jetzt ermitteln», sagte die Sprecherin. Personenbezogene Daten seien bei dem Angriff nach ersten Erkenntnissen der Staatsanwaltschaft nicht abgegriffen worden. Die reguläre Arbeit der Polizei sei nicht betroffen.

Ein Ransomware-Angriff ist eine Form der Cyberkriminalität, bei der eine Schadsoftware eingesetzt wird. Damit werden Daten oder Computersysteme verschlüsselt oder gesperrt. Angreifer fordern dann oft ein Lösegeld.

Nach Informationen von «buten un binnen» legte der Angriff bei der Werkstatt Bremen große Teile der IT-Infrastruktur lahm. Demnach konnten Computer nicht mehr gestartet werden. Elektronische Kommunikation sei so gut wie nicht mehr möglich, hieß es. Bei der Werkstatt Bremen arbeiten zahlreiche Menschen mit Beeinträchtigungen.

Quelle:
https://www.welt.de/regionales/niedersachsen/article698385c62dfdd2aa24525c7f/hackerangriff-betrifft-it-der-beweisstueckstelle-der-polizei.html


Ubuntu-Desktop
Activities
Oct 24 09:48
Bedrohungslage Phishing
linux
Trash

Bedrohungslage IT-Abteilung

Fachkräftemangel im IT-Security Bereich

- Fachwissen
- Fluktuation

Komplexere IT-Umgebungen

- BYOD
- Cloud Dienste
- Home Office
- Hosting
- Housing

Verwaltung kann komplex sein

- Komplexe Sicherheitsregeln
- Spezifische Anforderungen einzeln umsetzen
- Viele unterschiedliche Oberflächen und Hersteller

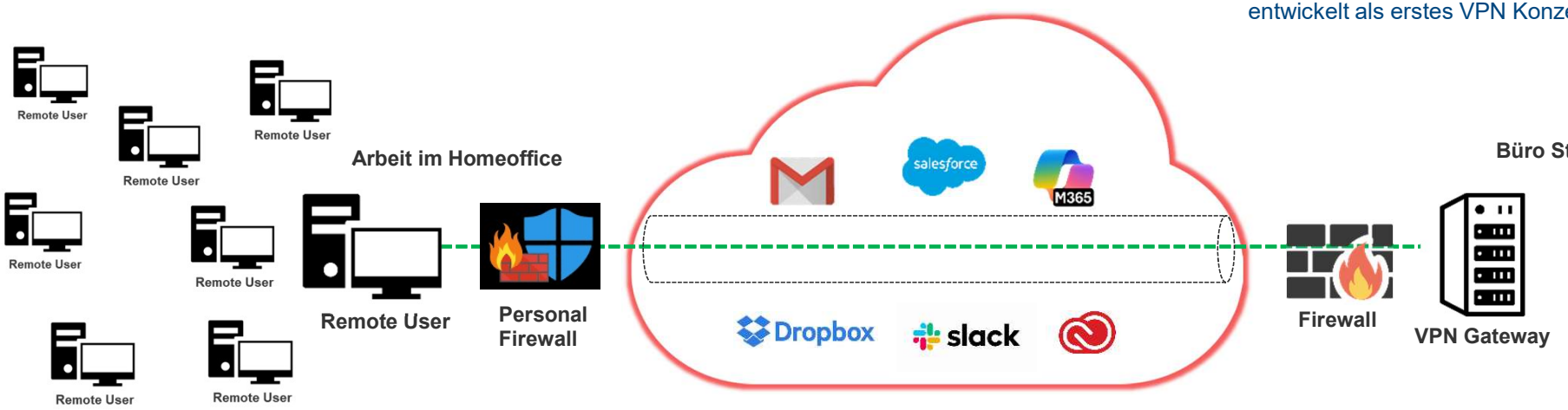
Steigende Gefahr

- Menge der Angriffe steigt kontinuierlich
- Anzahl fortschrittlicher Angriffe steigt

VPN Rückblick

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

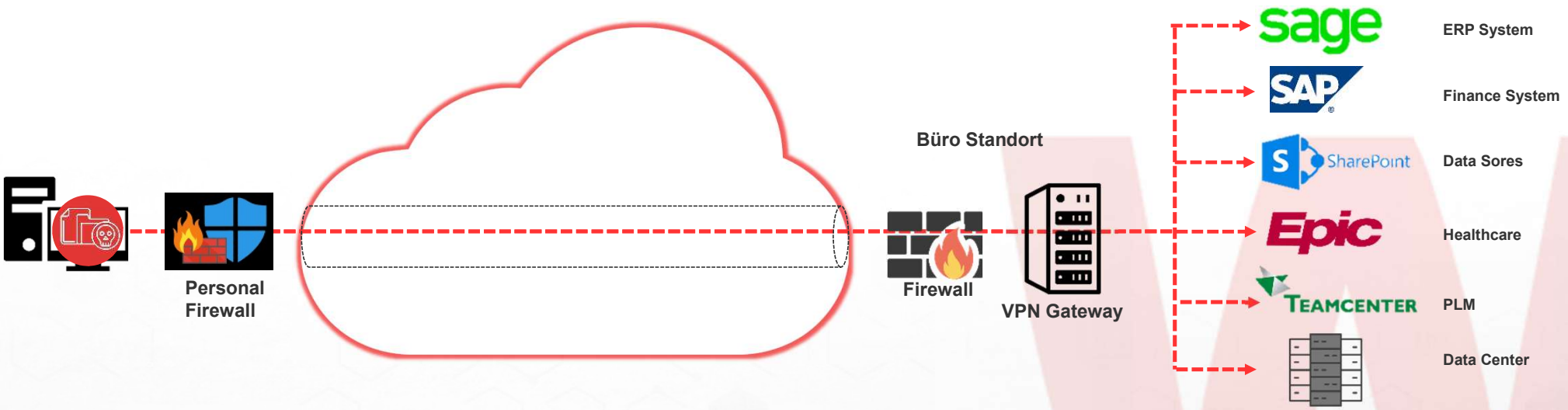
Heute: Hunderte Personen arbeiten außerhalb der Standorte, SaaS Anwendungen und Cloud-Infrastruktur werden intensiv genutzt und hybride Umgebungen sind die Normalität.

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

Und so entsteht die Falle!

Die VPN Falle: 5 Herausforderungen

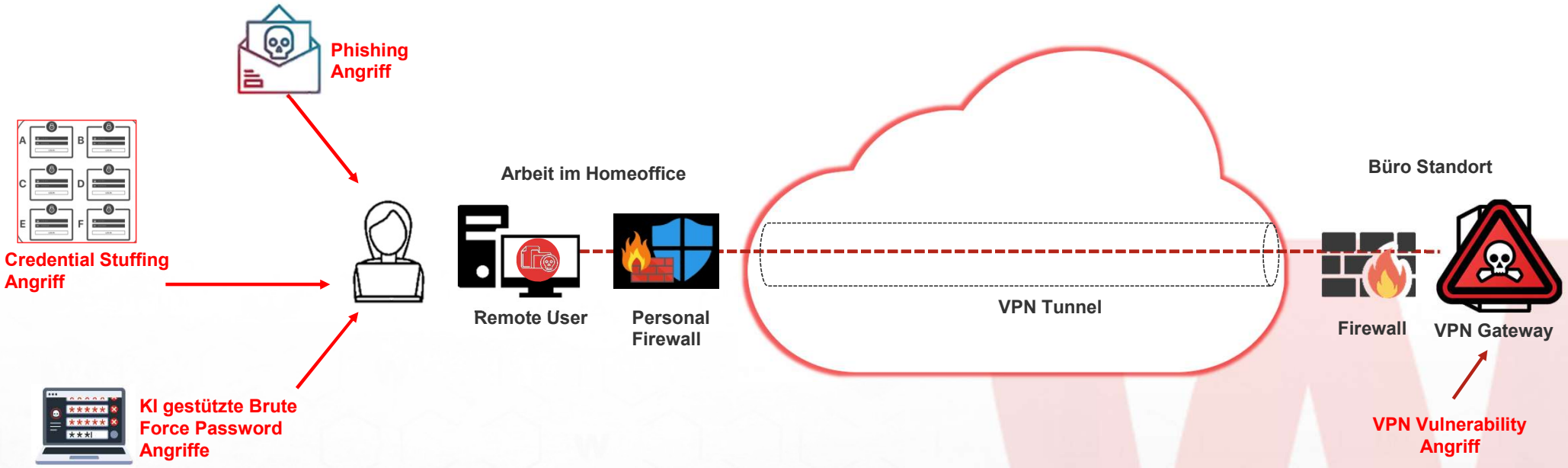
1. Uneingeschränkte Zugriffe auf Netzwerke



Laterale Bewegung, zu leichter Zugriff bei Ransomware Angriffen und Datendiebstahl

Die VPN Falle: 5 Herausforderungen

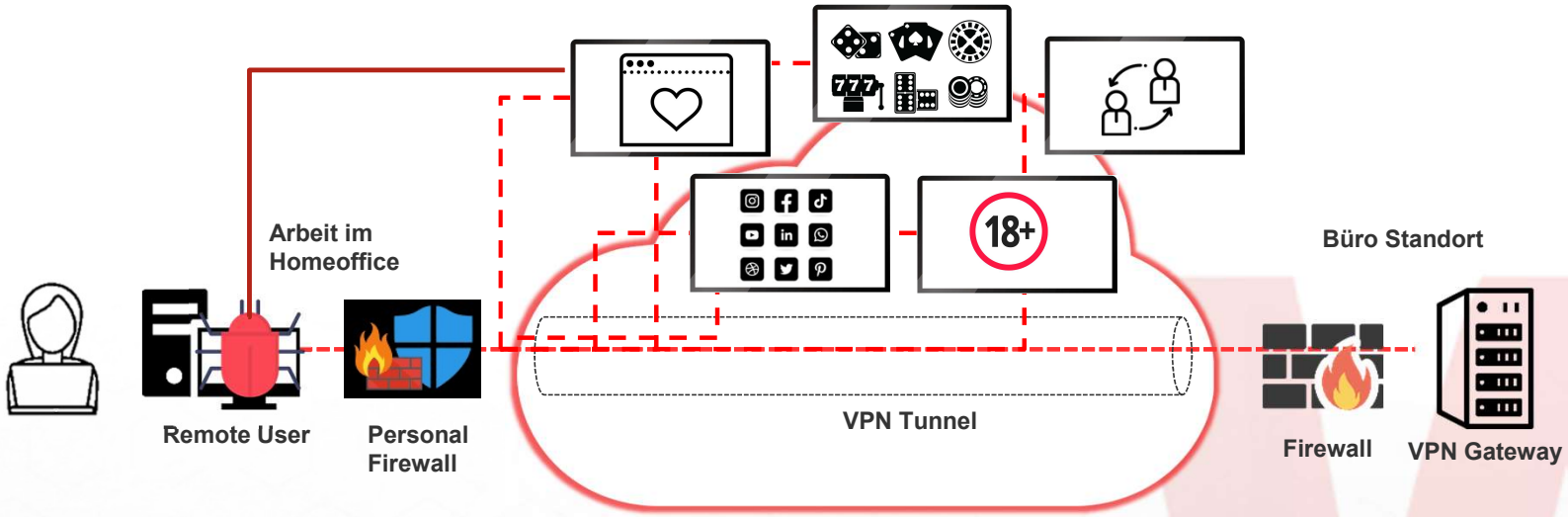
2. Identitäten als Risiko: Passwort + VPN = Angriffsmöglichkeit



Kompromittierte Zugangsdaten → VPN Anmeldung → Zugriff → Ransomware Infektion

Die VPN Falle: 5 Herausforderungen

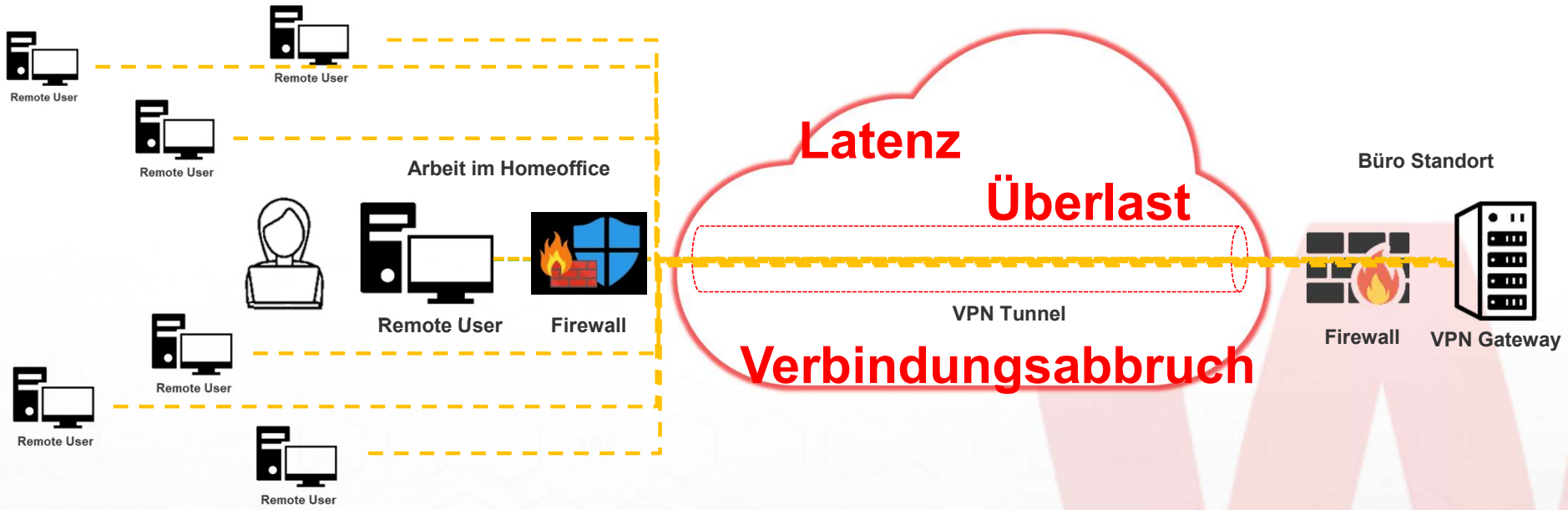
3. Im Blindflug – Gerätesicherheit bleibt unklar



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

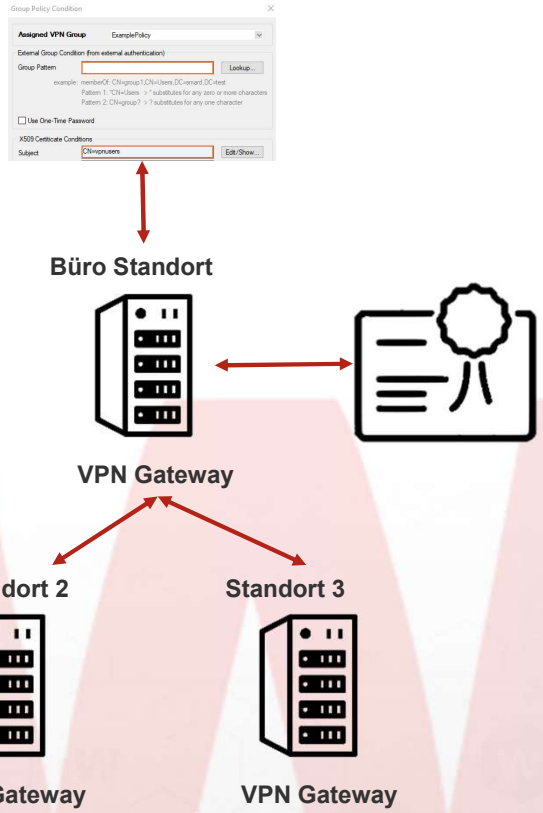
Average IT hourly cost (USD)
90

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

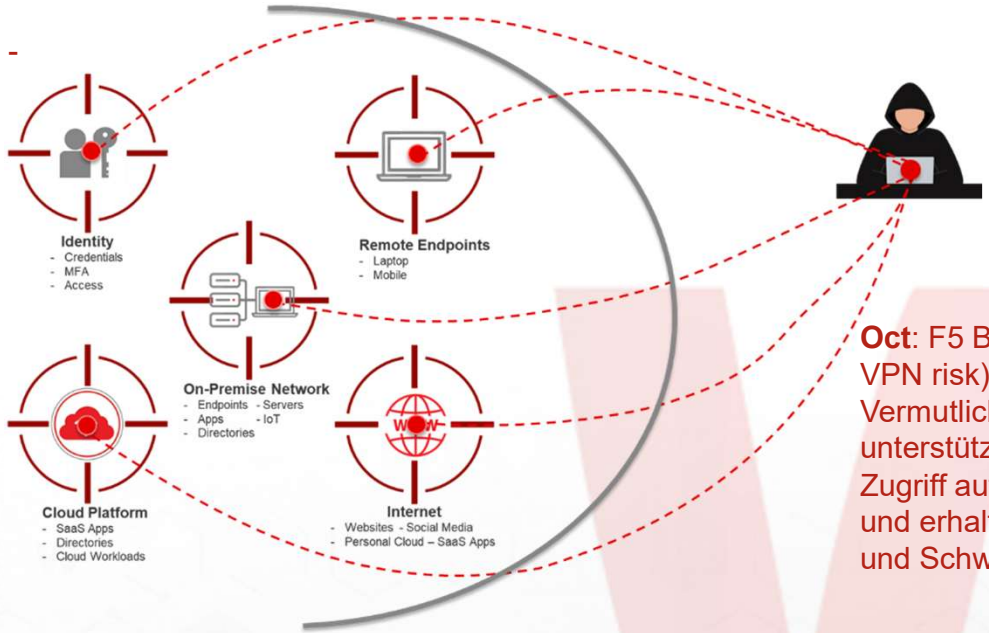
Jan: Ivanti Connect Secure / Policy Secure / ZTA
Zwei Schwachstellen gemeldet (CVE-2025-0282, -0283); eine davon wurde seit Dezember 2024 als Zero Day ausgenutzt.

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.

Ein echtes Beispiel – Akira Ransomware

- Ransomware-as-a-Service
- Kompromittierte Anmeldedaten
- Zugriff per Mobile VPN
- Scan des Netzwerks
- Zugriff auf interne Systeme
- Erweiterung der Rechte und Zugriffsmöglichkeiten
- Ausführung von Akira.exe und Verschlüsselung über SMB

Configuration of IT-Security solutions matter – and sometimes a single parameter can cause big trouble

02 July 2025 By **Jonas Spieckermann**

Sometimes supposedly small things make a huge difference. This can also be true in cyber security configurations. In recent weeks, multiple partners described very similar cyber attacks their customers faced, and in some cases, the criminals were unfortunately even successful in compromising customer networks. Specifically speaking, cyber criminals first exfiltrated and then encrypted data with Akira ransomware. Akira ransomware is already out in the wild since march 2023 and many companies fell victim (Cisa has published a very detailled description and also many helpful recommendations in this advisory: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a)

kurze Pause

Zero Trust: Never Trust, Always Verify

Sicherheit durch kontinuierliche Validierung, kein implizites Vertrauen.

Zero Trust ist ein Konzept der Cyber-Sicherheit. Selbst innerhalb eines Netzwerks sollte Benutzer*innen, Geräten oder Applikationen nicht “blind” vertraut werden. Zugriffe werden pro Verbindung gewährt und regelmäßig neu bewertet.

- ❑ Überprüfung der Identität, des Geräts und des Zusammenhangs bei jeder Verbindung.
- ❑ Dynamische Anpassung der Regeln basierend auf Risiko und Verhalten.

Prinzipien:

1. **Explizite Verifizierung:** Überprüfen und authentifizieren jeder Verbindungsanfrage.
2. **Zugang einschränken:** Das Prinzip der geringsten Zugriffsrechte wird angewendet.
3. **Annahme einer Sicherheitsverletzung:** Erwarten, dass Kompromittierungen entstehen oder schon vorhanden sind.
4. **Kontinuierliche Überprüfung:** Inspektion und Überwachung aller Aktivitäten.

Zero Trust = Identität + Gerät + Zusammenhang + regelmäßige Überprüfung

Schutz jeder Verbindung, von überall und von jedem Gerät.

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

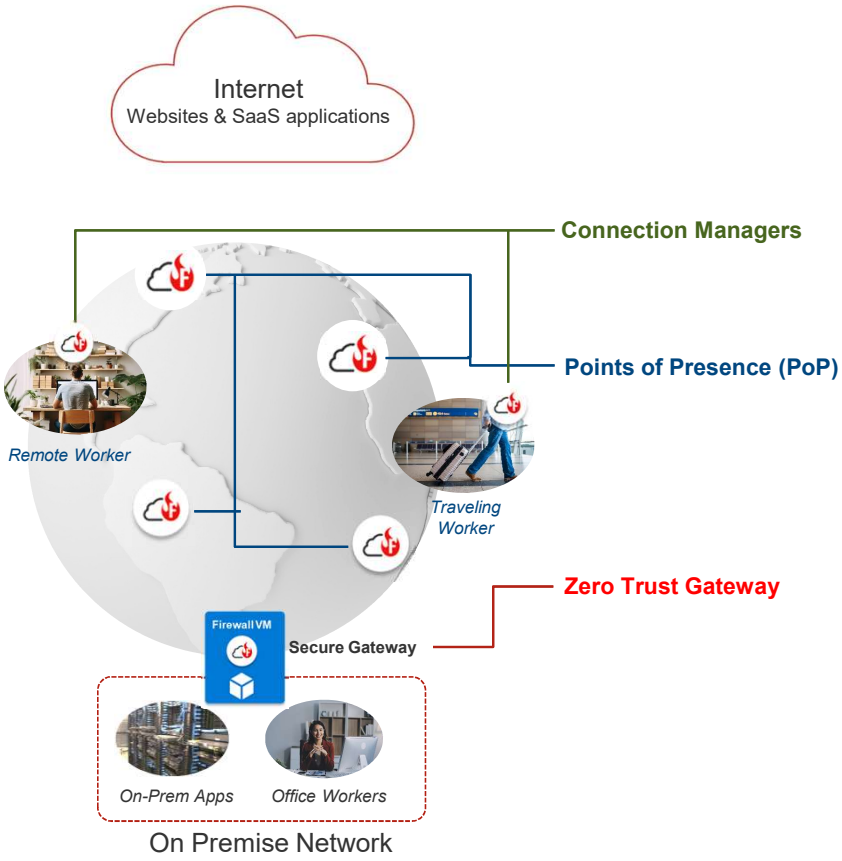
- die Authentifizierung verwaltet,
- den Datenverkehr an PoPs weiterleitet,
- Richtlinien gemeinsam nutzt und die Kommunikation sichert.

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

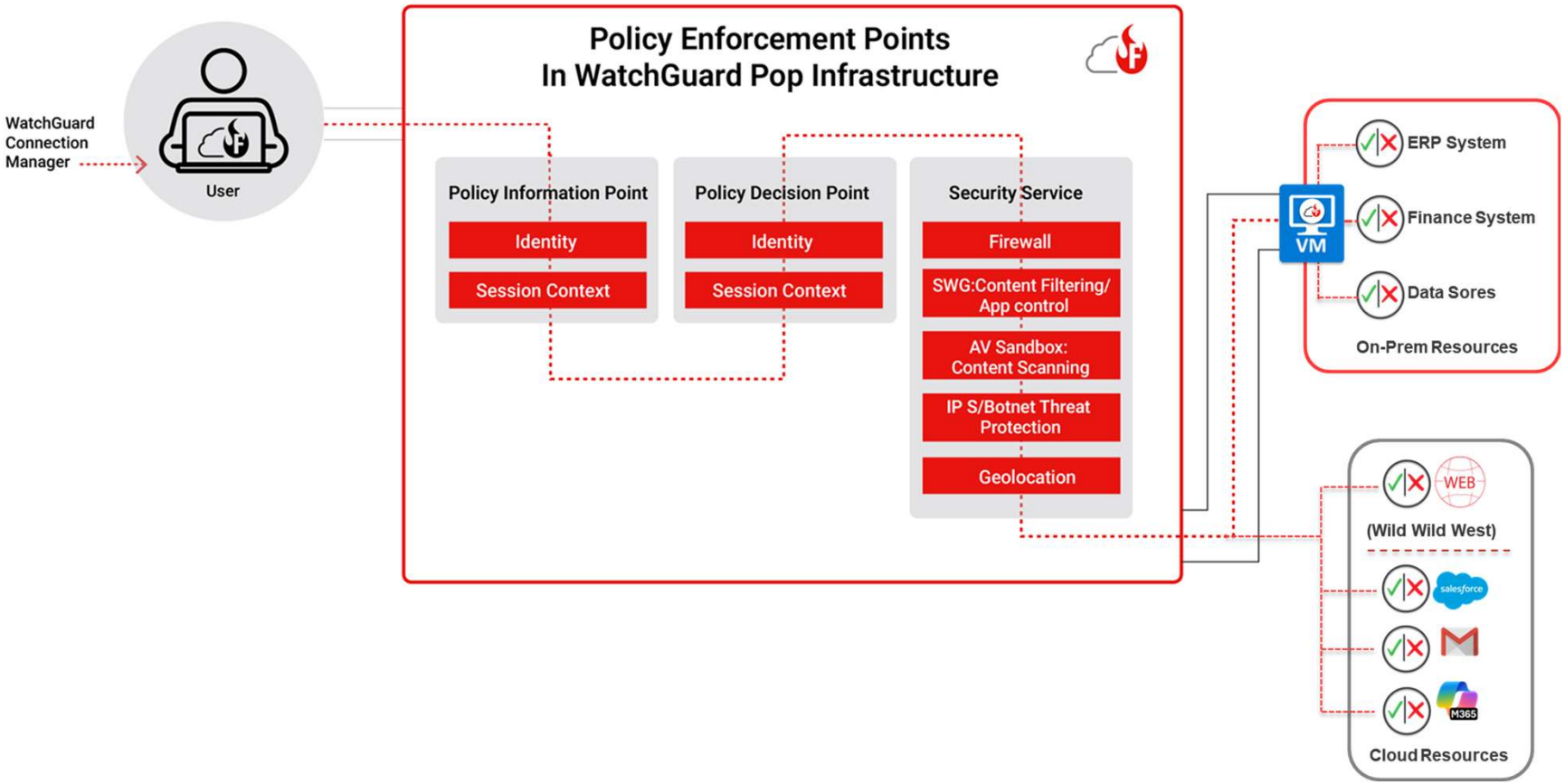
- verschlüsseln, optimieren und Verbindungen kontrollieren
- als Durchsetzungspunkte für Richtlinien und Zero Trust fungieren
- die Leistung optimieren und für Skalierbarkeit und Redundanz sorgen.

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

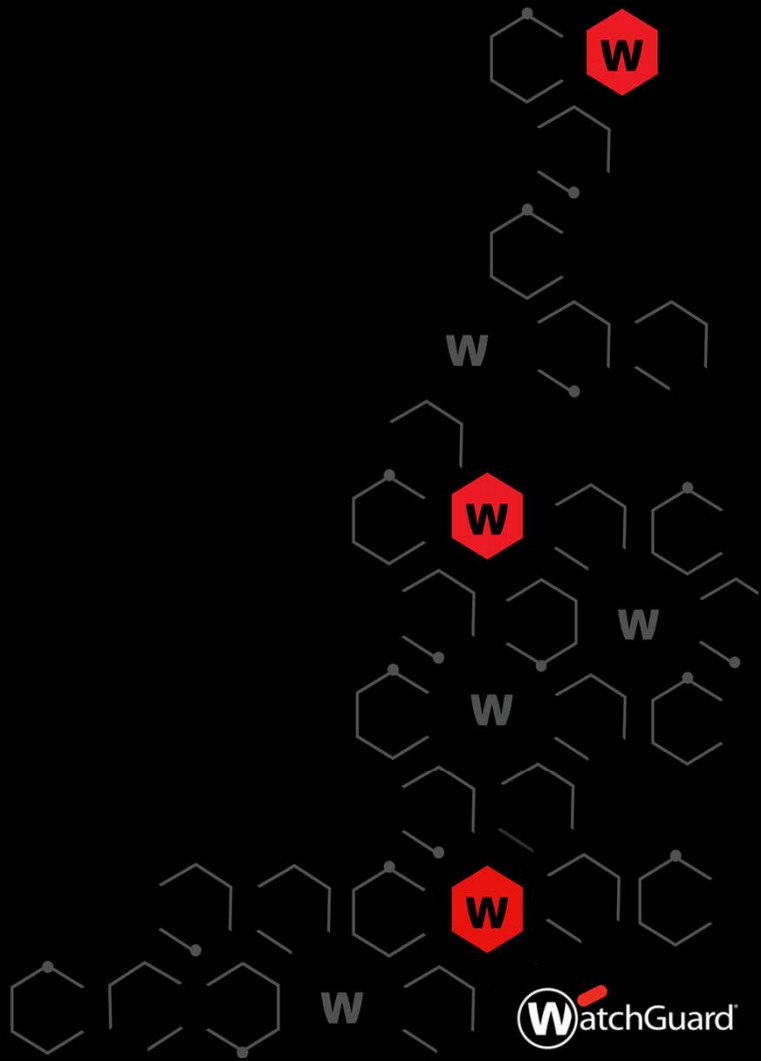
- sichere, verschlüsselte Verbindungen zwischen FireCloud-PoPs und privaten Anwendungen bereitstellt.
- Zero Trust Network Access (ZTNA) für lokale Anwendungen ohne offene Ports ermöglicht.
- identitätsbasierte Richtlinien für Benutzerzugriffe durchsetzt.



FireCloud Total Access



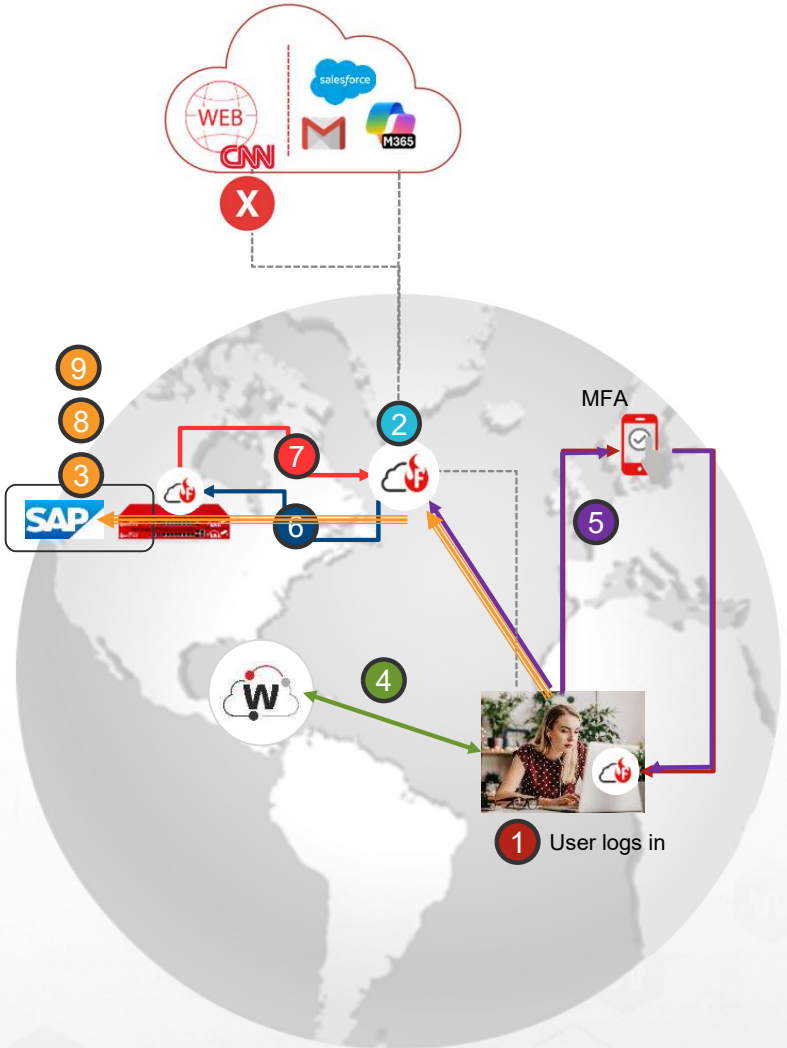
Live Demo



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.

Zero Trust Hersteller/Partner Checkliste

Zero Trust Lösungen

- ❑ Multi-Factor Authentication,
- ❑ Endpoint Detection and Response,
- ❑ Firewall as a Service,
- ❑ Secure Web Gateway
- ❑ Zero Trust Network Access.

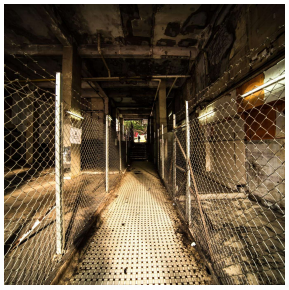
Unified Policy Management ist wichtig

- ❑ Zentralisierte Cloud-basierte Umsetzung von Richtlinien
- ❑ Einheitlicher / Unified Endpoint Agent
- ❑ Einheitliche Zero Trust Richtlinien
- ❑ Session Level Enforcement
- ❑ Globale PoP Infrastruktur

Mehrwerte für Anwender*innen

- ❑ Sicherheit und Verwaltung ohne Lücken
- ❑ Schnelle und sichere Verbindung von jedem Ort

Zusammenfassung

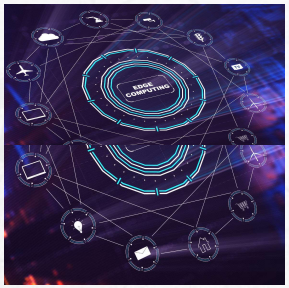


Einschränkungen traditioneller VPNs

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

Moderne Sicherheits Prinzipien

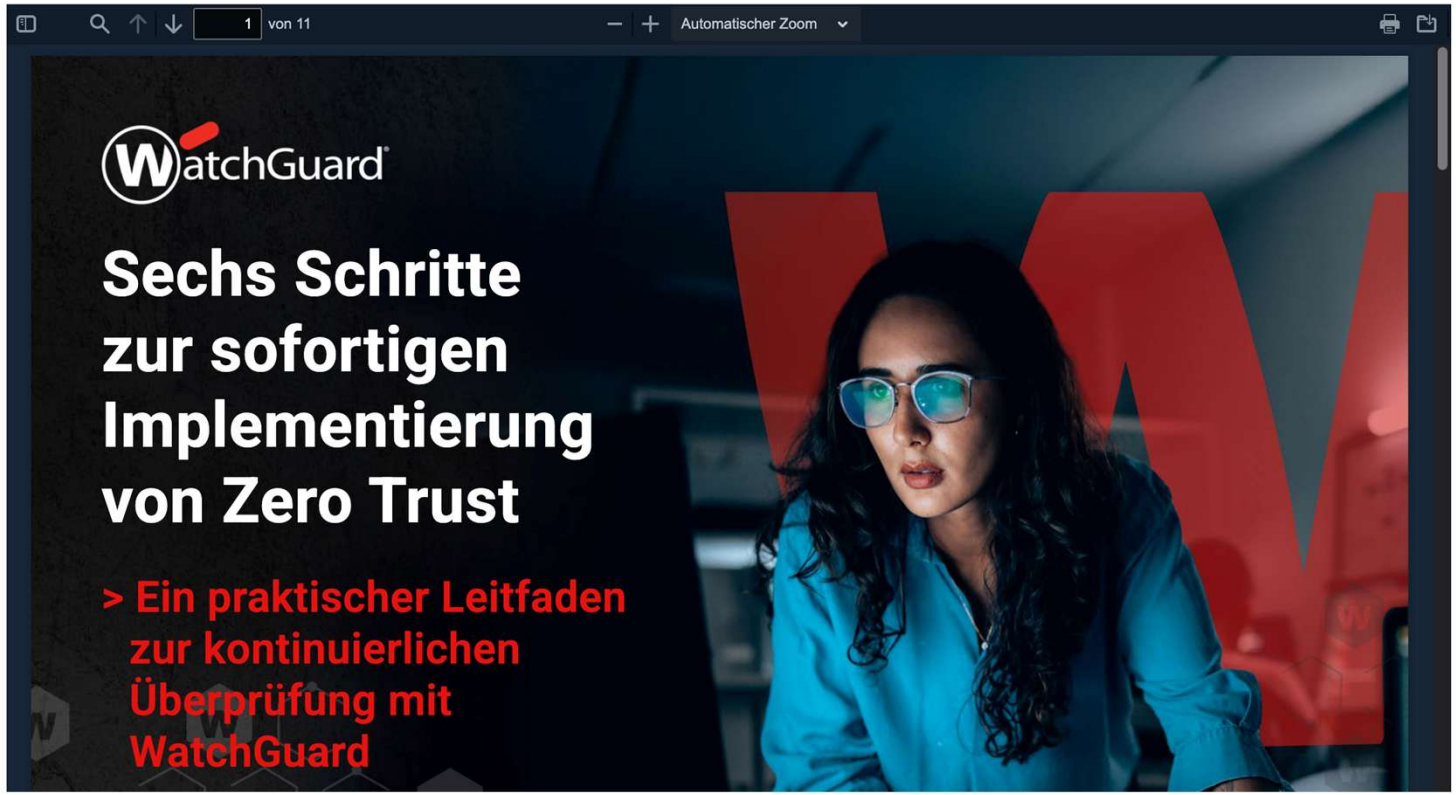
Überprüfung der Identitäten, des Geräte-Zustands, Anwendung des Prinzips der geringsten Zugriffsrechte und kontinuierliche Überwachung sind erforderlich für eine robuste, moderne Sicherheits-Strategie.



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.

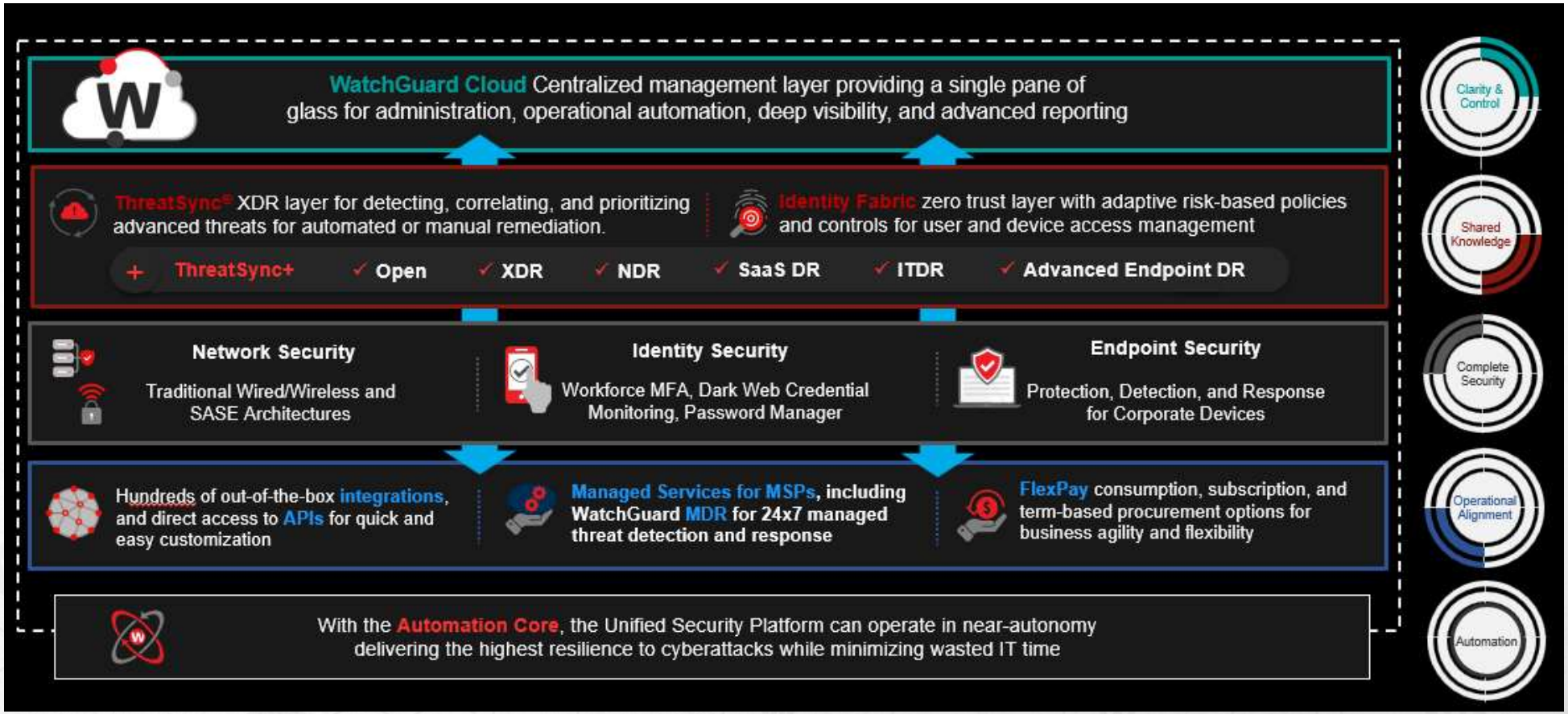
eBook - Sechs Schritte zur Implementierung von Zero-Trust



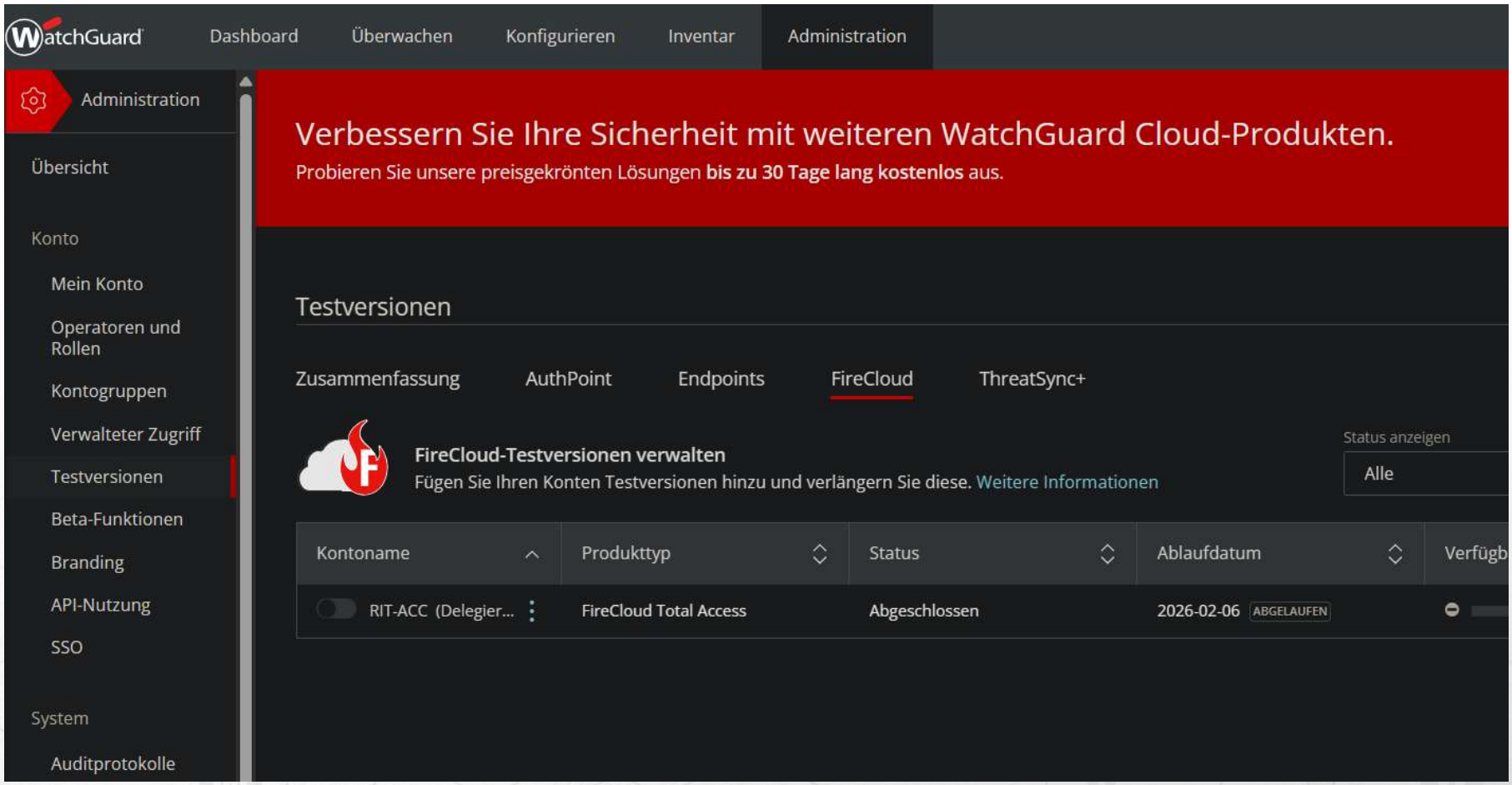
https://www.watchguard.com/de/wgrd-resource-center/ebook/6-steps-deploying-zero-trust

Brauchen wir jetzt keine Firewalls mehr?

WatchGuard Cloud – Unified Security Platform



WatchGuard Cloud – Unified Security Platform



Real Security for the Real World

WatchGuard

Thomas Runte

Senior Sales Engineer

Frage & Antwort

Vielen Dank!