Real Security for the Real World

Sebastian Goll
Channel Account Manager
sebastian.goll@watchguard.com

WatchGuard MDR – 24/7 Security für Jedermann!

Stand der Cybersicherheit

Das Problem:

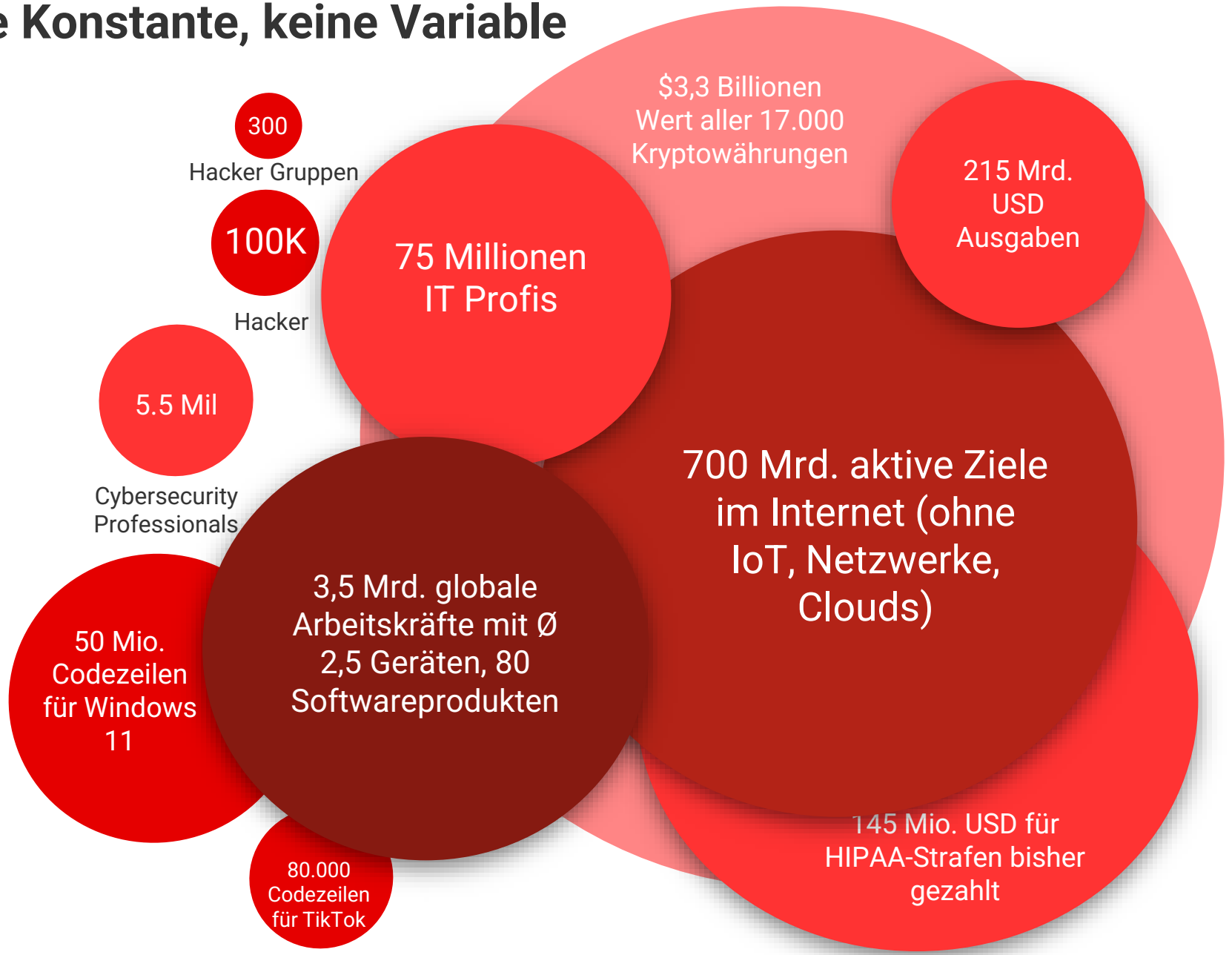
- Wachsende Angriffsflächen
- Bedrohungen werden komplexer
- Eingeschränkte Fachkenntnisse
- Teure Produkte und Dienstleistungen machen Sicherheit für viele unzugänglich

Ergebnisse und Risiken:

- Verwundbare Sicherheitslage
- Schlechte Erkennungsfähigkeiten und langsame Reaktion
- Eingeschränkte Abdeckung außerhalb der Geschäftszeiten

Cybersicherheit ist eine Konstante, keine Variable

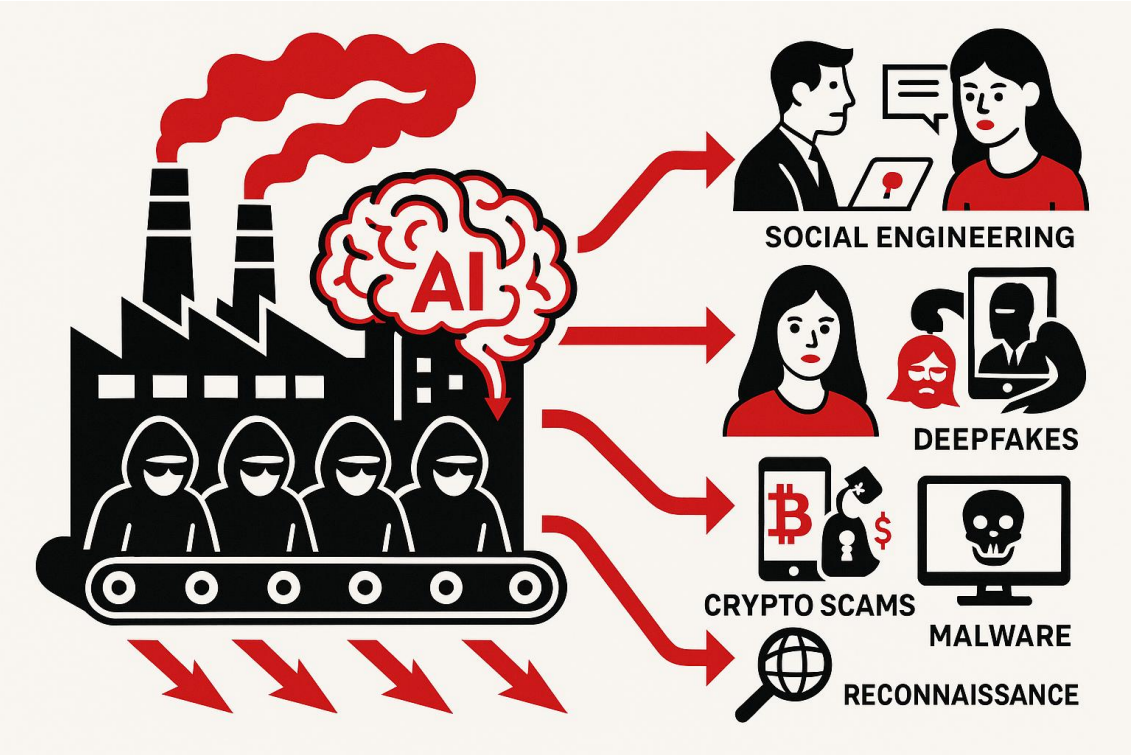
- **$10.5 Billionen:** geschätzter Schaden durch Cyberkriminalität bis 2025
- **Hoche/Kritische Schwachstellen:**
  - Linux > 150
  - Windows > 200
  - Mac >100
- **Ø 55 Tage** zur Behebung kritischerSchwachstellen
- **1 pro 5.000** Codezeilen geschätzte Schwachstelle
- **12,5 Tage** Aufenthaltsdauer von Angreifern im System
- **Ø 48 Minuten** bis zur Eskalation eines Angriffs



Hybrid-IT ist gekommen, um zu bleiben

- IoT
- Angriffsfläche vergrößert
- Legacy- und Cloud/SaaS-native-Systeme
- …

KI beschleunigt Angriffe:



- **Besser:**
  - Deepfakes,
  - Social Engineering
- **Schneller:** Automatisierung von
  - Ausspähung
  - Zero-Day-Exploits
  - Malware
- **Stärker:**
  - kompromittierte E-Mails für Unternehmen steigert Klickraten um 50 Prozent.

Warum MDR?

heutige Bedrohungen entwickeln sich schnell, die IT-Teams können meist nicht Schritt halten.

- 24/7-Bedrohungen = 24/7-Verteidigung
- Angreifer umgehen traditionelle Tools
- Es fehlt an Zeit, Tools oder Expertise zur Reaktion
- MDR schließt diese Lücke
  - durch Experten, nicht nur durch Alarme
- Weniger Risiko ohne zusätzliche interne Belastung

Neue Richtlinien

Regierungs-/ Industrievorgaben NIST	NIS2	ISO27001
DORA	CMMC	Cyber Essentials
staatlicher Datenschutz	EU-Vorgaben	Cyberversicherung

Polling Question #3

Wie wichtig ist das Thema Reputationsschutz in der Lieferkette für Ihre Kunden?

Antwortoptionen:

- Sehr wichtig – ein zentraler Verkaufsfaktor
- Mittel – wird zunehmend relevanter
- Eher unwichtig – spielt kaum eine Rolle
- Weiß ich nicht / Noch nie thematisiert

Core MDR

Endpoint

- Vollständig verwalteter
- 24/7 aktiver Cybersecurity-Service
- kein eigenes SOC (Security Operations Center) nötig

- Kombiniert KI-gestützte Bedrohungserkennung
- SOC-Experten zur schnellen / effizienten Erkennung
- Untersuchung und Reaktion auf Cyberbedrohungen

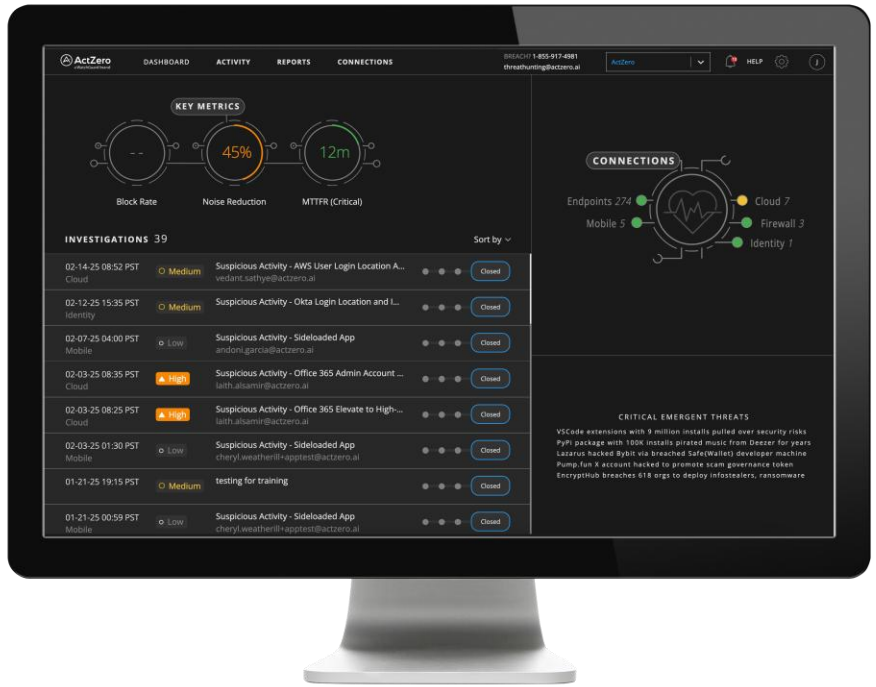
Einfache Integration & kosteneffizient

- WatchGuard
  - EDR (Endpoint Detection & Response)
  - EPDR (Endpoint Protection Detection & Response)
  - Adv. EPDR
  - Lieferanten für Telemetrie -> keinen Connector
- Sie gestalten das Verkaufsmodell –
  - Monatlich / Jährlich
  - Projekt oder Subscription
  - Alleine oder im Security-Bundle, …

WatchGuard Managed Services Portal

Das Fenster zu allem, was unser SOC sieht und tut.

- Echtzeit-Transparenz über Bedrohungen
- Alarmmetriken, Fallaktivität und Erkennungsdaten
- Schnellere Entscheidungsfindung und mehr Vertrauen



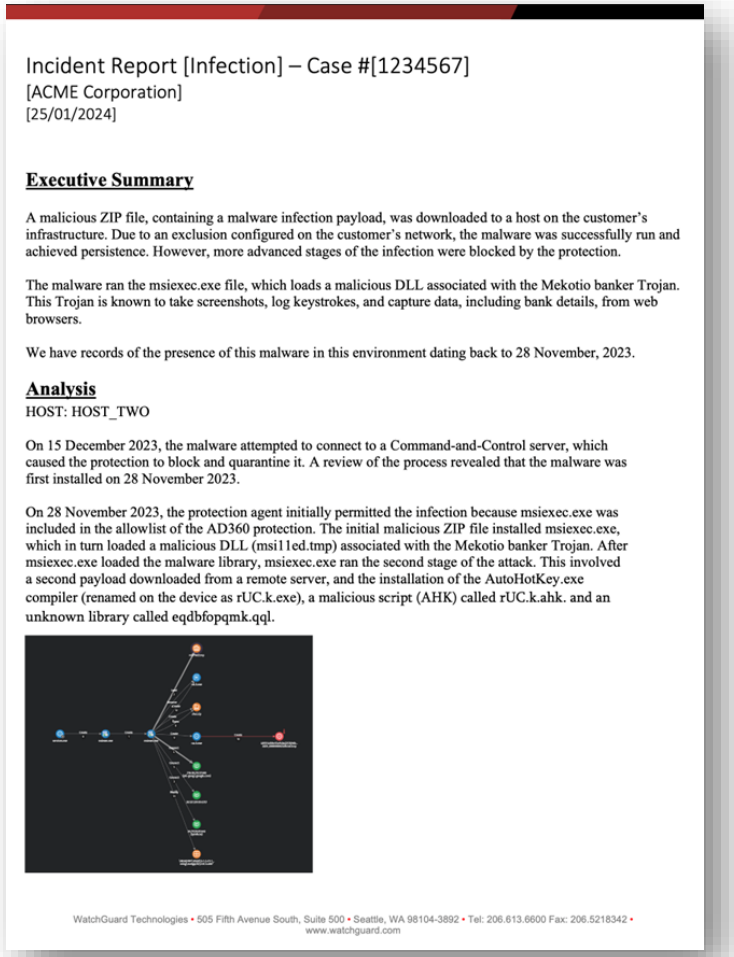
See the click through demo.

Partner Onboarding in 30 Minuten

- Onboarding einfach, simple, schnell loslegen
  - Kontaktdaten des Service Managers angeben,
  - technischen Ansprechpartner für die Alarmkette definieren
  - Eure Verfügbarkeit definieren
  - “Terms of Service” unterschrieben

Unverzügliche Meldung von Vorfällen

- Sofortige Benachrichtigung über Vorfälle und detaillierte Angriffsberichte
  - Nutzung des MITRE ATT&CK-Frameworks
- Maßgeschneiderte Playbooks zur automatischen Eindämmung
  - Richtlinien zur Schadensbegrenzung und -behebung
  - Kontinuierliche Bewertung der Angriffsoberfläche



Incident Report [Infection] – Case #[1234567]
[ACME Corporation]
[25/01/2024]

Executive Summary

A malicious ZIP file, containing a malware infection payload, was downloaded to a host on the customer's infrastructure. Due to an exclusion configured on the customer's network, the malware was successfully run and achieved persistence. However, more advanced stages of the infection were blocked by the protection.

The malware ran the msiexec.exe file, which loads a malicious DLL associated with the Mekotio banker Trojan. This Trojan is known to take screenshots, log keystrokes, and capture data, including bank details, from web browsers.

We have records of the presence of this malware in this environment dating back to 28 November, 2023.

Analysis

HOST: HOST_TWO

On 15 December 2023, the malware attempted to connect to a Command-and-Control server, which caused the protection to block and quarantine it. A review of the process revealed that the malware was first installed on 28 November 2023.

On 28 November 2023, the protection agent initially permitted the infection because msiexec.exe was included in the allowlist of the AD360 protection. The initial malicious ZIP file installed msiexec.exe, which in turn loaded a malicious DLL (msi11ed.tmp) associated with the Mekotio banker Trojan. After msiexec.exe loaded the malware library, msiexec.exe ran the second stage of the attack. This involved a second payload downloaded from a remote server, and the installation of the AutoHotKey.exe compiler (renamed on the device as rUC.k.exe), a malicious script (AHK) called rUC.k.ahk. and an unknown library called eqdbfopqmk.qql.

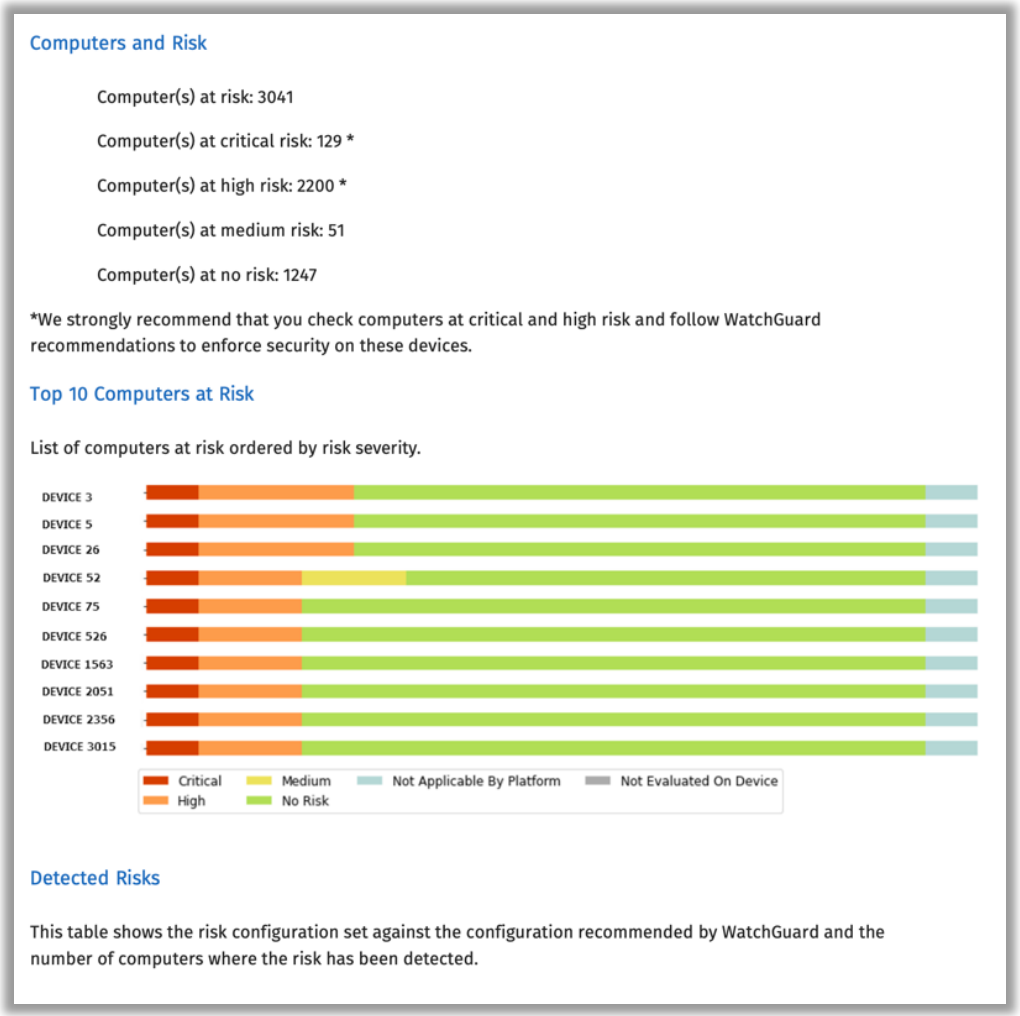
WatchGuard Technologies • 505 Fifth Avenue South, Suite 500 • Seattle, WA 98104-3892 • Tel: 206.613.6600 Fax: 206.5218342 • www.watchguard.com

Beispiel-Bericht: https://watchguard.widen.net/s/ld5s7nfxz6

Wöchentlicher Bericht

- schnellen Überblick über die Sicherheitslage der Endpoints
- schnelle Risiko-Identifizierung

- Abschnitte über:
  - Entdeckte ungeschützte Endpoints
  - Top 10 der am meisten gefährdeten Endpoints
  - Erkannte Risiken auf den Endpoints
  - Entwicklung der Risiken



Computers and Risk

Computer(s) at risk: 3041

Computer(s) at critical risk: 129 *

Computer(s) at high risk: 2200 *

Computer(s) at medium risk: 51

Computer(s) at no risk: 1247

*We strongly recommend that you check computers at critical and high risk and follow WatchGuard recommendations to enforce security on these devices.

Top 10 Computers at Risk

List of computers at risk ordered by risk severity.

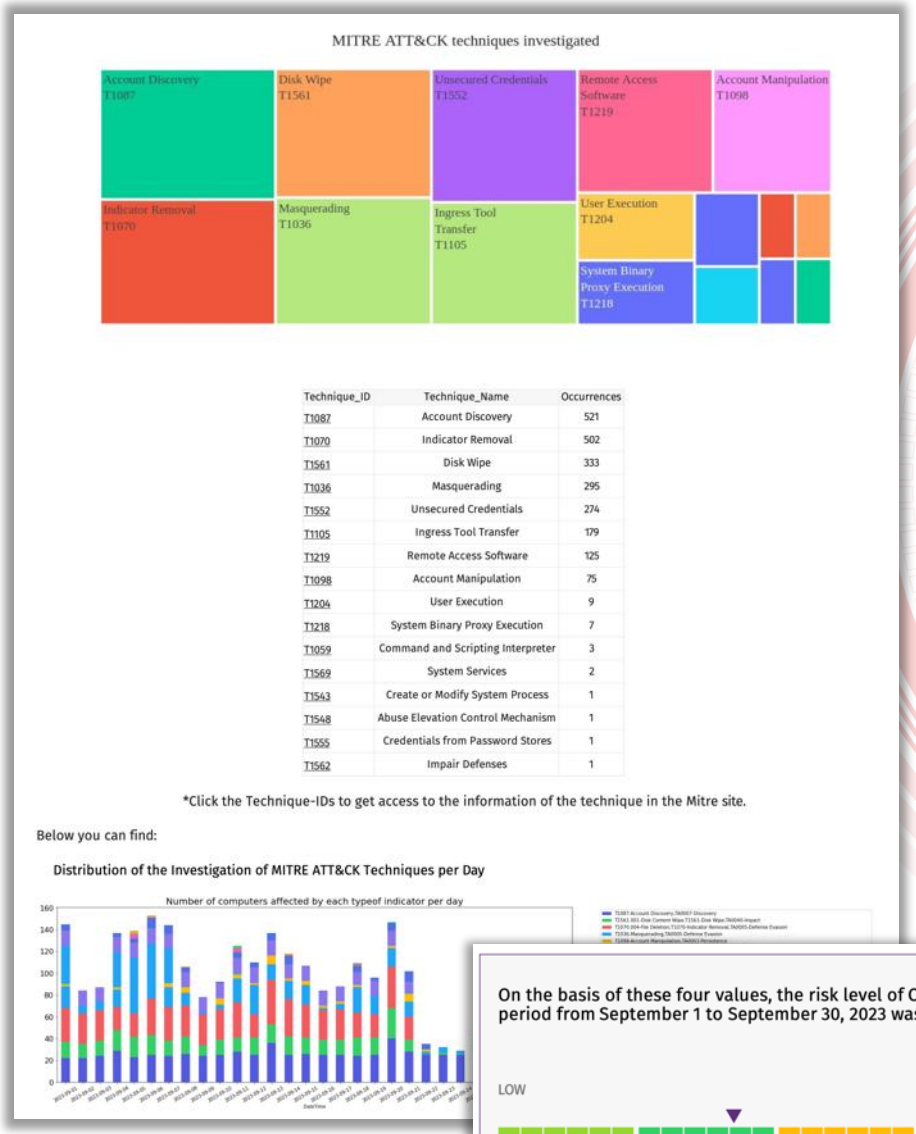
Detected Risks

This table shows the risk configuration set against the configuration recommended by WatchGuard and the number of computers where the risk has been detected.

Beispiel-Bericht: https://watchguard.widen.net/s/frs6j6jbcm

Monatlicher Bericht

- Überblick über Erkennungen
- Untersuchungen und Aktivitäten zur Eindämmung von Vorfällen
- Enthält Abschnitte über:
  - Aktuelle Situation
  - Sicherheitsempfehlungen zur Stärkung des Schutzes
  - Schutzniveau der Organisation
  - Bedrohungsgrad der Organisation
  - Monatlich durchgeführte Aktivitäten
  - Untersuchung anomaler Aktivitäten
  - Identifizierte und mitgeteilte Angriffsversuche



Beispiel-Bericht: https://watchguard.widen.net/s/x6wfxzw7gs

Core MDR für Microsoft

Erweitert Microsoft Defender mit:

- KI-gestützter Bedrohungsüberwachung
- Unterstützung durch ein Experten-SOC
- Nahtlose Integration
- Schnellere Reaktion
- bessere Transparenz
- stärkere Sicherheit

Wichzige Zahlen

- 90 % weniger Alarme
- < 6 Minuten Zeit bis zur ersten Reaktion
- < 6 Alarme pro Monat
- Automatisches Blockieren in < 10 Millisekunden
- < 1 Fehlalarm pro Monat

Kernfunktionen von MDR

- Einzelansicht über das gesamte Sicherheitsportfolio.
- 24/7-Überwachung und Reaktion
- Intelligente Erkennung durch KI/ML
- Proaktive Bedrohungssuche
- Automatisierte Reaktionen
- Weniger Lärm, mehr Relevanz
- Eingebaute Expertenführung

Total MDR

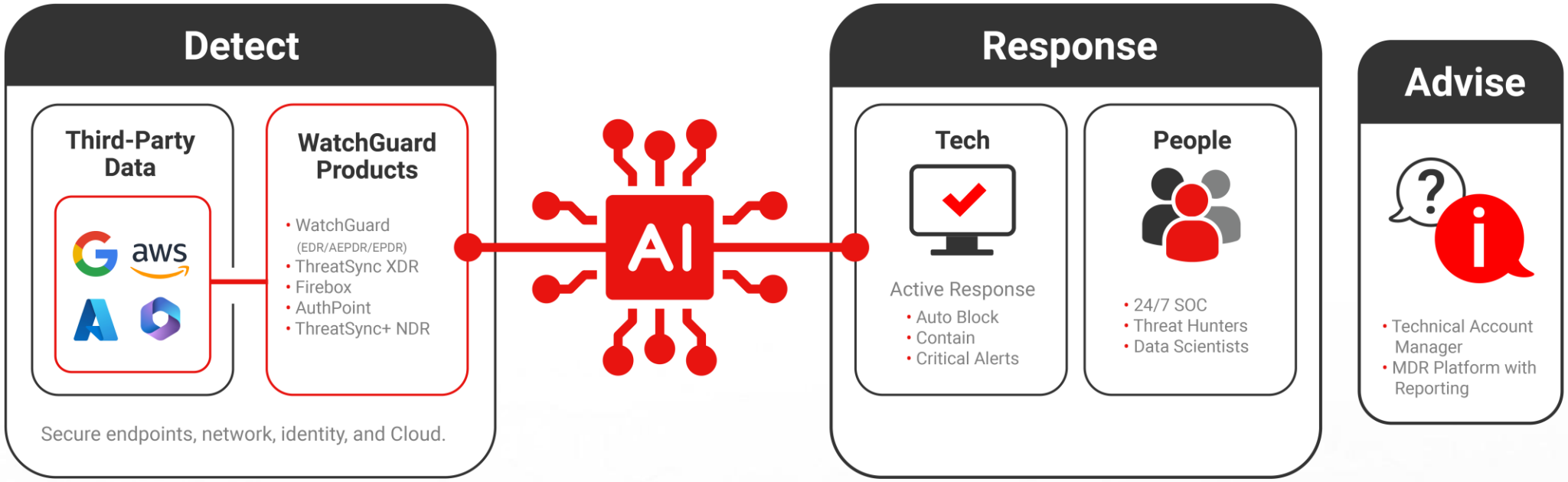
AuthPoint MFA | Endpoint | NetSec

WatchGuard Total MDR

- vollständig verwalteter 24/7-Service
- Bedrohungserkennung und reaction
- WatchGuard-Sicherheitsstack integriert.

Integrierte Komponenten:
Endpoints: WatchGuard EDR, EPDR
Firewall: WatchGuard Firebox
Identität: AuthPoint
Netzwerk: ThreatSync + NDR
Cloud: Microsoft 365 / Azure, AWS CloudTrail, Google Workspace

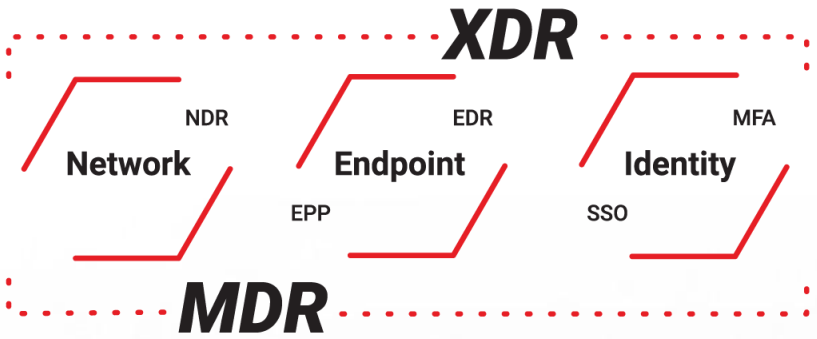
Total MDR Überblick



- **Endpoints:** WatchGuard EDR, EPDR
- **Firewall:** WatchGuard Firebox
- **Identity:** AuthPoint
- **Network:** ThreatSync+ NDR
- **Cloud:** Microsoft 365 / Azure, AWS CloudTrail, Google Workspace

Sicherung der gesamten Angriffsfläche

Endpoint

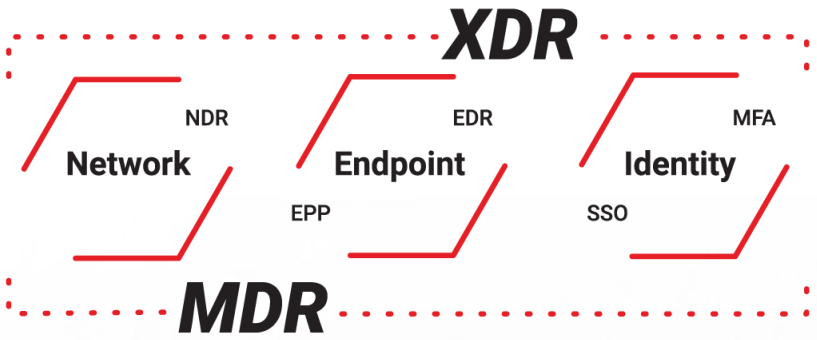


Sind Ziel für Ransomware, Phishing, dateilose Angriffe

- Erkennung von:
  - Anmeldeinformationsdiebstahl
  - Rechteausweitung
- Sofortige Isolation
- Prozessbeendigung
- Reaktion durch Analysten

Sicherung der gesamten Angriffsfläche

Identität

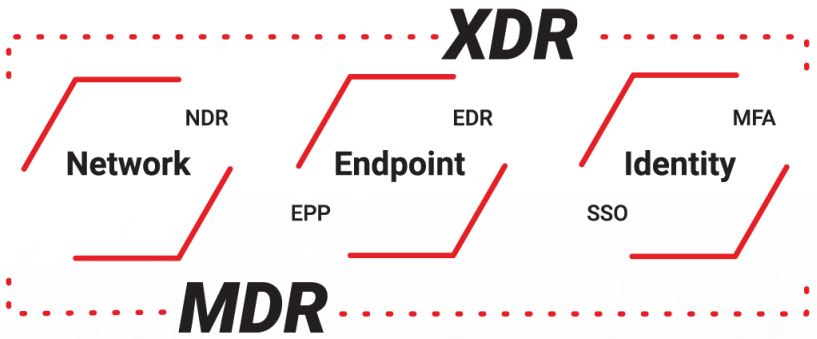


Integration mit AuthPoint

- Erkennung verdächtiger Logins
- Account-Erstellung
- Deaktivierung kompromittierter Konten in Echtzeit.

Sicherung der gesamten Angriffsfläche

Netzwerk



Erkennung von:

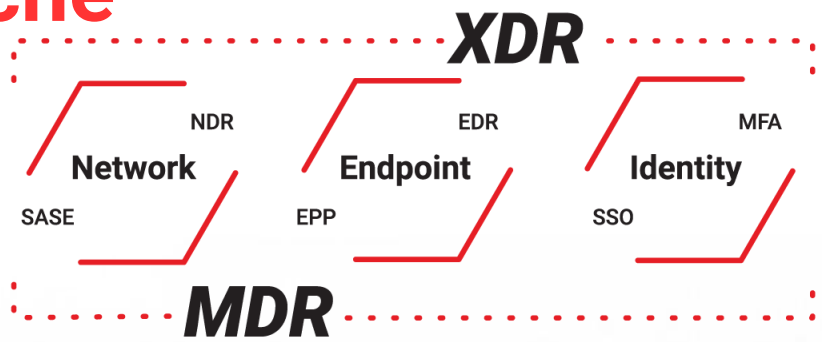
- lateraler Bewegung
- Port-Scans
- C2-Traffic

Sofortige Reaktion:

- IP blockieren
- Ports schließen
- Datenexfiltration stoppen

Sicherung der gesamten Angriffsfläche

Cloud

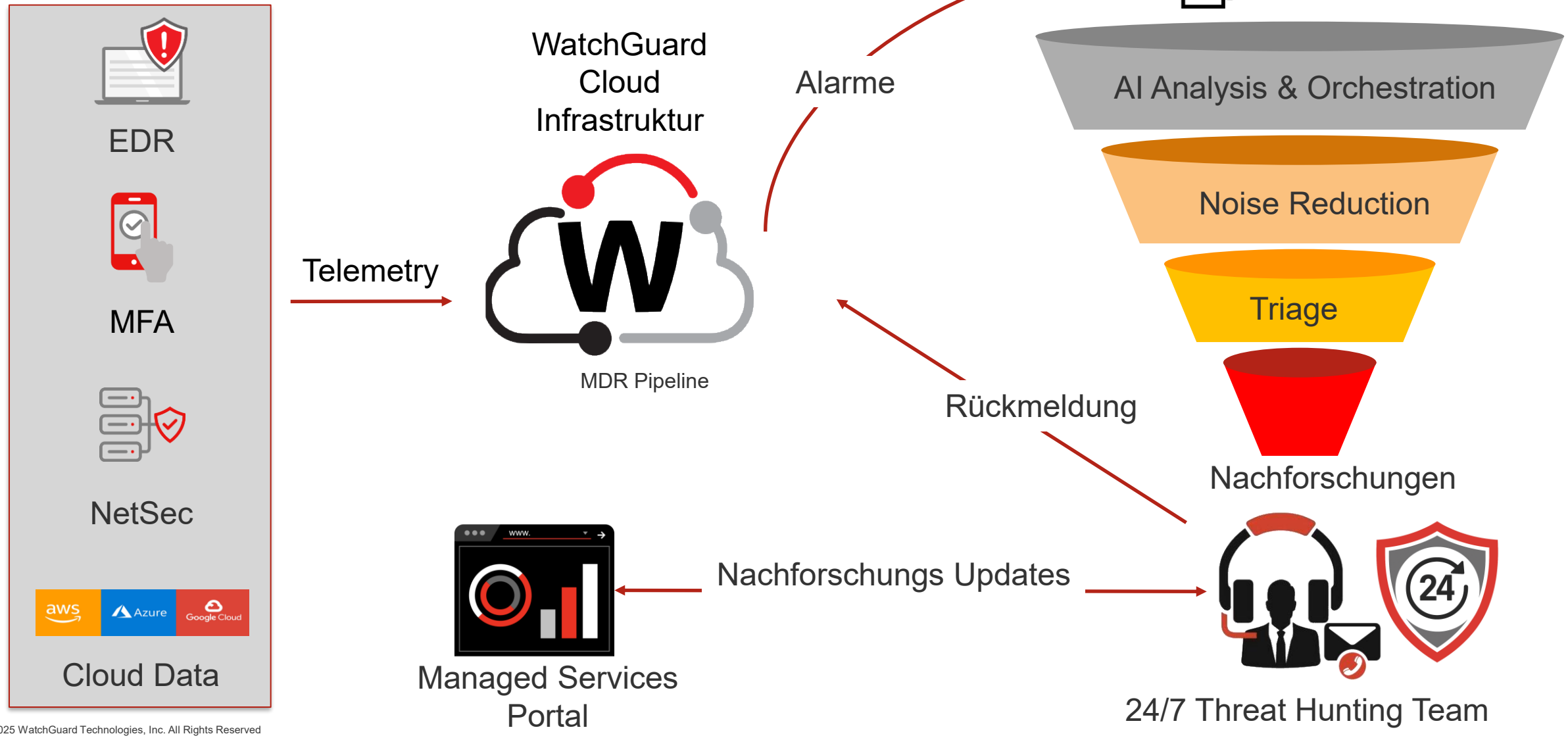


Überwachung von Microsoft 365, AWS, Google Workspace

API-basierte Reaktion:

- Zugriffsentzug
- Passwort zurücksetzen
- Angriffe eindämmen

Sichern Sie die gesamte Angriffsfläche



Beispiel aus der Praxis: Gib den Keks weiter!

1. Dark Web erfasst Anmeldedaten
2. Phishing löst MFA-Müdigkeit aus und führt zu Kontoverletzungen (Cookie-Diebstahl!)
3. Weitergabe des Cookies an den Hacker, Stellt Verbindung zu 365 her ändert Verknüpfungen von einem Laufwerk zu Command-and-Control-Link
4. Erstellen einer Mail-Weiterleitungsregel zum Abfangen von Nachrichten und E-Discover-Daten
5. Überweisungsbetrug an Kunden, Erpressung für Datenverlust oder Ransomware durch Links

Wie wir es stoppen –
Gib den Keks nicht weiter!

1. Dark-Web-Scans sind dem Diebstahl von Zugangsdaten einen Schritt voraus
2. MFA-Müdigkeit erzeugt einen Alarm und stoppt die Push-Nachrichten
3. EDR blockiert jeglichen Cookie-Diebstahl auf Geräten, denen der Zugriff auf das Netzwerk oder die Cloud nur bedingt erlaubt ist
4. Die Cloud-API-Datenerfassung informiert über Aktivitäten wie E-Mail-Weiterleitungen und verdächtige neue Anmeldeorte, die eine Zurücksetzung oder Sperrung des Kontos auslösen
5. Laterale Bewegungen zu internen Anlagen, die von NDR entdeckt werden, und IP-Adressen, die von Firewalls blockiert werden

What's Next in MDR?

First Half Highlights

- WatchGuard Core MDR
- WatchGuard Core MDR for Microsoft
- **WatchGuard Total MDR**

WatchGuard Total MDR

End Point
- EPDR

Network
- Firebox, Firebox Cloud
- ThreatSync+ NDR

IDENTITY
- AuthPoint

Second Half Highlights

- WatchGuard Open MDR
- Enhanced Reporting
- Integrated Onboarding
- Additional Open Integrations
- Client Tech Stack Refresh
- Additional AI/Data Science Ideation

Q1/25

- Release of WatchGuard Core MDR
- Release of WatchGuard Core for Microsoft
- Release of the WatchGuard MDR Partner Portal

Q2/25

- Release of WatchGuard Total MDR

Q3/25

- Release of WatchGuard Open MDR
- Integrated Onboarding

Q4/25

- Enhanced Reporting
- Additional Open Integrations
- Client Tech Stack Refresh

Real Security for the Real World

Dirk Albrecht

Territory Sales Manager

dirk.albrecht@watchguard.com

www.linkedin.com/in/dirk-albrecht-5245041

Sebastian Goll

Channel Account Manager

sebastian.goll@watchguard.com

www.linkedin.com/in/sebastian-goll-71594b17b

Vielen Dank!

WatchGuard Real Security for the Real World