



Hybride Sicherheitsstrategien für moderne IT-Infrastrukturen

Die Arbeitswelt hat sich verändert

- Hybrid- und Remote-Work als neue Normalität
- Verbreitete Verwendung von public Cloud und SaaS Lösungen
- Angriffe über weniger geschützte Wege nehmen zu
- Schutz von Remote Work wird zur Herausforderung
 - Unsichere Netzwerke (zu Hause, Cafés, Hotel, etc.)
 - Verwendung nicht bekannter Cloud Dienste (shadow IT)
 - Erhöhtes Risiko nicht autorisierter Zugriffe
 - Gefahr von Fehlkonfigurationen durch erhöhte Komplexität der hybriden Netzwerke

Der Schutz von Anwenderinnen und Anwendern muss die veränderte Arbeitswelt einbeziehen!



Remote & Hybrid Workforces

Cloud Adoption



Evolving Cyberattacks

Rising Compliance Standards



Cybersecurity Insurance Requirements

Typische Risiken und Gefahren



Gefährliche Aktivitäten

- Zugriff auf gefährliche / kompromittierte Websites
- Download infizierter Dateien
- VPN Regeln werden ignoriert
- Erfolgreiche Phishing Angriffe
- Sensible Firmen Daten oder Informationen werden local gespeichert
- Nicht freigegebene Cloud Lösungen und Applikationen werden genutzt



Angriffs-Vektoren

- Man-in-the-middle Angriffe
- Schadcode in Webzugriffen
- Phishing und Diebstahl von Anmeldeinformationen
- Infektionen mit Keyloggern
- Ransomware Angriffe
- Remote Access Trojaner
- VPN hijacking ermöglicht Zugriff auf sensible Bereiche und Daten



Hoher Aufwand / Hohe Kosten

- Frustration durch langsame Umsetzung
- Überlastung der IT-Abteilungen
- Zusätzliche Regularien
- Kleines IT Budget trotz zunehmender Anforderungen
- IT-Security Personal fehlt
- Fehlende Visualisierung von Risiken und Gefahren.

Ein einziges kompromittiertes System kann für Cyber-Angreifer den Zugang auf sensible Daten eines Unternehmens ermöglichen.

Umfassende Sicherheitskonzepte und Dienste sind erforderlich

WatchGuard bietet effiziente Lösungen, um die moderne Bedrohungslandschaft zu bewältigen



Network Security



Identity Security

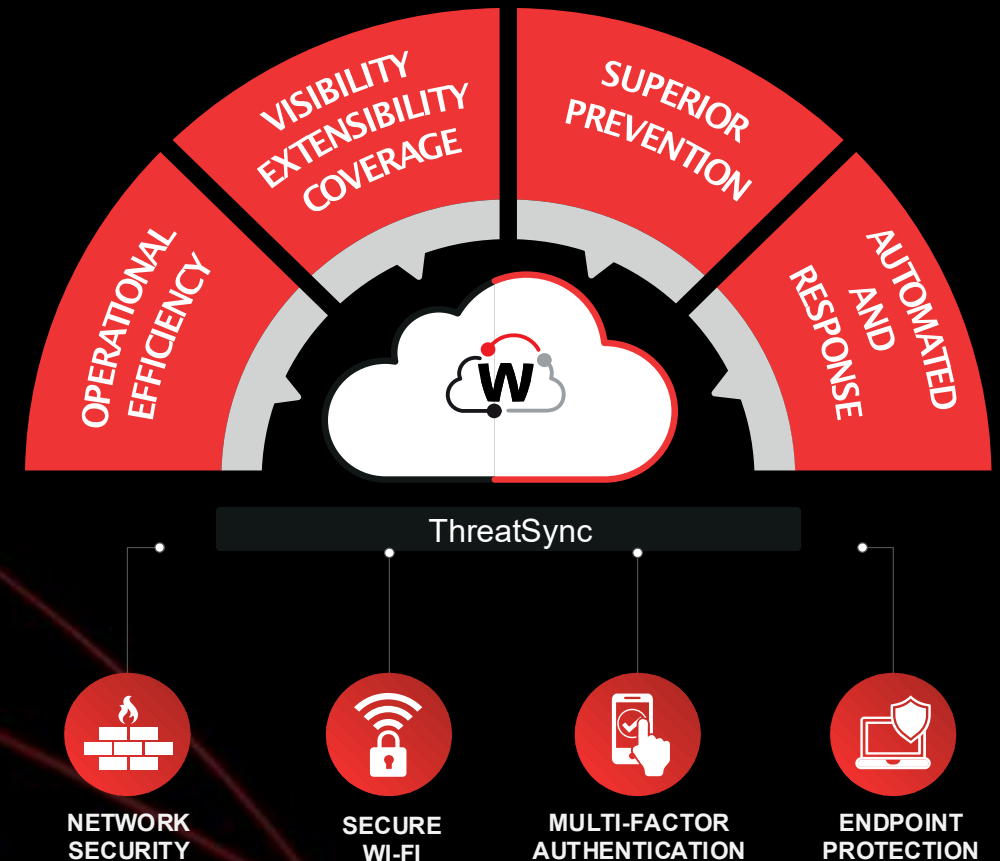


Endpoint Security

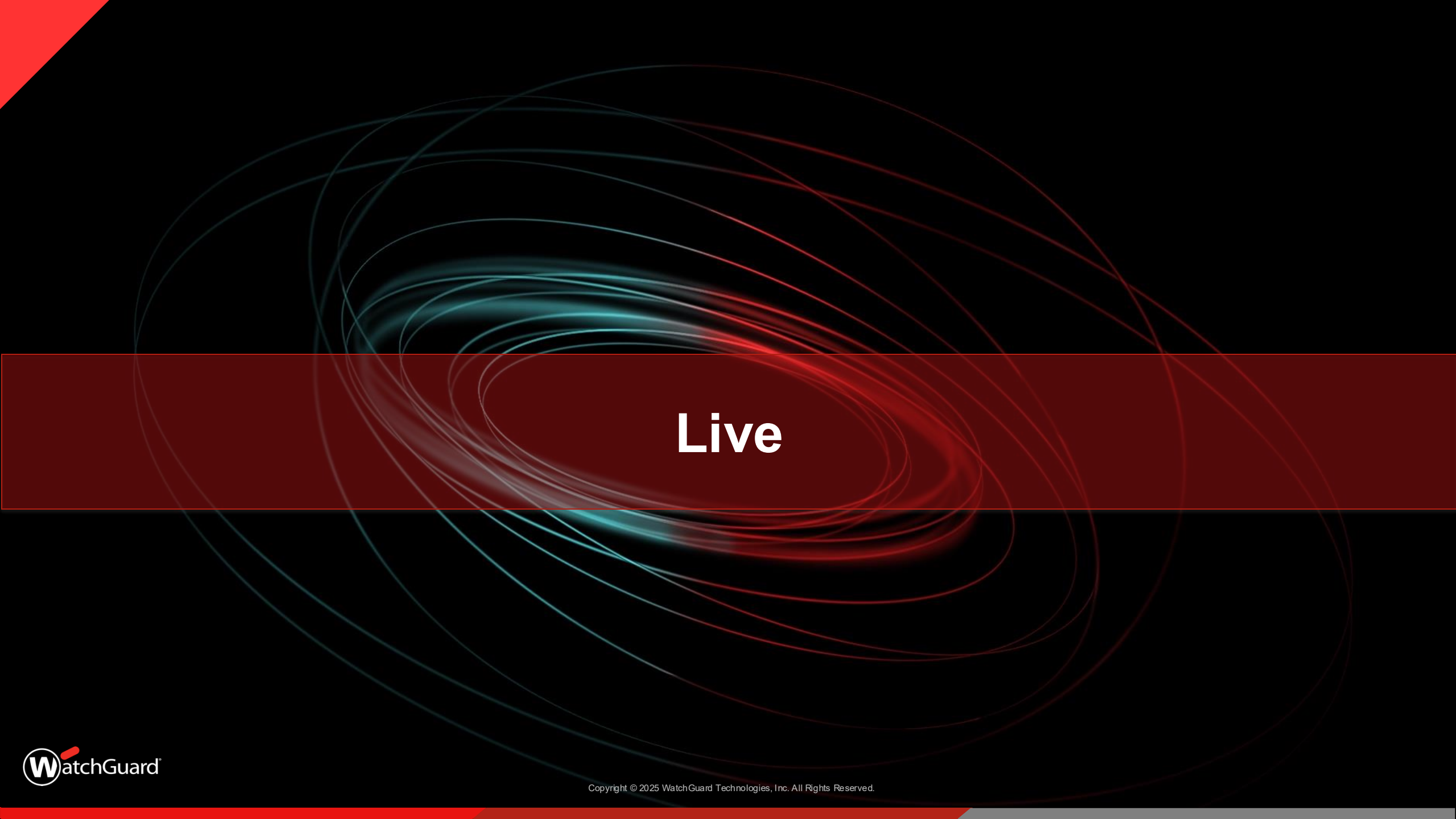
Unified Security Platform

WatchGuard Cloud

- Multi-Tier, Multi-Tenant
- Instanz in Europa und weitere datenschutzrelevante Maßnahmen
- Schnelle und einfache Verwaltung der Sicherheitsfunktionen
- Zero-touch Deployment für Netzwerk-Sicherheit, Endgeräte-Sicherheit und Multi-Faktor Authentifizierung
- Automatisierung und Erleichterung



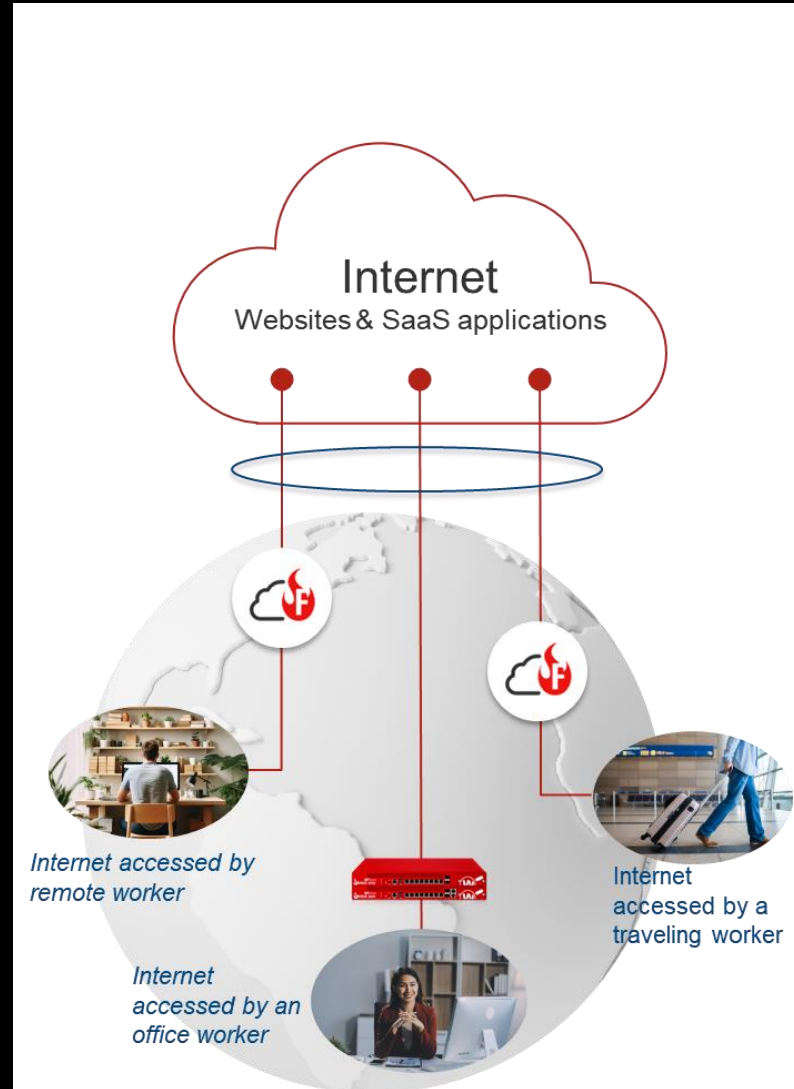
**Simplify Every Aspect of
Security Delivery**



Live

Optimaler Schutz hybrider Infrastruktur

- Network Security
 - Firewalls
 - Wi-Fi Sicherheit
- Endpoint Security
 - Protection
 - Detection & Response
- Identity Security
 - MFA
- WatchGuard Cloud Verwaltung



WatchGuard FireCloud

- Firewall-as-a-Service (FWaaS)
- Secure Web Gateway (SWG)
- User Authentication
- WatchGuard Cloud Verwaltung

FireCloud Internet Access

Firewall as a Service (FWaaS)

-  DNS Filtering
-  Botnet Detection
-  Intrusion Prevention Service (IPS)
-  APT Blocker Cloud Sandboxing
-  TLS Inspection
-  Gateway AntiVirus (GAV)
-  Geolocation Blocking

User Authentication

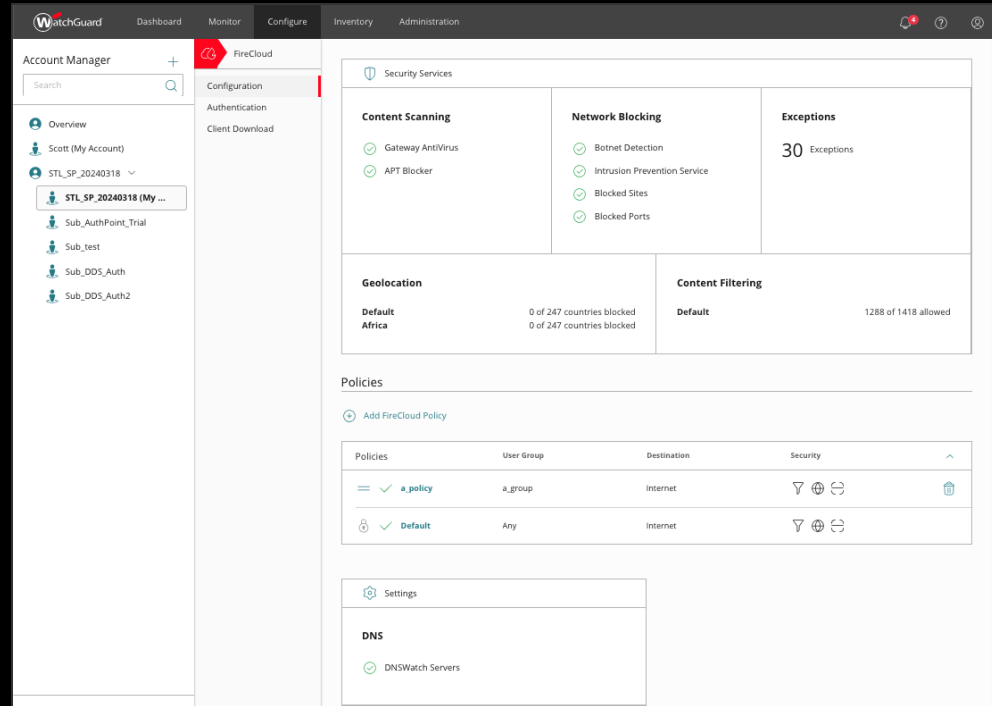
-  Connection Manager
-  Identity Provider (IdP)



Secure Web Gateway (SWG)

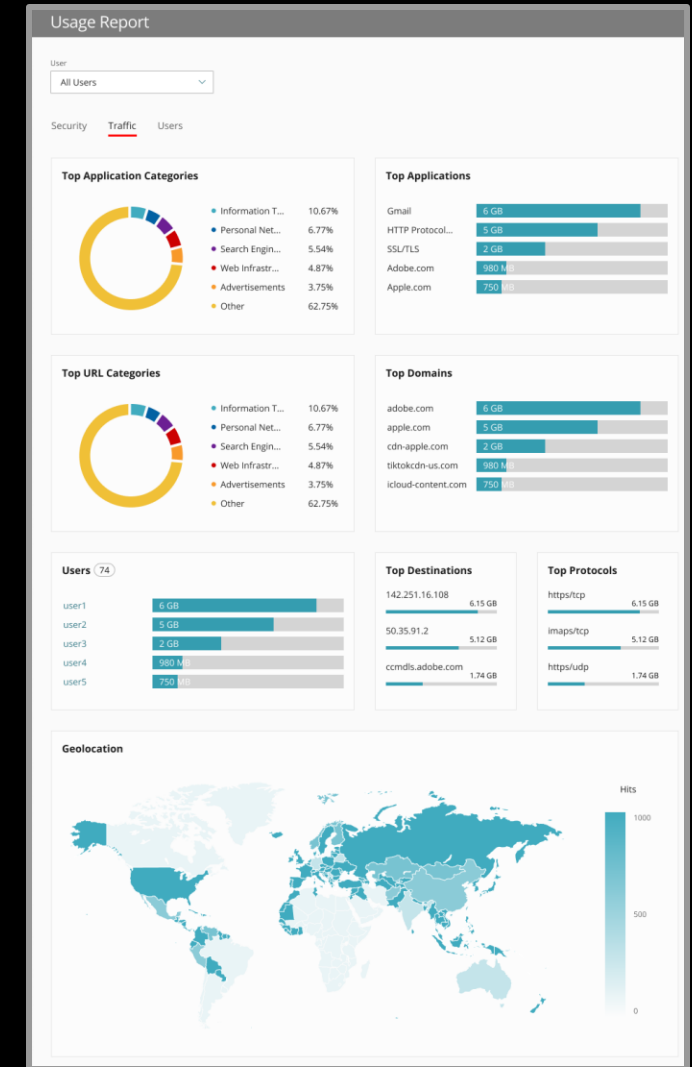
-  WebBlocker URL Filtering
-  Application Control

Einfache Verwaltung



The screenshot shows the WatchGuard FireCloud Configuration page. The left sidebar contains the Account Manager with a search bar and a list of users. The main content area is divided into several sections: Security Services (Content Scanning, Network Blocking, Exceptions, Geolocation, Content Filtering), Policies (Add FireCloud Policy, Table of Policies), and Settings (DNS). The Network Blocking section shows Botnet Detection, Intrusion Prevention Service, Blocked Sites, and Blocked Ports. The Exceptions section shows 30 Exceptions. The Geolocation section shows 0 of 247 countries blocked. The Content Filtering section shows 1288 of 1418 allowed. The Policies section shows a table with columns for Policies, User Group, Destination, and Security.

Policies	User Group	Destination	Security
a_policy	a_group	Internet	Internet
Default	Any	Internet	Internet



The screenshot shows the WatchGuard FireCloud Usage Report page. The left sidebar contains the Account Manager with a search bar and a list of users. The main content area is divided into several sections: Top Application Categories, Top Applications, Top URL Categories, Top Domains, Users, Top Destinations, Top Protocols, and Geolocation. The Top Application Categories section shows a donut chart and a list of categories. The Top Applications section shows a bar chart of top applications. The Top URL Categories section shows a donut chart and a list of categories. The Top Domains section shows a bar chart of top domains. The Users section shows a bar chart of top users. The Top Destinations section shows a bar chart of top destinations. The Top Protocols section shows a bar chart of top protocols. The Geolocation section shows a world map with hits.

Top Application Categories	Percentage
Information T...	10.67%
Personal Net...	6.77%
Search Engin...	5.54%
Web Infrastr...	4.87%
Advertisements	3.75%
Other	62.75%

Top Applications	Usage
Gmail	6 GB
HTTP Protocol...	5 GB
SSL/TLS	2 GB
Adobe.com	980 MB
Apple.com	750 MB

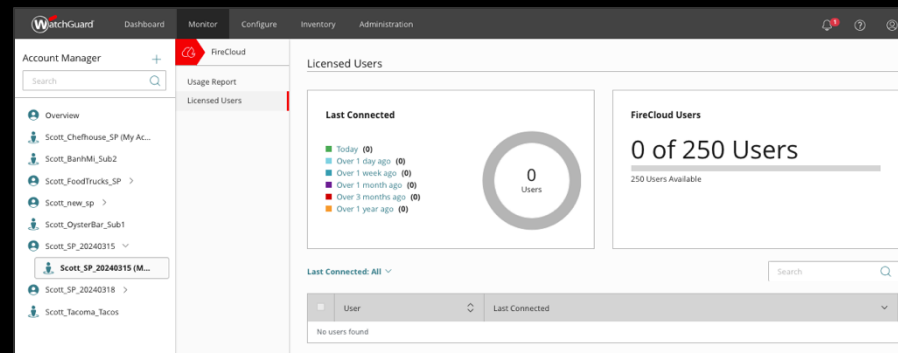
Top URL Categories	Percentage
Information T...	10.67%
Personal Net...	6.77%
Search Engin...	5.54%
Web Infrastr...	4.87%
Advertisements	3.75%
Other	62.75%

Top Domains	Usage
adobe.com	6 GB
apple.com	5 GB
cdn-apple.com	2 GB
tiktokcdn-us.com	980 MB
icloud-content.com	750 MB

Users	Usage
user1	6 GB
user2	5 GB
user3	2 GB
user4	980 MB
user5	750 MB

Top Destinations	Usage
142.251.16.108	6.15 GB
50.35.91.2	5.12 GB
ccndis.adobe.com	1.74 GB

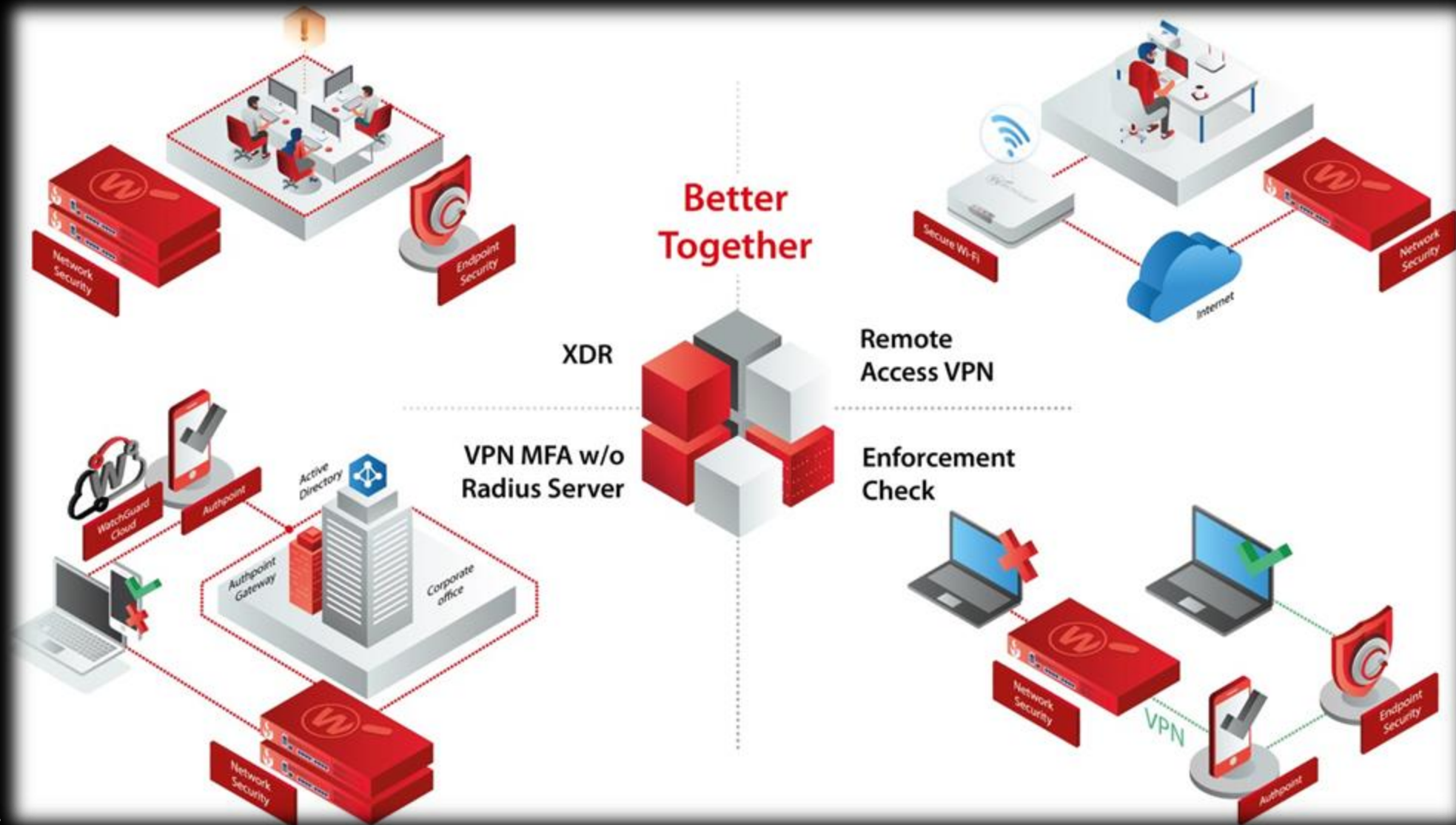
Top Protocols	Usage
https/tcp	6.15 GB
imaps/tcp	5.12 GB
https/udp	1.74 GB



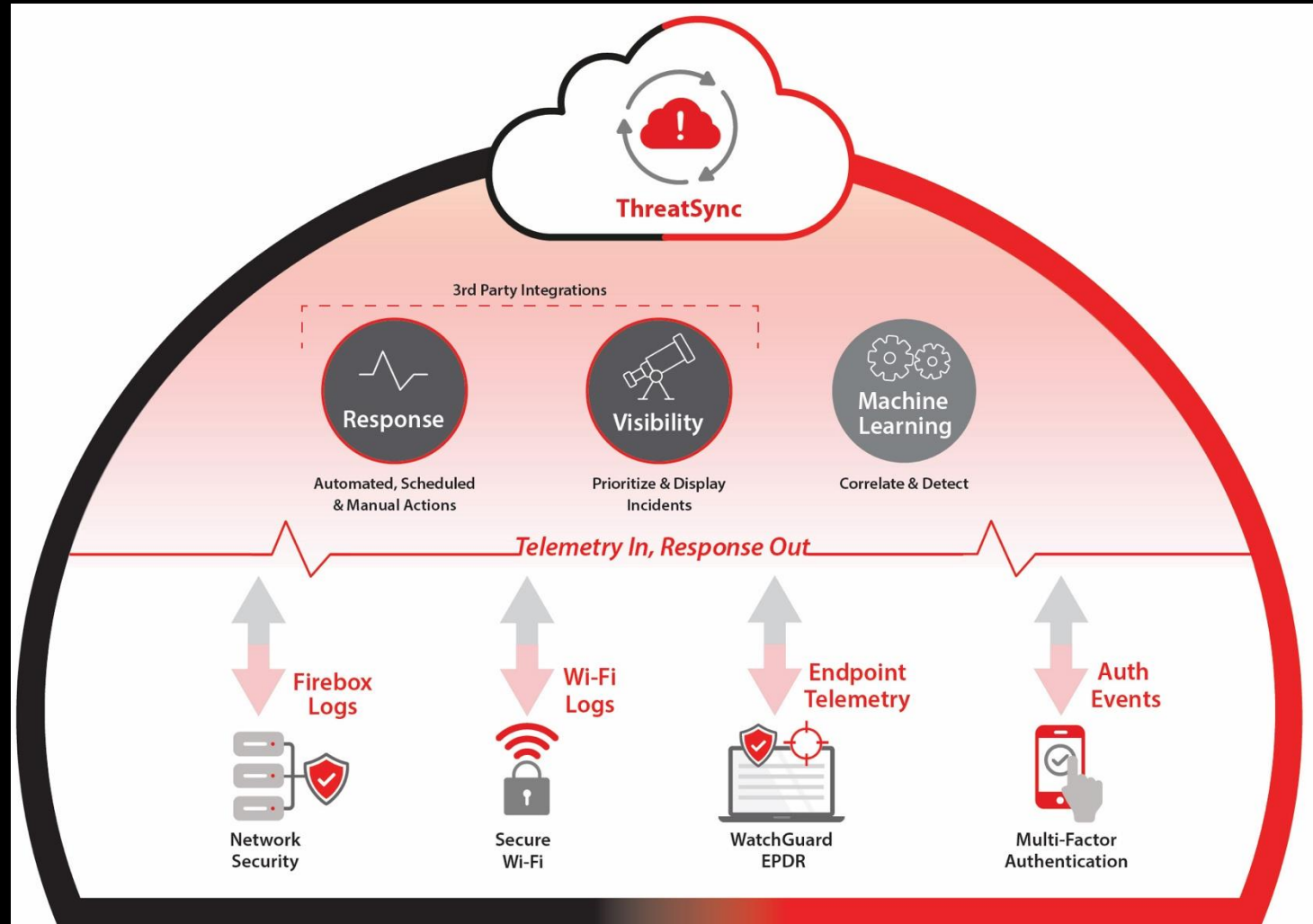
The screenshot shows the WatchGuard FireCloud Licensed Users page. The left sidebar contains the Account Manager with a search bar and a list of users. The main content area is divided into several sections: Last Connected, FireCloud Users, and a table of users. The Last Connected section shows a donut chart and a list of categories. The FireCloud Users section shows a bar chart of top users. The table of users shows columns for User and Last Connected.

User	Last Connected
No users found	

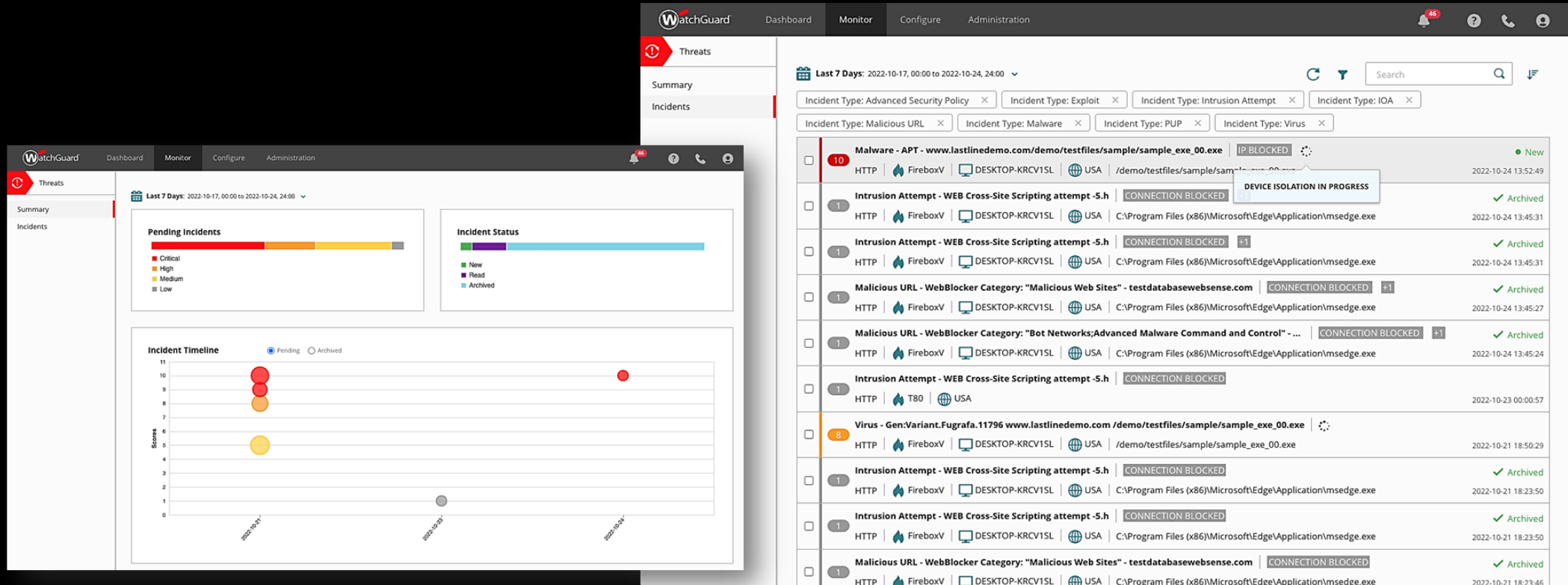
Optimales Zusammenspiel der Lösungen

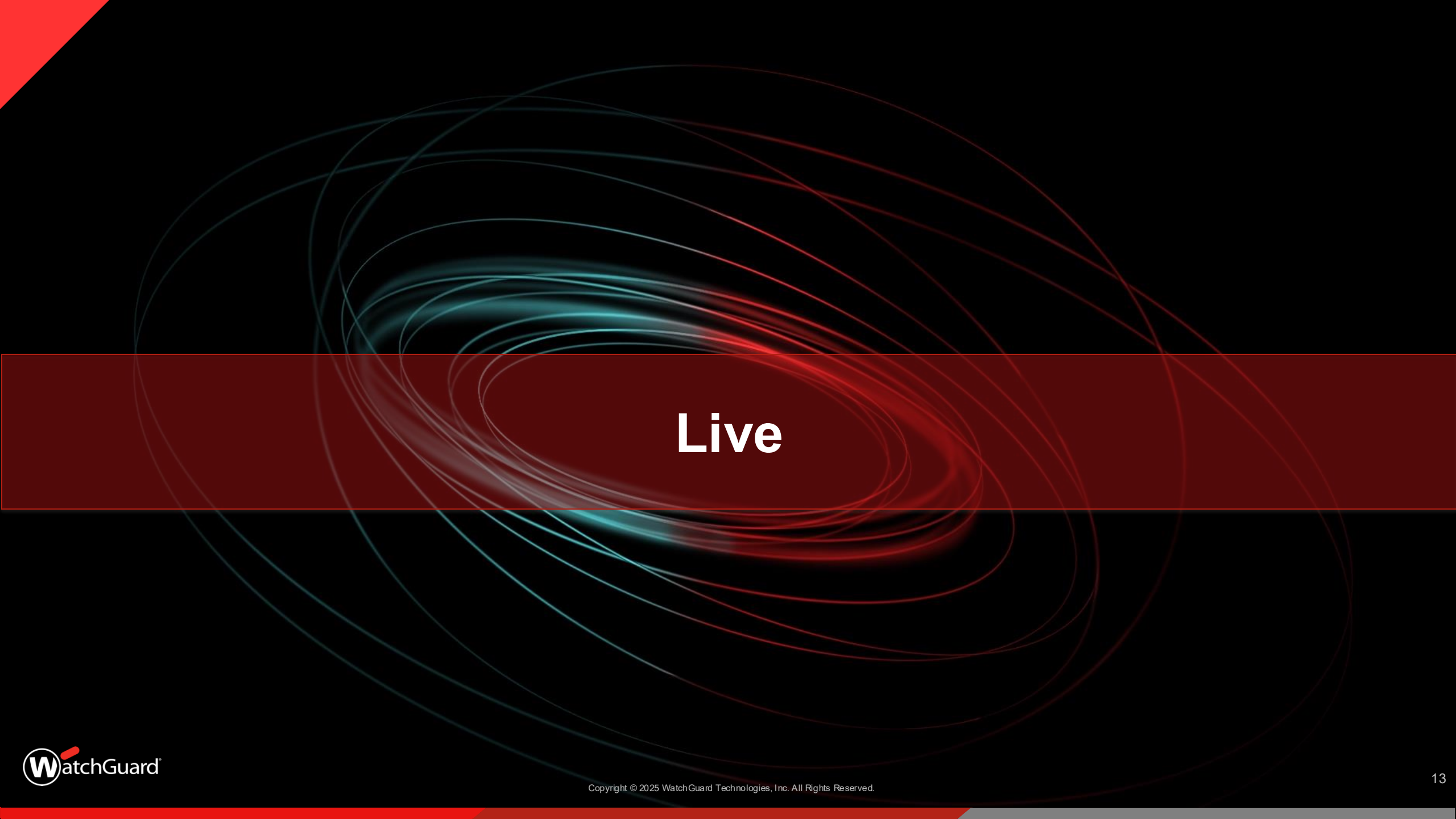


ThreatSync Core



ThreatSync Core



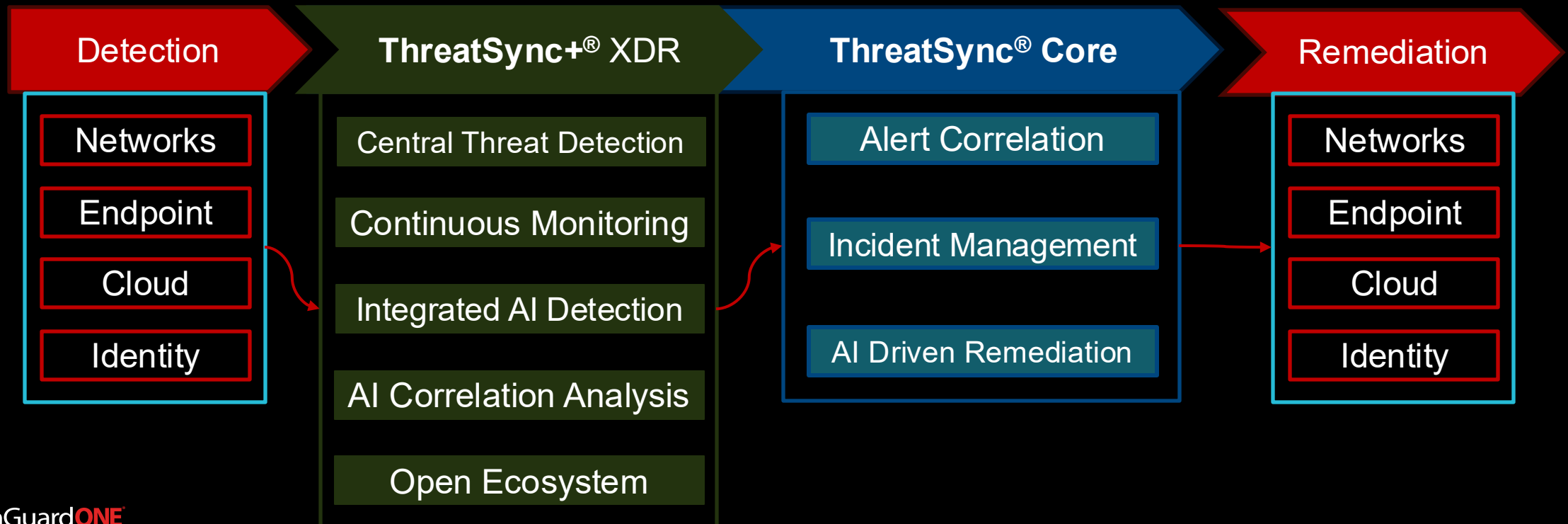


Live

ThreatSync+ über ihr ganzes Portfolio



ThreatSync+® ist eine umfassende, kontinuierliche Sichtbarkeit, die eine einheitliche, offene Korrektur, eine automatisierte, kontinuierliche Compliance und eine zentralisierte, ganzheitliche Erkennung bietet.

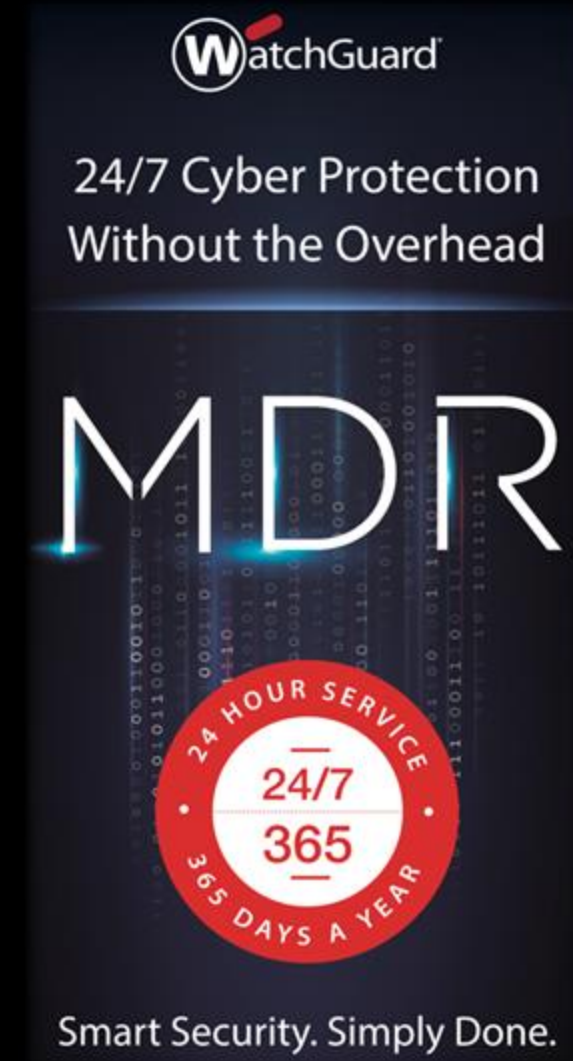


WatchGuard Managed Detection & Response

Entwickelt, damit **unsere Partner-Community** MDR-Dienste anbieten kann, ohne ein eigenes SOC zu benötigen

Bietet **rund um die Uhr** Überwachung, Bedrohungsjagd, Untersuchung, Eindämmung, Reaktionsrichtlinien und Sicherheitsbeurteilungen

24x7x365 durch ein Team von **Cybersecurity-Experten** des WatchGuard SOC, das sich auf IOAs konzentriert und nicht nur auf die Reaktion auf IOCs



The graphic features the WatchGuard logo at the top, followed by the text "24/7 Cyber Protection Without the Overhead". Below this, the letters "MDR" are displayed in a large, glowing font. A red circular seal in the center contains the text "24 HOUR SERVICE", "24/7", and "365 DAYS A YEAR". At the bottom, the slogan "Smart Security. Simply Done." is written.

WatchGuard

24/7 Cyber Protection
Without the Overhead

MDR

24 HOUR SERVICE
24/7
365 DAYS A YEAR

Smart Security. Simply Done.

WatchGuard MDR



Bereitstellung nach Maß



Do-It-Yourself (DIY)
"Do it myself"

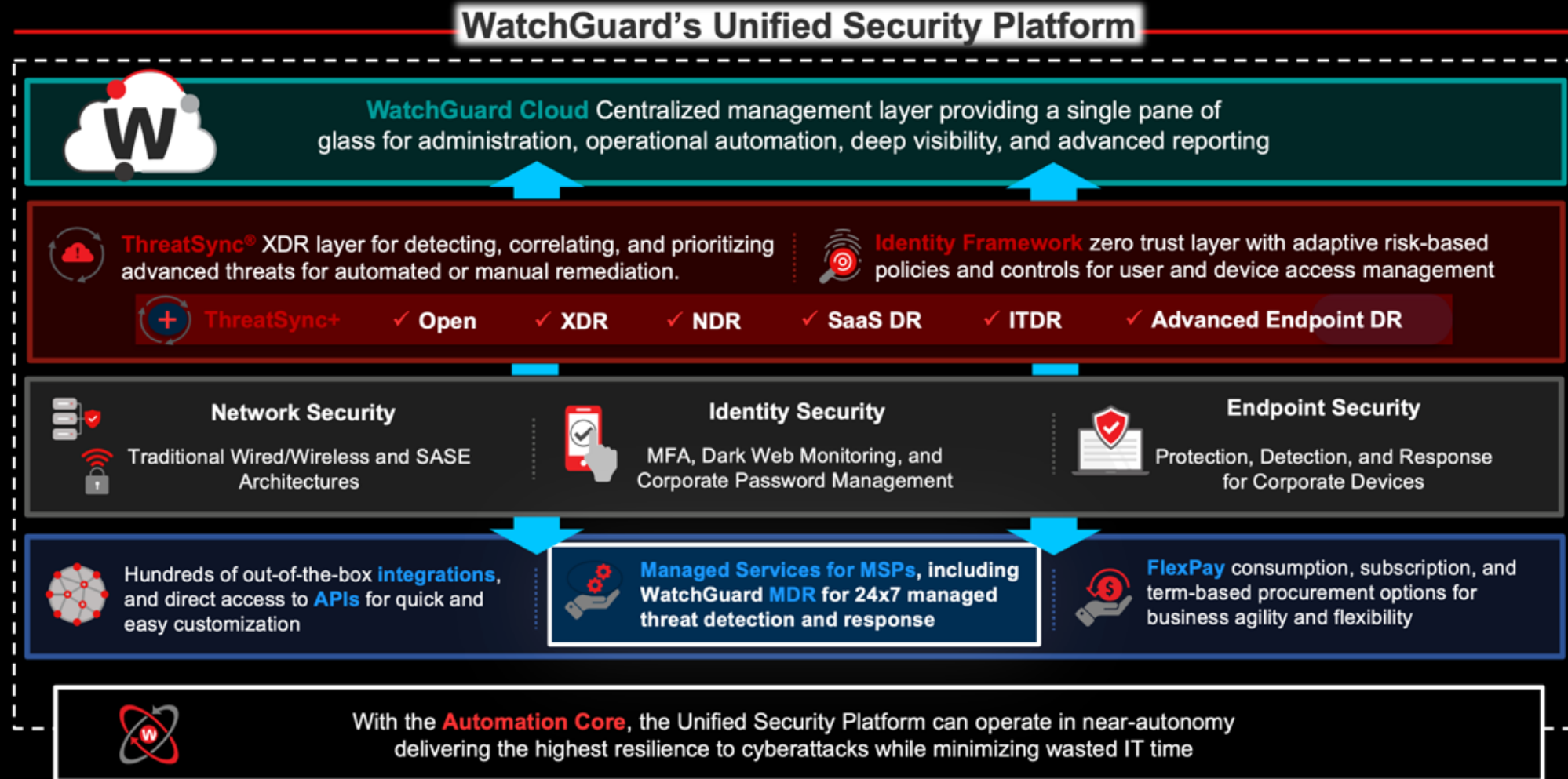


Schlüsselfertig
"Do it for me"



Hybrid
"Do it with me"

WatchGuard's USP



Q&A



Vielen Dank