

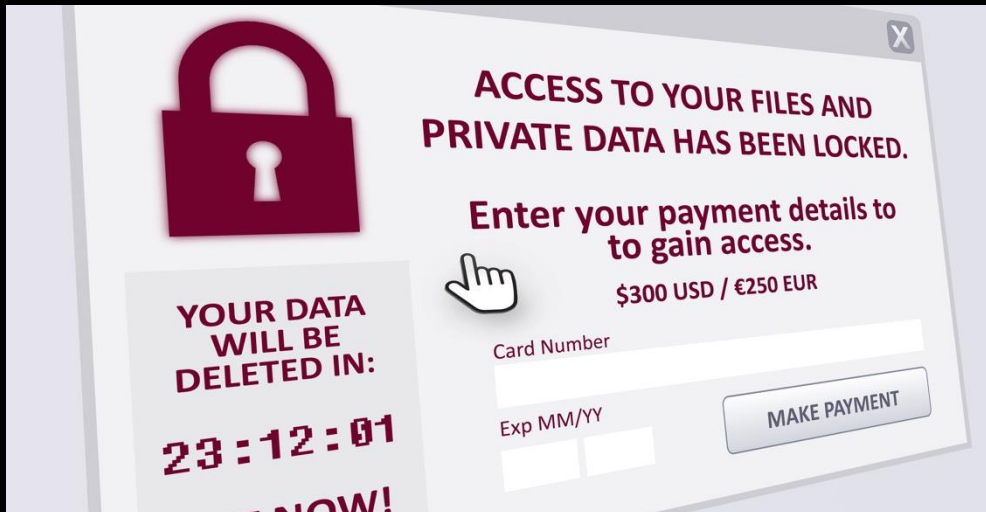


Real Security for a Real World

*Protect your modern hybrid IT-Infrastructure
with WatchGuard's Unified Security Platform*

Real Security
for the **Real World**

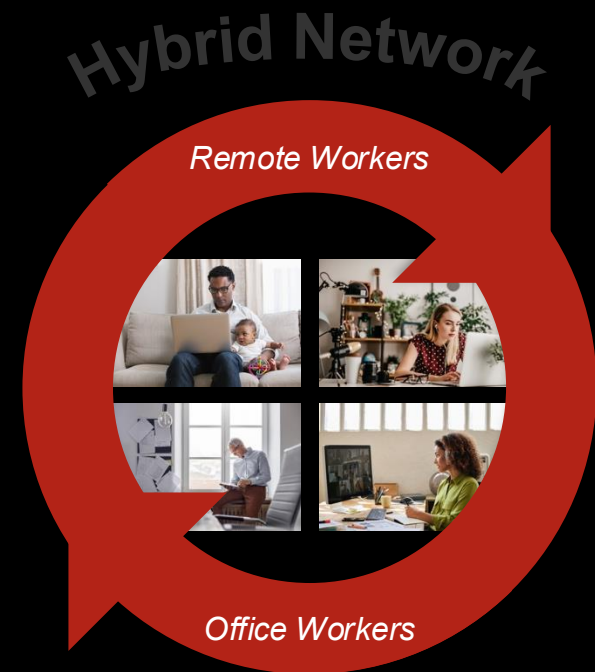
Real Threats



The Network Didn't Change – How We Work Did

Our approach to security must also change

- The new perimeter is where work is being done
- The network protection of a firewall is missing for many workers
- We need to defend against:
 - > Increased risk of unauthorized or overprivileged access
 - > Unsecured remote networks (Ex. home, café, hotel, etc.)
 - > Technology use without IT admin knowledge (Shadow IT)
 - > Misconfigurations resulting from adjustment to a hybrid network
 - > Attackers target individuals instead of corporations



Real Example – Akira Ransomware

- Ransomware as a Service
- Stolen or Brute-forced Credentials
- Access via VPN
- Scanned network
- Access to 2 servers
- Privilege Escalation
- Remotely encrypted files via SMB with Akira.exe

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 detailed description and also many helpful recommendations in this advisory: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>)

Security Concepts

WatchGuard provides effective solutions to solve the security needs in modern hybrid scenarios



Network Security

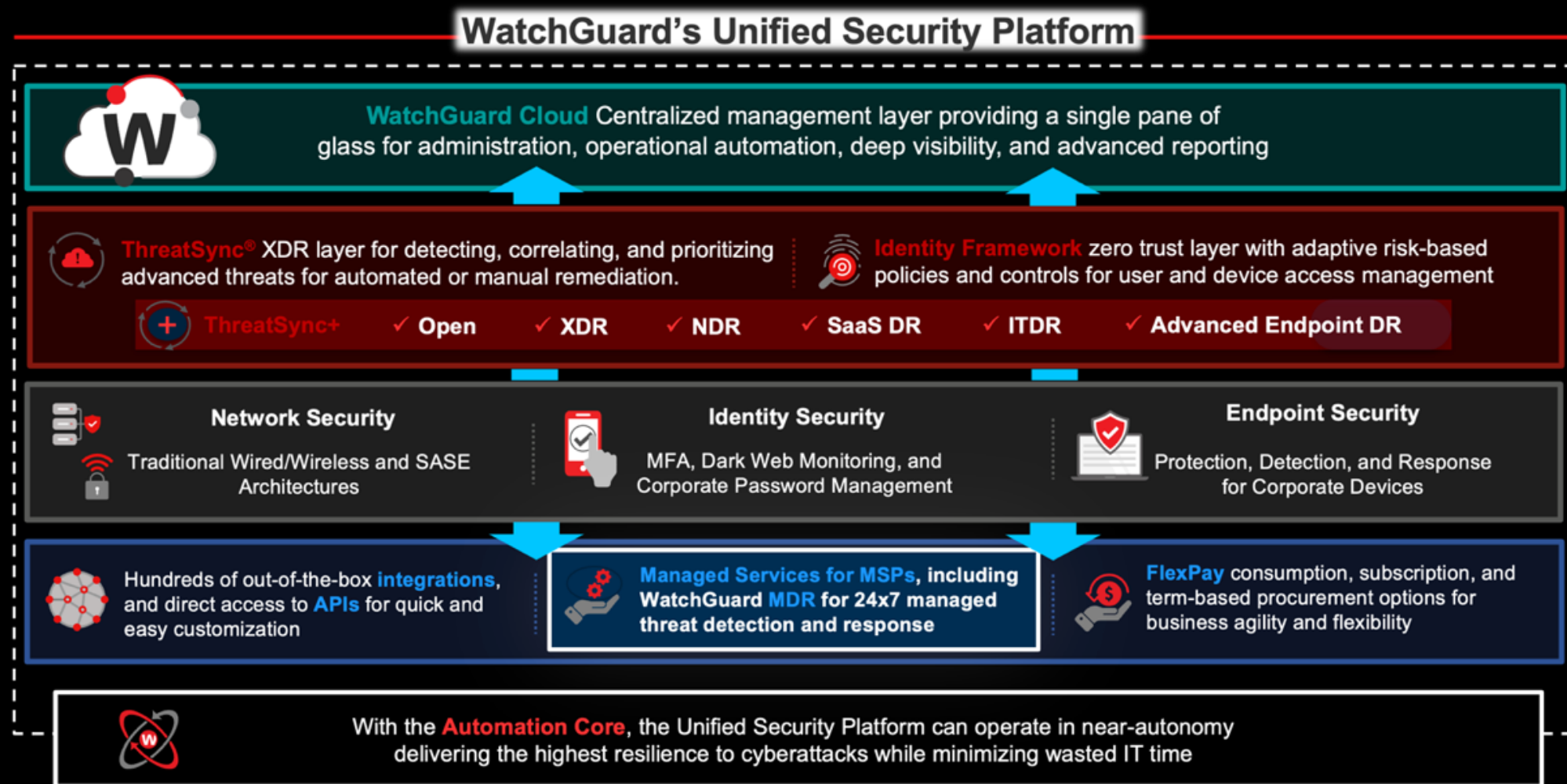


Identity Security



Endpoint Security

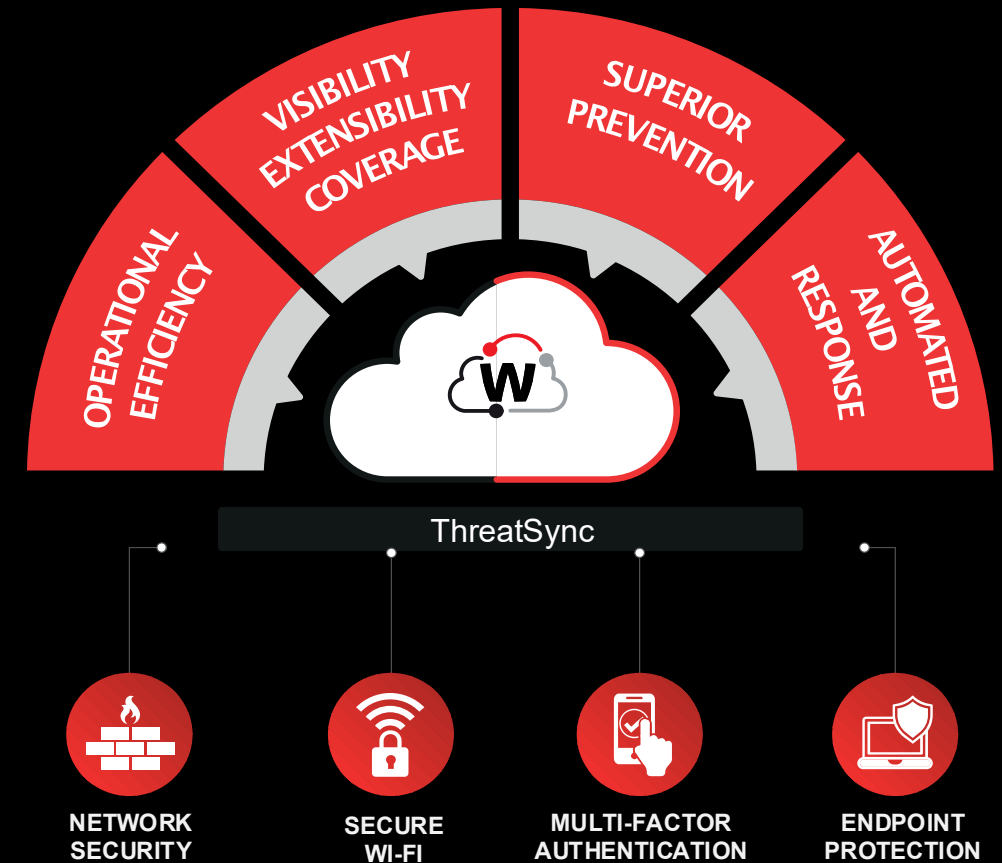
WatchGuard's USP



Unified Security Platform

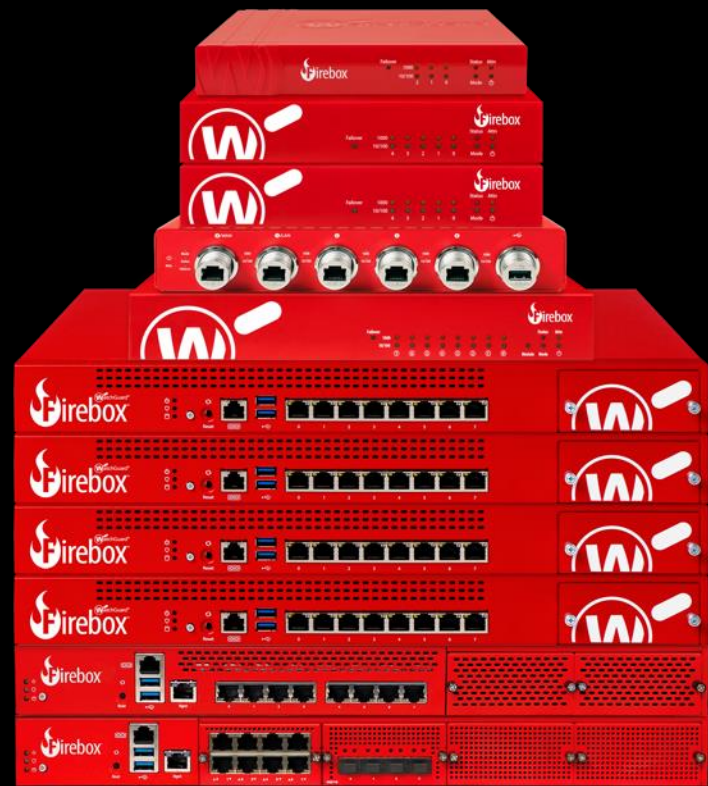
WatchGuard Cloud

- Multi-Tier, Multi-Tenant
- European instance – GDPR compliance
- Manage security settings in easy and efficiently
- Zero-touch Deployment for Network-, Endpoint- and Identity-Security
- Built-in automation
- API Framework



**Simplify Every Aspect of
Security Delivery**

Network Security



Account Manager

Search

Overview

WatchGuard Cloud Demo (My ...)

Acme Manufacturing

California

Oregon

Washington

Demo-M500-CBD5

FBv-Cluster-Demo-5B...

T15W_RapidDeploy

Avenger Information Tech

Customer - Total Security

Power IT

Prime Healthcare

Pumping Up Gyms

Pusheen Cafe

Safety Insurance

Spackler Landscaping (Delega...

Devices

Device Summary

Logs

Dashboards

Executive Dashboard

Security Dashboard

Subscription Dashboard

Threat Map

Firewatch

Policy Map

Web

Traffic

Services

Device

Detail

Compliance

Per Client Reports

Filtered On: All Logs

Top Blocked Countries

Name	Hits
Russian Federation (RUS)	148
China (CHN)	142
United States (USA)	9

Top Blocked Botnet Sites

Name	Hits
204.11.56.48	3
192.3.211.103	1

Top Blocked Destinations

Name	Bytes	Hits
52.109.6.42	2 KB	17
52.109.2.0	1 KB	9
52.109.20.75	960	8
64.94.121.170	0	10,886
10.148.52.105	0	4,124
10.148.52.255	0	3,436

Top Blocked Advanced Malware (APT)

Name	Hits
/demo/kernel-driver-64bit/sample	1

Top Blocked Clients

Name	Bytes	Hits
HealthMailbox2d577b@wgdemo.local	4 KB	34
Administrator@wgdemo.local	0	8,051
10.148.52.101	0	5,299
10.148.52.14	0	2,723
10.3.2.100	0	1,801
10.148.52.6	0	1,400
64.94.121.146	0	630
64.94.121.148	0	630
rocky@wgdemo.local	0	592
woody@wgdemo.local	0	555

Top Blocked URL Categories

Name	Hits
Sex	38
Games	6

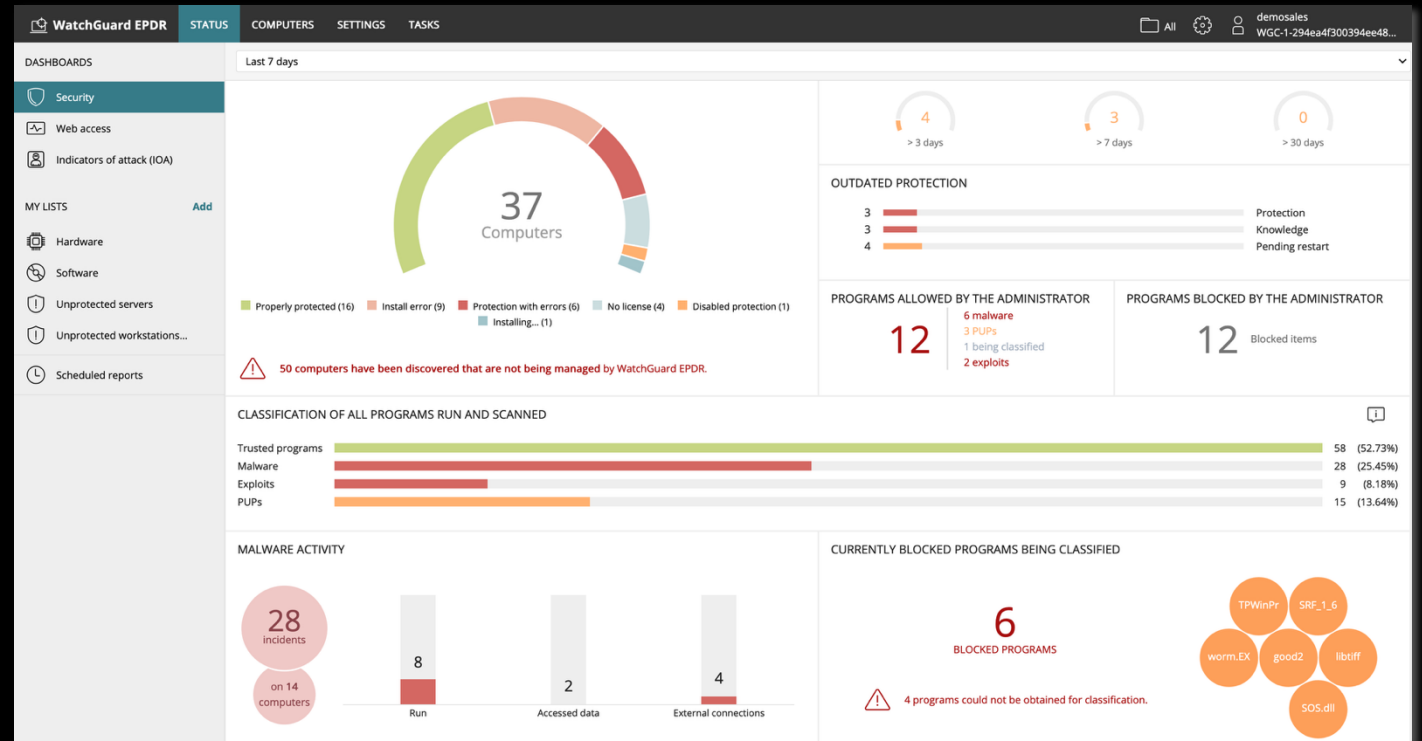
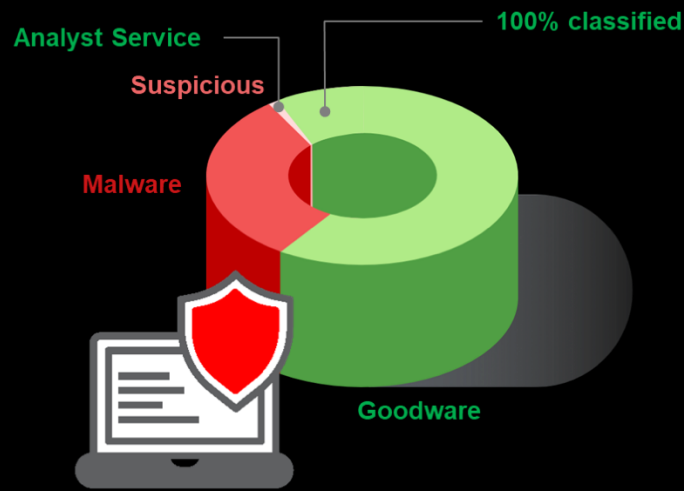
Endpoint Sicherheit with Zero-Trust



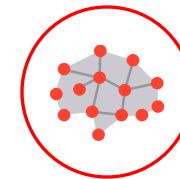
EDR | Endpoint
Detection &
Response



EPDR | Advanced EPDR
Endpoint Protection,
Detection & Response



Unique Protection Model: A Layered Protection



Zero-Trust model: a Layered Protection

ENDPOINT LAYERS

Layer 1 / Signature files, Collective Intelligence and heuristic technologies

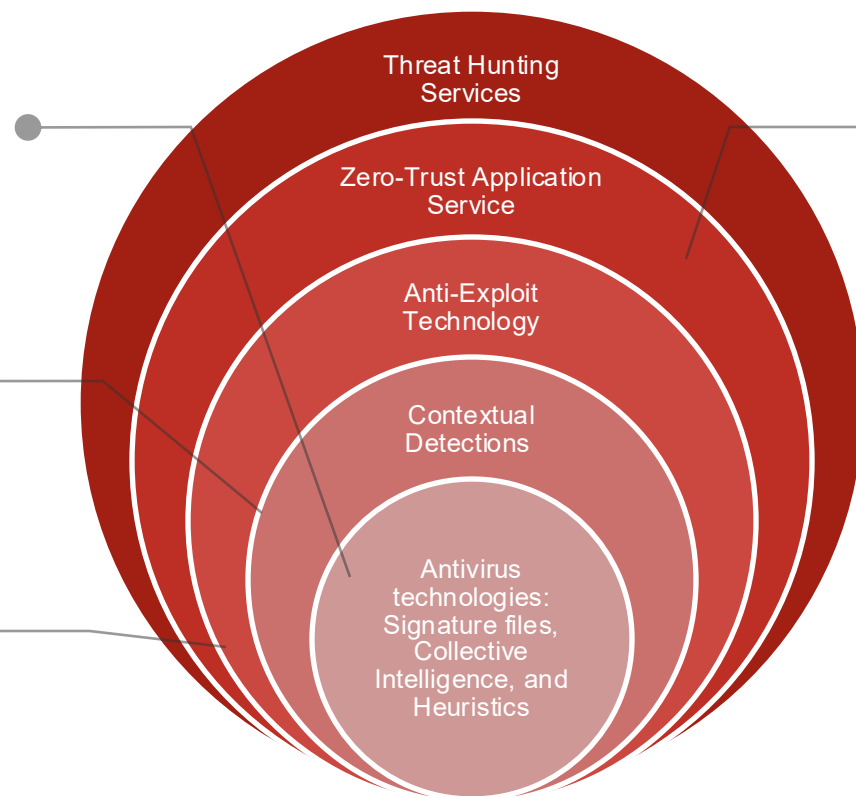
Effective, optimized technology to detect known attacks

Layer 2 / Contextual detections

They enable us to detect malwareless and fileless attacks

Layer 3 / Anti-exploit technology

It enables us to detect fileless attacks designed to exploit vulnerabilities



CLOUD-NATIVE LAYERS

Layer 4 / Zero-Trust App Service

Provides protection if a previous layer is breached, stops attacks on already-infected computers, and stops lateral movement attacks inside the network

Layer 5 / Threat Hunting services

They enable us to detect compromised machines, early-stage attacks, and suspicious activities

Secure Wi-Fi



🔥

Devices

Device Settings

Device Configuration

Deployment History

Device Password

AP432-EG

Monitor

Configure

Connected

↻

Reboot Device

🔌

Flash Device LEDs

📦

Upgrade Firmware to v2.4.4-0.B694615 (Beta - E

Device Information

License Details

Name

AP432-EG

Model

AP432

Description

On top of the Shelf

Version

2.2.22-0.B691305

Serial Number

A030027362052

Public IP

87.178.192.218

Local IP

192.168.100.12

MAC Address

00:01:21:30:60:2A

WatchGuard USP Wi-Fi

Status

Valid

Expiration

2024-07-15

Data Retention

30 Days

Radio Details

2.4 GHz

Channel

11 (20 MHz)

Transmit Power

12 dBm

JSP-Home

Edit

Configuration Details

Subscribed Devices

Deployment History

Wi-Fi Networks

SSIDs

Unsichtbar Wurrwarr

WPA3/WPA2 Personal WPA2 Personal

Radio Settings

Add 2.4 GHz

Add 5 GHz

Settings

Add Device Settings

Advanced Settings

✓

Airspace Monitoring

✗

Syslog Server

✗

SNMP

Authentication

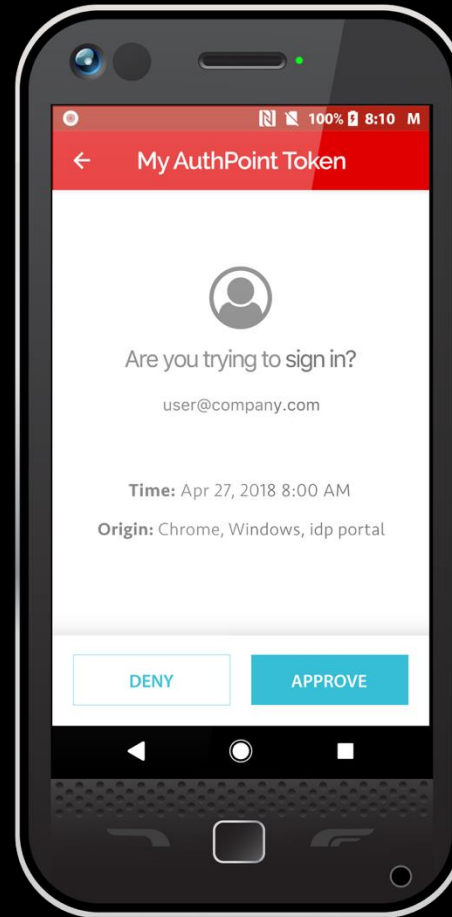
Domains

Add Authentication Domains

WatchGuard AuthPoint MFA

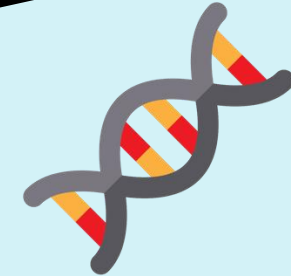
2 or more factors

- **Something you know**
(Password, PIN)
- **Something you have**
(Token, Mobile App)
- **Something you are**
(Fingerprint, Face)

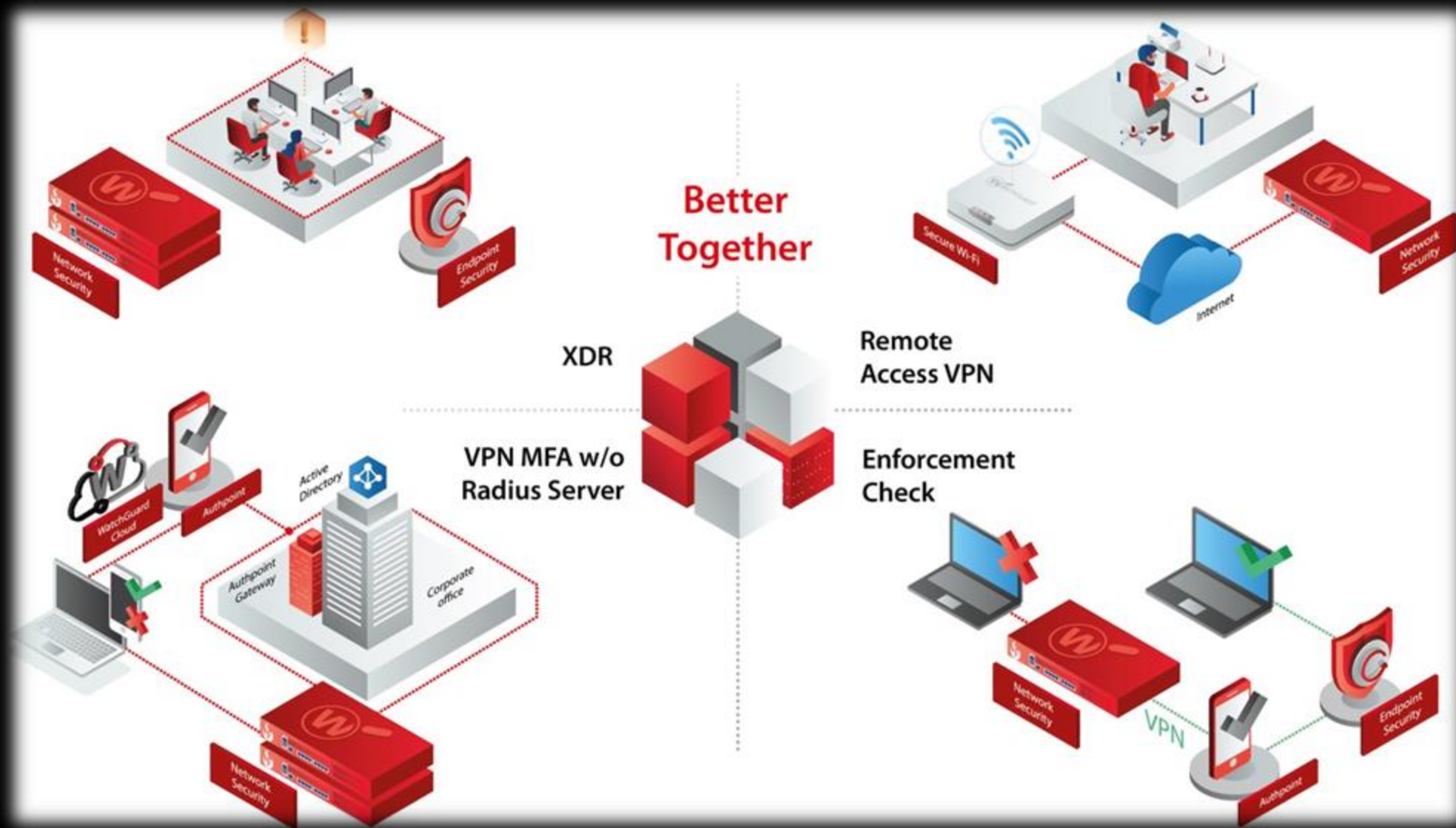


AuthPoint-Faktoren:

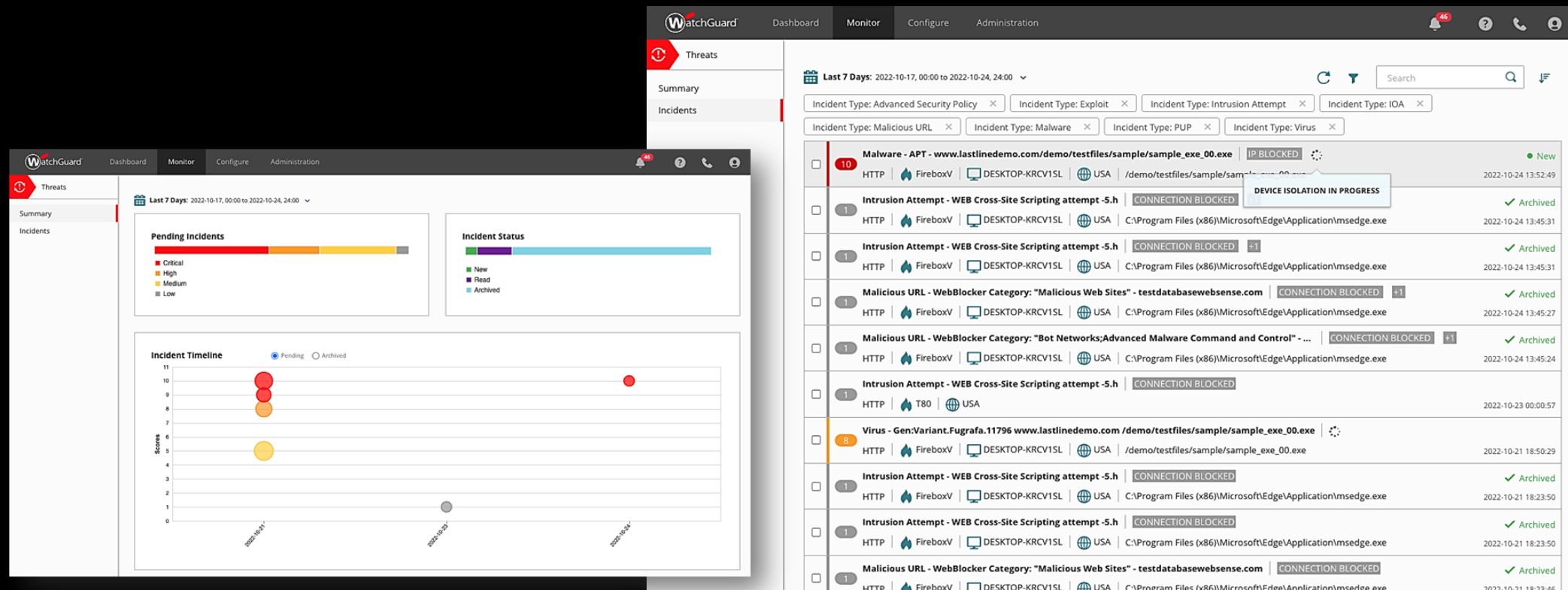
1. Password
2. Proof in mobile App
3. Handy-DNA
4. Fingerprint / Face Recognition



Better Together



ThreatSync Core



Live Demo

We Need an Effective Defense for Hybrid Networks

Introducing Secure Access Service Edge (SASE)

- Combines multiple network and security functions into a single Cloud-based service
- Simplifies IT infrastructure and improves security posture
- Delivers secure access to applications and data



Remote worker accessing something public



Connecting offices



Remote worker accessing something private



Office worker accessing something public

Key SASE Components

The solution building blocks

1. Firewall-as-a-Service (FWaaS)

Access control and inspection of all traffic; General security at the network level

2. Secure Web Gateway (SWG)

Protections from Internet threats and adherence to corporate internet usage policy; Specialized web security

3. Software-Defined Wide Area Network (SD-WAN)

Connect the office to key services by managing the WAN and steering traffic between multiple WAN connections

4. Zero Trust Network Access (ZTNA)

Secure service that connects primarily remote users to services hosted by the organization

5. Cloud Access Security Broker (CASB)

Policy and governance of SaaS applications, including protection and control of access to data; Specialized SaaS security

*Remote worker accessing
something public
(FWaaS + SWG)*



*Connecting offices
(SD-WAN)*



*Remote worker accessing
something private
(FWaaS + ZTNA + CASB)*



*Office worker accessing
something public
(FWaaS + SWG)*



Introducing WatchGuard FireCloud



FireCloud Critical Use Case Coverage



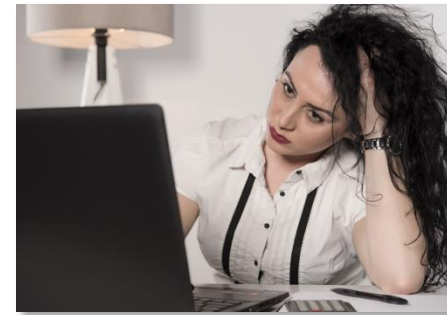
Secure Remote & Hybrid Work

- Continuous security allows employees to work securely from any location, protecting from web-based threats on unmanaged networks
- Boosts productivity, protects against online threats, minimizes data breaches, ensures compliance, safeguards brand reputation, and reduces IT workload.



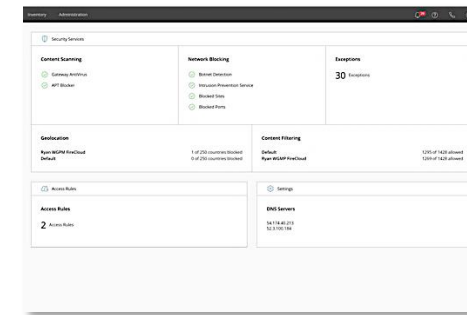
Secure Access to Cloud & Private Resources

- Enforces identity-based policies and traffic inspection so users can safely connect only to authorized SaaS and public cloud applications
- Seamless, identity-based access to internal apps (e.g., finance, HR, CRM) without exposing them to the Internet.



Modernizing Legacy VPN Infrastructure

- Replace VPNs with secure, zero trust, app-level access to eliminate exposed ports, shrink the attack surface, and block lateral movement
- Retire tunnels, firewall rules, and legacy VPN overhead to cut support costs, simplify management, and improve user experience.



Centralized Policy Enforcement Across Devices and Locations

- Centrally manage and enforce consistent security and access policies regardless of user location or device.
- Simplifies operations, ensures compliance, and eliminates gaps in protection caused by multi-product, decentralized setups.

Security is Our Differentiator

Firewall as a Service (FWaaS)

DNS Filtering

TLS Inspection

Botnet Detection

Gateway AntiVirus (GAV)

Intrusion Prevention Service (IPS)

Geolocation Blocking

APT Blocker Cloud Sandboxing

User Authentication

Connection Manager

Identity Provider (IdP)

Secure Web Gateway (SWG)

WebBlocker URL Filtering

Application Control



How FireCloud Internet Access Works

- 1 Login/Logout
- 2 User sessions and Policies Sync
- 3 User Traffic (Encrypted)

Remote worker
accessing
something public



FireCloud PoP
(with Security Services)



WatchGuard Cloud
(Authentication and Authorization Service + Policy Store)

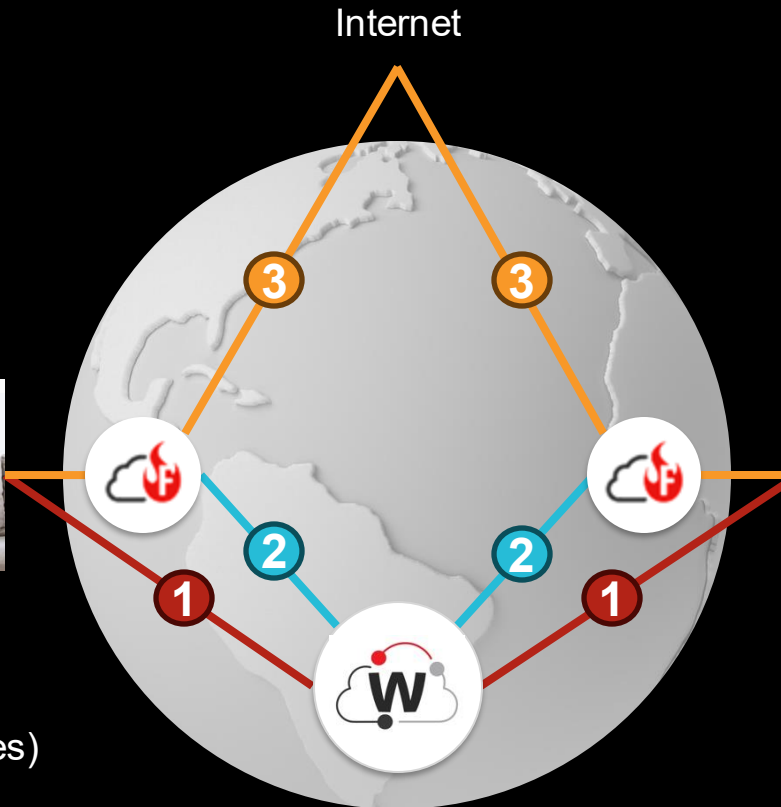
How FireCloud Internet Access Works

- 1 Login/Logout
- 2 User sessions and Policies Sync
- 3 User Traffic (Encrypted)

Remote worker
accessing
something public



FireCloud PoP
(with Security Services)



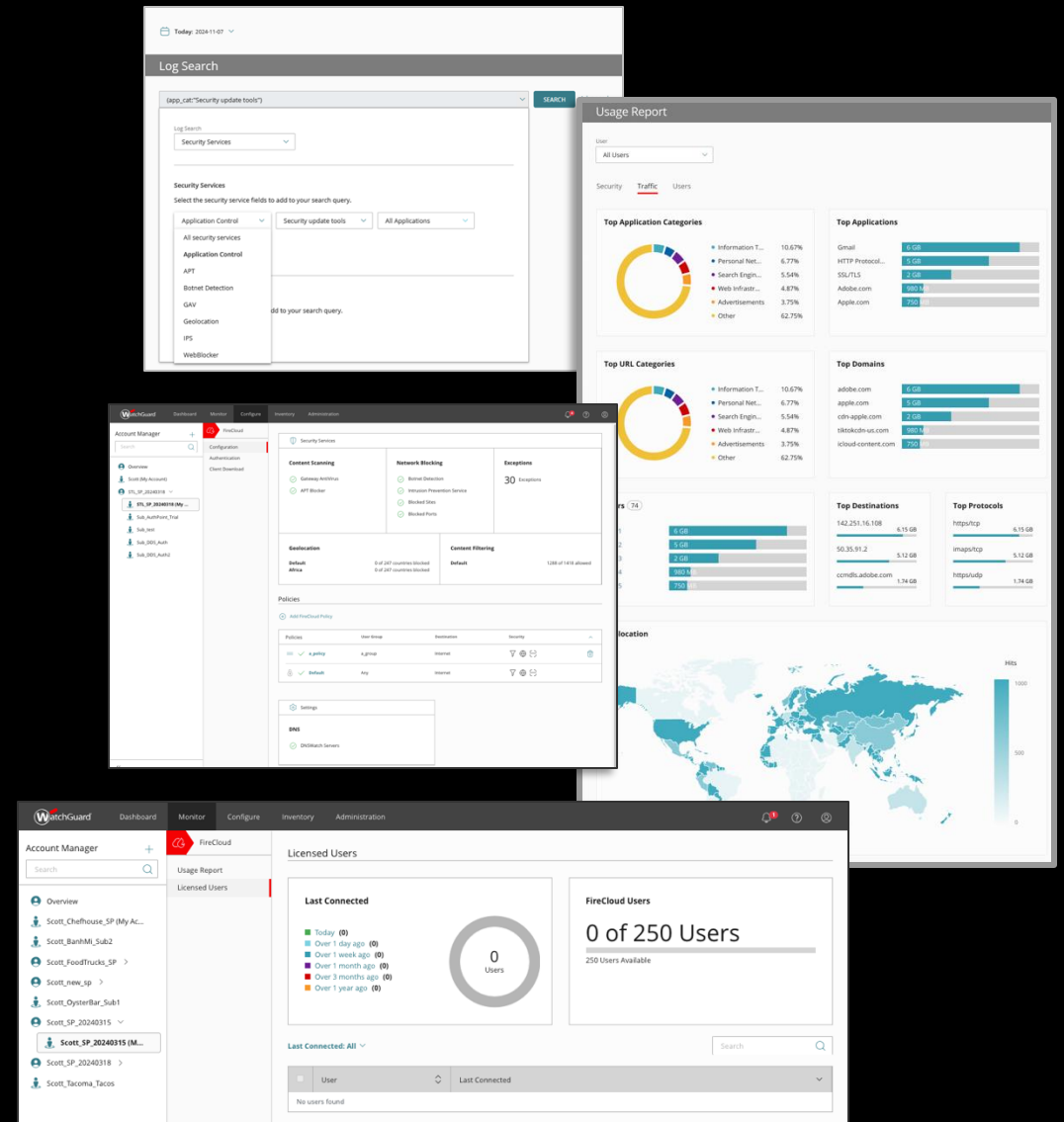
Remote worker
accessing
something public
while traveling

WatchGuard Cloud
(Authentication and Authorization Service + Policy Store)

Ease of Use

Simple to set up and manage

- Access Rules and Configuration
 - Primary Focus on the Who, Not the What
 - Configuration Interface and Terminology Consistent with Cloud-Managed Firebox
 - TLS Certificate Installed by Connection Manager
 - Simplified Log Search Interface
 - First-Time User Trial Wizard
- Licenses are activated/allocated like any other WatchGuard product
 1. Connect the user accounts
 - SAML integration for Identity Provider (IdP) or set up local accounts
 2. Configure security policies
 - Almost identical to Cloud-managed Firebox
 3. Install the FireCloud Connection Manager client
 - Deploy using RMM tools



In Beta Now – FireCloud Total Access

FireCloud Total Access Beta

This beta introduces a new FireCloud license – Total Access. With Total Access, you can give FireCloud users access to local resources on the company network without a VPN.

FireCloud Total Access includes all current FireCloud features.

 Private Resources

Private Resources

2 Gateways

10 Resources

Private Resources

+ Add FireCloud Gateway

JSP-At-Home

VMWare ESXi

5 Resources

FireCloud Gateway Homeoffice

Edit Details | Delete Gateway

Universe-DMZ-Network

VMWare ESXi

5 Resources

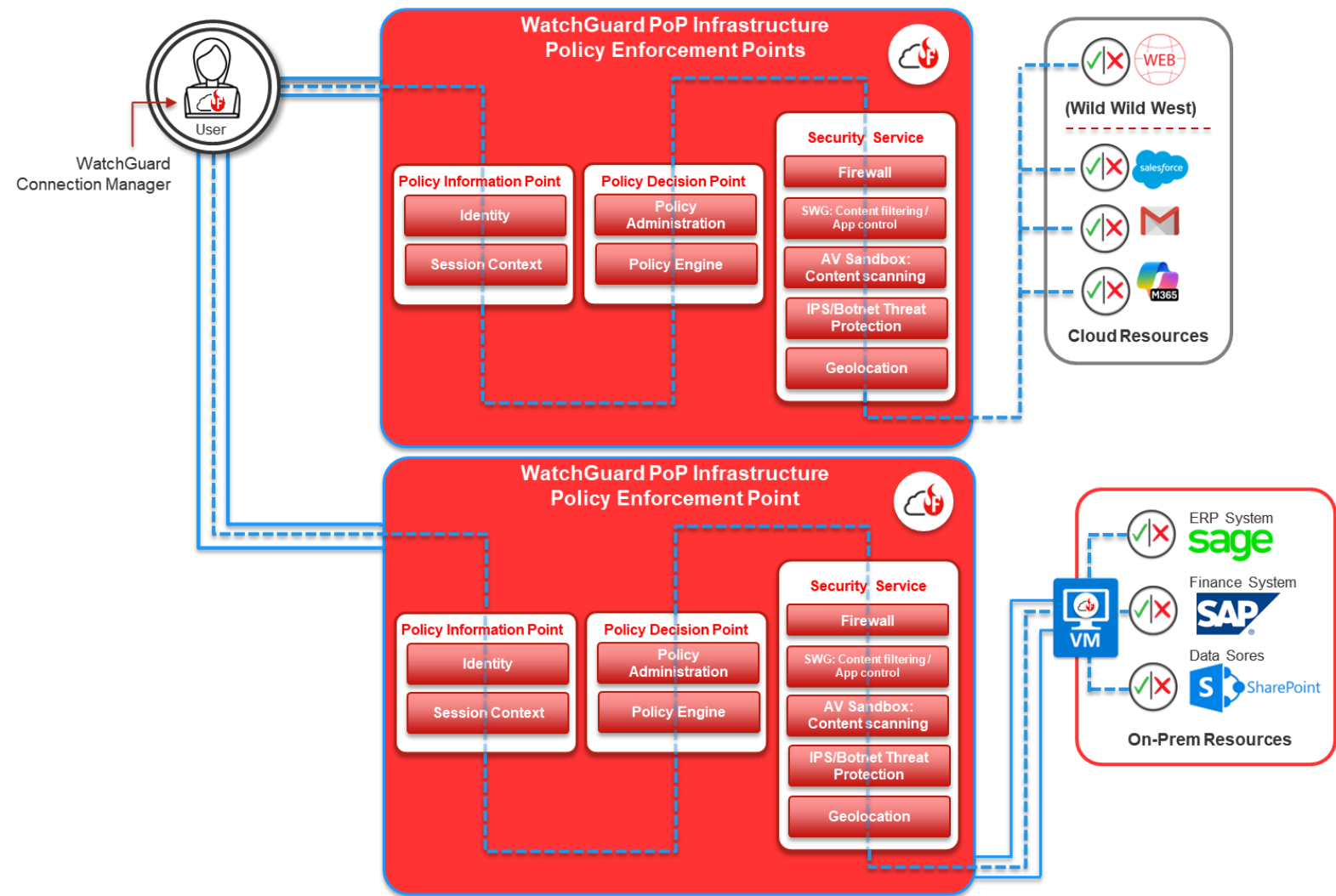
Edit Details | Delete Gateway

+ Add Resource

Search

	Resource		FQDN		IP Address		Port/Protocol
☐	dmz-server.universe.it-lab.cloud	⋮	dmz-server.universe.it-lab.cl...		192.168.237.11		TCP ICMP 22
☐	proxmox.universe.it-lab.cloud	⋮	proxmox.universe.it-lab.cloud		167.235.115.43		TCP 8006
☐	earth.universe.it-lab.cloud-SMB	⋮	earth.universe.it-lab.cloud		192.168.224.10		SMB
☐	earth.universe.it-lab.cloud	⋮	earth.universe.it-lab.cloud		192.168.224.10		TCP ICMP UDP 3389 3389
☐	mars.universe.it-lab.cloud	⋮	mars.universe.it-lab.cloud		192.168.225.11		TCP UDP 3389 3389

Protects Users Accessing On-premise & Cloud Resources



Live

Real Security for the Real World



Questions?
Thank You!