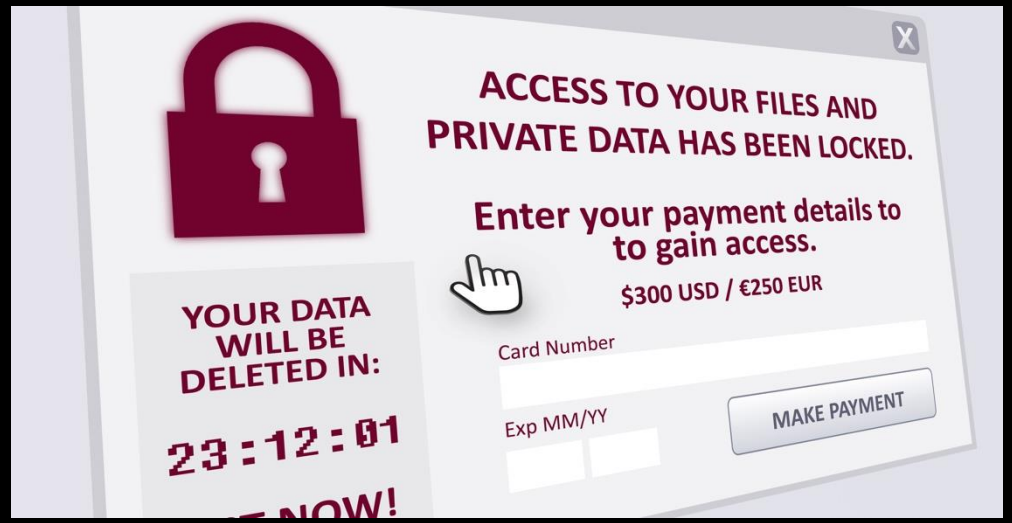
Real Security for a Real World

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

Real Security for the Real World

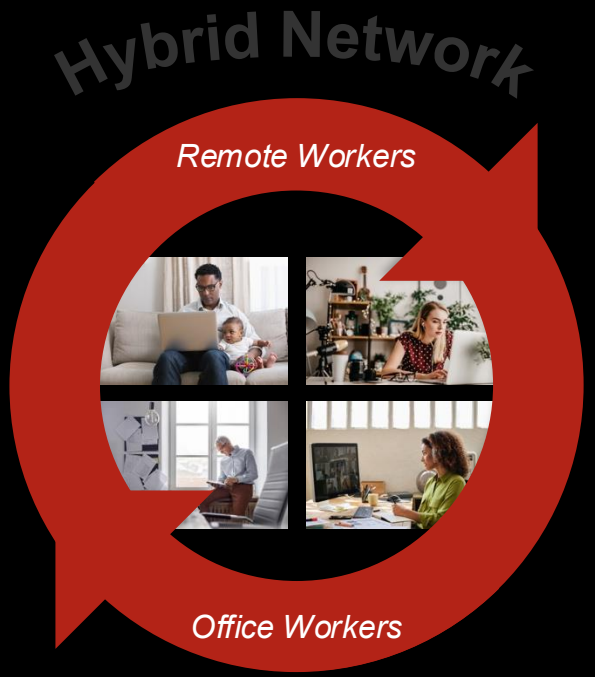
Real Threats



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

Security Concepts

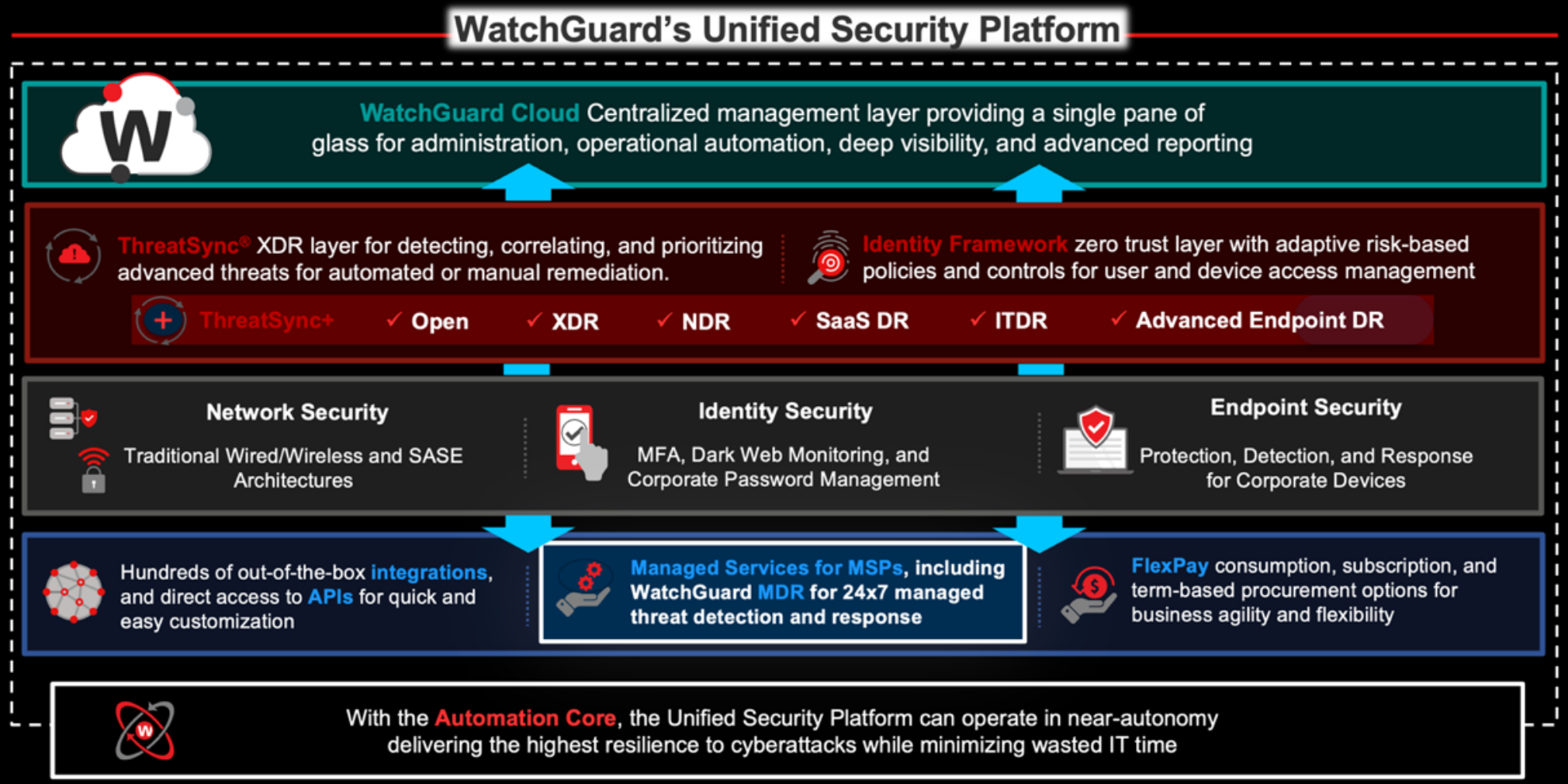
WatchGuard provides effective solutions to solve the security needs in modern hybrid szenarios

Network Security

Identity Security

Endpoint Security

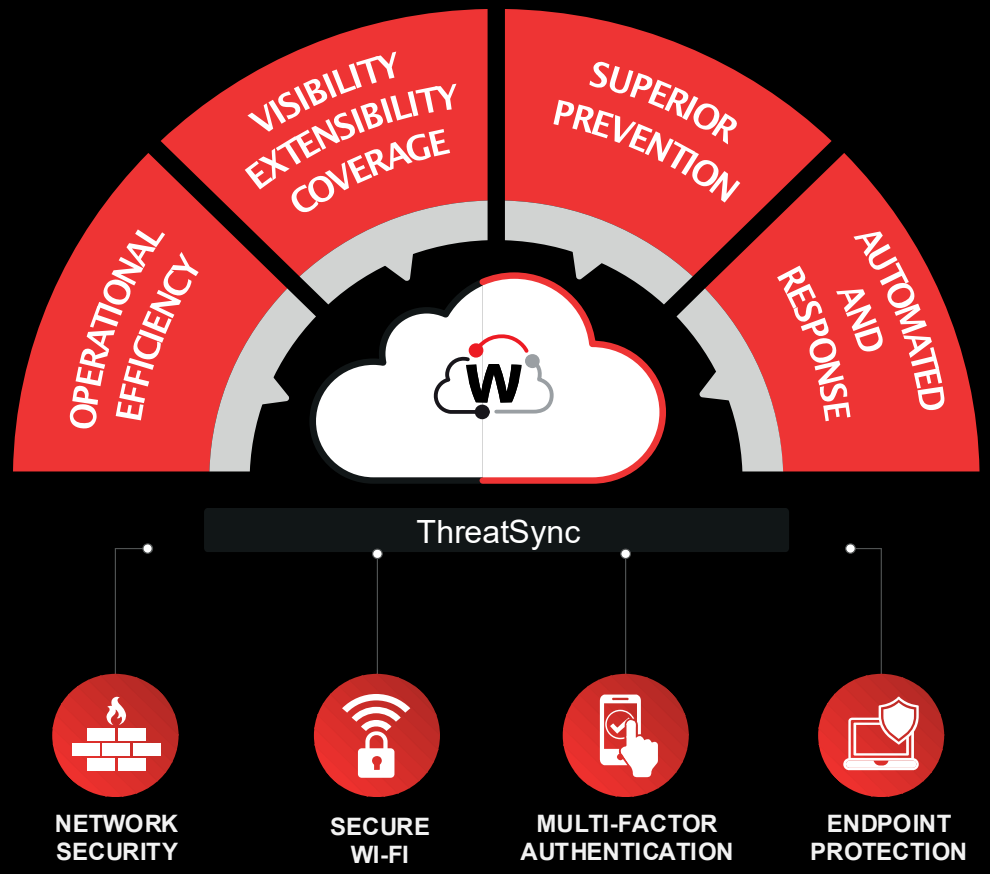
WatchGuard‘s USP



Unified Security Platform

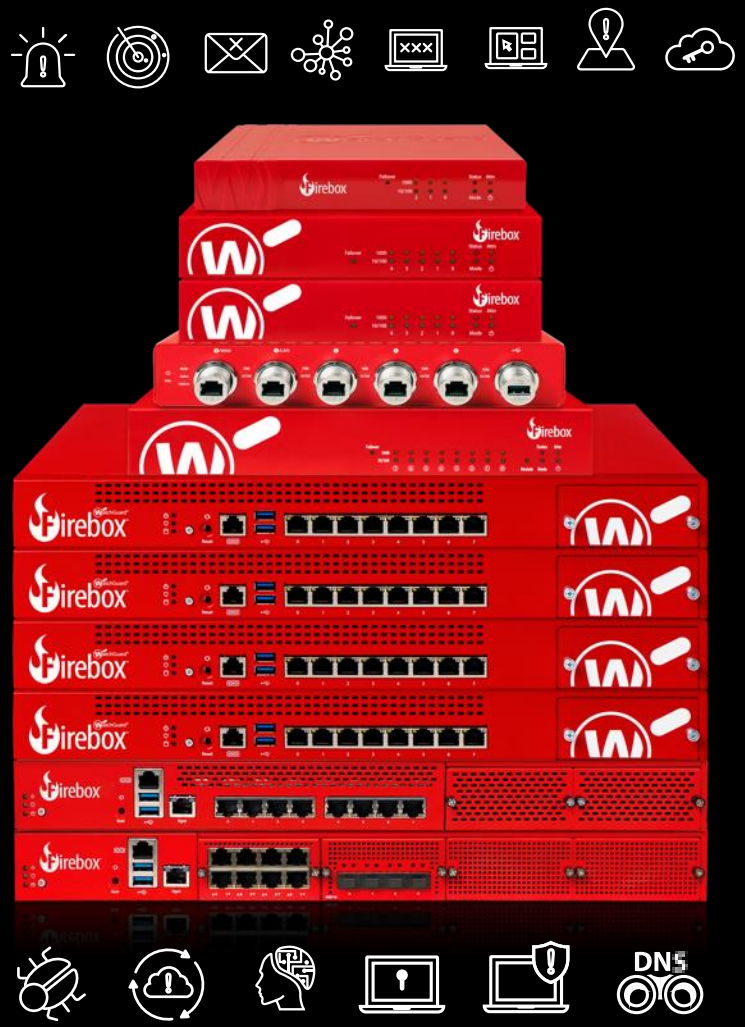
WatchGuard Cloud

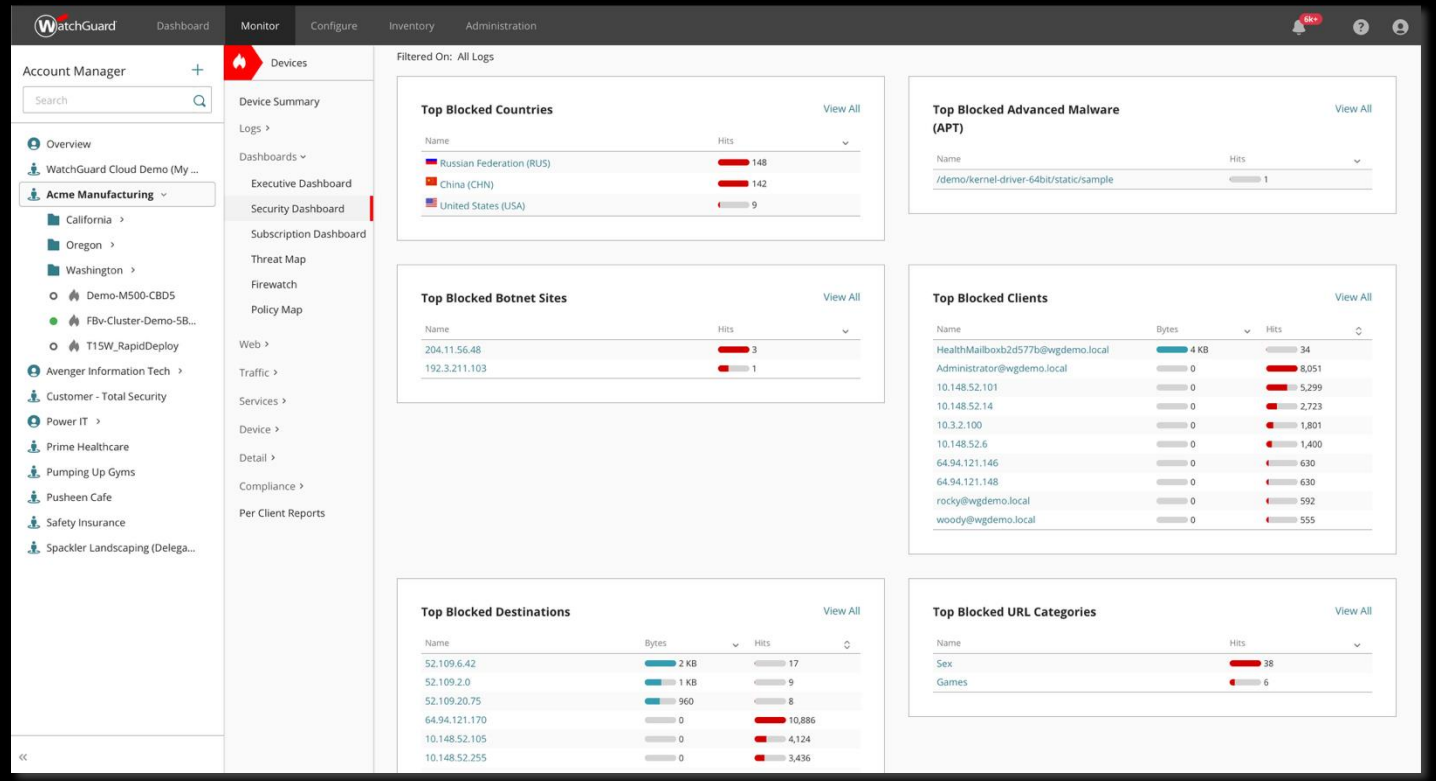
- Multi-Tier, Multi-Tenant
- European instance – GDPR compliance
- Manage security settings in easy and efficiently
- Zero-touch Deployment for Network-, Endpoint- and Identity-Security
- Built-in automation
- API Framework



Simplify Every Aspect of Security Delivery

Network Security

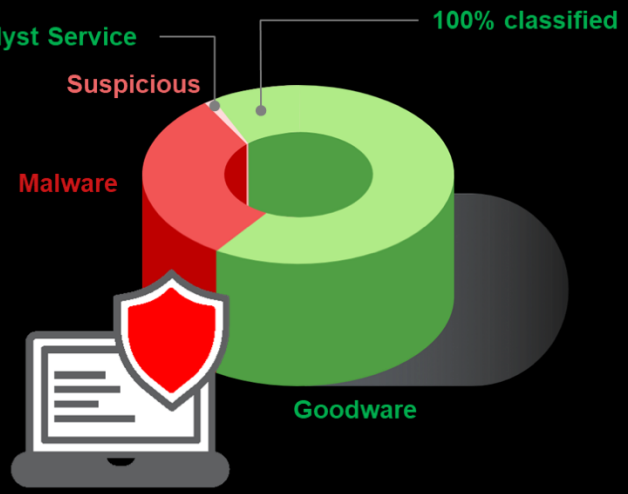


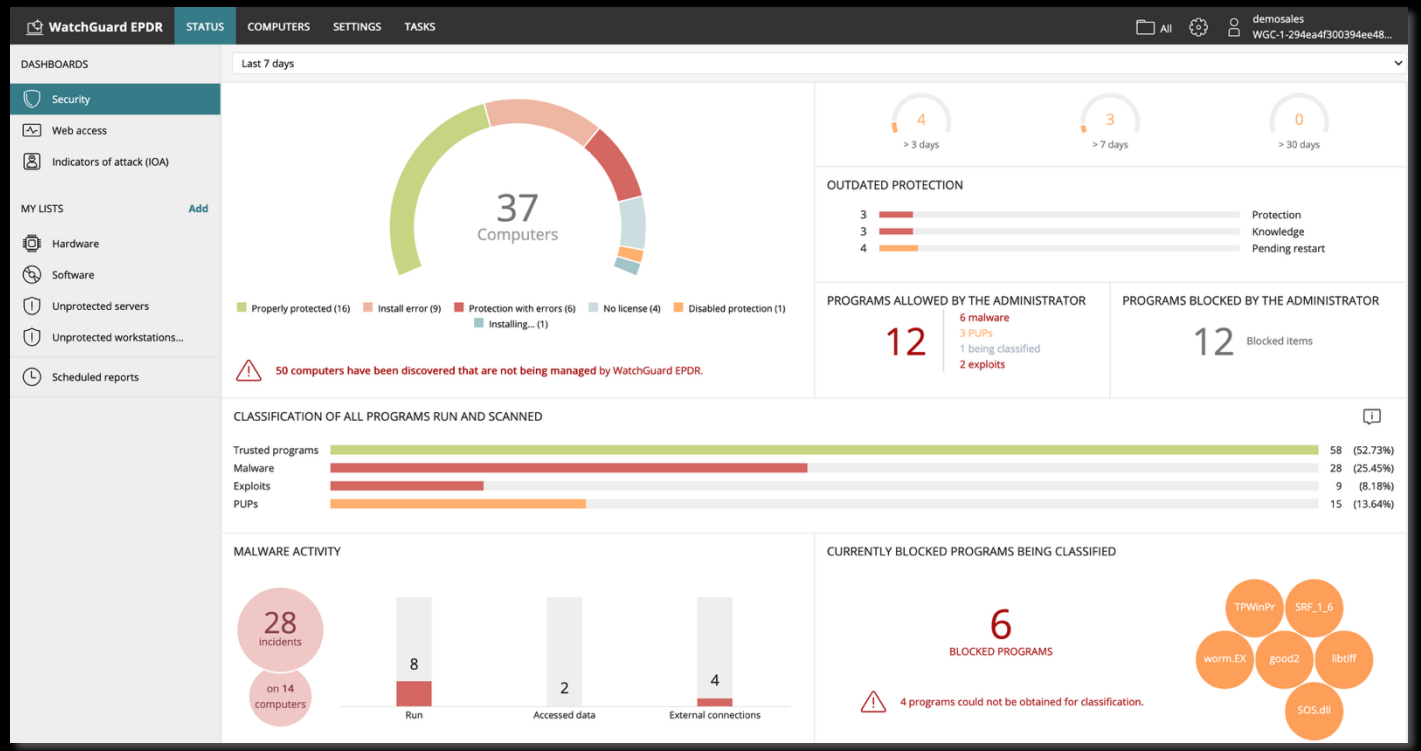


Endpoint Sicherheit with Zero-Trust

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

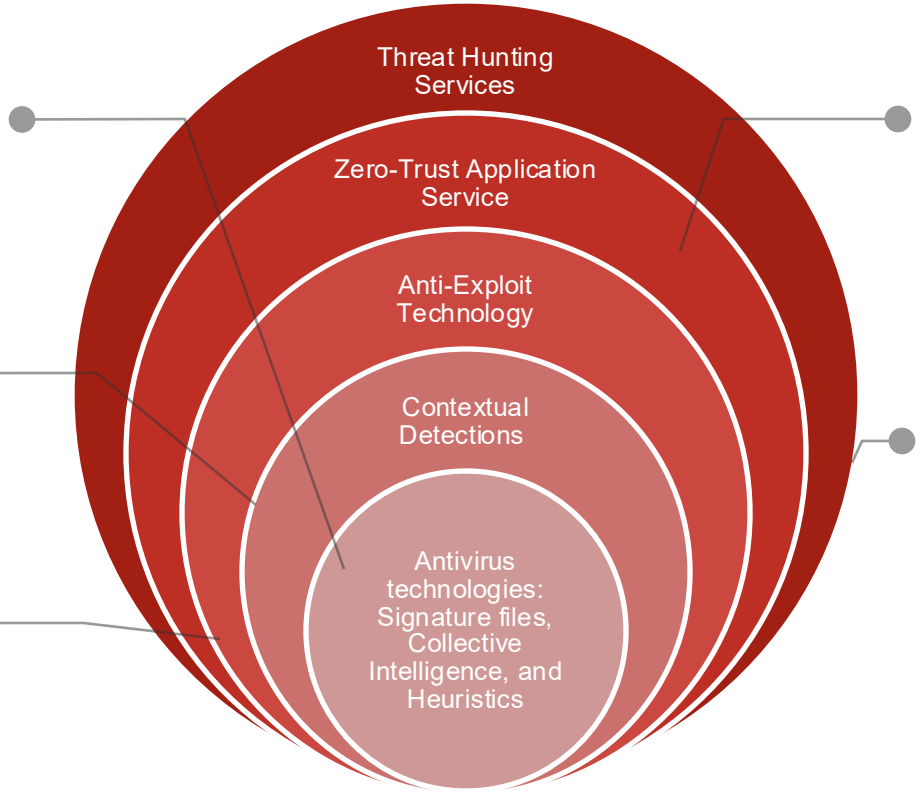
Effective, optimized technology to detect known attacks

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

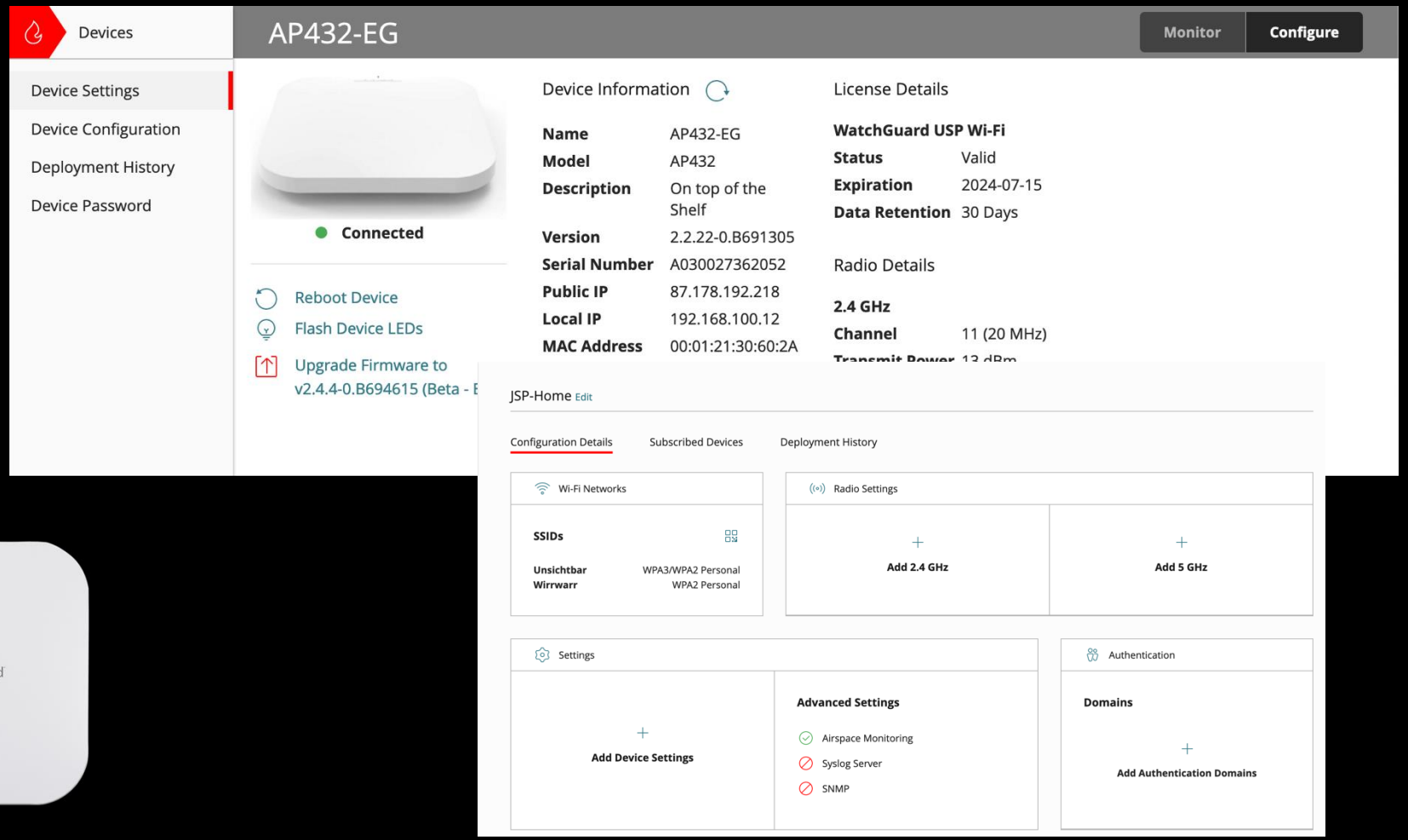
Layer 4 / Zero-Trust App Service

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

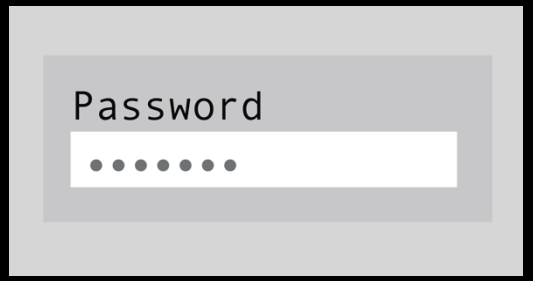
Secure Wi-Fi

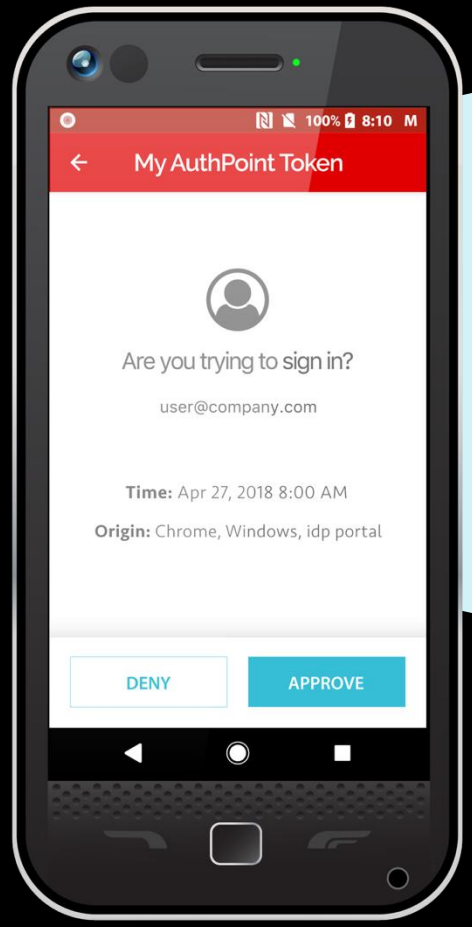


WatchGuard AuthPoint MFA

2 or more factors

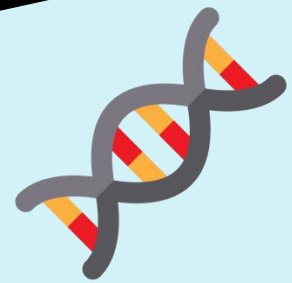
- **Something you know**
  (Passwort, PIN)
- **Something you have**
  (Token, Mobile App)
- **Something you are**
  (Fingerprint, Face)



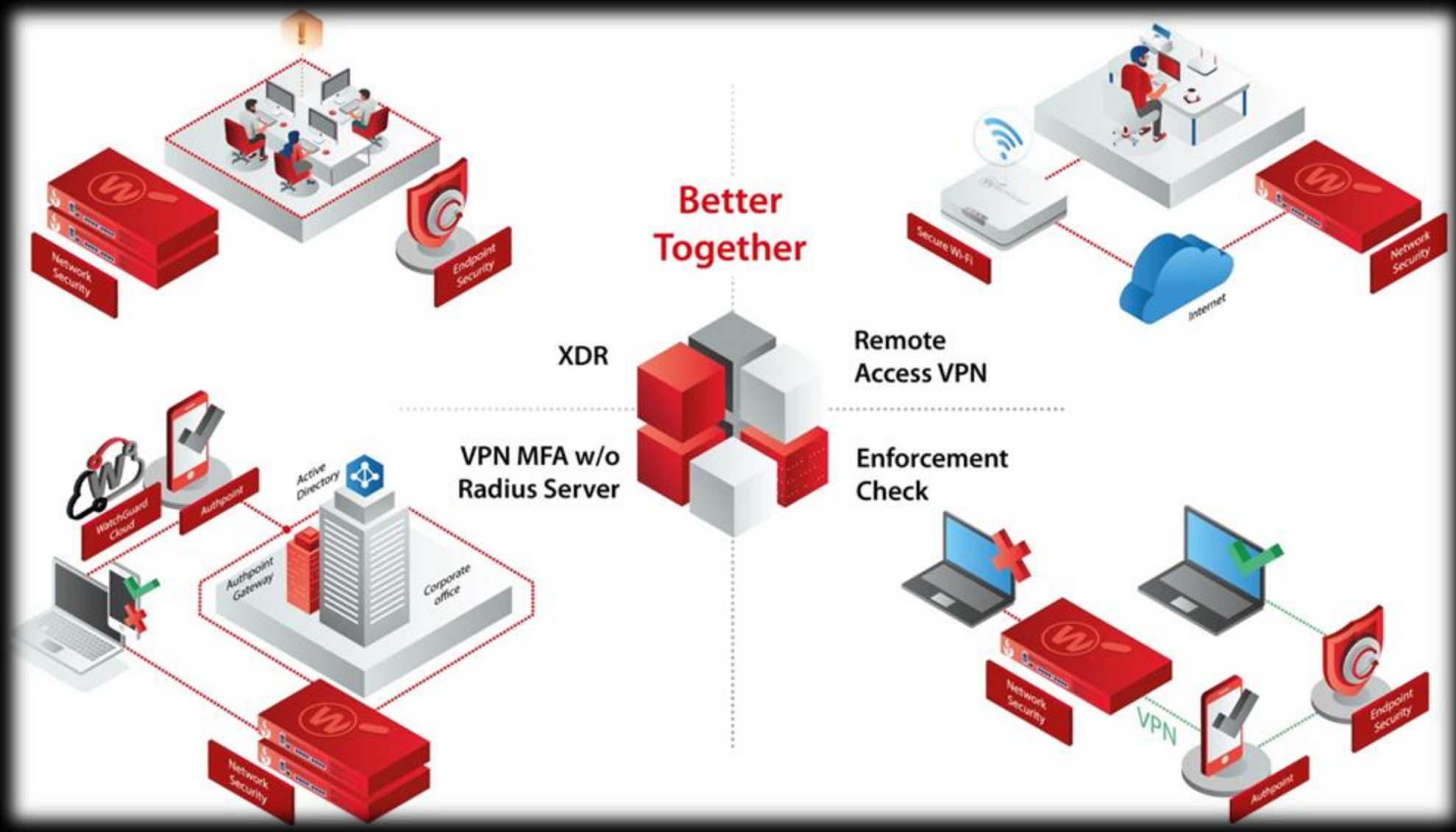


AuthPoint-Faktoren:

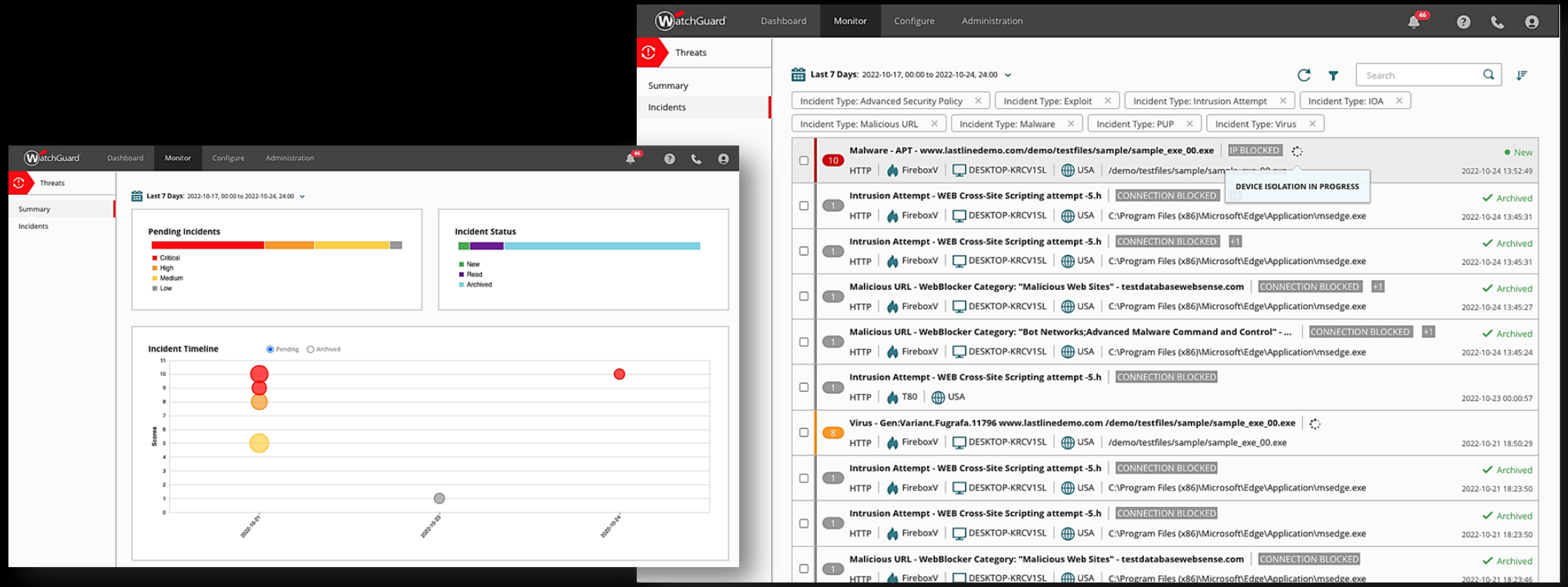
1. **Password**
2. **Proof in mobile App**
3. **Handy-DNA**
4. **Fingerprint / Face Recognition**



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

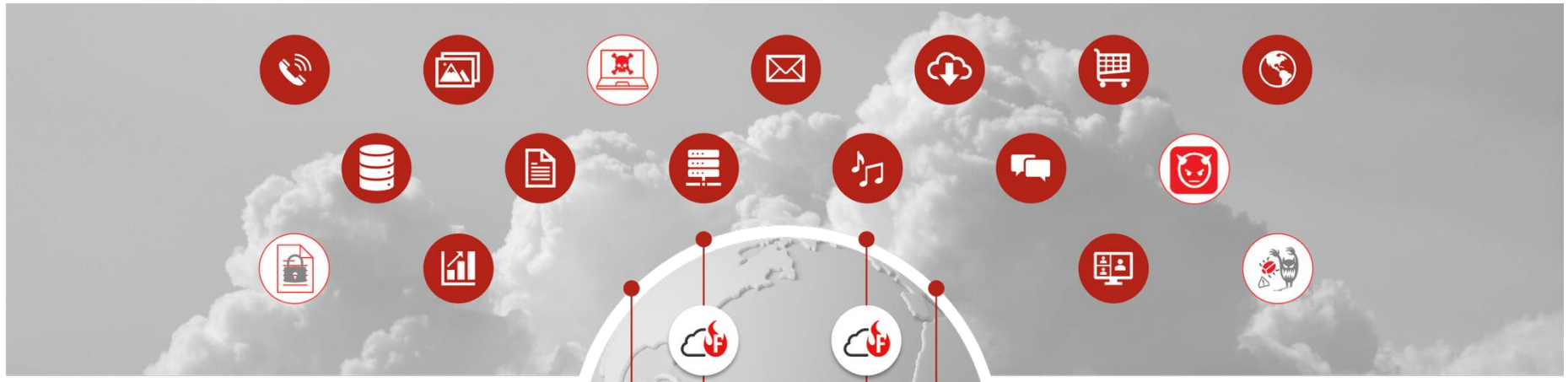
Remote worker accessing something public (FWaaS + SWG)

Connecting offices (SD-WAN)

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

Office worker accessing something public (FWaaS + SWG)

Introducing WatchGuard FireCloud



Remote worker accessing something public

Remote worker accessing something private

Connecting offices

Office worker accessing something public

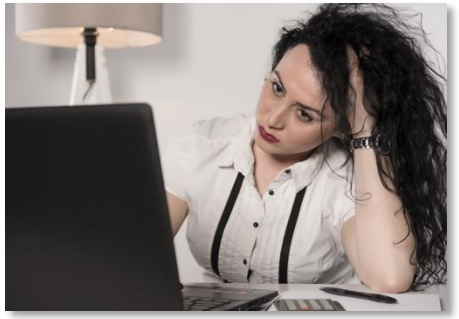
FireCloud Critical Use Case Coverage

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.

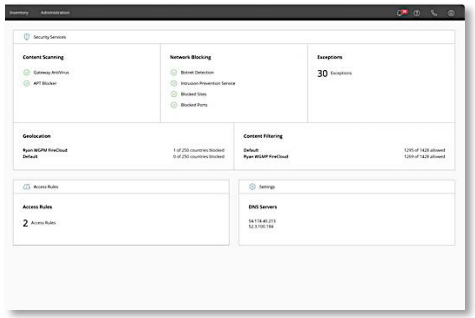
Secure Access to Cloud & Private Resources

- 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

Botnet Detection

Intrusion Prevention Service (IPS)

APT Blocker Cloud Sandboxing

TLS Inspection

Gateway AntiVirus (GAV)

Geolocation Blocking

User Authentication

Connection Manager

Identity Provider (IdP)

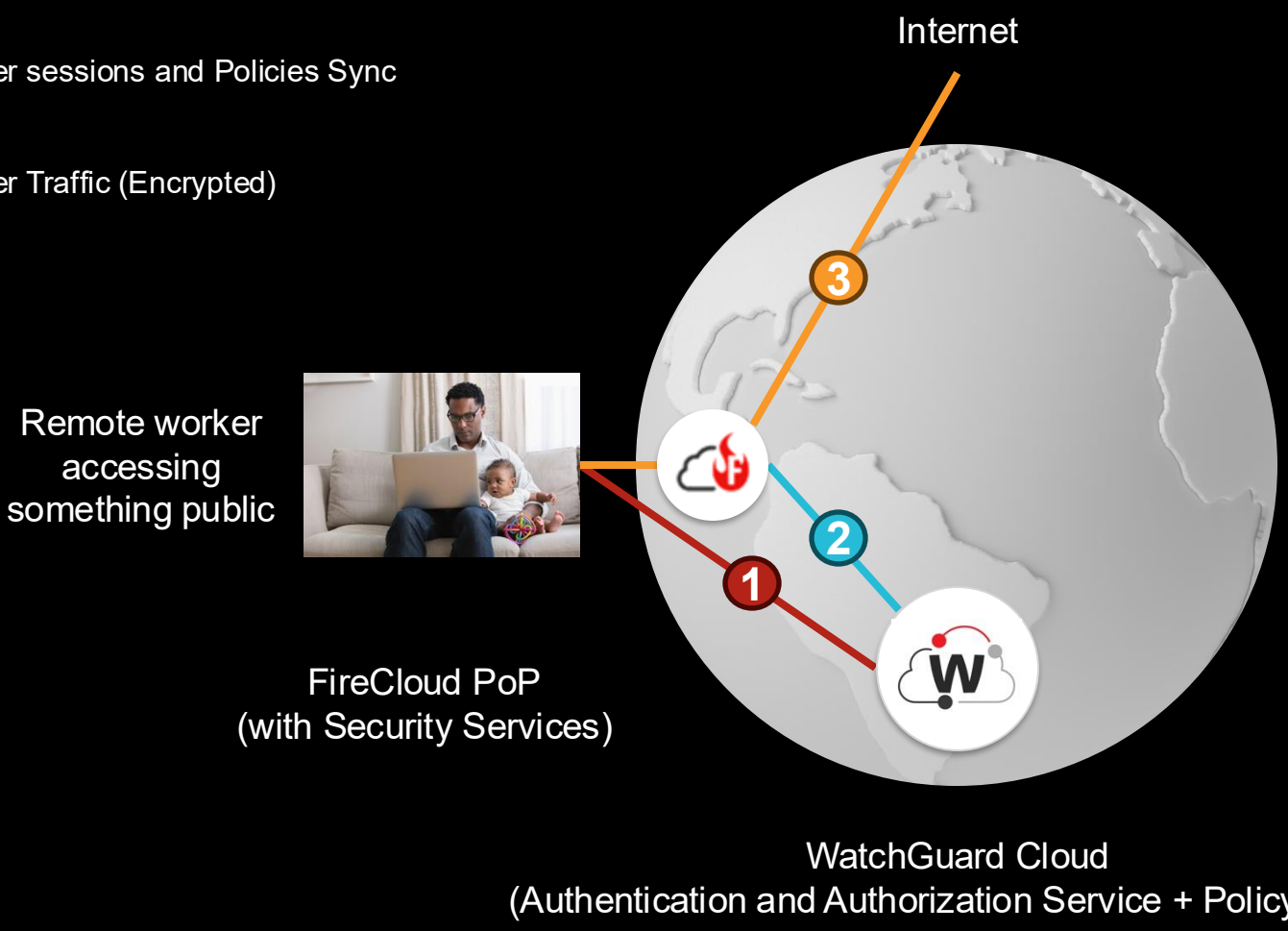
Secure Web Gateway (SWG)

WebBlocker URL Filtering

Application Control

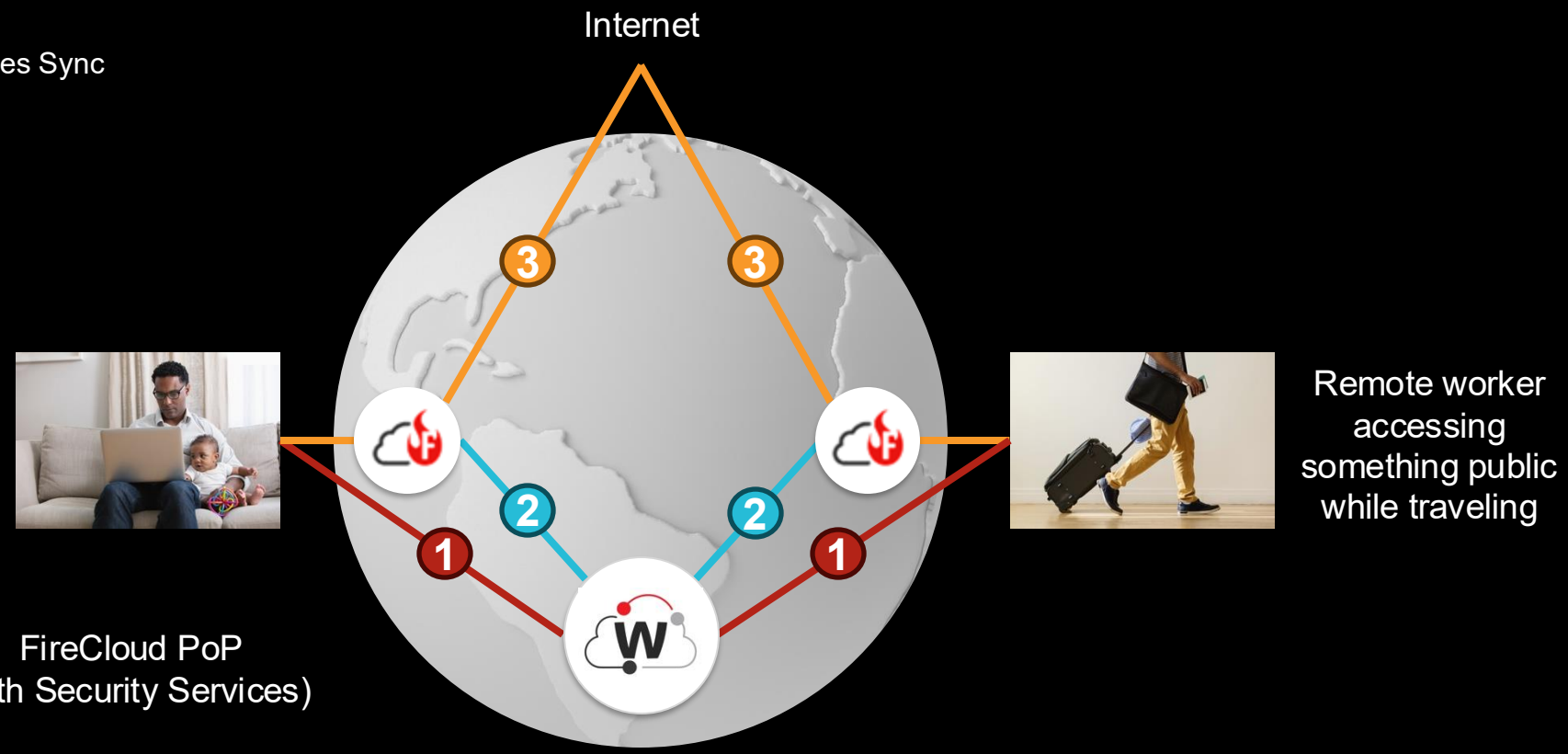
How FireCloud Internet Access Works

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



How FireCloud Internet Access Works

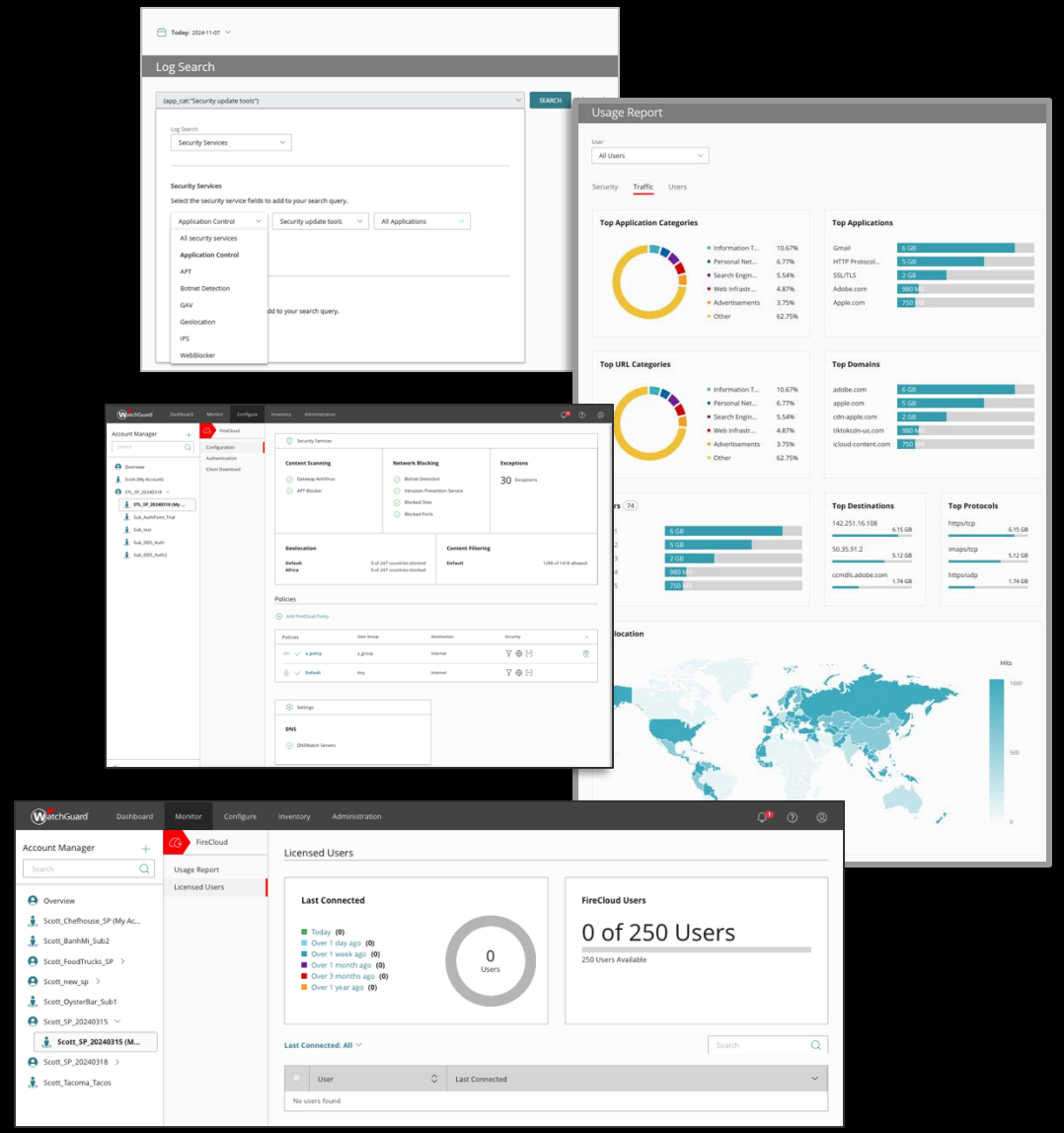
1. Login/Logout
2. User sessions and Policies Sync
3. User Traffic (Encrypted)



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

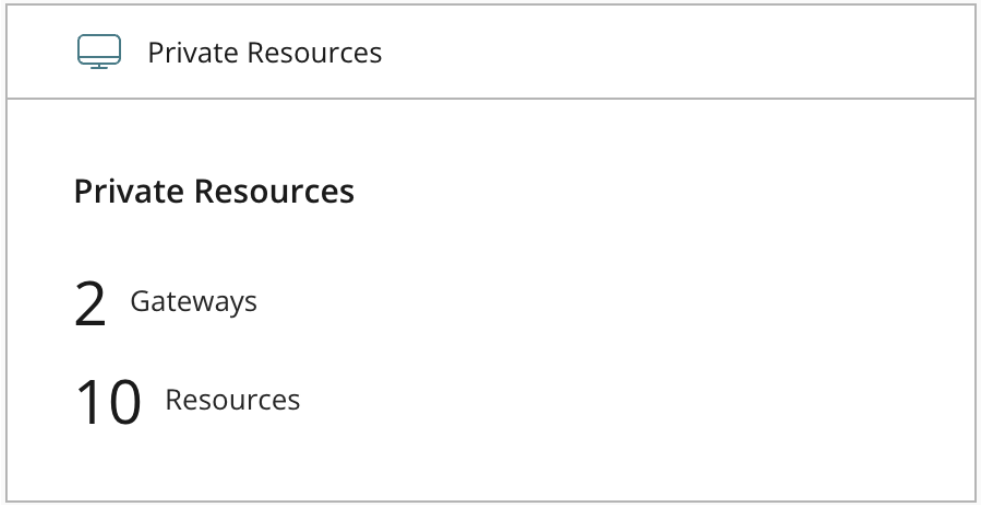


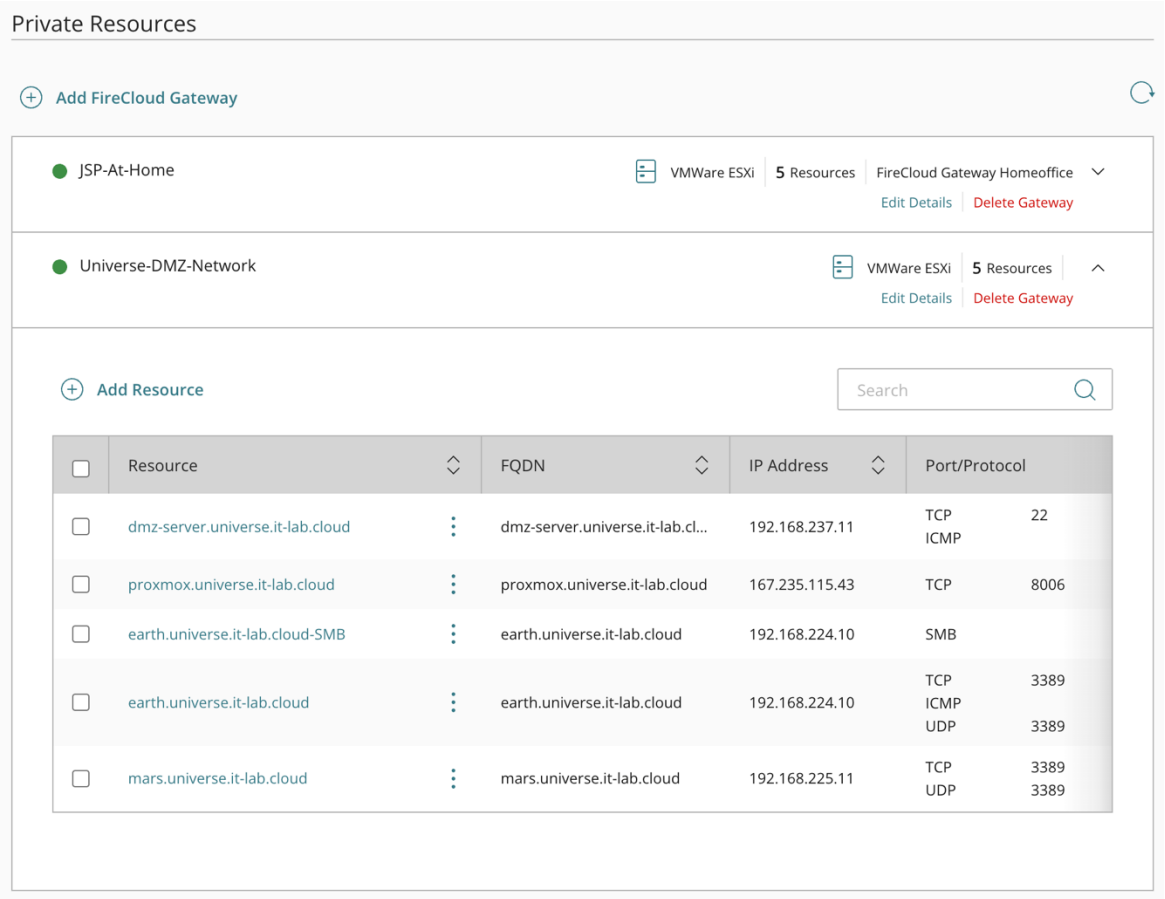
In Beta Now – FireCloud Total Access

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.

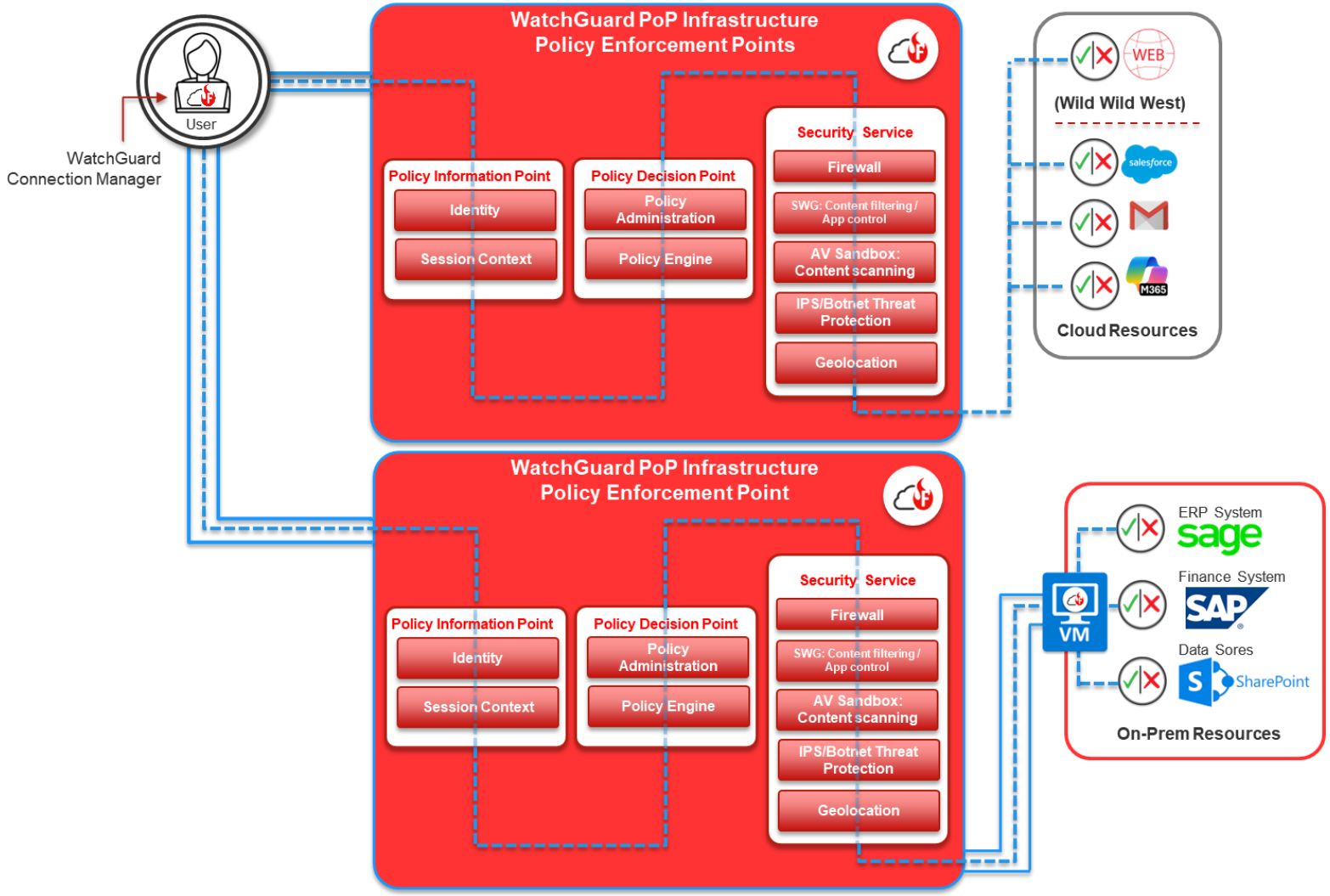
FireCloud Total Access includes all current FireCloud features.





Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Protects Users Accessing On-premise & Cloud Resources



Live

Real Security for the Real World

WatchGuard

Questions?
Thank You!