Proteggi gli ambienti ibridi con l'Open-XDR

Gianluca Pucci | Manager Sales Engineering Italy,
WatchGuard Technologies

The World Has Changed:
Hybrid infrastructures

Why This Matters For Clients

- If the organization has value, they will be targeted

- Companies cannot afford the people to operate the tech
- They are not prepared for the coming attack
- A significant proportion (46%) will not survive

Why This Matters For Partners

- **Partners must create and maintain TRUST with their clients**

  CRITICAL CYBERSECURITY SKILLS

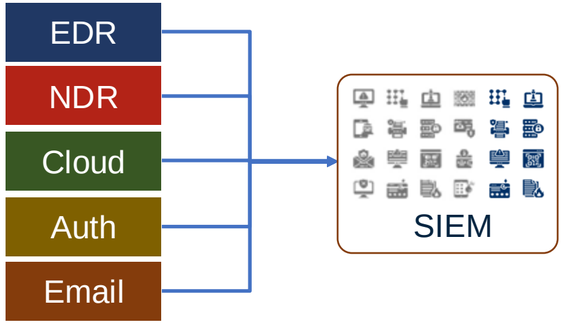
  - **Protect Complex Environments: Hybrid Networks, Supply Chain integration, Remote Workers, IoT Devices**
  - **Utilize emerging technologies: NDR, XDR, SASE and identity-based security**
  - **Fill the skills and operational cybersecurity gaps for their clients**

- **Partner success depends on delivering scalable, affordable, and comprehensive solutions and making money……**

  CRITICAL GO-TO-MARKET SKILLS

  - **Maintain a cybersecurity staff - deliver cybersecurity services**
  - **Partner with vendors who will support their offerings, not compete**
  - **Partner with vendors whose technology supports their business model**

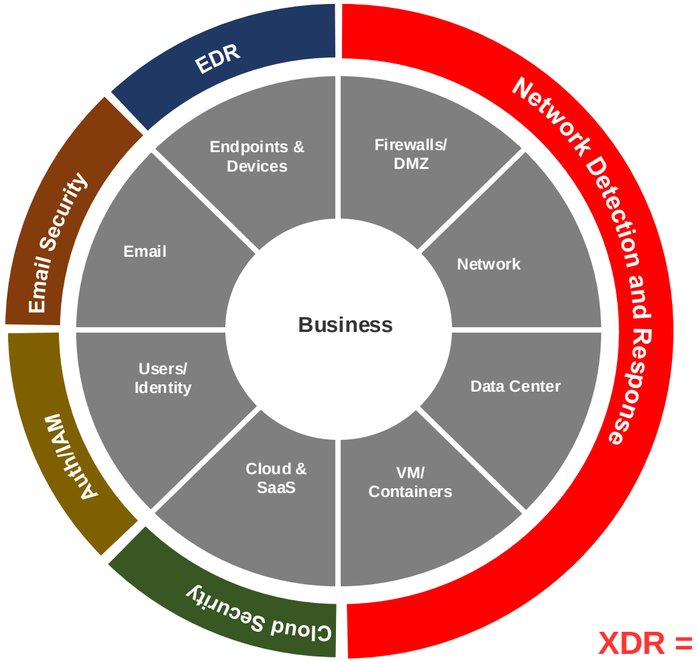
Understanding the Extended Detection and Response Market

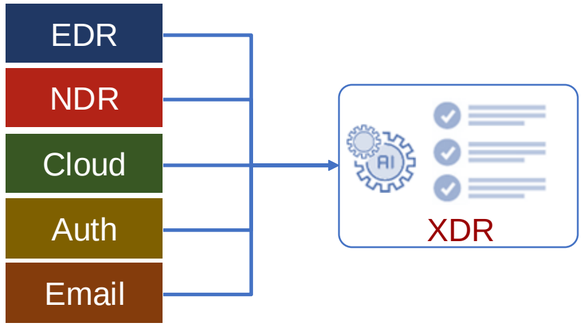


- ❑ Too many products
- ❑ No correlation
- ❑ Complexity
- ❑ Alert Fatigue

- ❑ Closer, but
- ❑ Alert Fatigue
- ❑ 8-12 people to operate
- ❑ Complex & Expensive

Understanding the Extended Detection and Response Market





- ❑ Too many products
- ❑ No correlation
- ❑ Complexity
- ❑ Alert Fatigue

- ❑ Full correlation
- ❑ Risk scored incidents
- ❑ Single UI
- ❑ Automation
- ❑ Integrated remediation

XDR = Simple, affordable, effective

XDR is a Promise Unfulfilled

“Effective deployment and management of XDR require skilled personnel. Organizations ***will need to invest in training existing staff or hiring new experts, adding to the overall cost.”***

SECURITY BOULEVARD

“Users have reported that many XDR tools require significant time and effort to configure. ***This complexity can delay deployment and hinder optimal utilization.”***

GARTNER

“Many XDR solutions are simply expansions of existing EDR tools. ***They lack network coverage, drive vendor lock-in and increase costs over time.”***

TechTarget

“Without proper tuning, XDR systems may ***generate false positive alerts, overwhelming security teams.”***

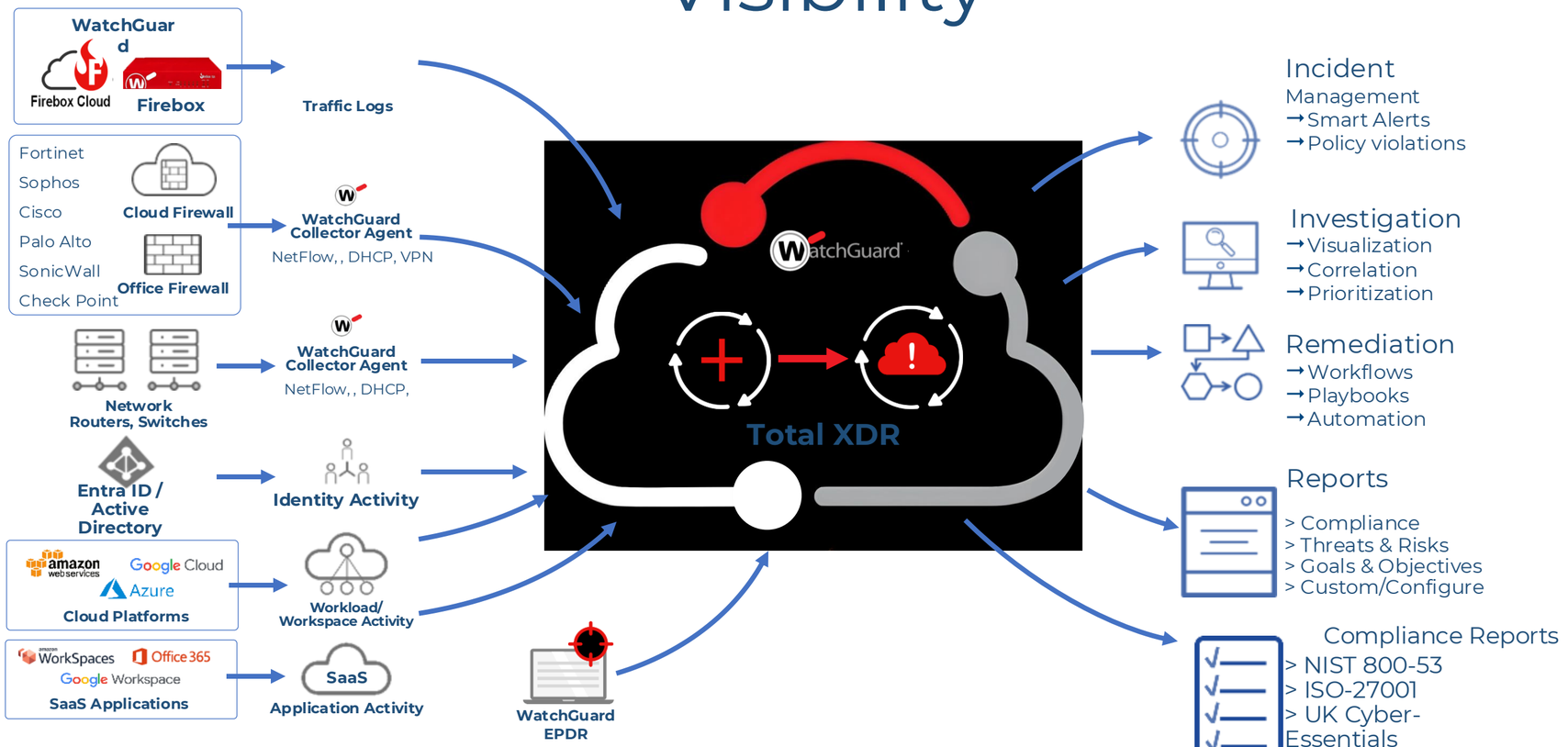
GARTNER

WatchGuard Total XDR

Threat Surface	Ingest Data	Comments
Endpoint	Yes, Native	EDPR integrates with ThreatSync, ThreatSync+ future
On-Prem Network	Yes, Native	Includes AI models, policy engine, ThreatSync native
Data Centers	Yes, Native	Includes AI models, policy engine, ThreatSync native
Firewalls	Yes, Native	Includes AI models, policy engine, ThreatSync native
VM/Containers	Yes, Native	Includes AI models, policy engine, ThreatSync native
Cloud	Yes, Native	Includes AI models, policy engine, ThreatSync native
User/Auth	Yes, Native & AD	Includes AI models, policy engine, ThreatSync native
Email	Integration	Future integration
Compliance	Yes, Native	Compliance control and reporting engine

More than other vendors in the XDR market today!

WatchGuard Total XDR: Expand Risk and Threat Visibility



WatchGuard Total XDR – Our New Bundle

ThreatSync Core

XDR remediation platform for the WatchGuard network and endpoint security products. ThreatSync Core includes foundational XDR capabilities of

- Threat information correlation
- Incident scoring and management
- Intelligent automated remediation

ThreatSync+ NDR

100% Cloud-native, AI-powered threat detection solution that defends on-premises network, VPN, and identity threat surfaces.

ThreatSync+ SaaS

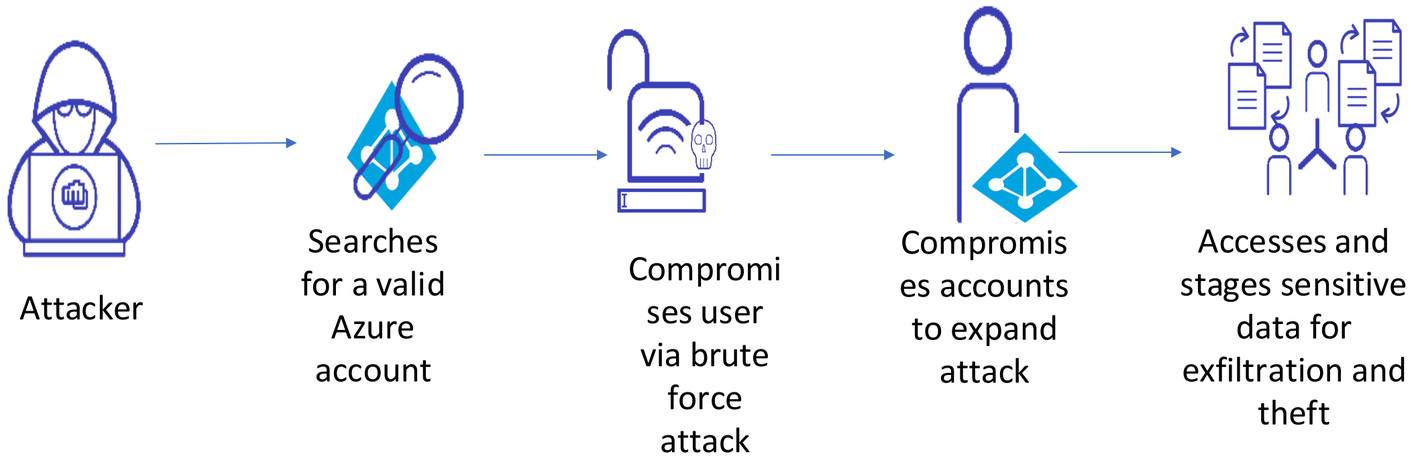
ThreatSync+ SaaS: a 100% Cloud-native, AI-powered threat detection solution that defends SaaS applications, Cloud platforms, and Cloud identity threat surfaces.

WatchGuard Compliance Reporting

Augments reports available with ThreatSync+ solutions to provide a rich package of Regulatory and Compliance reports.

ThreatSync+ SaaS in action

Brute Force Attack against M365

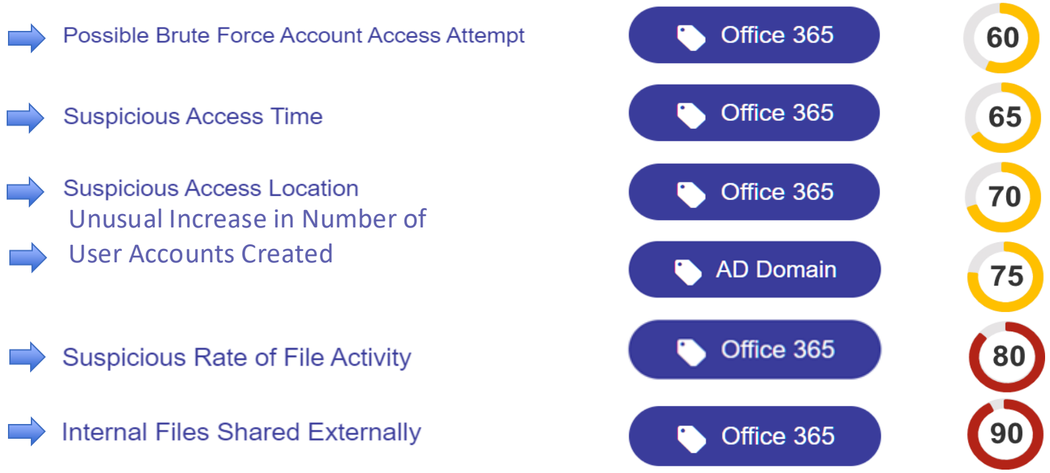


Azure Accounts are a Priority Target

- Compromise leads to lateral movement and privileged escalation
- Misconfiguration enables movement to sensitive data locations and mission-critical networks

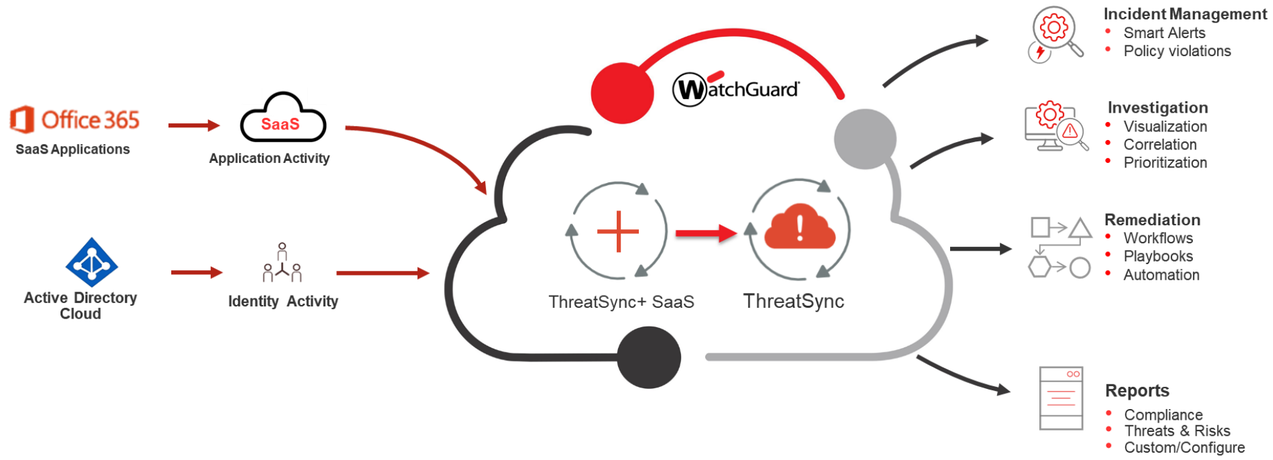
Hybrid Cloud Protection

- Detects attacks on Azure accounts
- Detects downstream attack activities
  - Impossible location, suspicious file activity
- Connects attacks to user accounts, IP addresses, and locations for effective remediation



ThreatSync+ SaaS M365: How It Works

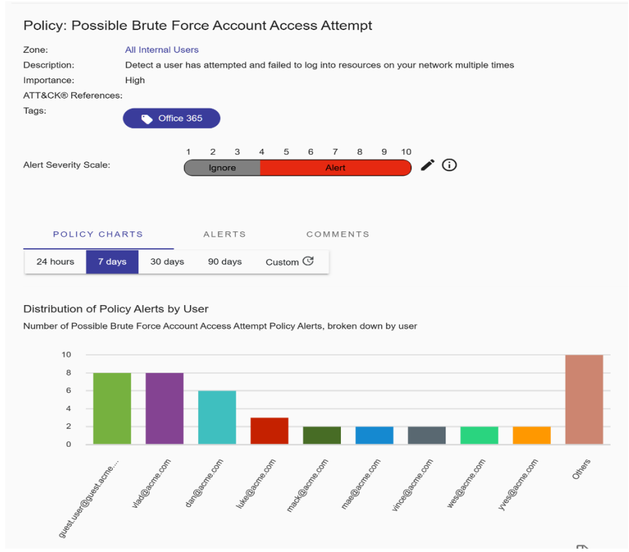
- ThreatSync+ SaaS collects M365, Teams, and Azure AD logs
- Data flows are analyzed by the ThreatSync+ Machine Learning and AI policy engine
- Machine learning models create normal baselines for all activities and search out risks and threats
- Risk and threats are captured and correlated
- Risk-prioritized alerts and details are presented in the ThreatSync+ UI
- Example set of continuous monitoring AI:

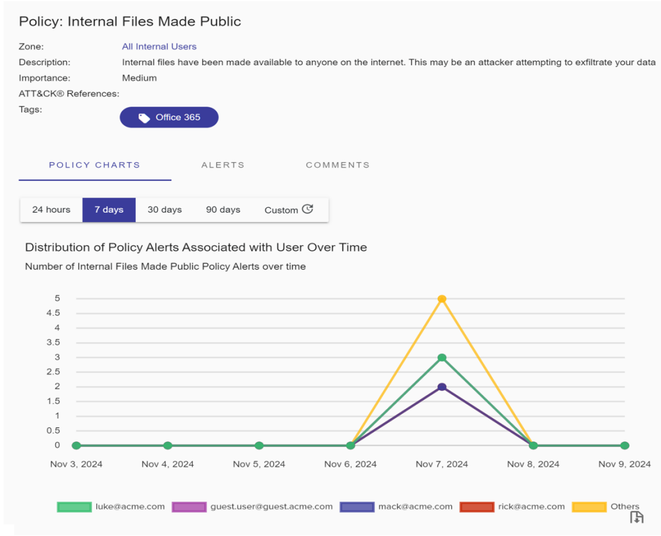


- Suspicious access location
- Suspicious access time
- Impossible travel/access
- Suspicious access rate

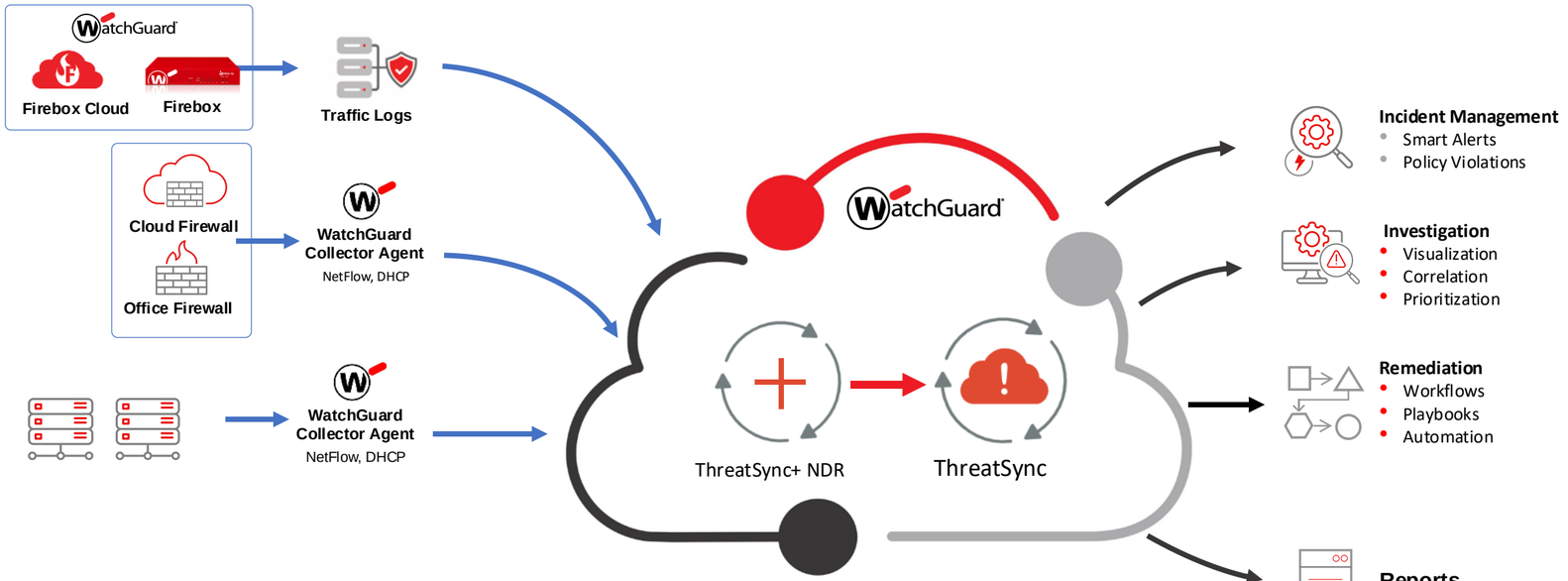
- Brute force password attack
- Suspicious admin changes, rate
- Suspicious admin changes, time

- Internal files share externally
- Suspicious file activity by rate
- Anonymous file activity
- Internal files made public





ThreatSync+ NDR - North/South & East/West Network Focus



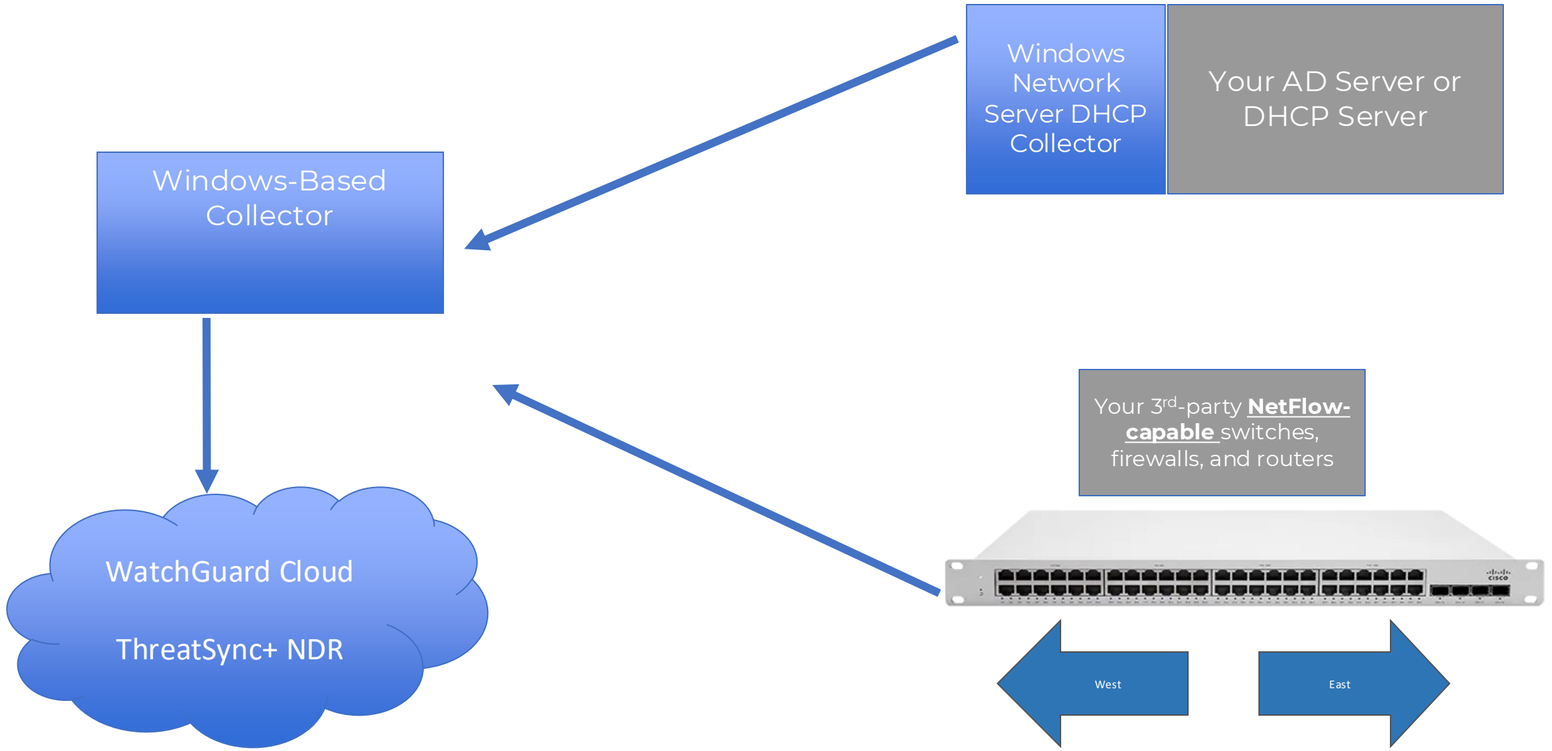
Incident Management
- Smart Alerts
- Policy Violations

Investigation
- Visualization
- Correlation
- Prioritization

Remediation
- Workflows
- Playbooks
- Automation

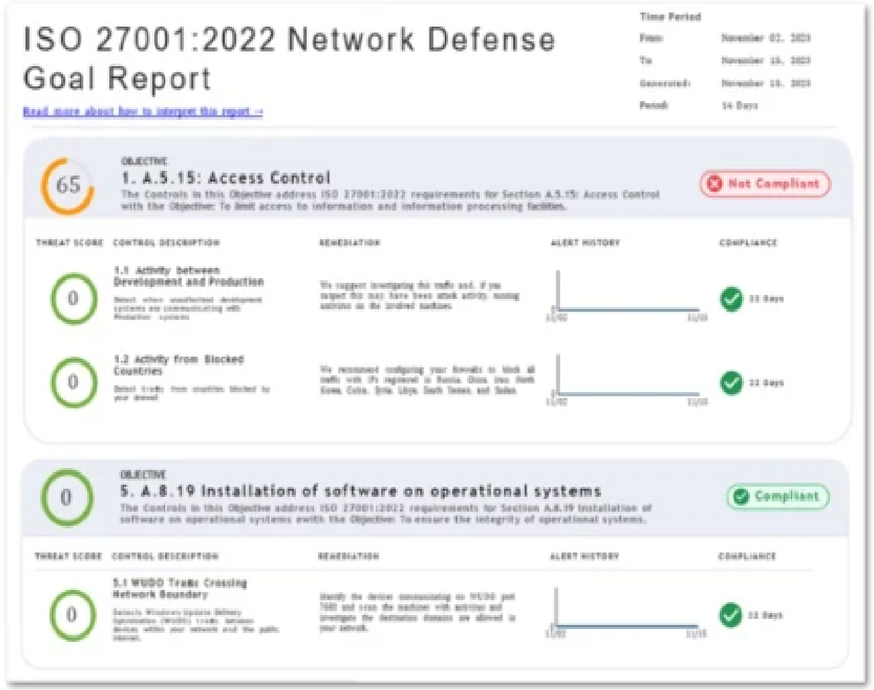
Reports
- Compliance
- Threats & Risks
- Custom/Configure

3rd-Party Network Appliances - East-West Traffic



Netflow V5 or V9 is used for the NDR analytics

Compliance Report



ISO 27001:2022 Network Defense Goal Report

Read more about how to interpret this report →

Time Period
From November 01, 2023
To November 15, 2023
Generated: November 15, 2023
Period: 14 Days

65

OBJECTIVE
1. A.5.15: Access Control
The Controls in this Objective address ISO 27001:2022 requirements for Section A.5.15: Access Control with the Objective: To limit access to information and information processing facilities.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	1.1 Activity between Development and Production	We suggest investigating this traffic and, if you suspect this may have been attack activity, moving [illegible] to the isolated machines.	11/02 11/15	13 Days
0	1.2 Activity from Blocked Countries	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Sudan, and Sudan.	11/02 11/15	13 Days

0

OBJECTIVE
5. A.8.19 Installation of software on operational systems
The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.19 Installation of software on operational systems ewith the Objective: To ensure the integrity of operational systems.

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	5.1 WUDO Traffic Crossing Network Boundary	Identify the devices communicating on TCP/30 port 7680 and scan the machines with antivirus and investigate the destination domains are allowed in your network.	11/02 11/15	13 Days

Continuous Compliance with Reporting

The ThreatSync Suite combines hundreds of pre-built ISO 27001 and NIST 800-53 best practice controls with a compliance reporting engine delivering automated regulatory and compliance reporting.

Q&A

Contatti:
gianluca.pucci@watchguard.com

Vieni a trovarci al nostro stand!