Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY SUMMIT
STREAMING EDITION

ASTREA Advanced Security, Training
Research, Events Agency

Un quadro vale più di mille parole: è tempo di una visione unificata della sicurezza

Alessio Pennasilico, Comitato Scientifico, Clusit

Gianluca Pucci, Manager Sales Engineering, WatchGuard

9 – 10 novembre 2022 orario 16.20 – 17.20

Alessio L.R. Pennasilico aka -=mayhem=-

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

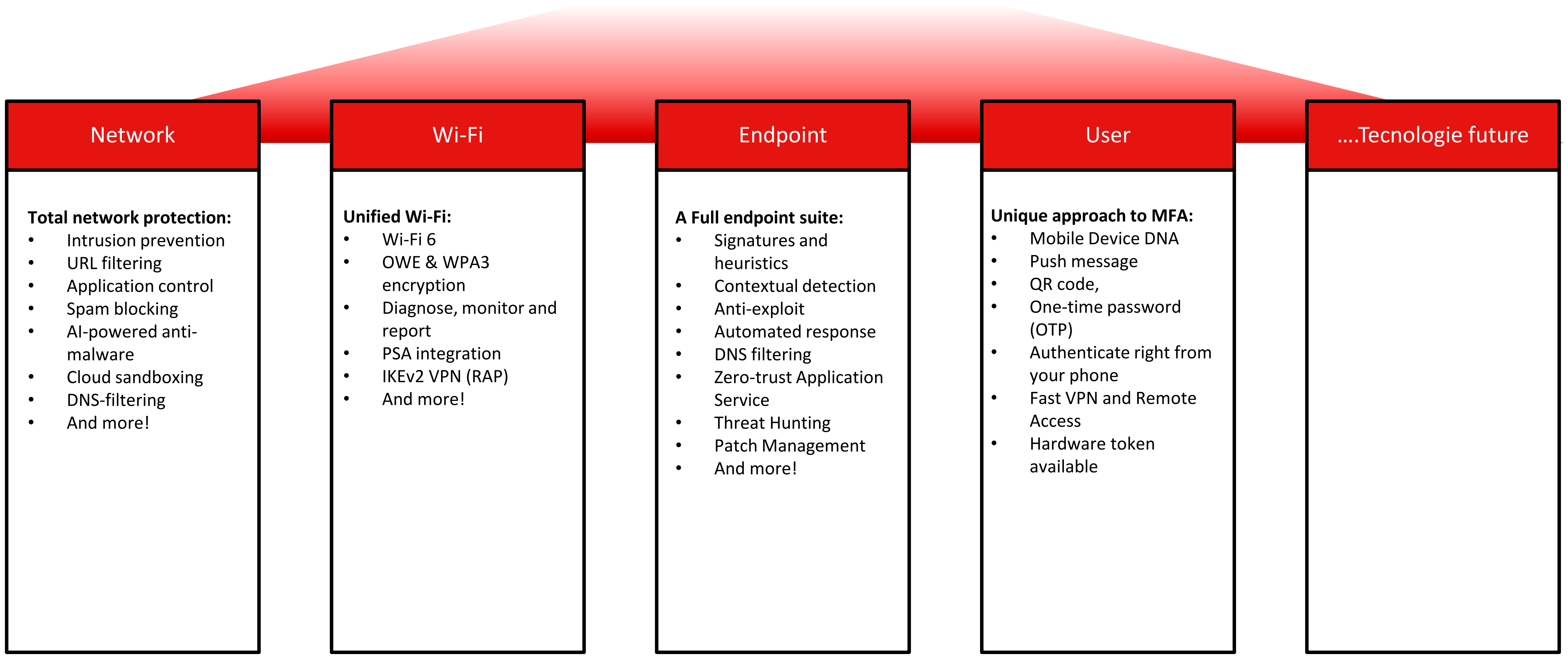
Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

Gianluca Pucci

MANAGER SALES ENGINEERING
WATCHGUARD TECHNOLOGIES



Network

Total network protection:
- Intrusion prevention
- URL filtering
- Application control
- Spam blocking
- AI-powered anti-malware
- Cloud sandboxing
- DNS-filtering
- And more!

Wi-Fi

Unified Wi-Fi:
- Wi-Fi 6
- OWE & WPA3 encryption
- Diagnose, monitor and report
- PSA integration
- IKEv2 VPN (RAP)
- And more!

Endpoint

A Full endpoint suite:
- Signatures and heuristics
- Contextual detection
- Anti-exploit
- Automated response
- DNS filtering
- Zero-trust Application Service
- Threat Hunting
- Patch Management
- And more!

User

Unique approach to MFA:
- Mobile Device DNA
- Push message
- QR code,
- One-time password (OTP)
- Authenticate right from your phone
- Fast VPN and Remote Access
- Hardware token available

....Tecnologie future

La Sicurezza informatica… Quali necessità porta? Quali porterà in futuro? Un solo prodotto non basta perchè l’infrastruttura ha più componenti… A chi mi rivolgo?

Come orientare la scelta tecnologica?

- Un solo riferimento tecnico (supporto, progettazione, Servizi..)
- Gestione semplificata
- Visibilità reportistica/ compliance
- Integrazione
- Scalabilità
- Affidabilità

Focus: Organizzazione, gestione, ottimizzazione….

…..Reportistica/Visibilità

…..Flessibilità/Organizzazione

…..Semplicità

…..Automazione

…..Accessi controllati e sicuri

…..Personalizzazione

Network

Firebox

Total network protection:

- Intrusion prevention
- URL filtering
- Application control
- Spam blocking
- AI-powered anti-malware
- Cloud sandboxing
- DNS-filtering
- And more!

Wi-Fi

Unified Wi-Fi:

- Wi-Fi 6
- OWE & WPA3 encryption
- Diagnose, monitor and report
- PSA integration
- IKEv2 VPN (RAP)
- And more!

Endpoint

DNS GO

A Full endpoint suite:

- Signatures and heuristics
- Contextual detection
- Anti-exploit
- Automated response
- DNS filtering
- Zero-trust Application Service
- Threat Hunting
- Patch Management
- And more!

User

Unique approach to MFA:

- Mobile Device DNA
- Push message
- QR code,
- One-time password (OTP)
- Authenticate right from your phone
- Fast VPN and Remote Access
- Hardware token available

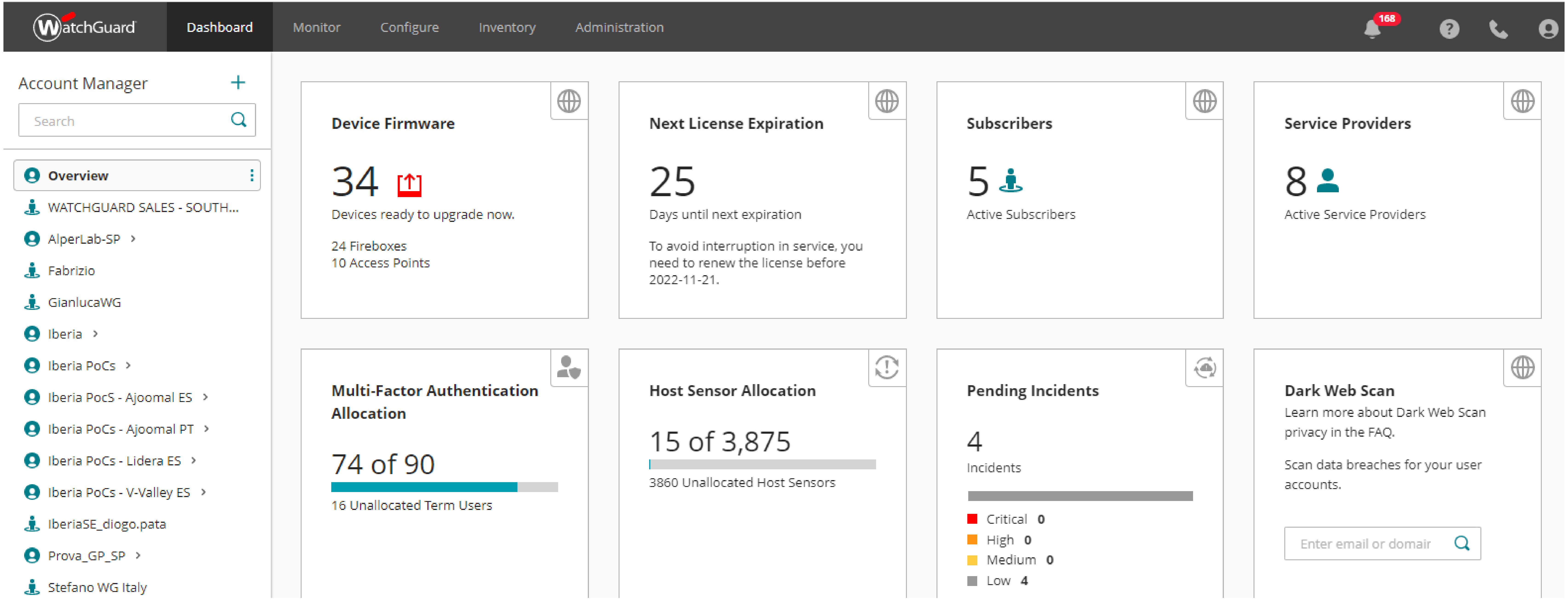
....Tecnologie future

Come orientare la scelta tecnologica?

- Un solo riferimento tecnico (supporto, progettazione, Servizi..)
- Gestione semplificata
- Visibilità reportistica/ compliance
- Integrazione
- Scalabilità
- Affidabilità

WatchGuard

WatchGuard Unified Security Platform



Account Manager +

Search

- Overview
- WATCHGUARD SALES - SOUTH...
- AlperLab-SP ›
- Fabrizio
- GianlucaWG
- Iberia ›
- Iberia PoCs ›
- Iberia PocS - Ajoomal ES ›
- Iberia PoCs - Ajoomal PT ›
- Iberia PoCs - Lidera ES ›
- Iberia PoCs - V-Valley ES ›
- IberiaSE_diogo.pata
- Prova_GP_SP ›
- Stefano WG Italy

Device Firmware

34

Devices ready to upgrade now.

24 Fireboxes
10 Access Points

Next License Expiration

25

Days until next expiration

To avoid interruption in service, you need to renew the license before 2022-11-21.

Subscribers

5

Active Subscribers

Service Providers

8

Active Service Providers

Multi-Factor Authentication Allocation

74 of 90

16 Unallocated Term Users

Host Sensor Allocation

15 of 3,875

3860 Unallocated Host Sensors

Pending Incidents

4

Incidents

🟥 Critical 0
🟧 High 0
🟨 Medium 0
⬜ Low 4

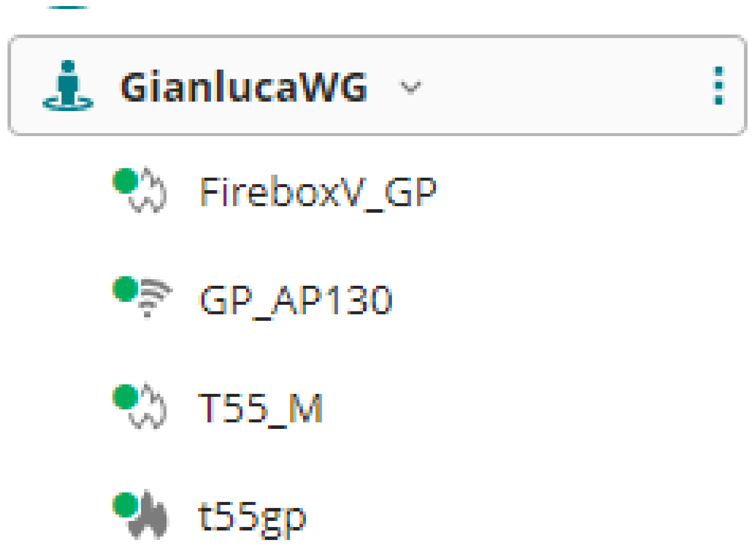
Dark Web Scan

Learn more about Dark Web Scan privacy in the FAQ.

Scan data breaches for your user accounts.

Enter email or domair

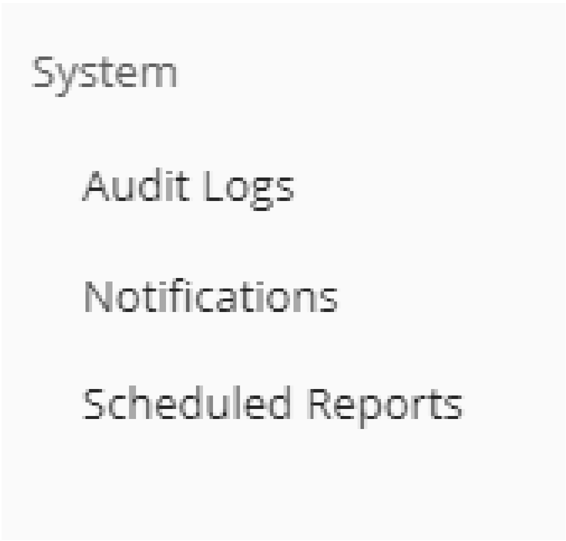
WatchGuard Unified Security Platform: Visibilità



GianlucaWG

- FireboxV_GP
- GP_AP130
- T55_M
- t55gp

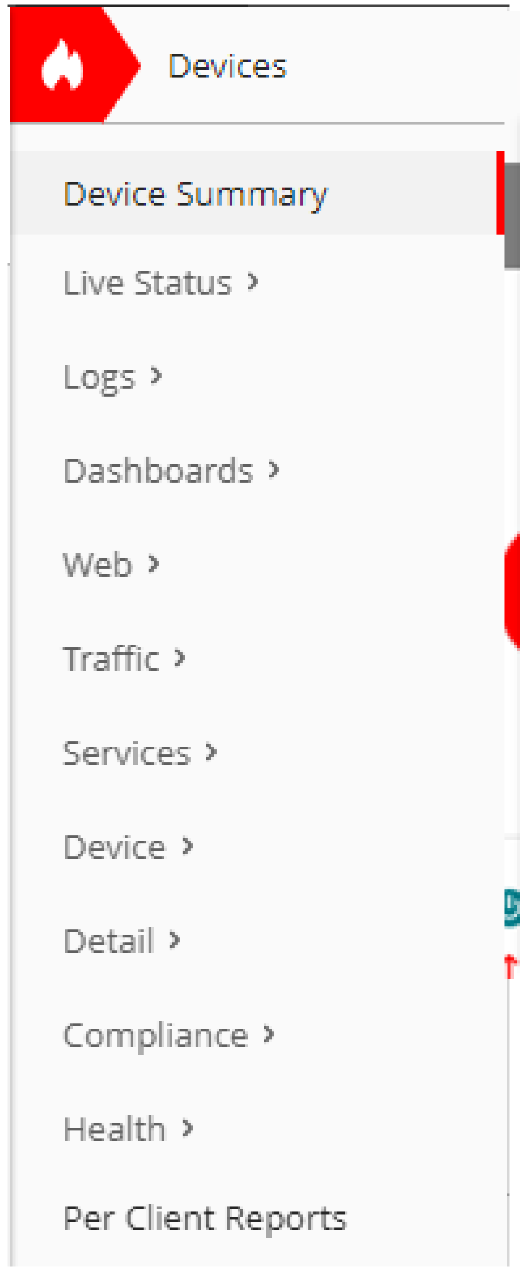
Monitoring/Logging/ Reporting degli apparati allocati nel proprio tenant



System

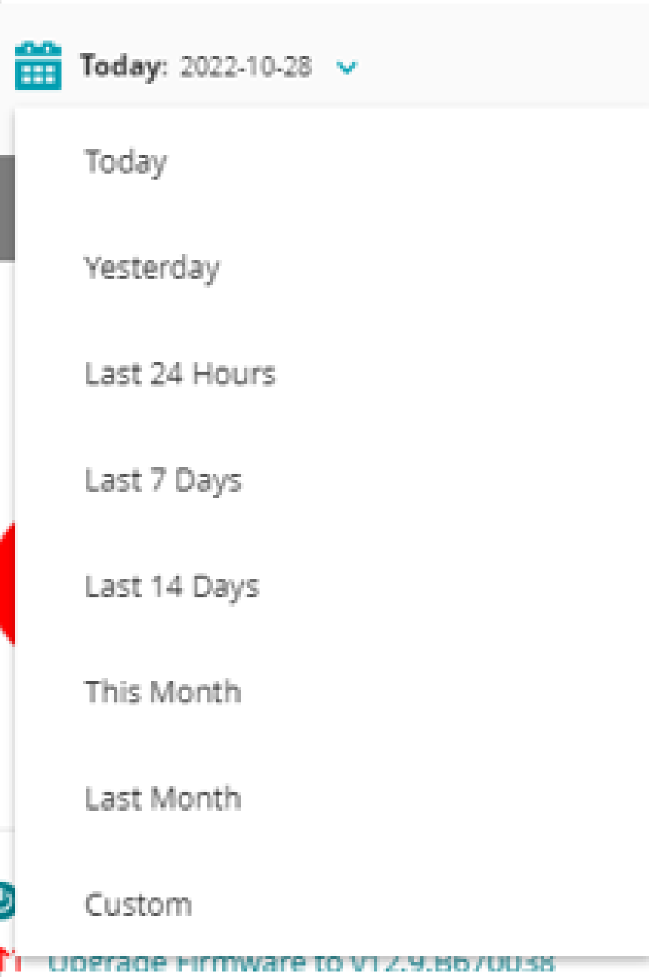
- Audit Logs
- Notifications
- Scheduled Reports

Funzioni di Audit, Notifiche e reporting



Devices

- Device Summary
- Live Status ›
- Logs ›
- Dashboards ›
- Web ›
- Traffic ›
- Services ›
- Device ›
- Detail ›
- Compliance ›
- Health ›
- Per Client Reports



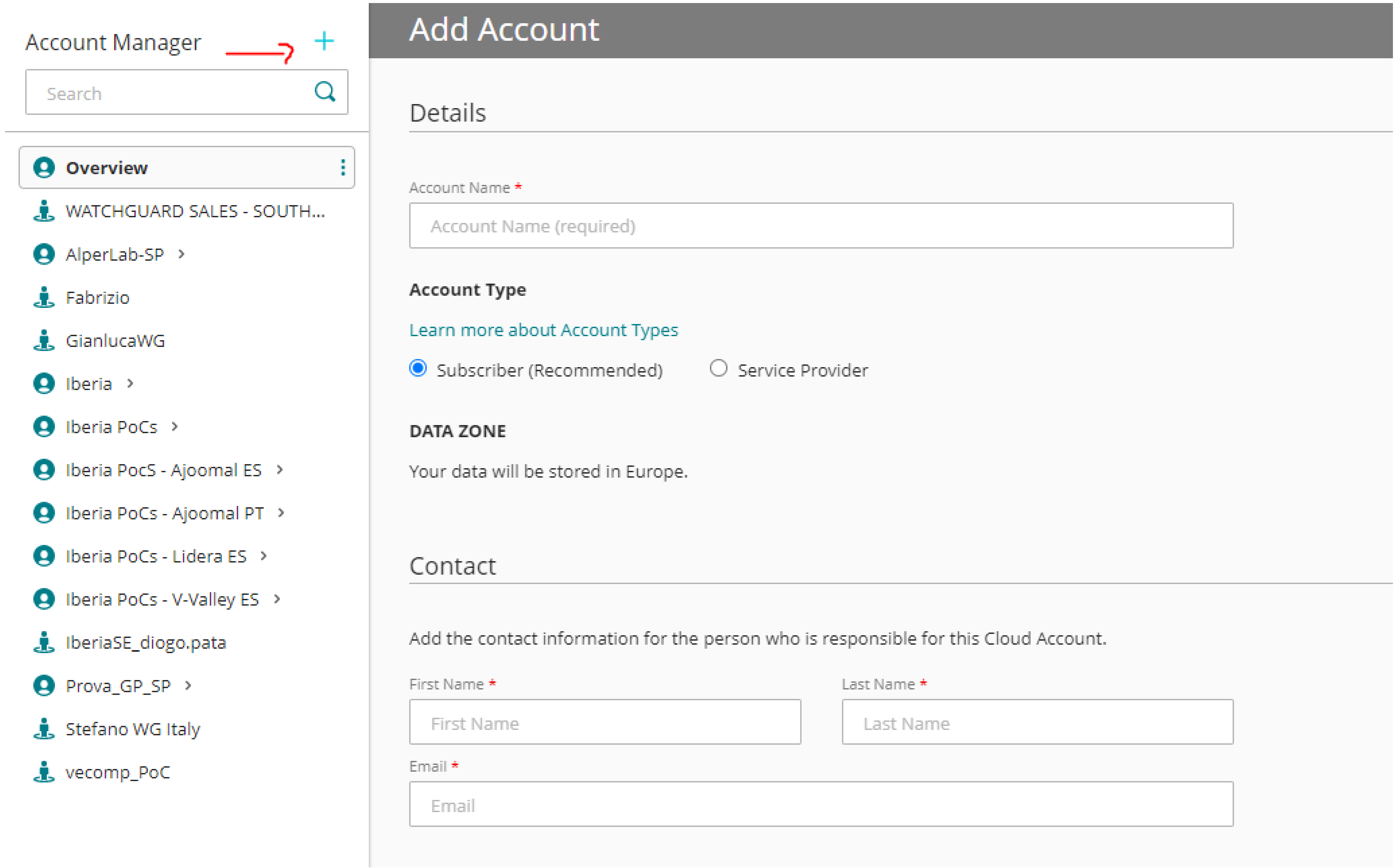
Today: 2022-10-28

- Today
- Yesterday
- Last 24 Hours
- Last 7 Days
- Last 14 Days
- This Month
- Last Month
- Custom

Upgrade Firmware to v12.9.B670038

Dashboard predefinite e query temporale

WatchGuard Unified Security Platform: Semplicità



Account Manager +

Search

- Overview
- WATCHGUARD SALES - SOUTH...
- AlperLab-SP ›
- Fabrizio
- GianlucaWG
- Iberia ›
- Iberia PoCs ›
- Iberia PocS - Ajoomal ES ›
- Iberia PoCs - Ajoomal PT ›
- Iberia PoCs - Lidera ES ›
- Iberia PoCs - V-Valley ES ›
- IberiaSE_diogo.pata
- Prova_GP_SP ›
- Stefano WG Italy
- vecomp_PoC

Add Account

Details

Account Name *

Account Name (required)

Account Type

Learn more about Account Types

● Subscriber (Recommended) ○ Service Provider

DATA ZONE

Your data will be stored in Europe.

Contact

Add the contact information for the person who is responsible for this Cloud Account.

First Name *

First Name

Last Name *

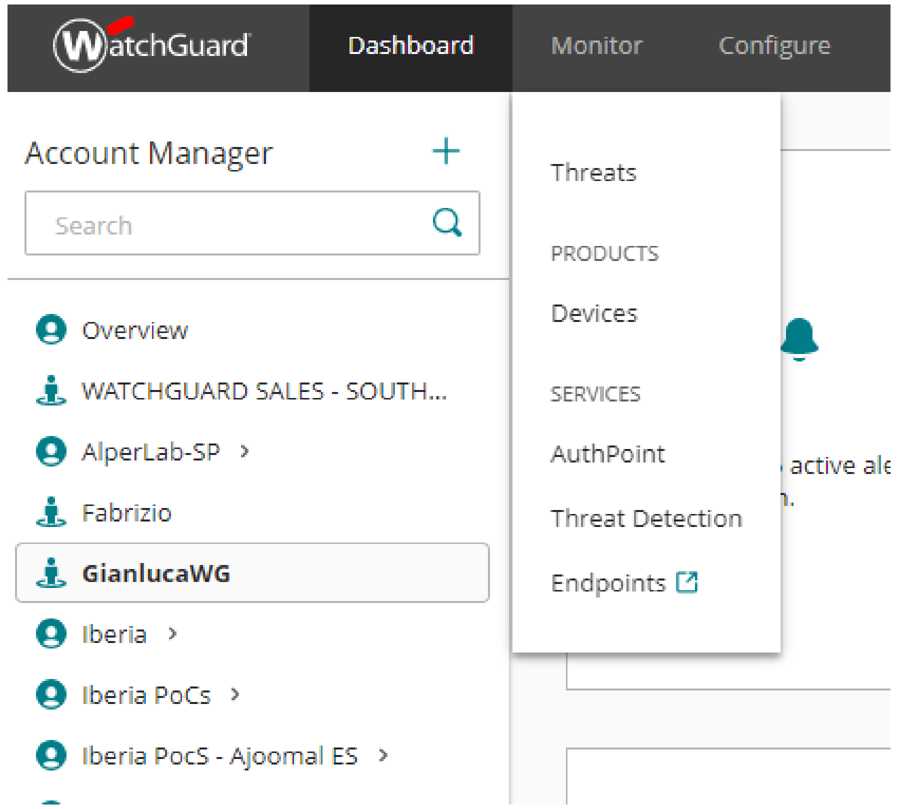
Last Name

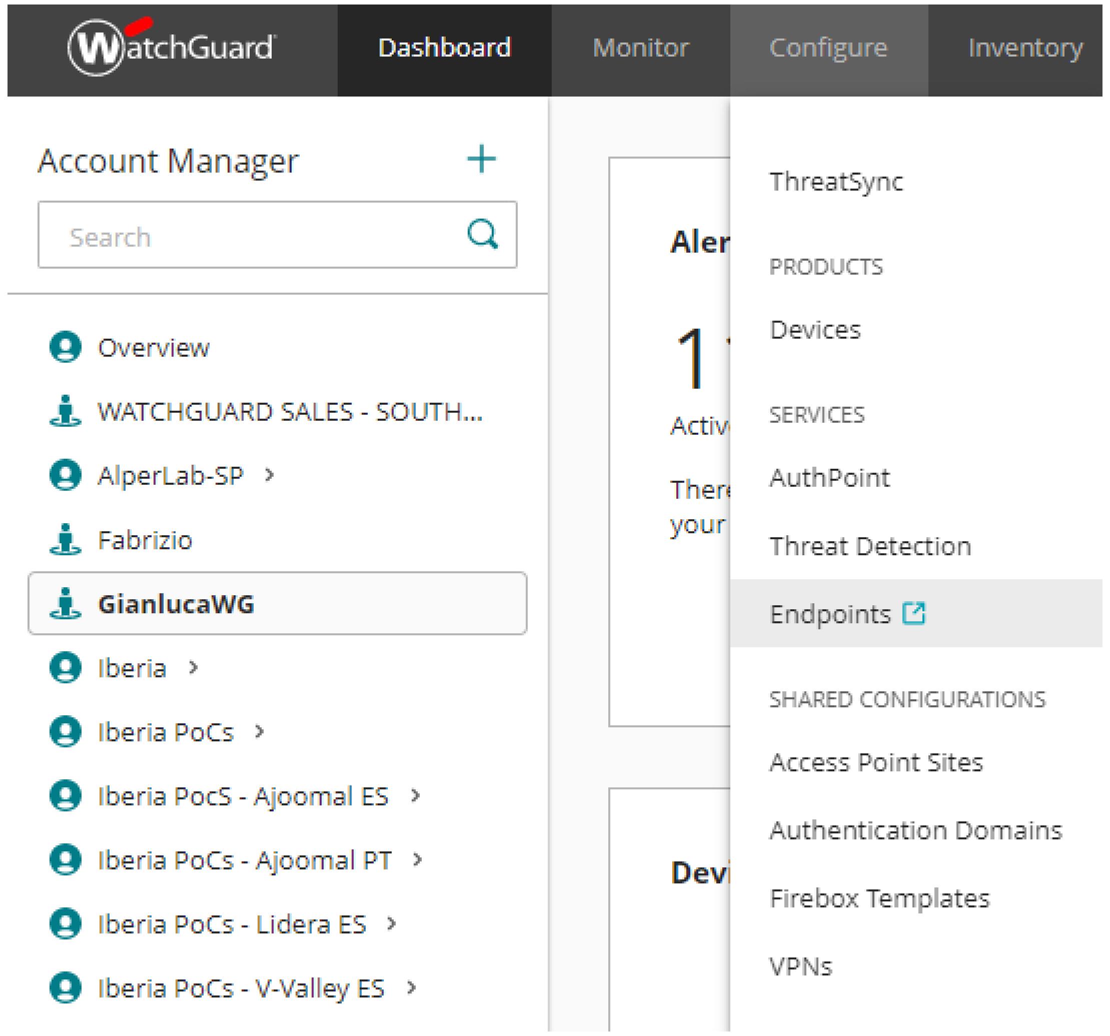
Email *

Email

Creazione nuovi tenant intuitiva e guidata, con identificazione tenant standard (Subscriber) e tenant strutturato (Service Provider)

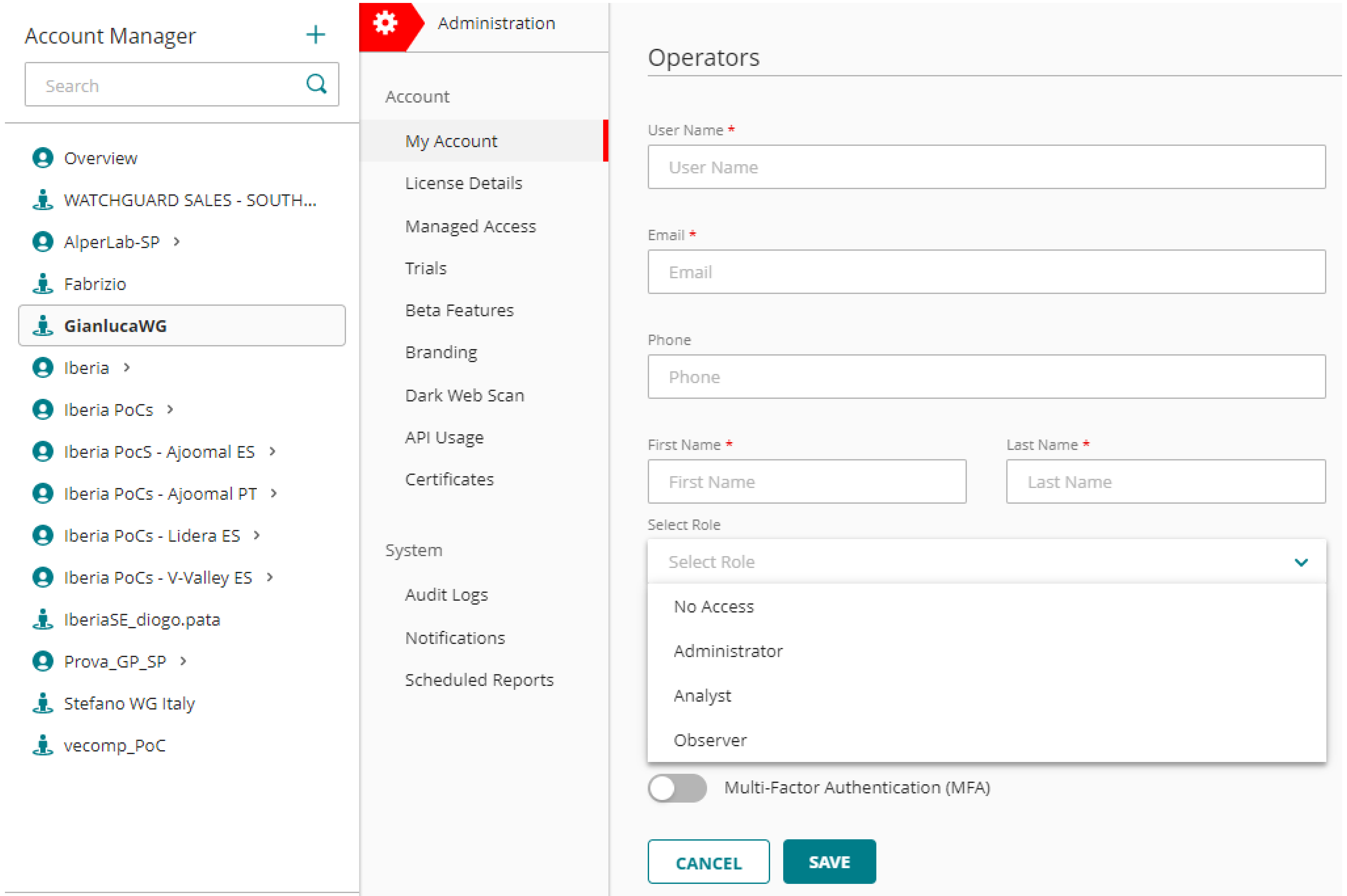
WatchGuard Unified Security Platform: Semplicità





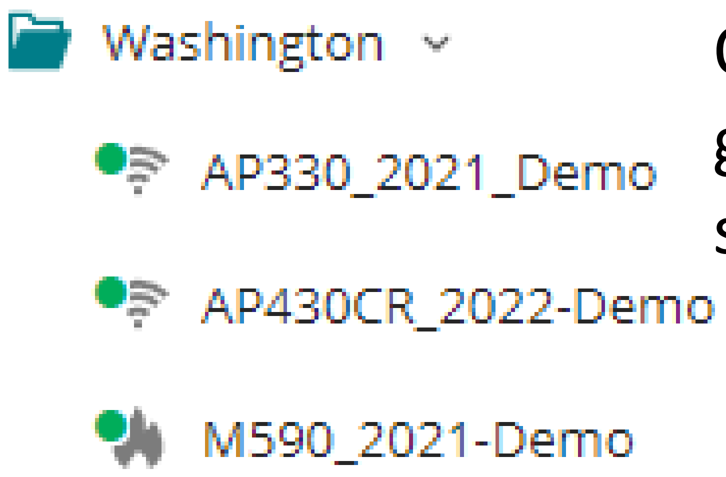
Menù principali di monitoring & configuration specifici per i vari tenant con accesso diretto ai device e Servizi allocati

WatchGuard Unified Security Platform: Accesso sicuro

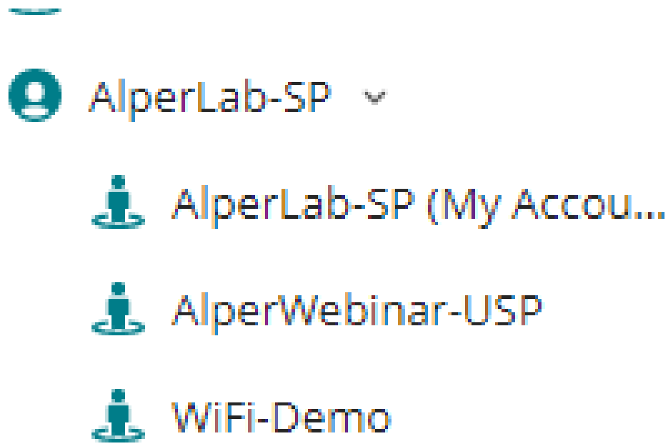


Possibilità di creare operatori di accesso al tenant con vari livelli di permesso, e attivare per ciascuno di loro la protezione multifattore al fine di rendere assolutamente esclusivo e certificato l’accesso al tenant e il relativo ambito di operatività

WatchGuard Unified Security Platform: Flessibilità/Organizzazione


Washington
- AP330_2021_Demo
- AP430CR_2022-Demo
- M590_2021-Demo

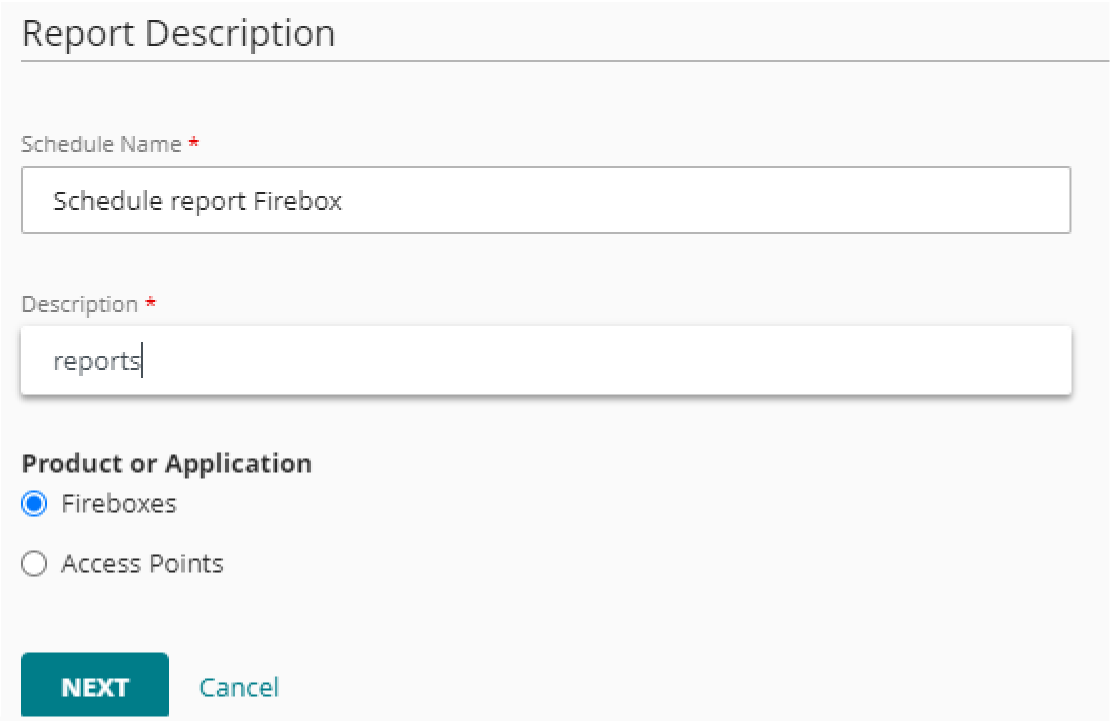
Organizzazione per gruppi di device sotto unico tenant


AlperLab-SP
- AlperLab-SP (My Accou...
- AlperWebinar-USP
- WiFi-Demo

Account standard ed account Service provider per clienti strutturati con più sedi

Flessibilità massima: Scalabilità illimitata per numero di tenant e numero di device, non legata al licensing

WatchGuard Unified Security Platform: Automazione



Report Description

Schedule Name *

Schedule report Firebox

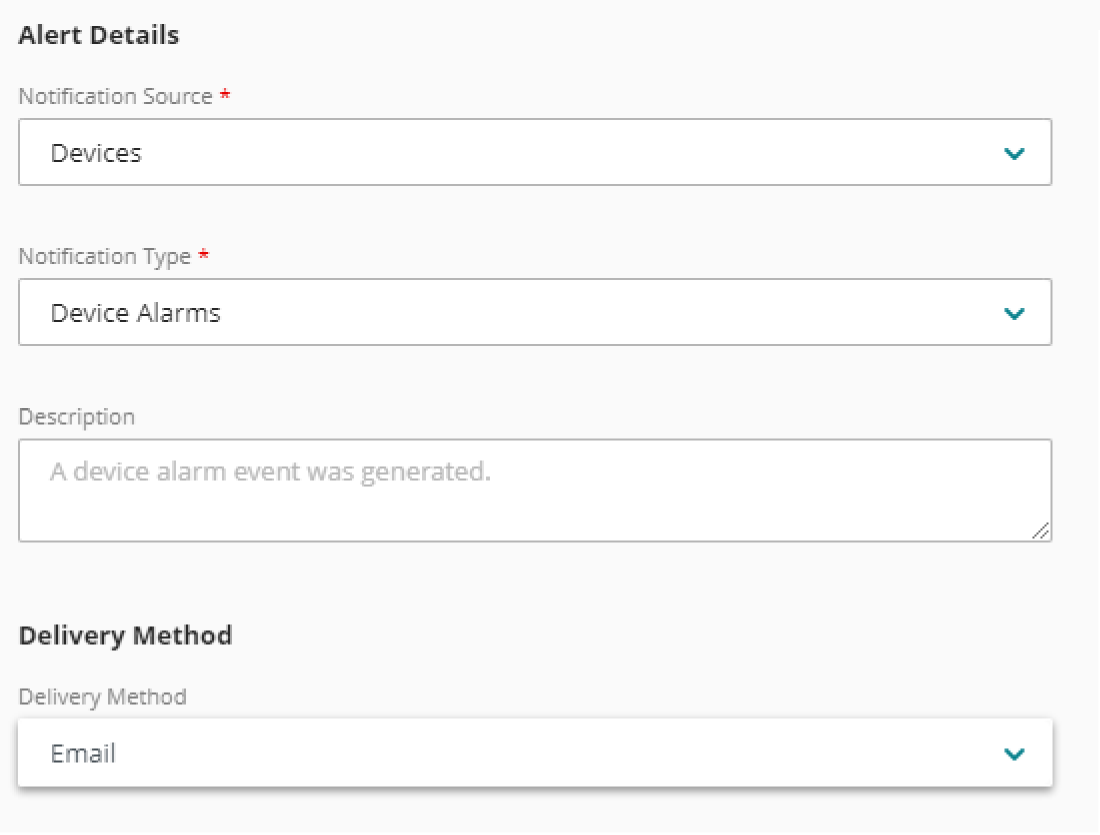
Description *

reports

Product or Application

● Fireboxes

○ Access Points



Alert Details

Notification Source *

Devices

Notification Type *

Device Alarms

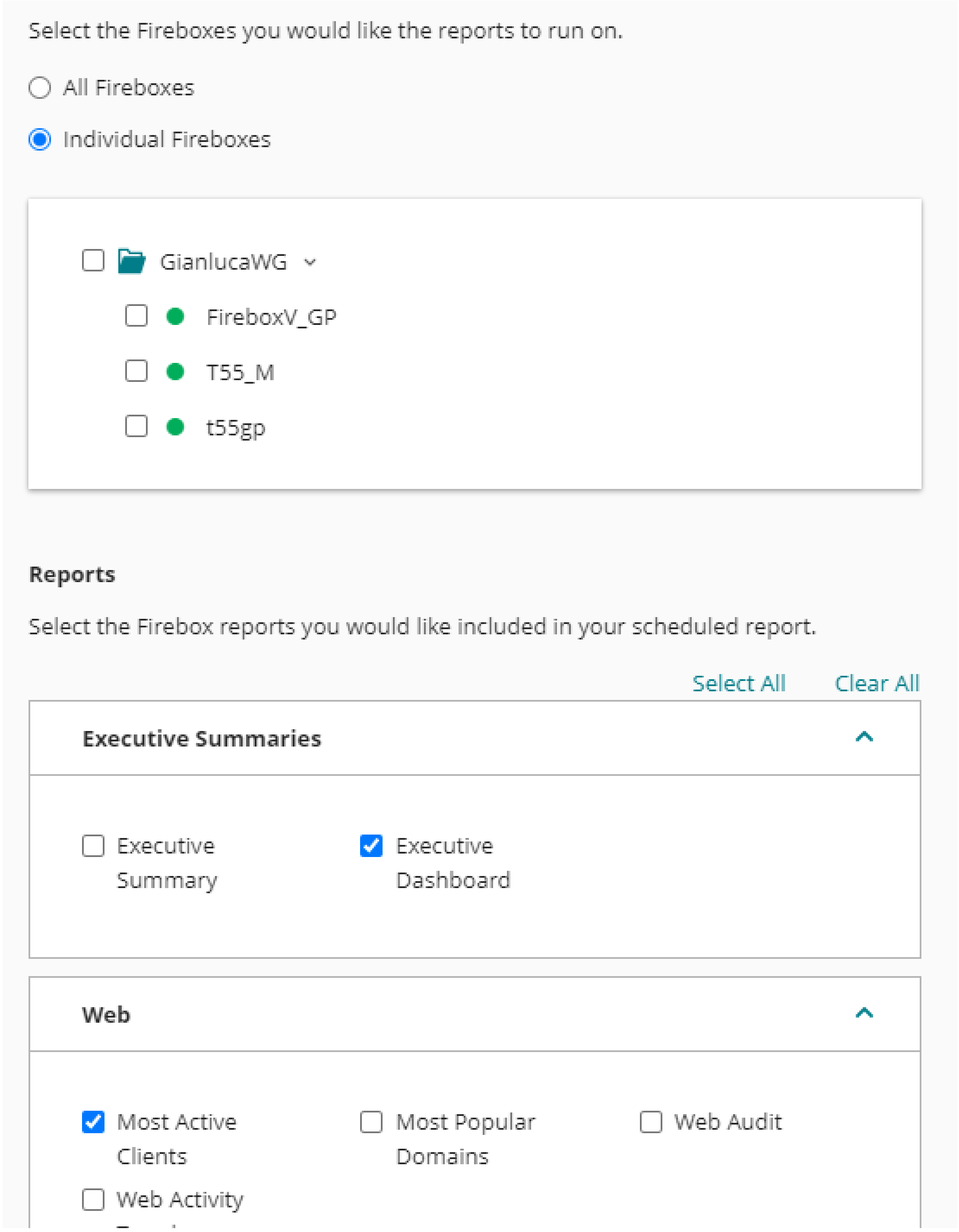
Description

A device alarm event was generated.

Delivery Method

Delivery Method

Email



Select the Fireboxes you would like the reports to run on.

○ All Fireboxes

● Individual Fireboxes

☐ GianlucaWG
- ☐ ● FireboxV_GP
- ☐ ● T55_M
- ☐ ● t55gp

Reports

Select the Firebox reports you would like included in your scheduled report.

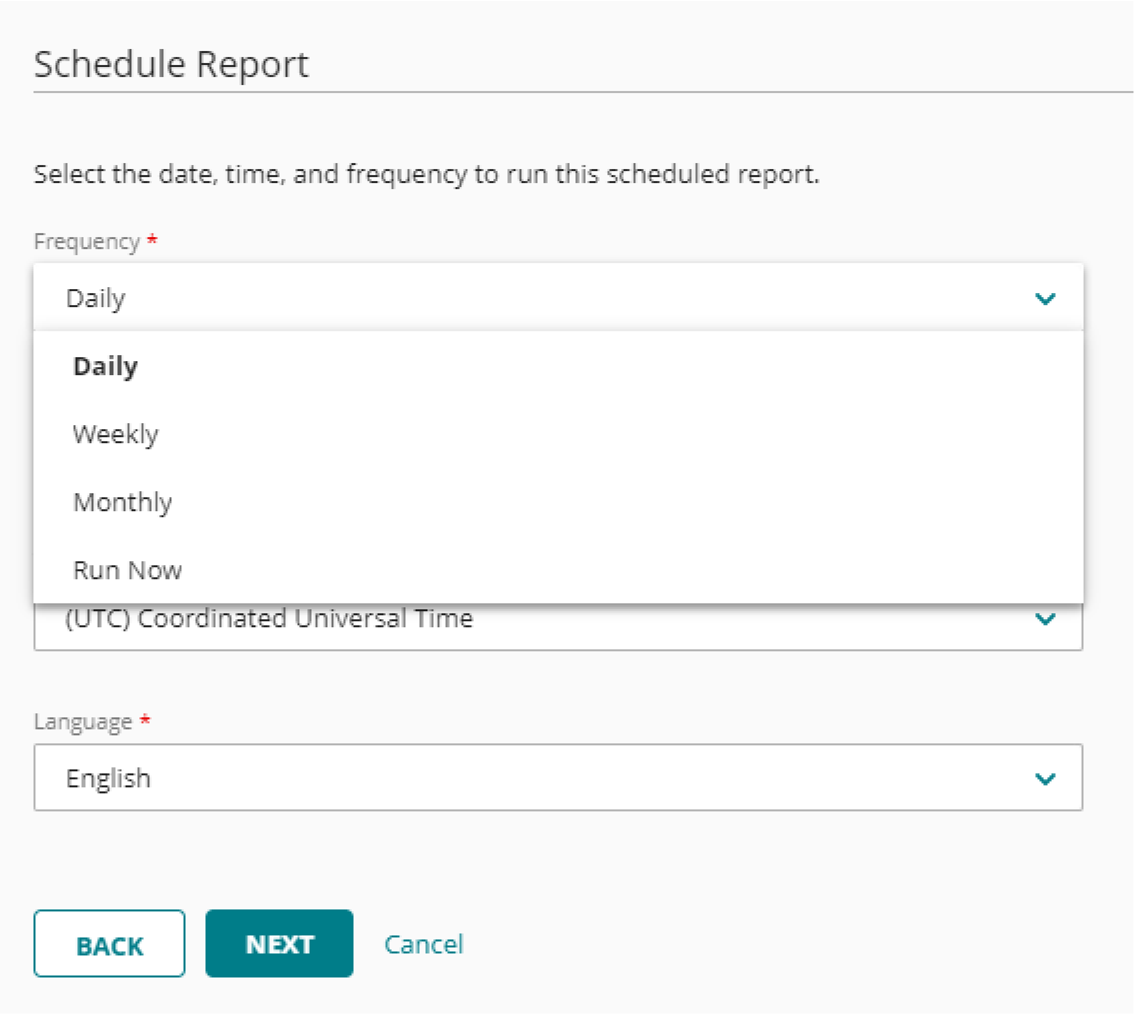
Executive Summaries

☐ Executive Summary ☑ Executive Dashboard

Web

☑ Most Active Clients ☐ Most Popular Domains ☐ Web Audit

☐ Web Activity



Schedule Report

Select the date, time, and frequency to run this scheduled report.

Frequency *

Daily

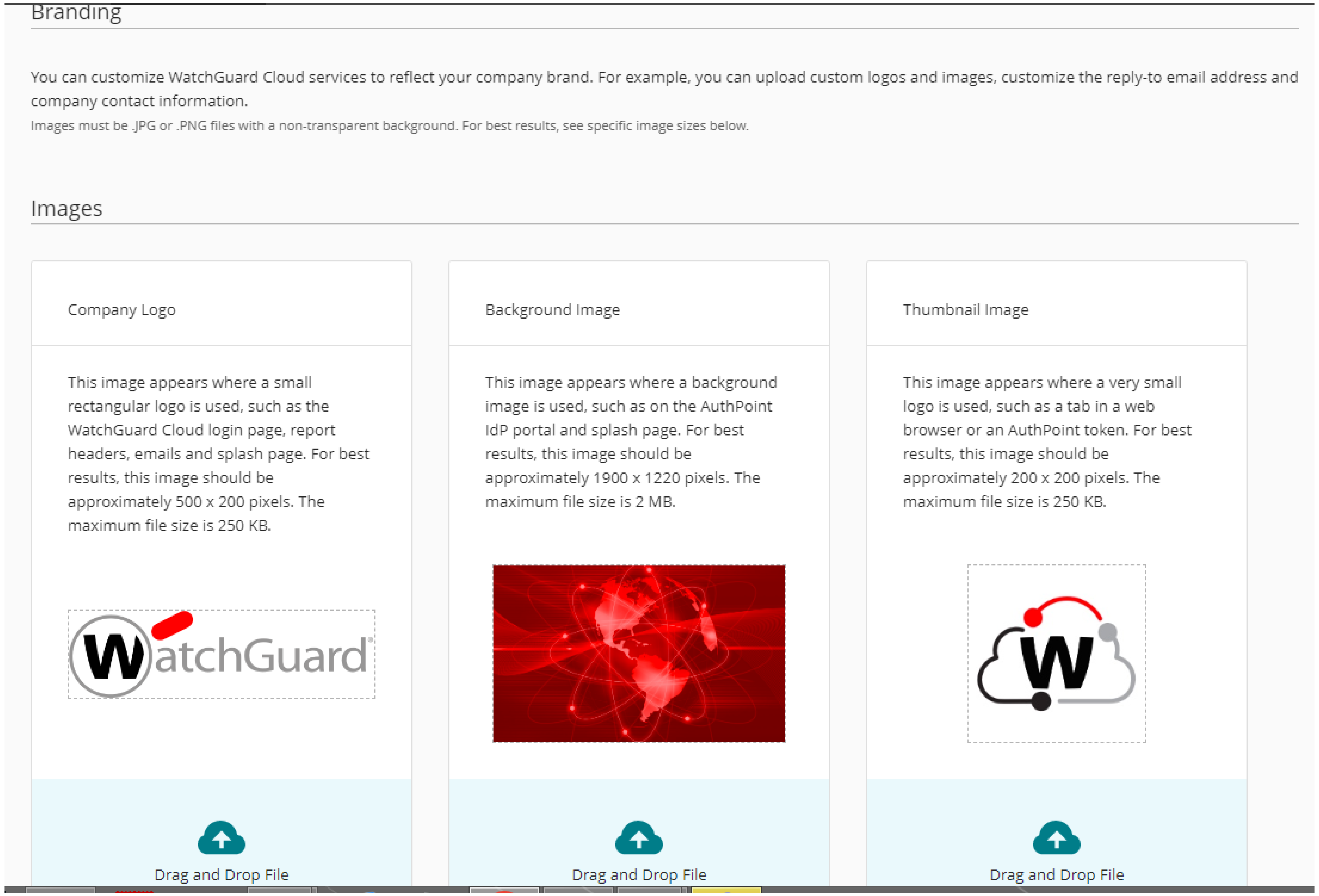
(UTC) Coordinated Universal Time

Language *

English

Automazione: invio report e notifiche schedulate con programmazione e differenziazione di più task

WatchGuard Unified Security Platform: Personalizzazione



Branding

You can customize WatchGuard Cloud services to reflect your company brand. For example, you can upload custom logos and images, customize the reply-to email address and company contact information.

Images must be .JPG or .PNG files with a non-transparent background. For best results, see specific image sizes below.

Images

Company Logo

This image appears where a small rectangular logo is used, such as the WatchGuard Cloud login page, report headers, emails and splash page. For best results, this image should be approximately 500 x 200 pixels. The maximum file size is 250 KB.

Drag and Drop File

Background Image

This image appears where a background image is used, such as on the AuthPoint IdP portal and splash page. For best results, this image should be approximately 1900 x 1220 pixels. The maximum file size is 2 MB.

Drag and Drop File

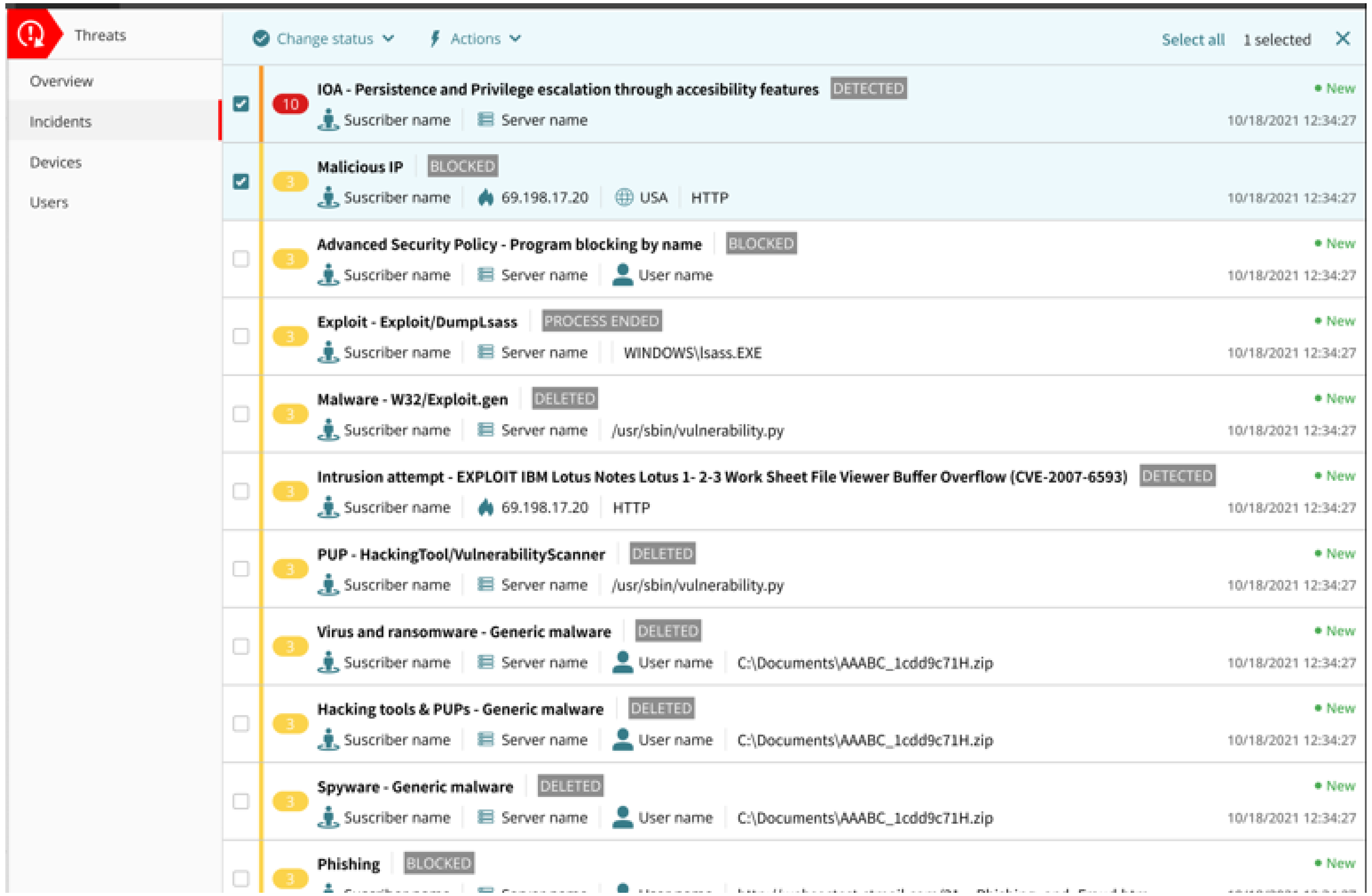
Thumbnail Image

This image appears where a very small logo is used, such as a tab in a web browser or an AuthPoint token. For best results, this image should be approximately 200 x 200 pixels. The maximum file size is 250 KB.

Drag and Drop File

Customizzazione dei portali di accesso, autenticazione e delle varie mail di delivery

WatchGuard Unified Security Platform: Next Step….
XDR!!



☑ 10 IOA - Persistence and Privilege escalation through accesibility features DETECTED • New
Suscriber name | Server name 10/18/2021 12:34:27

☑ 3 Malicious IP BLOCKED
Suscriber name | 69.198.17.20 | USA | HTTP 10/18/2021 12:34:27

□ 3 Advanced Security Policy - Program blocking by name BLOCKED • New
Suscriber name | Server name | User name 10/18/2021 12:34:27

□ 3 Exploit - Exploit/DumpLsass PROCESS ENDED • New
Suscriber name | Server name | WINDOWS\lsass.EXE 10/18/2021 12:34:27

□ 3 Malware - W32/Exploit.gen DELETED • New
Suscriber name | Server name | /usr/sbin/vulnerability.py 10/18/2021 12:34:27

□ 3 Intrusion attempt - EXPLOIT IBM Lotus Notes Lotus 1- 2-3 Work Sheet File Viewer Buffer Overflow (CVE-2007-6593) DETECTED • New
Suscriber name | 69.198.17.20 | HTTP 10/18/2021 12:34:27

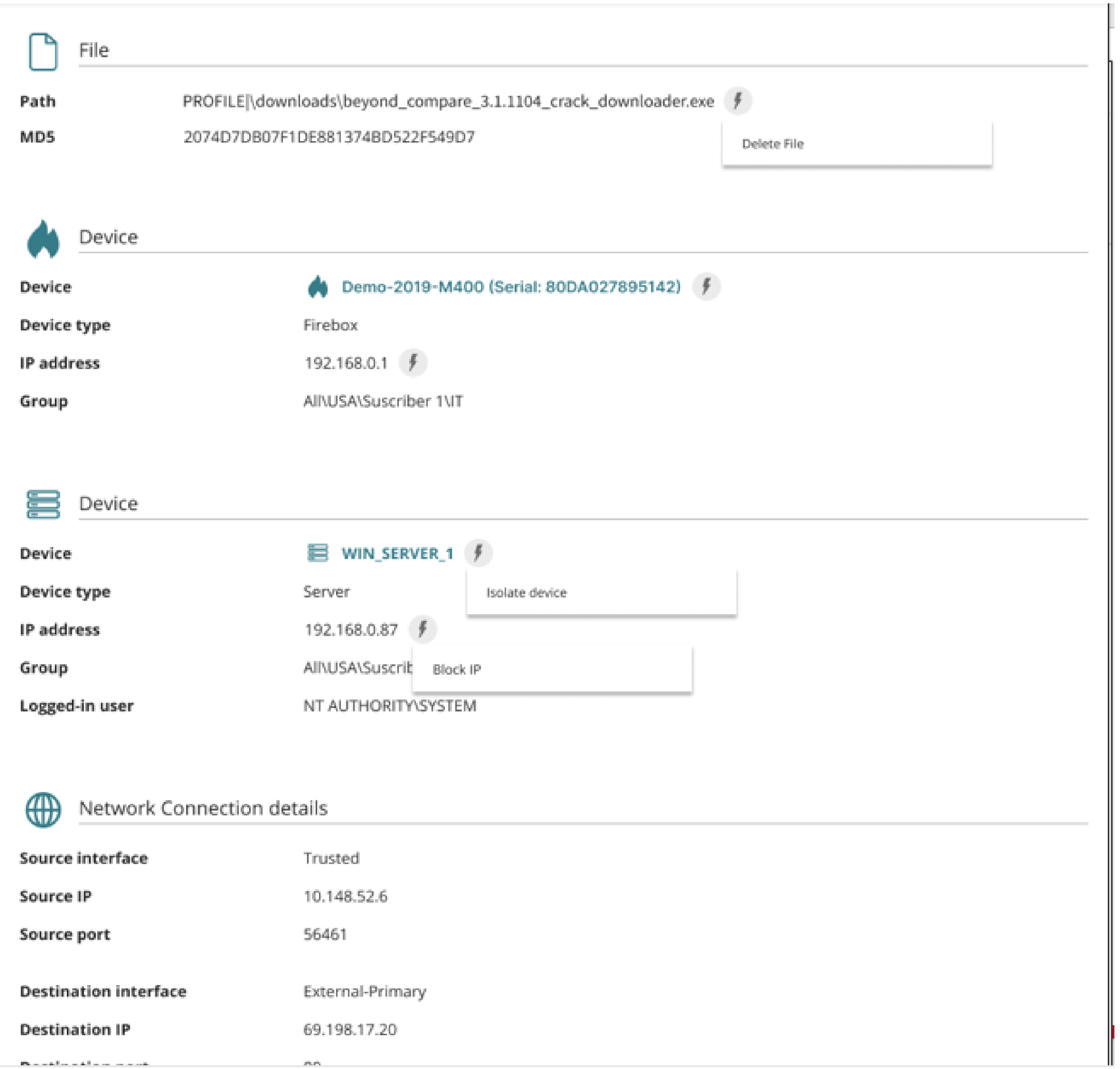
□ 3 PUP - HackingTool/VulnerabilityScanner DELETED • New
Suscriber name | Server name | /usr/sbin/vulnerability.py 10/18/2021 12:34:27

□ 3 Virus and ransomware - Generic malware DELETED • New
Suscriber name | Server name | User name | C:\Documents\AAABC_1cdd9c71H.zip 10/18/2021 12:34:27

□ 3 Hacking tools & PUPs - Generic malware DELETED • New
Suscriber name | Server name | User name | C:\Documents\AAABC_1cdd9c71H.zip 10/18/2021 12:34:27

□ 3 Spyware - Generic malware DELETED • New
Suscriber name | Server name | User name | C:\Documents\AAABC_1cdd9c71H.zip 10/18/2021 12:34:27

□ 3 Phishing BLOCKED • New



File

Path	PROFILE|\downloads\beyond_compare_3.1.1104_crack_downloader.exe
MD5	2074D7DB07F1DE881374BD522F549D7

Device

Device	Demo-2019-M400 (Serial: 80DA027895142)
Device type	Firebox
IP address	192.168.0.1
Group	All\USA\Suscriber 1\IT

Device

Device	WIN_SERVER_1
Device type	Server
IP address	192.168.0.87
Group	All\USA\Suscrit
Logged-in user	NT AUTHORITY\SYSTEM

Network Connection details

Source interface	Trusted
Source IP	10.148.52.6
Source port	56461
Destination interface	External-Primary
Destination IP	69.198.17.20

Q&A

CONTATTI RELATORI

GIANLUCA PUCCI

GIANLUCA.PUCCI@WATCHGUARD.COM