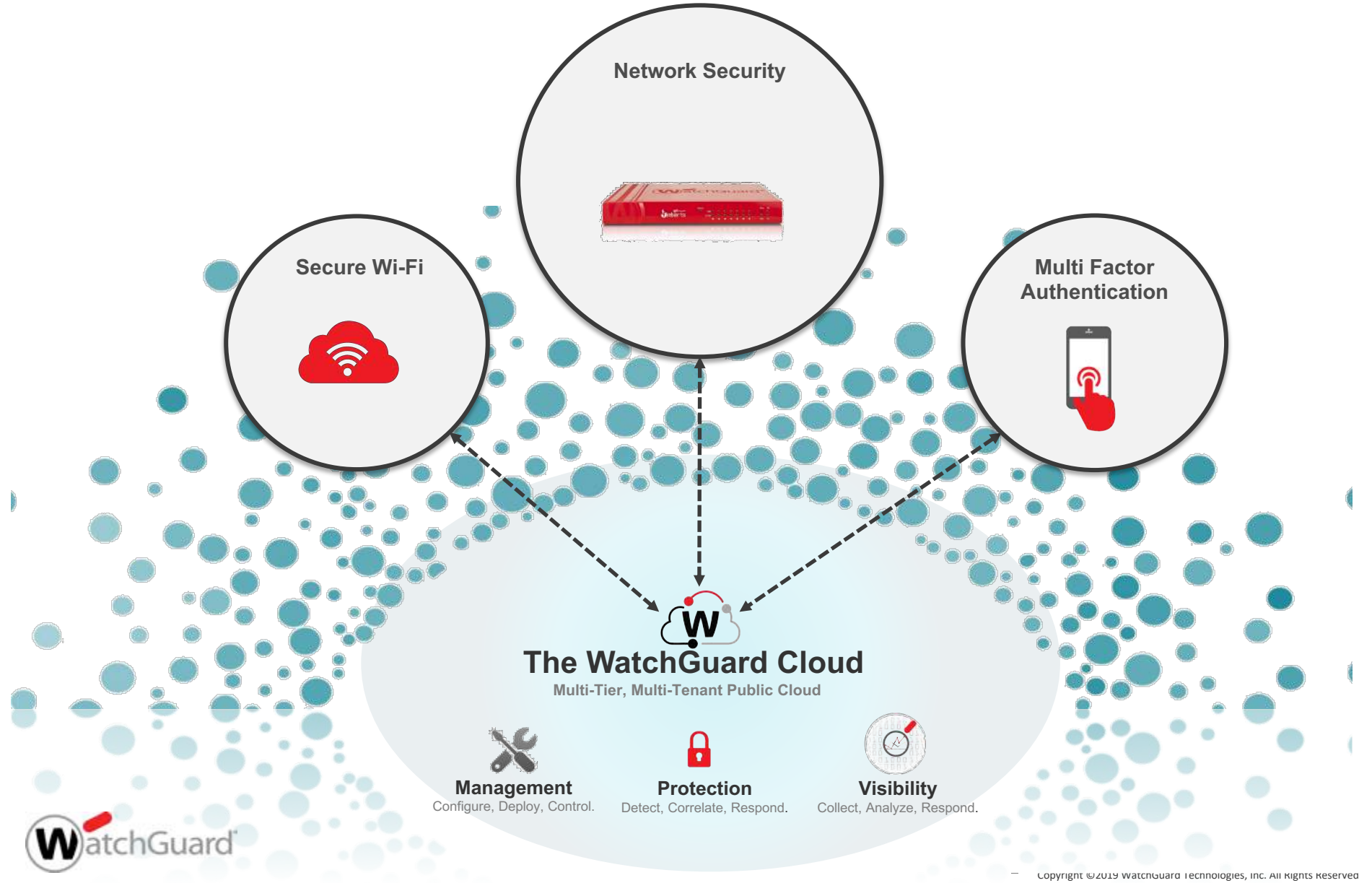
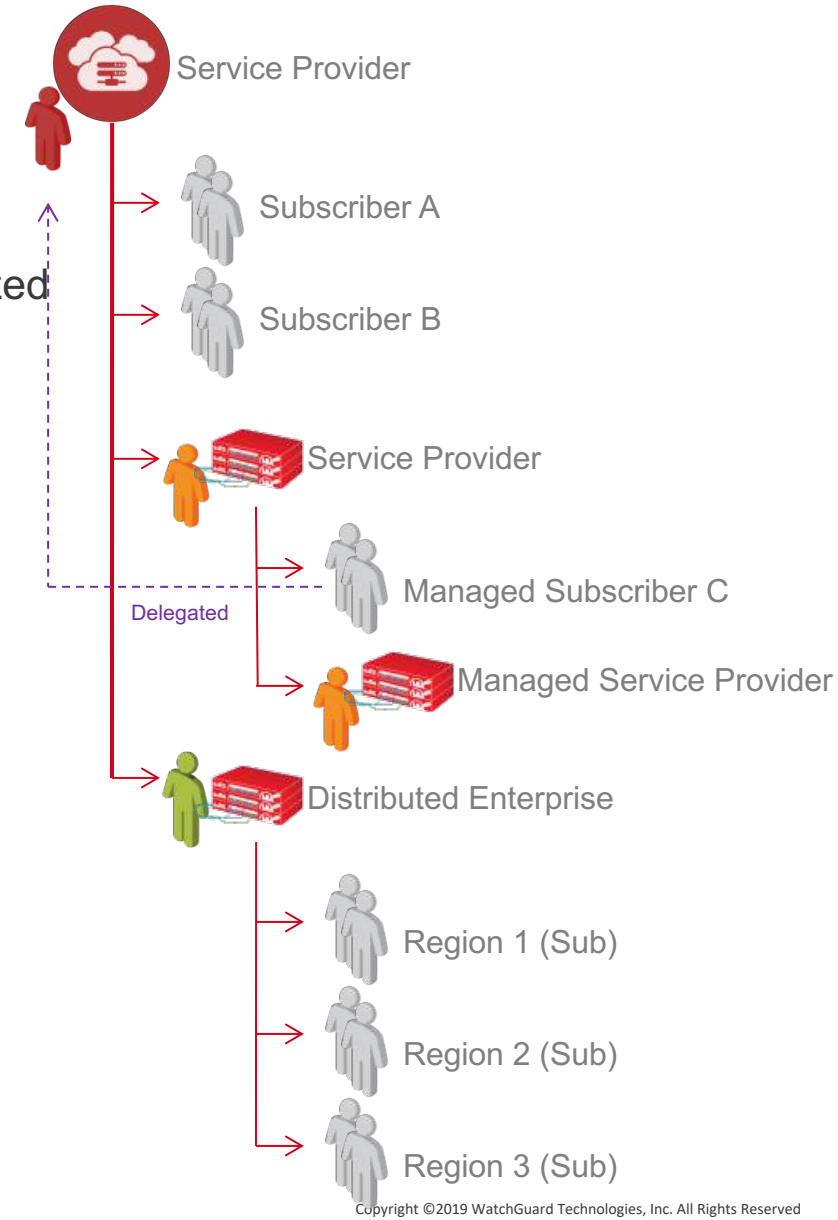
Best Practice – Visibility
Eine Funktion der WatchGuard Cloud

WatchGuard Cloud – Die Idee



Mandantenfähigkeit der WatchGuard Cloud

- Multi-tenant architecture
  - Complete segregation
  - Scales to thousands of companies
  - Unlimited numbers of users per company
- Manage multiple organizations from one centralized interface
  - Unlimited numbers of companies
  - Supports multiple groups/domains
- Secure
  - Only view one level down - you can see your own virtual server as well as the virtual servers of the accounts you create
- Delegated management for cross tiers
  - Deliver enhanced service wrappers
  - Great for multi-region networks and subsidiaries
- Inherit capabilities to lower level
  - Security templates
  - Branding

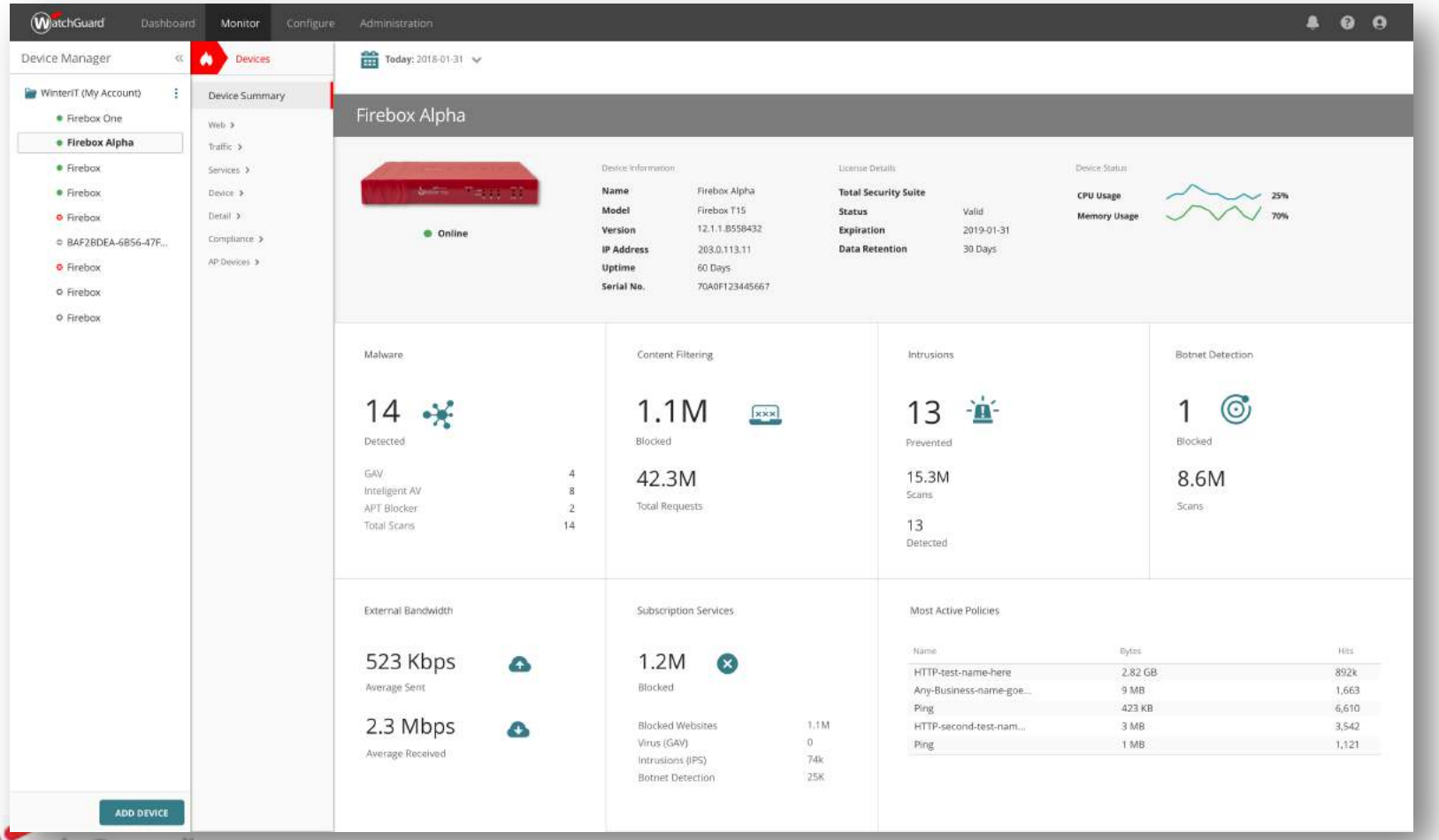


Insightful, actionable network security visibility

- Zugriff auf über 100 Reports und Dashboards
- Schneller Zugriff auf wichtige Details per Drill-Down
- Übersetzt Kommunikationsinformation in nutzbare Daten
- Skalierbar und ohne Aufbau eigener Systeme nutzbar
- Mandantenfähige Struktur
- Automatisierte Alarme und Benachrichtigungen
- Role-based Access Control (RBAC)
- Flexible Aufbewahrungszeiten der Daten

Device Summary Dashboard

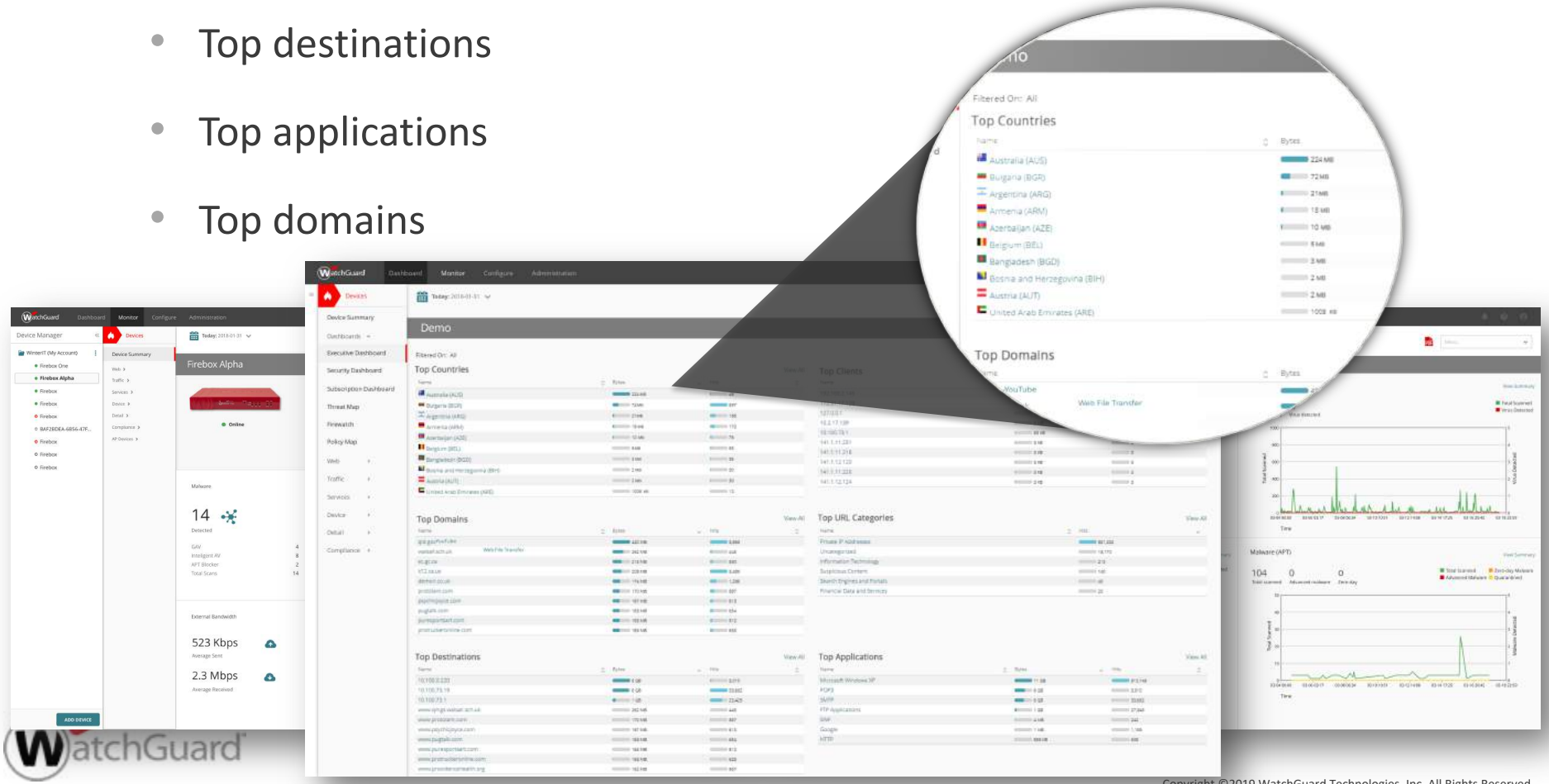
Übersicht der Systeme und Lizensierung



Executive Dashboards

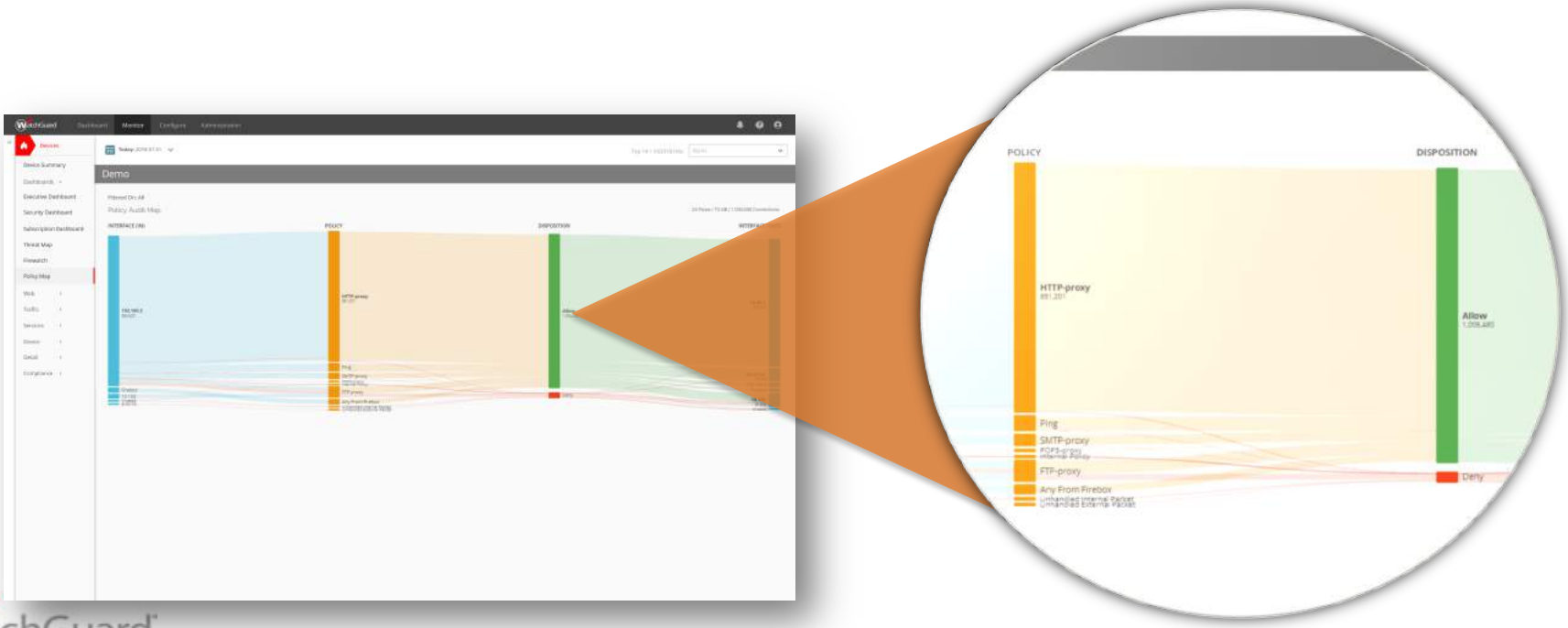
Übersicht zu Netzwerk-Kommunikation, u.A. über:

- Top users
- Top destinations
- Top applications
- Top domains



Policy Map

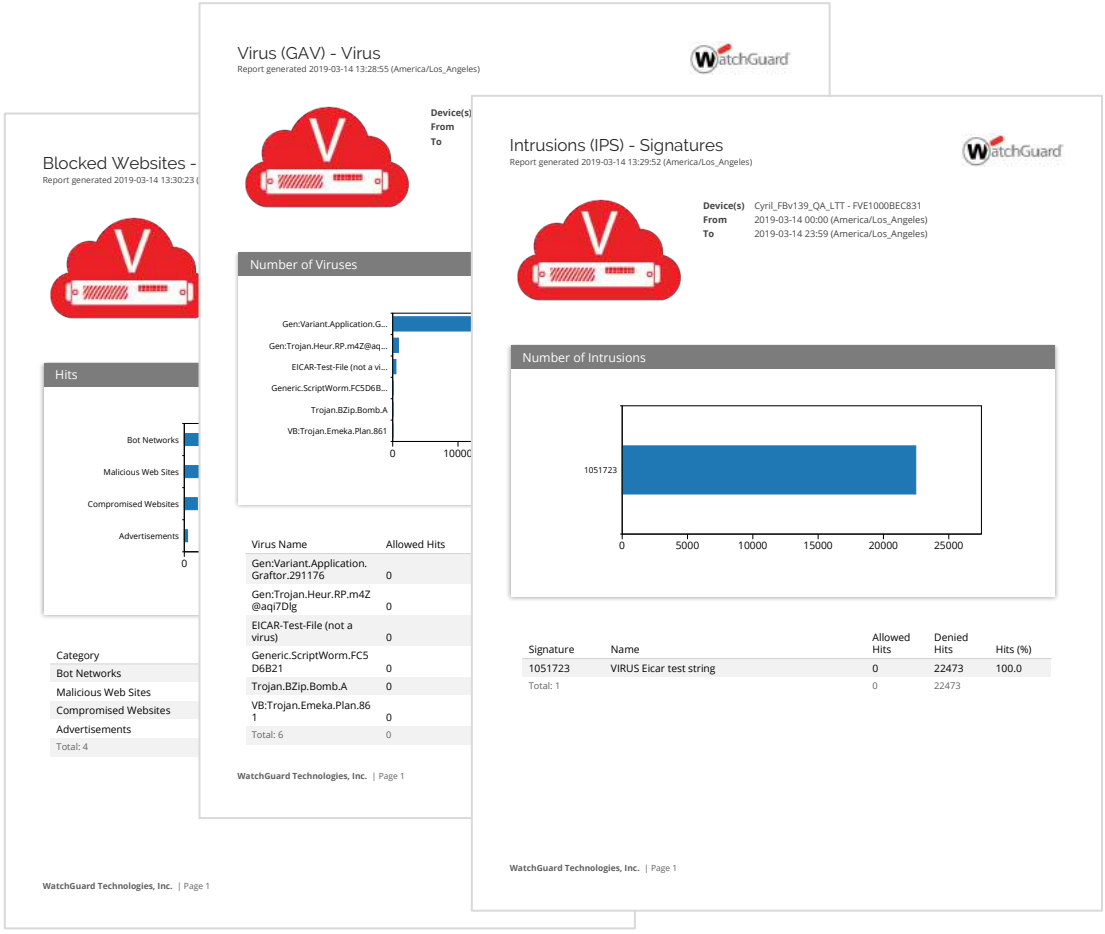
Die Policy Map stellt das Regelwerk Ihrer Firebox visuell dar. Hierin sehen Sie sofort welche Datenströme die jeweiligen Firewall-Regeln nutzen und können somit schnell und einfach Fehlkonfigurationen erkennen und daS Regelwerk optimieren.



Compliance Reports

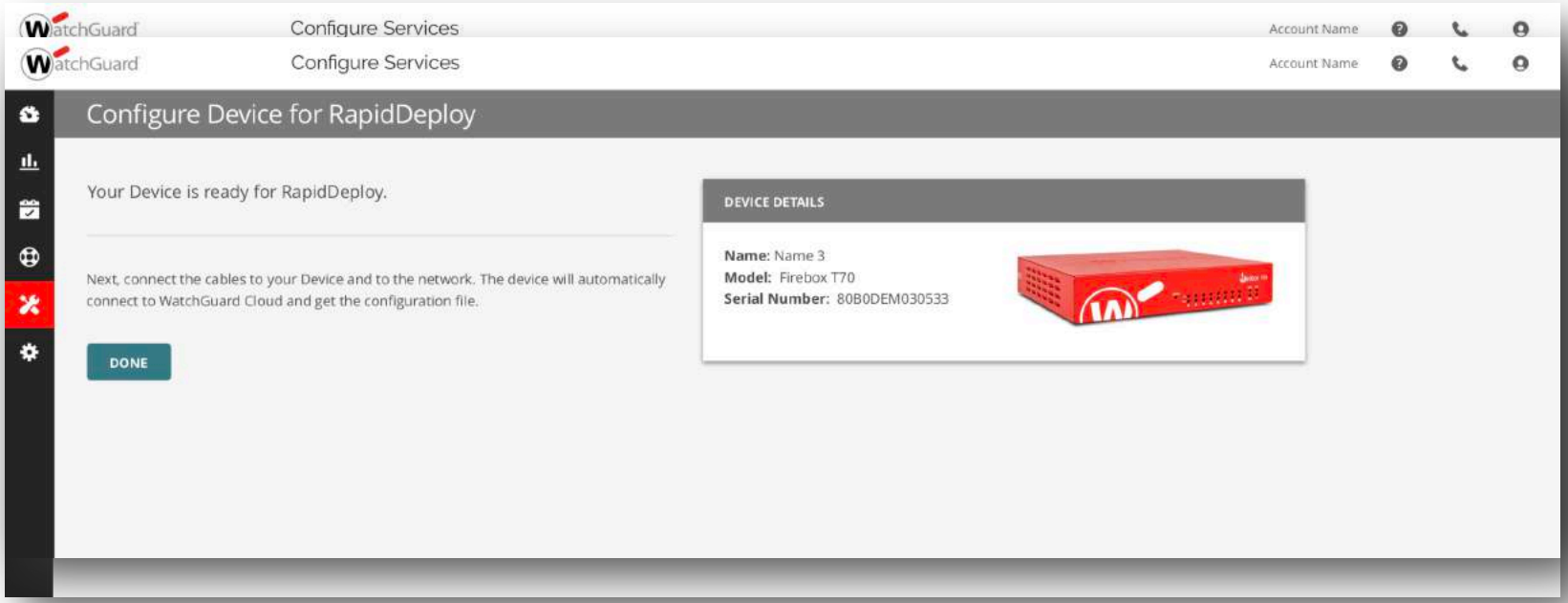
Eingebaute Compliance Report zu:

- PCI-DSS
- HIPAA
- KCSiE (UK)



RapidDeploy ist voll integriert

- Integration neuer Standorte ohne geschultes (IT-)Personal vor Ort
- Zero-touch deployment
- Laden Sie eine vorbereitete Konfigurationsdatei in die WatchGuard Cloud – die neuen Firebox Systeme wenden diese sofort an und schützen direkt.



Lizensierung

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
WatchGuard Cloud Visibility Data Retention	30 Days	1 Day
Support	Gold (24x7)	Standard (24x7)

*Available on latest generation M Series appliances

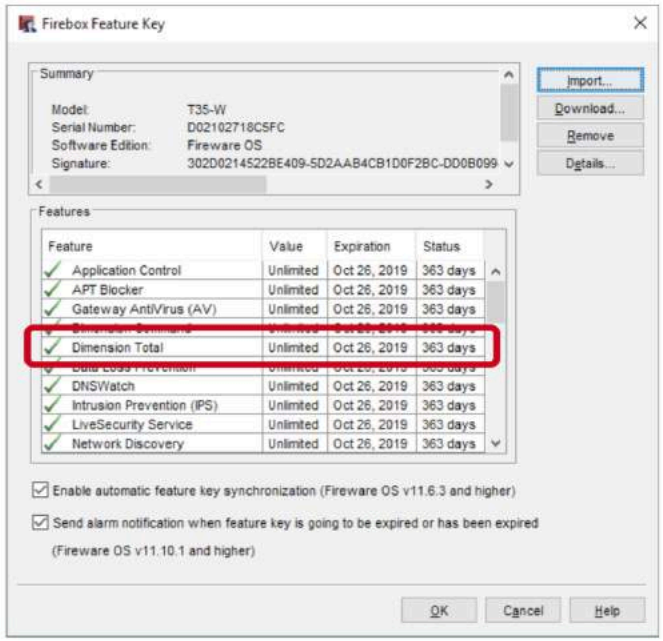
Note: Fireboxes can simultaneously log to WatchGuard Cloud and Dimension.

Anforderungen

- Unterstützte Firebox Systeme:
  - Hardware: Firebox M Series, T Series
  - Virtual: FireboxV, FireboxCloud
- Lizensierung:
  • Basic Security oder Total Security Suite
- Fireware Anforderungen:
  - Fireware v12.0 oder höher ist erforderlich
  - Fireware v12.4 oder höher ist für Firecluster erforderlich
  - WatchGuard Cloud RapidDeploy, benötigt ein „Manufacturing Release“ Fireware v12.3.1 oder höher

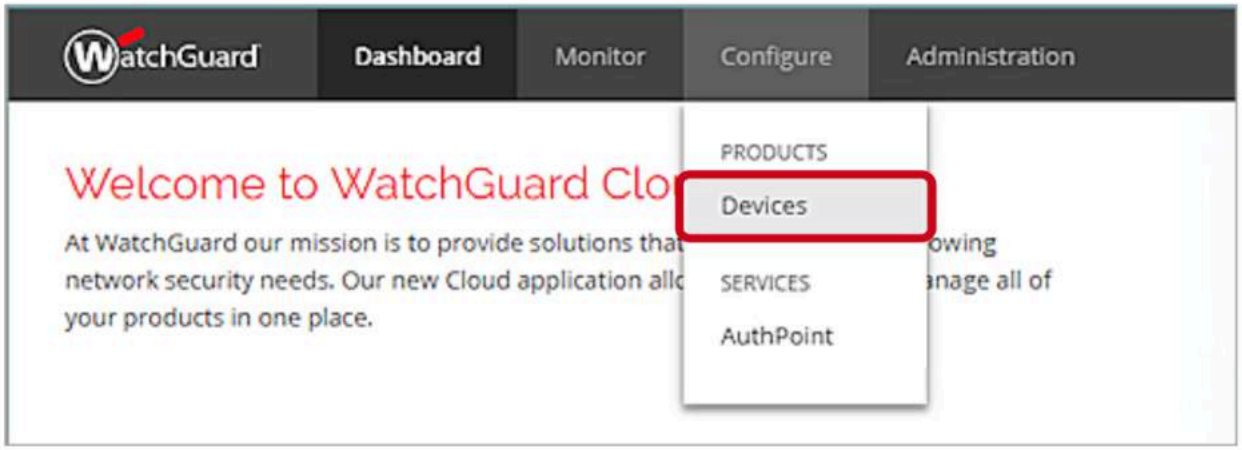
Feature Key für WatchGuard Cloud Visibility

- Einer der folgende Einträge muss im FeatureKey der Appliance vorhanden sein:
- Dimension Total
  - Für Systeme mit **Total Security Suite**
  - Enthält 30 Tage Aufbewahrungszeit in der WatchGuard Cloud
- Dimension Basic
  - Für Systeme mit **Basic Security Suite**
  - Enthält 1 Tag Aufbewahrungszeit in der WatchGuard Cloud



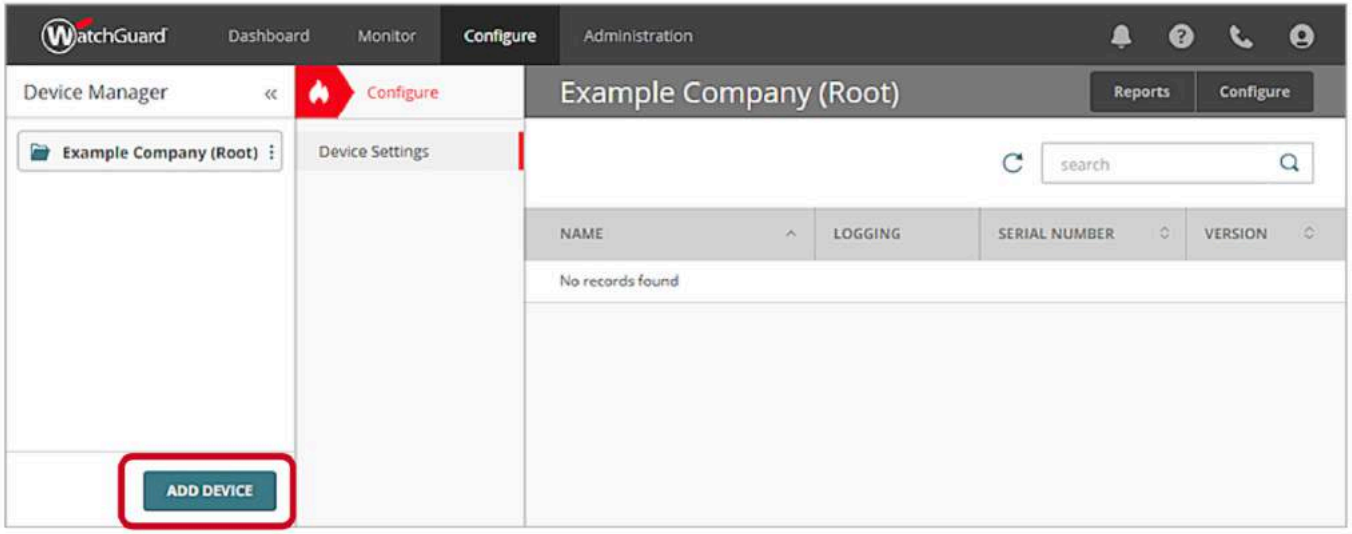
Hinzufügen einer Firebox

- Öffnen Sie cloud.watchguard.com
  - Die Anmeldung erfolgt mit dem üblichen WatchGuard Portal User
  - Die Ansicht kann für Endkunden und Partner variieren.
- ImWatchGuard Cloud Subscriber account gelangen Sie über **Configure> Devices** zu den neuen Visibility Funktionen



Hinzufügen einer Firebox

- Firebox Systeme werden nicht automatisiert hinzugefügt (wenn diese im www.watchguard.com Account aktiviert wurden).
- Um eine aktivierte Firebox hinzuzufügen nutzen Sie **Add Device**



Zwei Möglichkeiten zur Aktivierung

- Neue Firebox Systeme können über zwei Wege hinzugefügt werden:
  - **Apply Verification Code**
    - Hierbei wird ein Code genriert, der manuell in die Konfiguration der Firebox übernommen werden muss.
  - **Setup with RapidDeploy**
    - Hiermit kann RapidDeploy verwendet werden, um über die WatchGuard Cloud eine vorbereitete Konfiguration zu verwenden.
    - Diese Möglichkeit besteht nur für Firebox Systeme, die eine “Manufacturing Version” von Fireware v12.3.1 oder höher haben.

Hinzufügen über den Verification Code

WatchGuard Dashboard Monitor **Configure** Administration

Apply Verification Code

For your device to connect to WatchGuard Cloud, in the device configuration you must enable WatchGuard Cloud and add the Verification Code.

To set up a new device, connect to Fireware Web UI, run the Web Setup Wizard, and then enable WatchGuard Cloud.

Learn more about Verification Codes

Device Details

Name: T35-W_Seattle
Model: Firebox T35-W
Serial Number: D021027...

Copy Your Verification Code

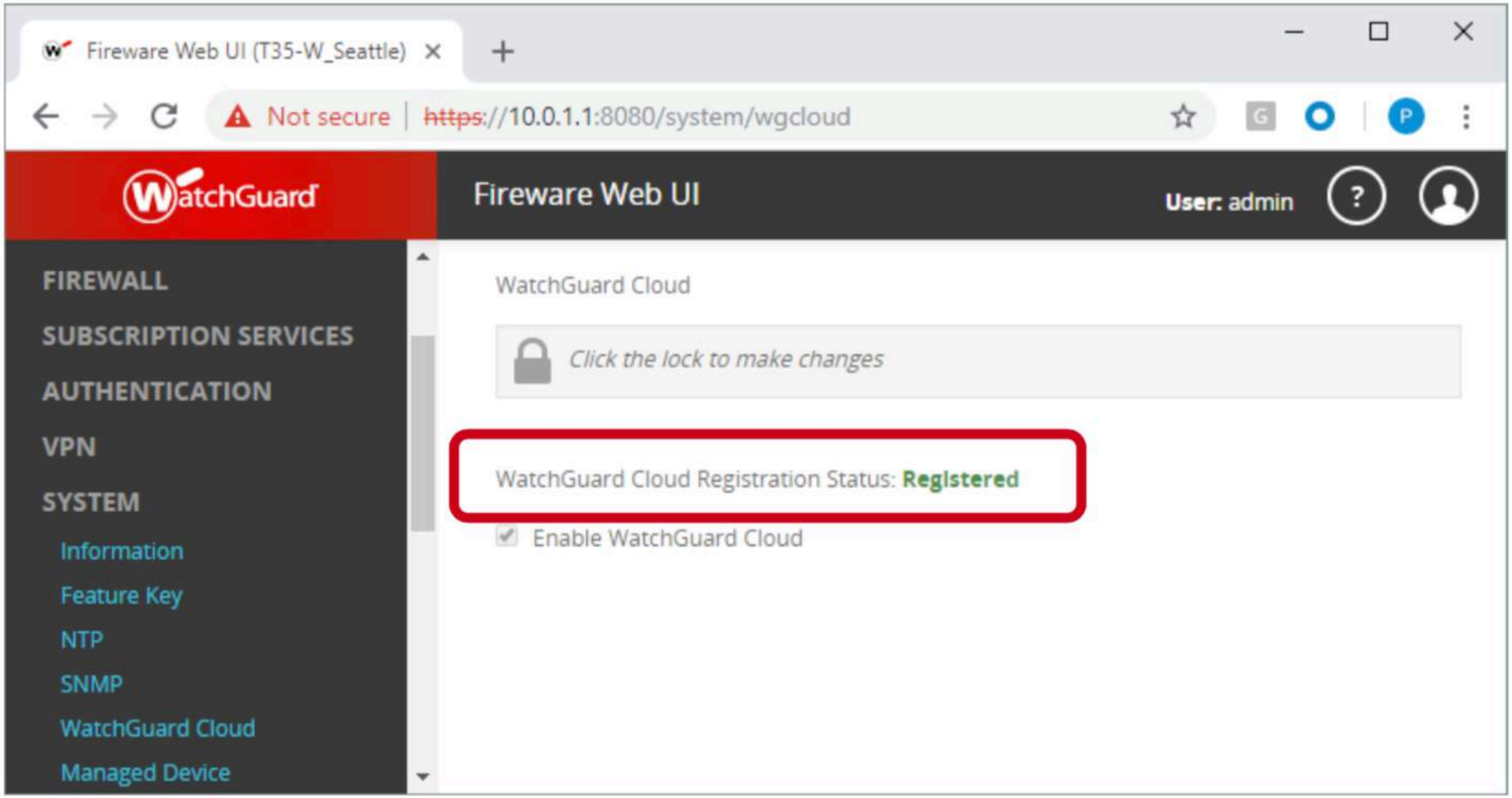
B1A538B59C934236A12586A5F19B6C48 **COPY CODE**

Add the Verification Code to Your Device

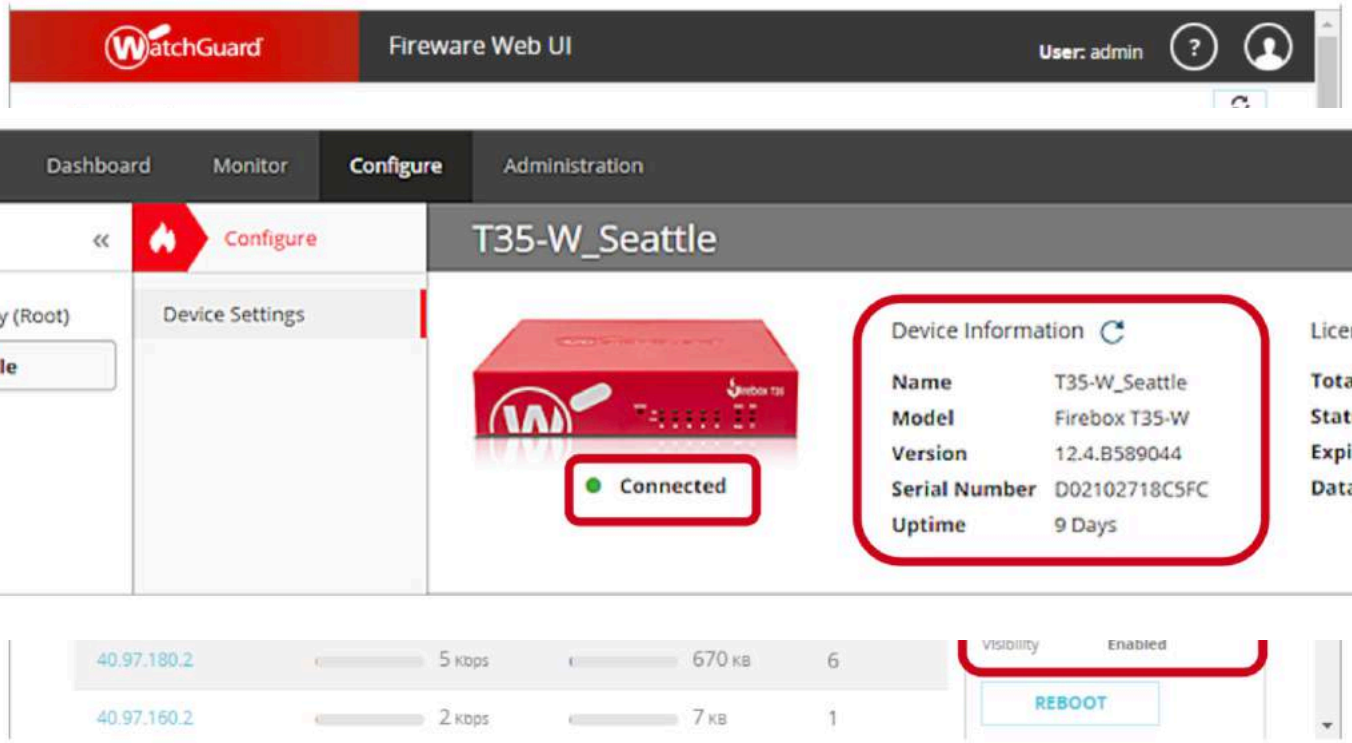
In your device configuration, enable WatchGuard Cloud and paste the Verification Code.

DONE

Firebox Konfiguration



Status der Verbindung prüfen

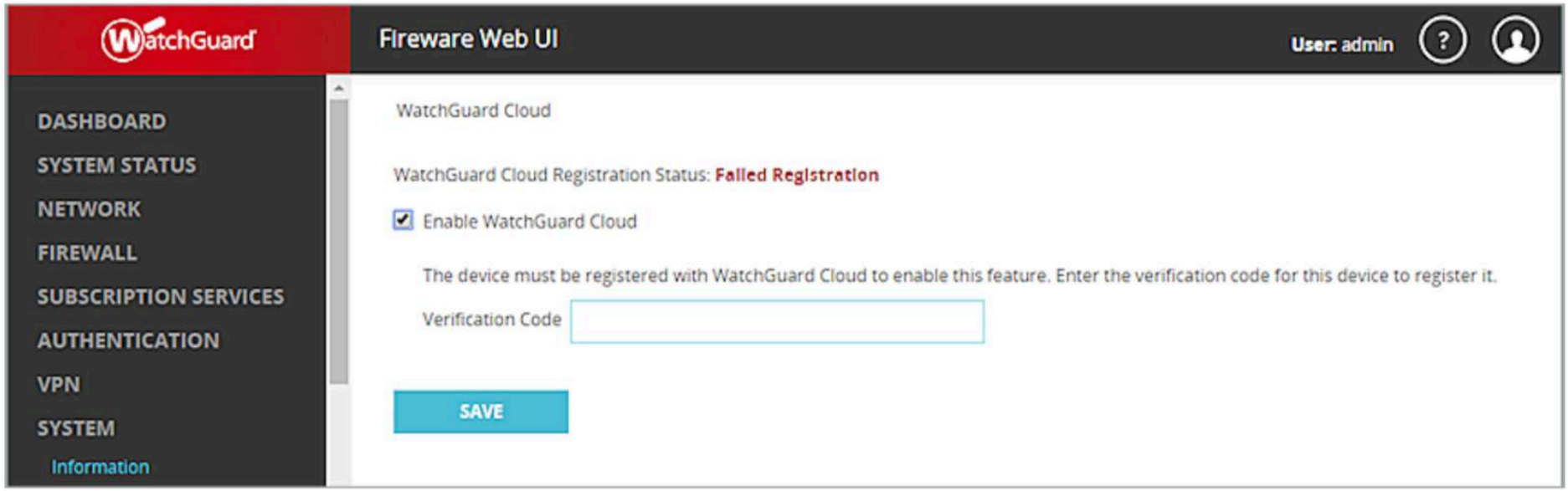


Besonderheit: FireCluster

- Spezielle Anforderung für FireCluster Systeme:
  - Fireware v12.4 muss installiert sein
- Active/Active FireCluster
  - Beide Systeme benötigen Total oder Basic Security
- Active/Passive FireCluster
  - Der Master benötigt Total oder Basic Security

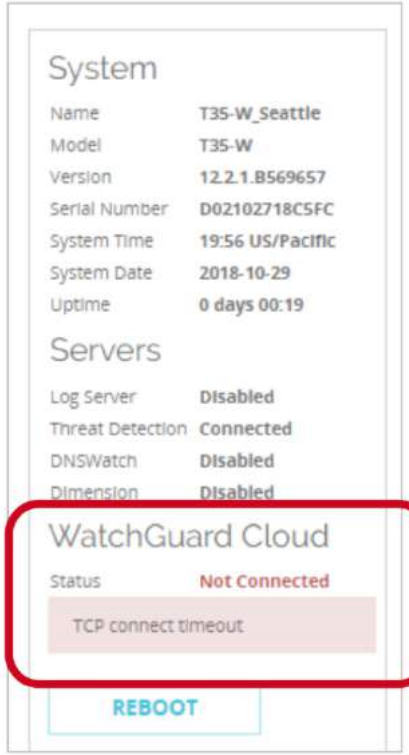
Troubleshooting der Verbindung

- Zeigt der Satus **Failed Registration**, prüfen Sie zunächst den Verification Code
  - Ein erzeugter Verification Code ist 30 Tage gültig.
  - Bei Bedarf kann ein neuer Code generiert werden.



Troubleshooting der Verbindung

- Nach der Registrierung der Firebox verbindet sich diese zur WatchGuard Cloud und überträgt Log Daten und Status Informationen.
  - In Fireware v12.0.x–v12.2.x wurde hierzu TCP port 8883 verwendet
  - In Firewarev12.3 und höher kommt TCP port 443 zum Einsatz
- Gibt es ein Kommunikationsproblem so zeigt dies z.B. die Web UI Front Panel Ansicht
- Prüfen Sie in dieser Situation, ob „vorgelagerte“ Sicherheitssysteme die Verbindung blockieren



Logging im Regelwerk aktivieren/prüfen

- Das Firebox System sendet Log Informationen an die WatchGuard Cloud, sodass Dashboards und Reports generiert werden können.
- Die Funktion Logging for Reports sollte für die meisten Firewall-Regeln aktiviert werden, um aussagekräftige Reports und Dashboards zu erhalten.
- Ein Firebox System kann parallel auch einen WatchGuard Dimension Server nutzen – beide Möglichkeiten sind gleichzeitig verwendbar.

Live Demo

Vielen Dank!

NOTHING GETS PAST RED.

WatchGuard