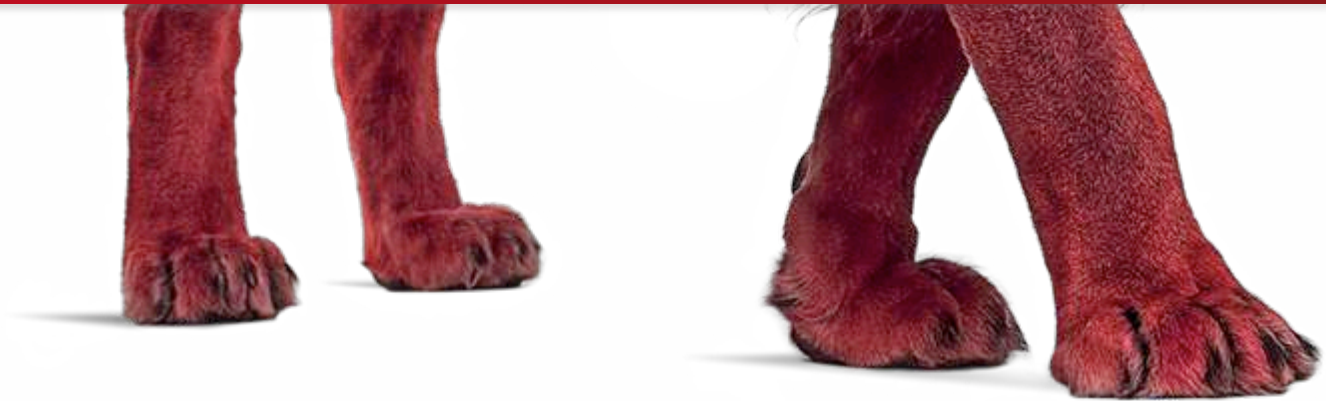


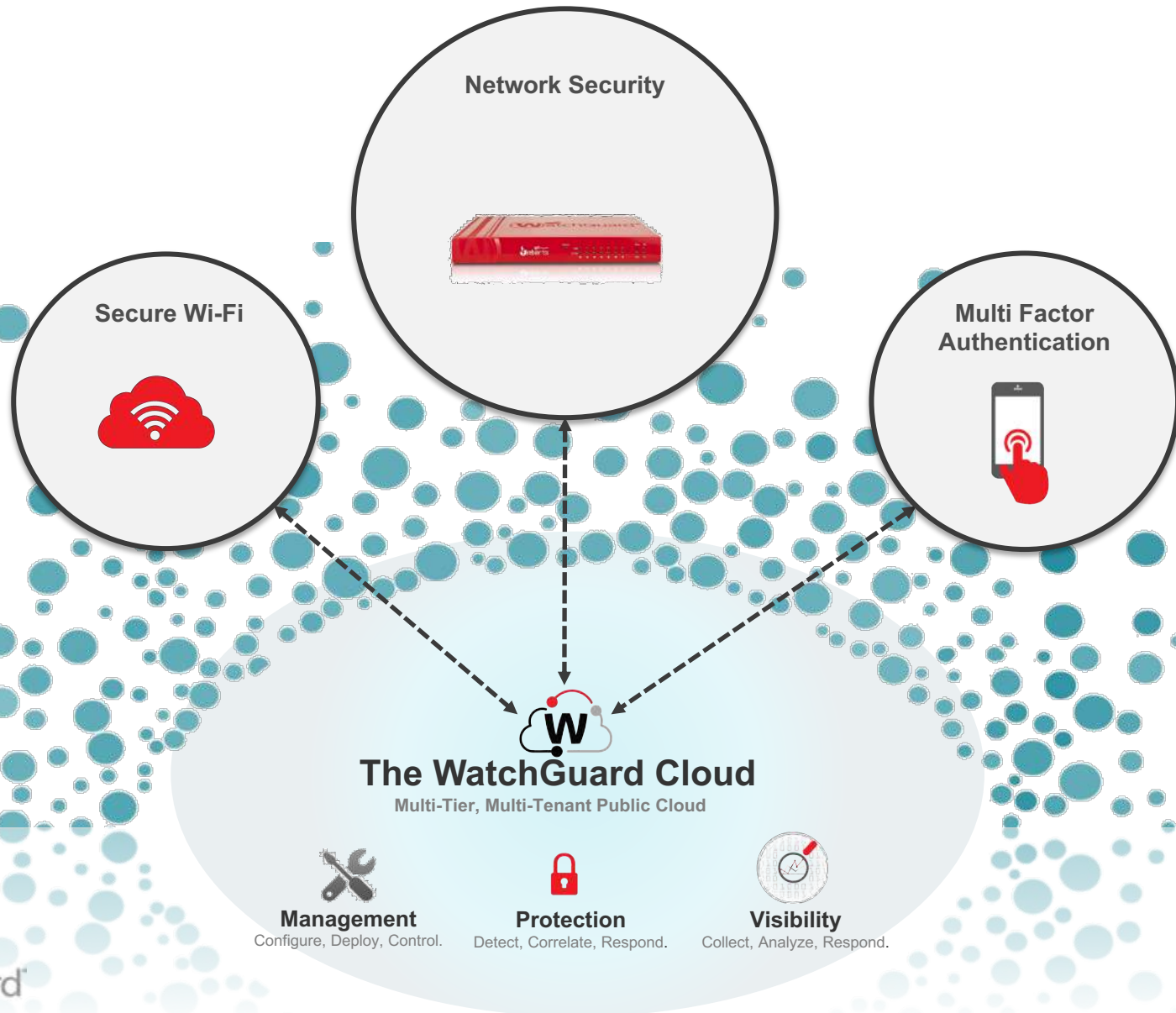


# Best Practice – Visibility

## Eine Funktion der WatchGuard Cloud

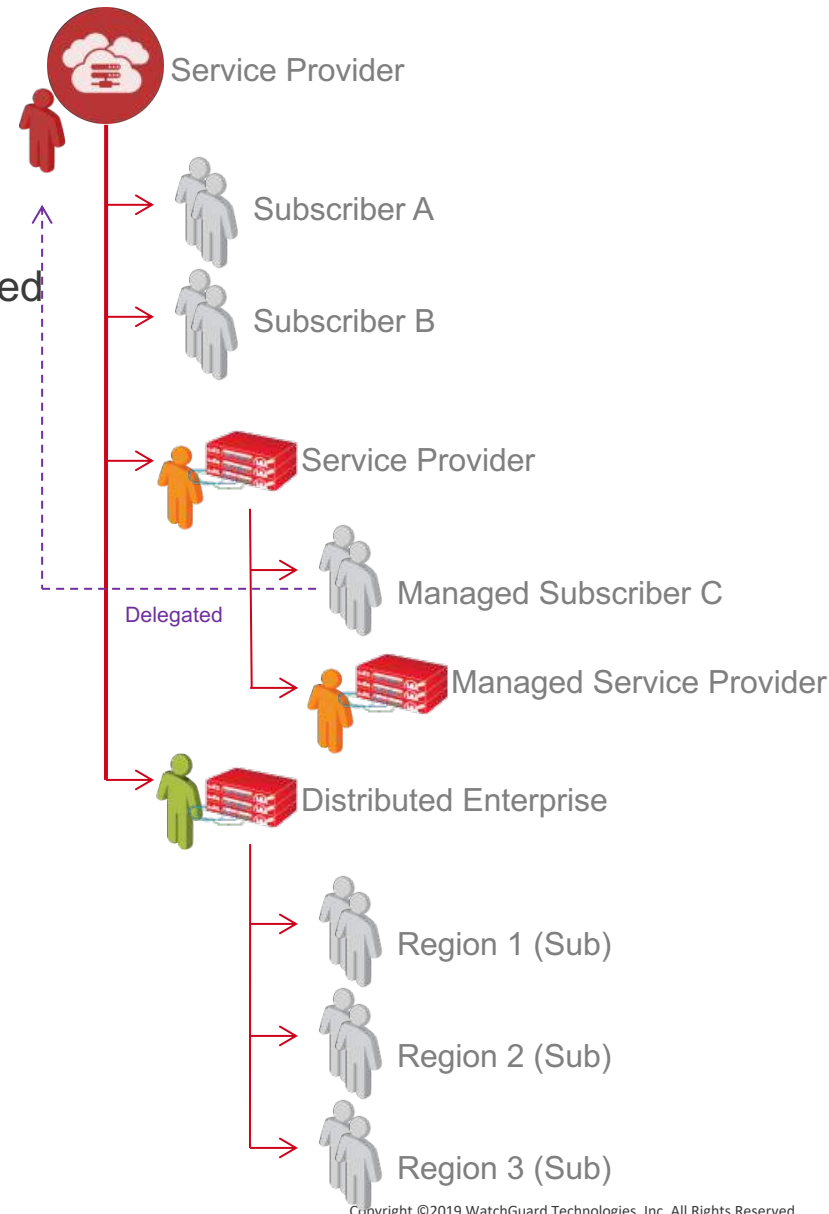


# WatchGuard Cloud – Die Idee



# 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 Alarmer und Benachrichtigungen
- Role-based Access Control (RBAC)
- Flexible Aufbewahrungszeiten der Daten





# Device Summary Dashboard

## Übersicht der Systeme und Lizenzierung

The screenshot displays the WatchGuard Device Summary Dashboard for a Firebox Alpha device. The interface includes a navigation menu on the left, a main content area with device information, license details, and various security metrics.

**Device Manager** (Left Sidebar):

- WinterT (My Account)
  - Firebox One
  - Firebox Alpha**
  - Firebox
  - Firebox
  - Firebox
  - BAF28DEA-6856-47F...
  - Firebox
  - Firebox
  - Firebox

**Device Summary** (Main Content):

**Firebox Alpha**

**Device Information:**

- Name: Firebox Alpha
- Model: Firebox T15
- Version: 12.1.1.B558432
- IP Address: 203.0.113.11
- Uptime: 60 Days
- Serial No.: 70A0F123445667

**License Details:**

- Total Security Suite Status: Valid
- Expiration: 2019-01-31
- Data Retention: 30 Days

**Device Status:**

- CPU Usage: 25%
- Memory Usage: 70%

**Security Metrics:**

- Malware:** 14 Detected
  - GAV: 4
  - Intelligent AV: 8
  - APT Blocker: 2
  - Total Scans: 14
- Content Filtering:** 1.1M Blocked
  - 42.3M Total Requests
- Intrusions:** 13 Prevented
  - 15.3M Scans
  - 13 Detected
- Botnet Detection:** 1 Blocked
  - 8.6M Scans

**External Bandwidth:**

- Average Sent: 523 Kbps
- Average Received: 2.3 Mbps

**Subscription Services:**

- Blocked: 1.2M
- Blocked Websites: 1.1M
- Virus (GAV): 0
- Intrusions (IPS): 74k
- Botnet Detection: 25k

**Most Active Policies:**

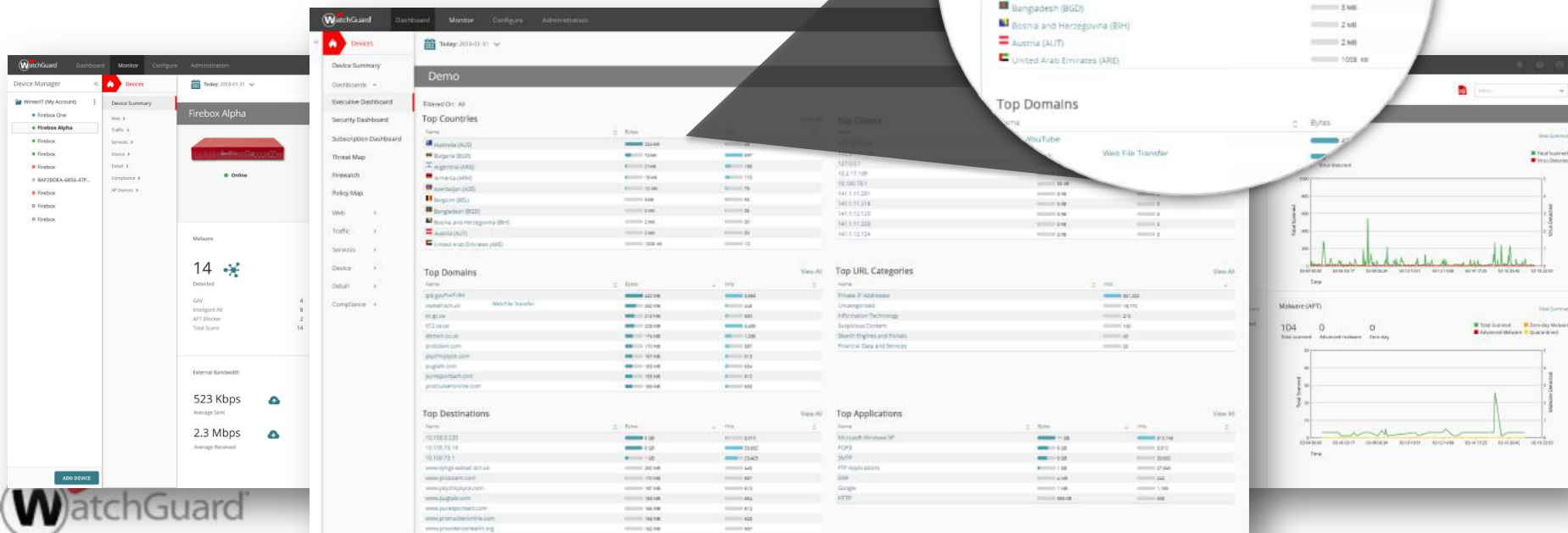
Name	Bytes	Hits
HTTP-test-name-here	2.82 GB	892k
Any-Business-name-goe...	9 MB	1,663
Ping	423 KB	6,610
HTTP-second-test-nam...	3 MB	3,542
Ping	1 MB	1,121

**ADD DEVICE** (Bottom Left Button)

# Executive Dashboards

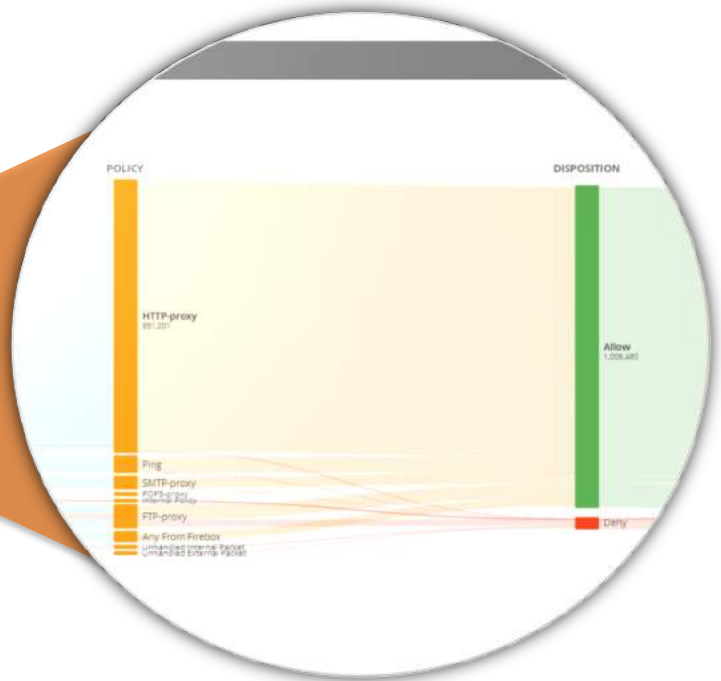
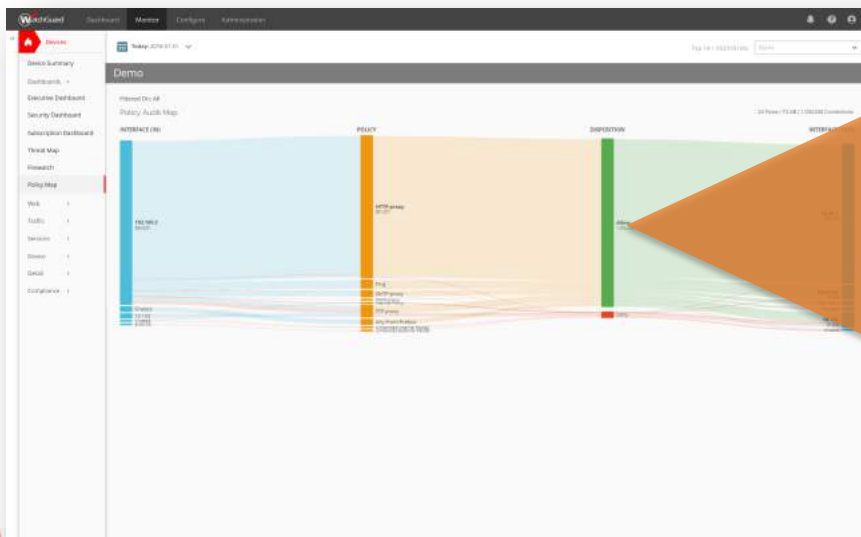
Übersicht zu Netzwerk-Kommunikation, u.A. über:

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



# Policy Map

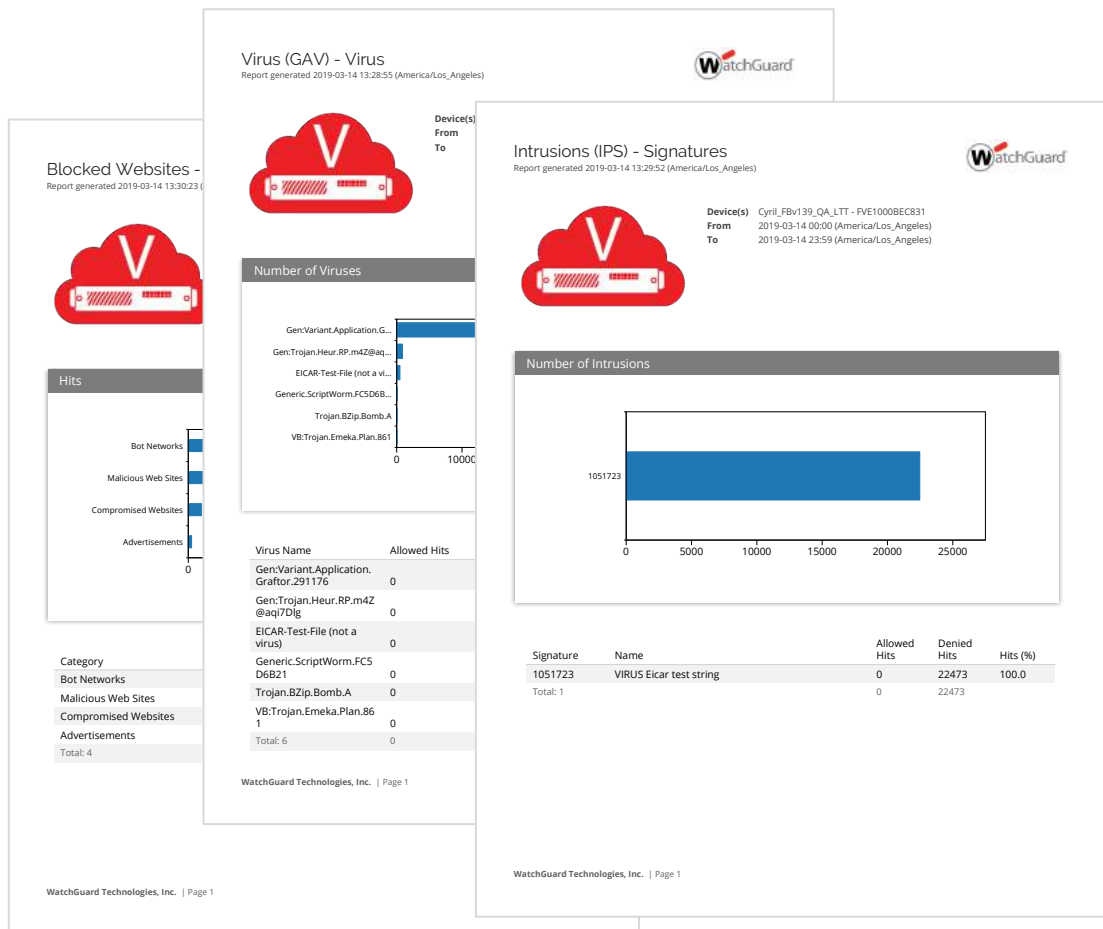
Die Policy Map stellt das Regelwerk Ihrer Firebox visuell dar. Hierin sehen Sie sofort welche Datenströme die jeweiligen Firewall-Regeln nutzen und können somit schnell und einfach Fehlkonfigurationen erkennen und das Regelwerk optimieren.



# 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.

The screenshot shows the WatchGuard web interface for configuring a device for RapidDeploy. The page title is "Configure Device for RapidDeploy". The main content area displays the message: "Your Device is ready for RapidDeploy." Below this, it instructs the user: "Next, connect the cables to your Device and to the network. The device will automatically connect to WatchGuard Cloud and get the configuration file." A "DONE" button is visible. On the right, a "DEVICE DETAILS" box shows the following information: Name: Name 3, Model: Firebox T70, and Serial Number: 80B0DEM030533. An image of the red Firebox T70 device is also shown. The interface includes a top navigation bar with "WatchGuard" logos and "Configure Services" links, and a sidebar with various icons.

# 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

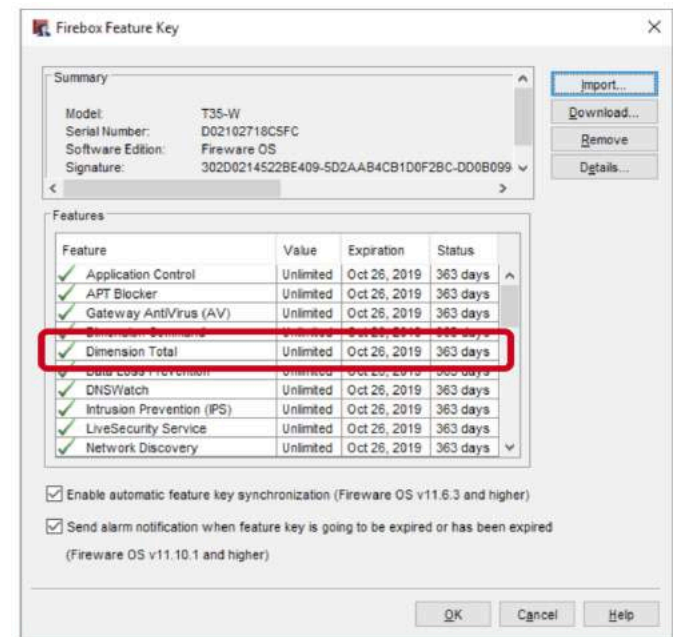
*Note: Fireboxes can simultaneously log to WatchGuard Cloud and Dimension.*

# Anforderungen

- Unterstützte Firebox Systeme:
  - Hardware: Firebox M Series, T Series
  - Virtual: FireboxV, FireboxCloud
- Lizenzierung:
  - 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

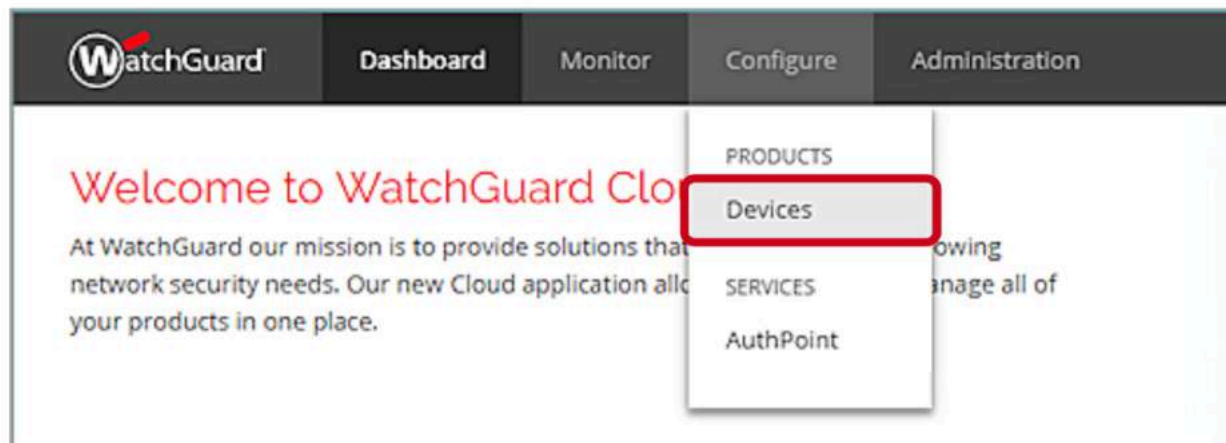
# Feature Key für WatchGuard Cloud Visibility

- 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

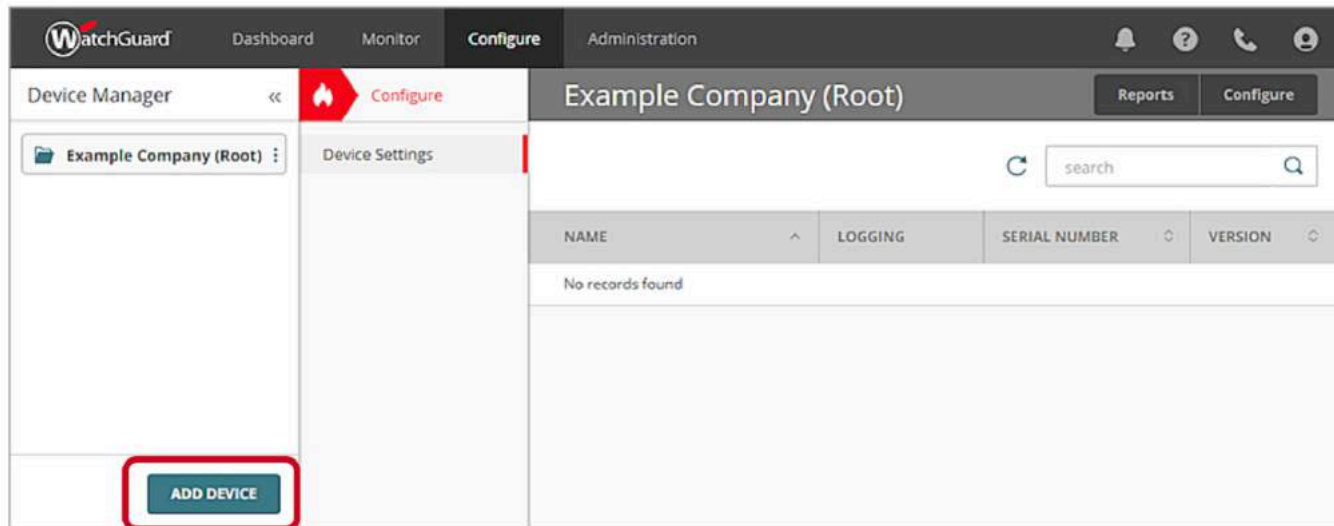
- Öffnen Sie cloud.watchguard.com
  - Die Anmeldung erfolgt mit dem üblichen WatchGuard Portal User
  - Die Ansicht kann für Endkunden und Partner variieren.
- Im WatchGuard Cloud Subscriber account gelangen Sie über **Configure > Devices** zu den neuen Visibility Funktionen





# Hinzufügen einer Firebox

- Firebox Systeme werden nicht automatisiert hinzugefügt (wenn diese im [www.watchguard.com](http://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 generiert, 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](#)

---

**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**

**Device Details**

**Name:** T35-W\_Seattle  
**Model:** Firebox T35-W  
**Serial Number:** D021027...



# Firebox Konfiguration

The screenshot displays the WatchGuard Fireware Web UI interface. The browser address bar shows the URL `https://10.0.1.1:8080/system/wgcloud`. The page title is "Fireware Web UI" and the user is logged in as "admin". The left sidebar contains a navigation menu with the following items: FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, SYSTEM, Information, Feature Key, NTP, SNMP, WatchGuard Cloud, and Managed Device. The main content area is titled "WatchGuard Cloud" and features a lock icon with the text "Click the lock to make changes". Below this, the "WatchGuard Cloud Registration Status" is displayed as "Registered", which is highlighted with a red rectangular box. A checkbox labeled "Enable WatchGuard Cloud" is checked.

# Status der Verbindung prüfen



WatchGuard Dashboard Monitor **Configure** Administration

Device Manager << **Configure** T35-W\_Seattle

Example Company (Root)

- T35-W\_Seattle

Device Settings

**Connected**

Device Information [↻](#)

Name	T35-W_Seattle
Model	Firebox T35-W
Version	12.4.B589044
Serial Number	D02102718C5FC
Uptime	9 Days

License Details

<b>Total Security Suite</b>	
Status	Valid
Expiration	2019-12-07
Data Retention	30 Days

40.97.180.2	5 kbps	670 KB	6	visibility Enabled	REBOOT
40.97.160.2	2 kbps	7 KB	1		

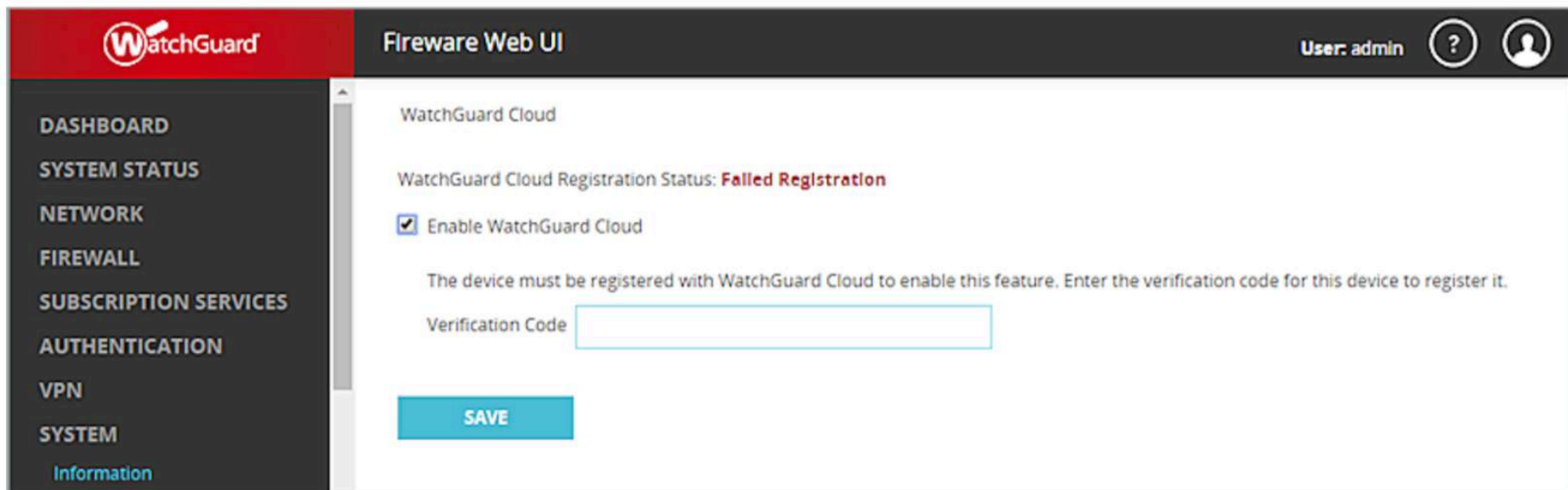


# Besonderheit: FireCluster

- 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.



The screenshot displays the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the title 'Fireware Web UI', and the user 'admin' with a help icon and a profile icon. The left sidebar contains a menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'WatchGuard Cloud' and shows the registration status as 'Failed Registration'. Below this, there is a checkbox labeled 'Enable WatchGuard Cloud' which is checked. A message states: 'The device must be registered with WatchGuard Cloud to enable this feature. Enter the verification code for this device to register it.' A text input field for the 'Verification Code' is present, followed by a blue 'SAVE' button.

# 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 Fireware v12.3 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

The screenshot displays the WatchGuard Cloud status page. It is divided into three sections: System, Servers, and WatchGuard Cloud. The System section lists details for a T35-W\_Seattle device, including its model, version (12.2.1.B569657), serial number, system time, date, and uptime. The Servers section shows the status of various services: Log Server (Disabled), Threat Detection (Connected), DNSWatch (Disabled), and Dimension (Disabled). The WatchGuard Cloud section, which is highlighted with a red box, shows a status of 'Not Connected' with a red error message 'TCP connect timeout' and a 'REBOOT' button below it.

System	
Name	T35-W_Seattle
Model	T35-W
Version	12.2.1.B569657
Serial Number	D02102718C5FC
System Time	19:56 US/Pacific
System Date	2018-10-29
Uptime	0 days 00:19

Servers	
Log Server	Disabled
Threat Detection	Connected
DNSWatch	Disabled
Dimension	Disabled

WatchGuard Cloud	
Status	Not Connected
TCP connect timeout	
<a href="#">REBOOT</a>	

# 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

The image displays a collage of overlapping screenshots from a software interface, likely a network monitoring or management tool. The screenshots show various dashboards with graphs, tables, and navigation menus. A large, semi-transparent watermark logo is centered over the collage. The logo consists of a stylized 'W' inside a circle, with a red arc above it and a red arrow pointing towards the top right. The background of the entire image is a bright blue sky with white clouds and a green field at the bottom.





**Vielen Dank!**



***NOTHING GETS  
PAST **RED.*****

