Schutz bestehender WLAN Netze “Trusted Wireless Environment”

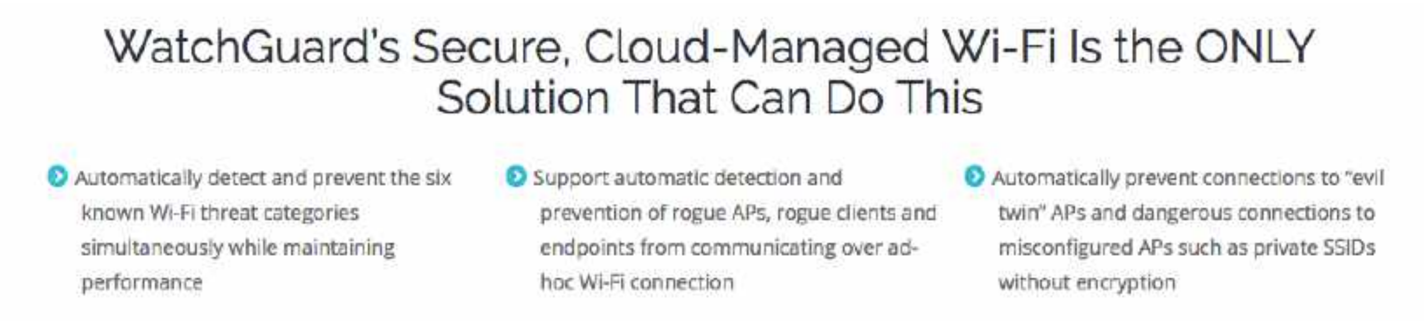
Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.

WatchGuard Wi-Fi Cloud

- Skalierbares Cloud management
- Patentierte WIPS Funtkionalität
- Intelligent Network Visibility und Troubleshooting
- Interaktion mit Gästen (Hotspot)
- Location-based analytics
- Reporting und Visibility

Verified Comprehensive Security

- WIPS steht für **W**ireless **I**ntrusion **P**revention **S**ystem
- Große Unterschiede in den Möglichkeiten von WIPS Lösungen
- WatchGuard’s WIPS bietet umfangreichsten Schutz durch **patentierte** Marker Packet™ Technologie

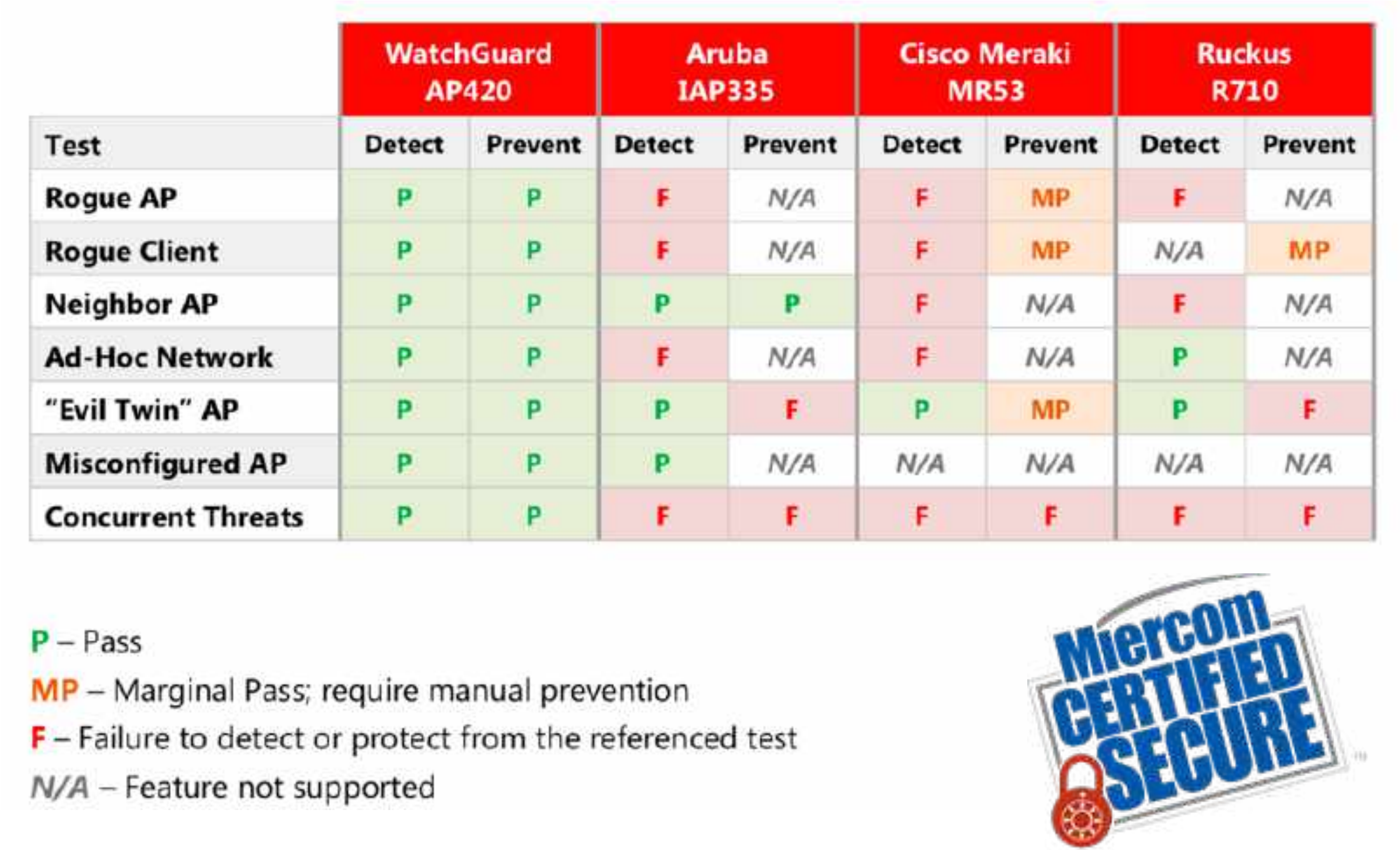


WatchGuard's Secure, Cloud-Managed Wi-Fi Is the ONLY Solution That Can Do This

- Automatically detect and prevent the six known Wi-Fi threat categories simultaneously while maintaining performance
- Support automatic detection and prevention of rogue APs, rogue clients and endpoints from communicating over ad-hoc Wi-Fi connection
- Automatically prevent connections to "evil twin" APs and dangerous connections to misconfigured APs such as private SSIDs without encryption

https://www.watchguard.com/wgrd-resource-center/wifi-wips-report

Verified, Comprehensive Security



Test	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
	Detect	Prevent	Detect	Prevent	Detect	Prevent	Detect	Prevent
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

P – Pass

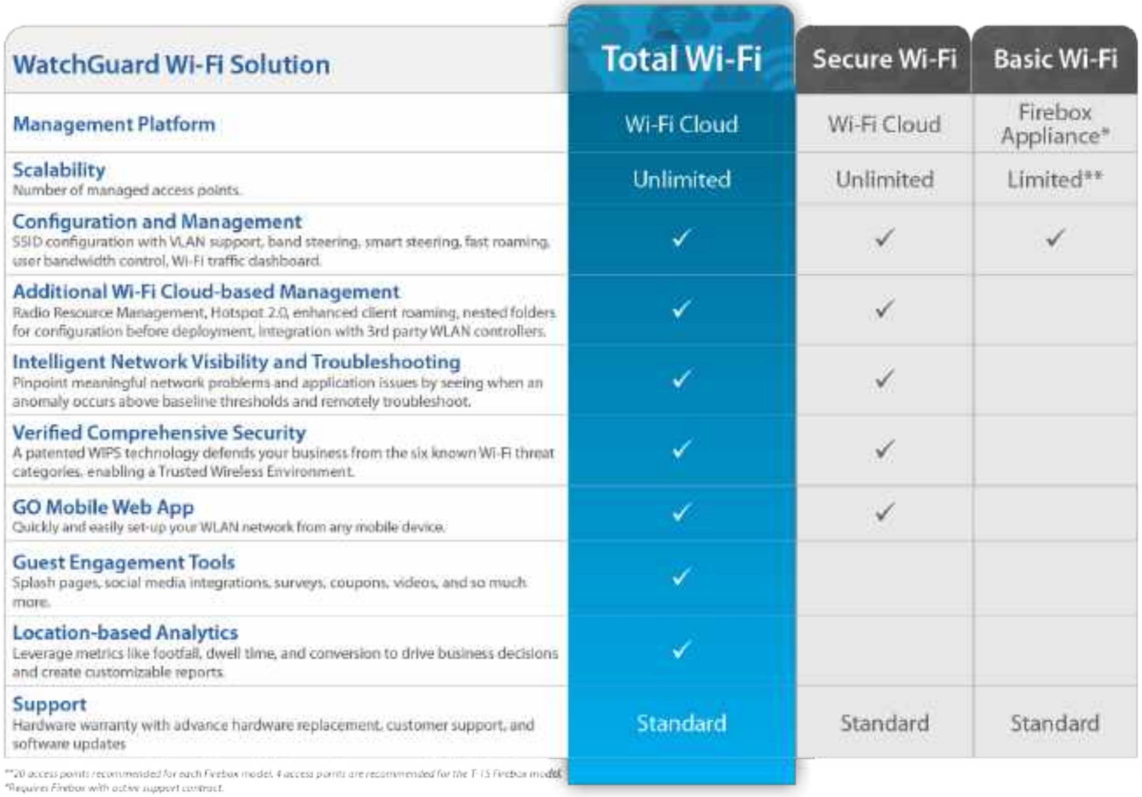
MP – Marginal Pass; require manual prevention

F – Failure to detect or protect from the referenced test

N/A – Feature not supported

Miercom CERTIFIED SECURE

Wi-Fi Subscriptions

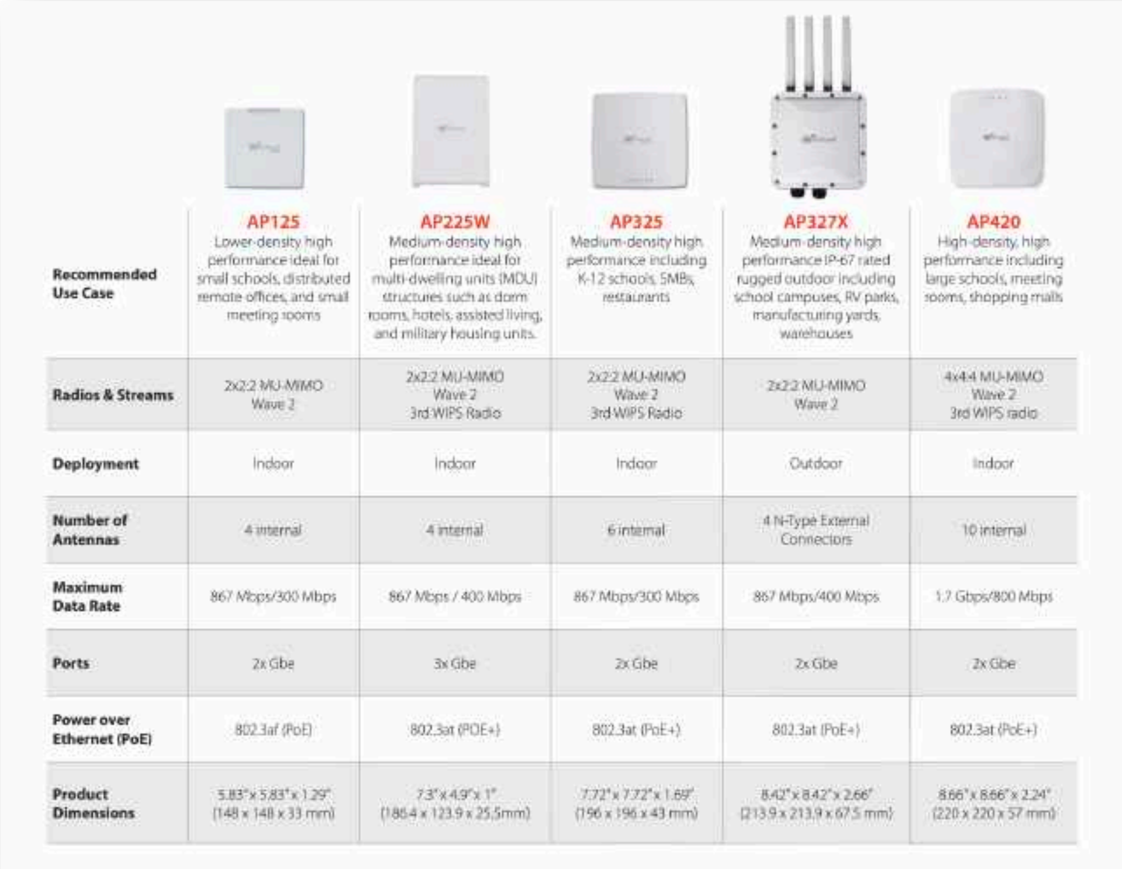


WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Management Platform	Wi-Fi Cloud	Wi-Fi Cloud	Firebox Appliance*
Scalability Number of managed access points.	Unlimited	Unlimited	Limited**
Configuration and Management SSID configuration with VLAN support, band steering, smart steering, fast roaming, user bandwidth control, Wi-Fi traffic dashboard.	✓	✓	✓
Additional Wi-Fi Cloud-based Management Radio Resource Management, Hotspot 2.0, enhanced client roaming, nested folders for configuration before deployment, integration with 3rd party WLAN controllers.	✓	✓	
Intelligent Network Visibility and Troubleshooting Pinpoint meaningful network problems and application issues by seeing when an anomaly occurs above baseline thresholds and remotely troubleshoot.	✓	✓	
Verified Comprehensive Security A patented WIPS technology defends your business from the six known Wi-Fi threat categories, enabling a Trusted Wireless Environment.	✓	✓	
GO Mobile Web App Quickly and easily set-up your WLAN network from any mobile device.	✓	✓	
Guest Engagement Tools Splash pages, social media integrations, surveys, coupons, videos, and so much more.	✓		
Location-based Analytics Leverage metrics like footfall, dwell time, and conversion to drive business decisions and create customizable reports.	✓		
Support Hardware warranty with advance hardware replacement, customer support, and software updates	Standard	Standard	Standard

**20 access points recommended for each Firebox model. 4 access points are recommended for the T-15 Firebox mod

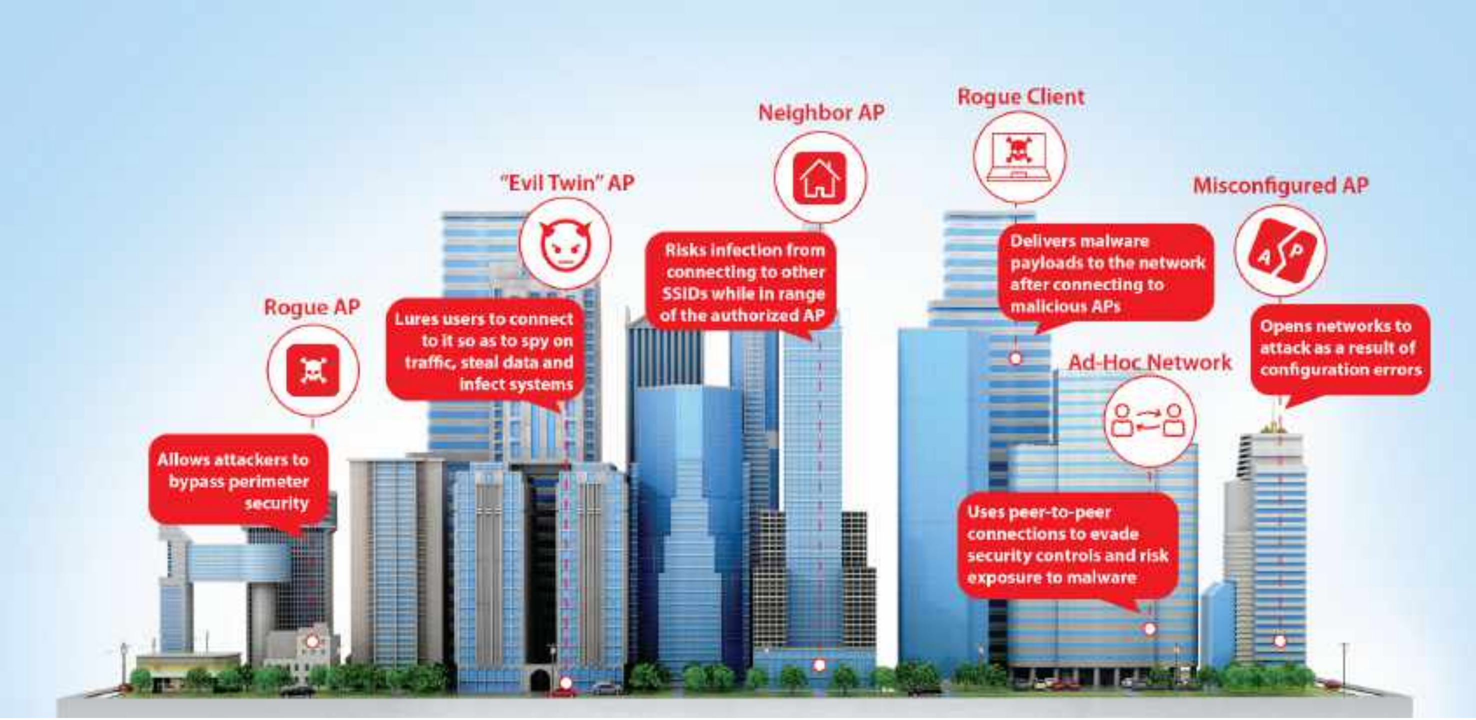
*Requires Firebox with active support contract.

Performance-Driven Wi-Fi Access Points

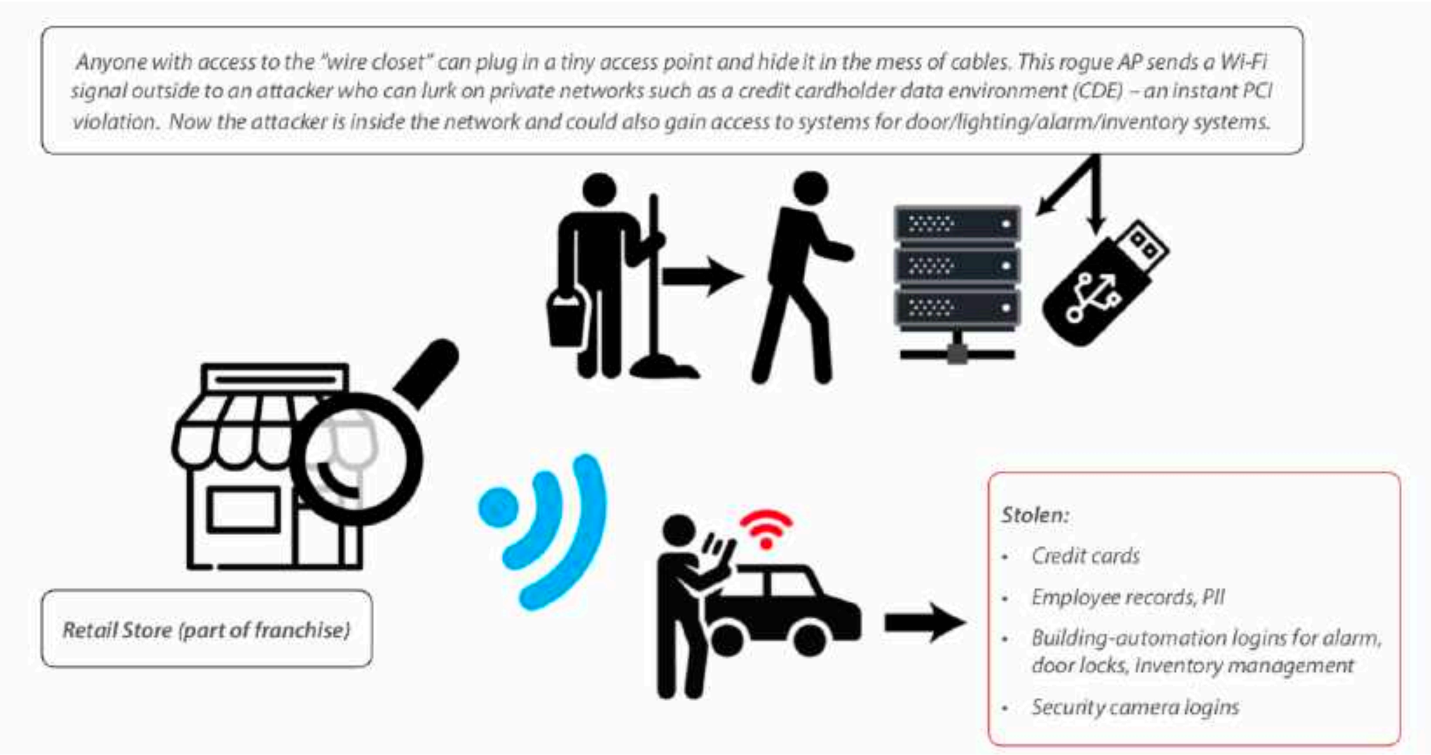


	AP125	AP225W	AP325	AP327X	AP420
Recommended Use Case	Lower-density high performance ideal for small schools, distributed remote offices, and small meeting rooms	Medium-density high performance ideal for multi-dwelling units (MDU) structures such as dorm rooms, hotels, assisted living, and military housing units.	Medium-density high performance including K-12 schools, SMBs, restaurants	Medium-density high performance IP-67 rated rugged outdoor including school campuses, RV parks, manufacturing yards, warehouses	High-density, high performance including large schools, meeting rooms, shopping malls
Radios & Streams	2x2:2 MU-MIMO Wave 2	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2	4x4:4 MU-MIMO Wave 2 3rd WIPS radio
Deployment	Indoor	Indoor	Indoor	Outdoor	Indoor
Number of Antennas	4 internal	4 internal	6 internal	4 N-Type External Connectors	10 internal
Maximum Data Rate	867 Mbps/300 Mbps	867 Mbps / 400 Mbps	867 Mbps/300 Mbps	867 Mbps/400 Mbps	1.7 Gbps/800 Mbps
Ports	2x Gbe	3x Gbe	2x Gbe	2x Gbe	2x Gbe
Power over Ethernet (PoE)	802.3af (PoE)	802.3at (POE+)	802.3at (PoE+)	802.3at (PoE+)	802.3at (PoE+)
Product Dimensions	5.83" x 5.83" x 1.29" (148 x 148 x 33 mm)	7.3" x 4.9" x 1" (186.4 x 123.9 x 25.5mm)	7.72" x 7.72" x 1.69" (196 x 196 x 43 mm)	8.42" x 8.42" x 2.66" (213.9 x 213.9 x 67.5 mm)	8.66" x 8.66" x 2.24" (220 x 220 x 57 mm)

6 Bedrohungen sind bekannt


Rogue AP
Allows attackers to bypass perimeter security
"Evil Twin" AP
Lures users to connect to it so as to spy on traffic, steal data and infect systems
Neighbor AP
Risks infection from connecting to other SSIDs while in range of the authorized AP
Rogue Client
Delivers malware payloads to the network after connecting to malicious APs
Ad-Hoc Network
Uses peer-to-peer connections to evade security controls and risk exposure to malware
Misconfigured AP
A P
Opens networks to attack as a result of configuration errors

Rogue AP



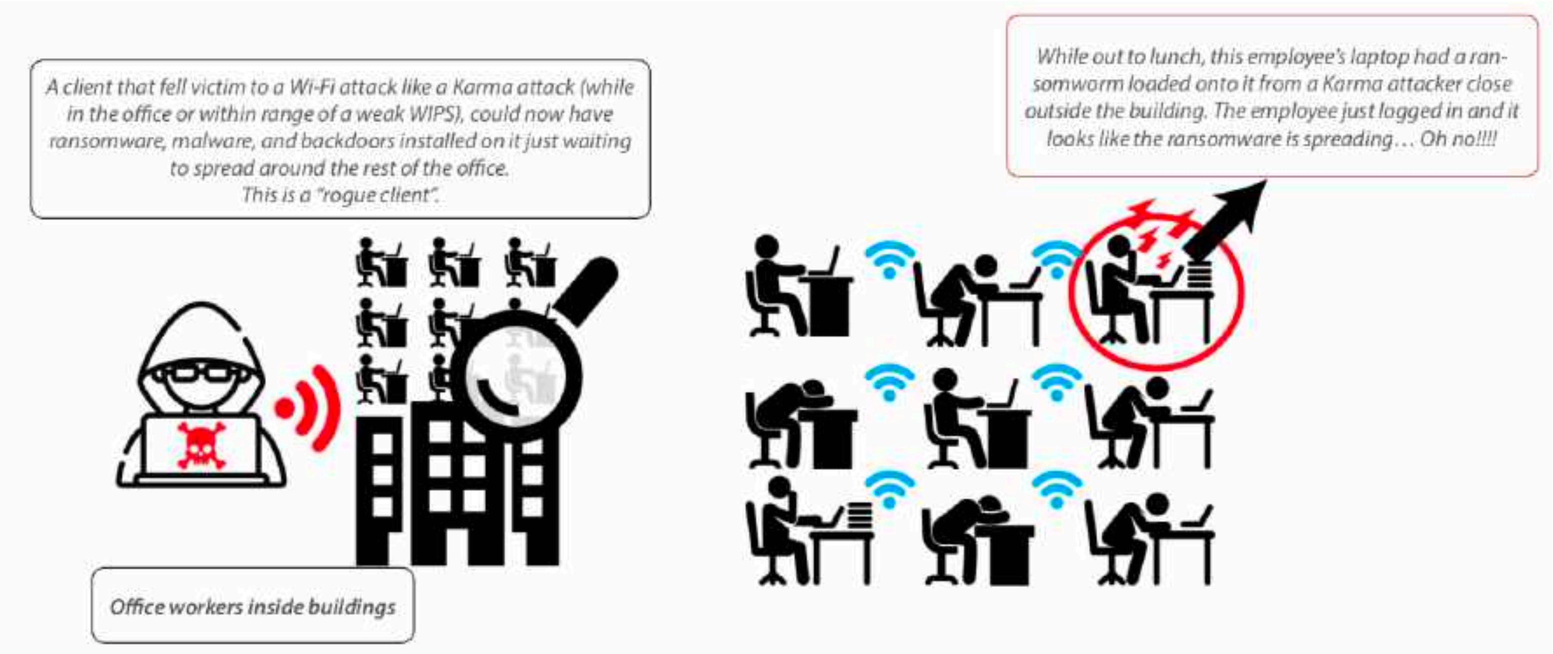
Anyone with access to the "wire closet" can plug in a tiny access point and hide it in the mess of cables. This rogue AP sends a Wi-Fi signal outside to an attacker who can lurk on private networks such as a credit cardholder data environment (CDE) – an instant PCI violation. Now the attacker is inside the network and could also gain access to systems for door/lighting/alarm/inventory systems.

Retail Store (part of franchise)

Stolen:

- *Credit cards*
- *Employee records, PII*
- *Building-automation logins for alarm, door locks, inventory management*
- *Security camera logins*

Rogue Client



A client that fell victim to a Wi-Fi attack like a Karma attack (while in the office or within range of a weak WIPS), could now have ransomware, malware, and backdoors installed on it just waiting to spread around the rest of the office.
This is a "rogue client".

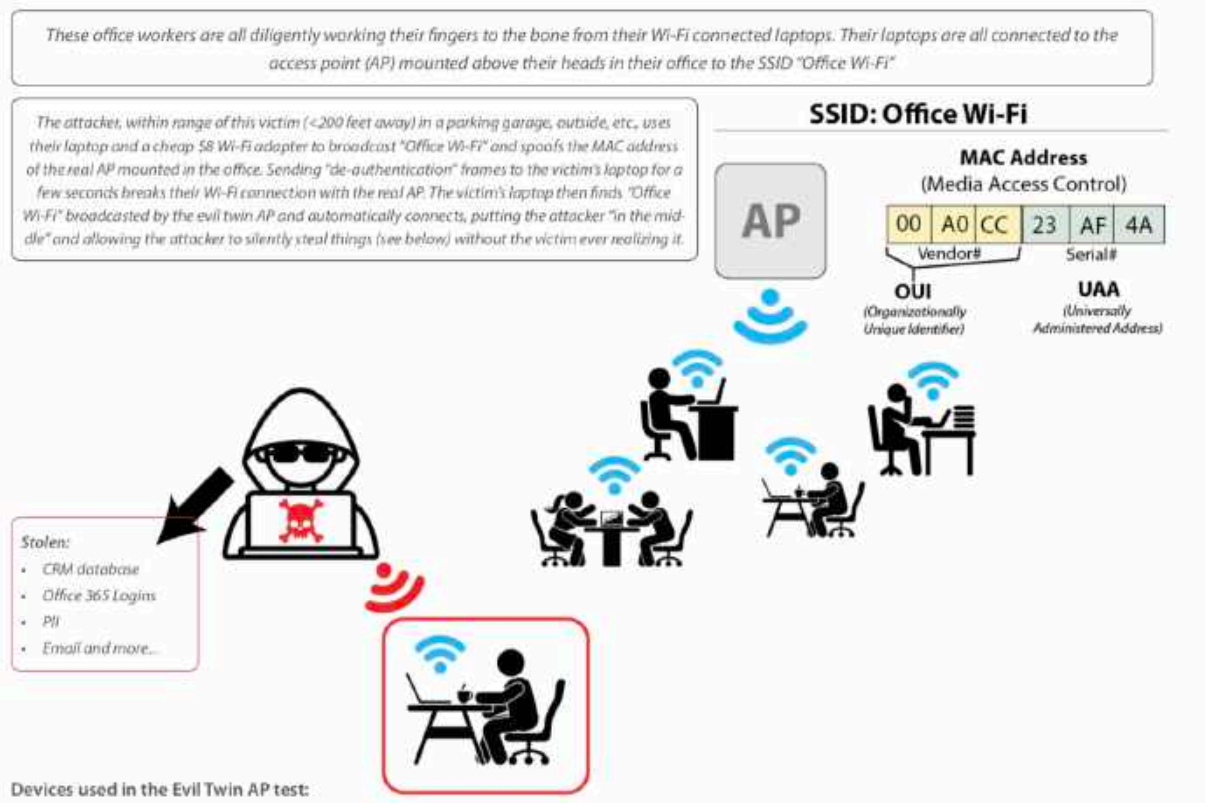
While out to lunch, this employee's laptop had a ransomworm loaded onto it from a Karma attacker close outside the building. The employee just logged in and it looks like the ransomware is spreading… Oh no!!!!

Office workers inside buildings

Neighbor AP

Employees frustrated by their corporate firewall blocking websites have cleverly figured out easy ways to bypass this important network security control: by using their smartphones' hotspot feature and tethering their corporate laptops to them or by connecting to guest Wi-Fi either inside the office or nearby from neighbors.

Evil Twin AP



These office workers are all diligently working their fingers to the bone from their Wi-Fi connected laptops. Their laptops are all connected to the access point (AP) mounted above their heads in their office to the SSID "Office Wi-Fi"

The attacker, within range of this victim (<200 feet away) in a parking garage, outside, etc., uses their laptop and a cheap $8 Wi-Fi adapter to broadcast "Office Wi-Fi" and spoofs the MAC address of the real AP mounted in the office. Sending "de-authentication" frames to the victim's laptop for a few seconds breaks their Wi-Fi connection with the real AP. The victim's laptop then finds "Office Wi-Fi" broadcasted by the evil twin AP and automatically connects, putting the attacker "in the middle" and allowing the attacker to silently steal things (see below) without the victim ever realizing it.

Stolen:

- *CRM database*
- *Office 365 Logins*
- *PII*
- *Email and more...*

Devices used in the Evil Twin AP test:

Misconfigured AP

Many companies, especially franchises and distributed enterprises, rely on non-technical staff to plug in access points shipped to them from corporate IT.

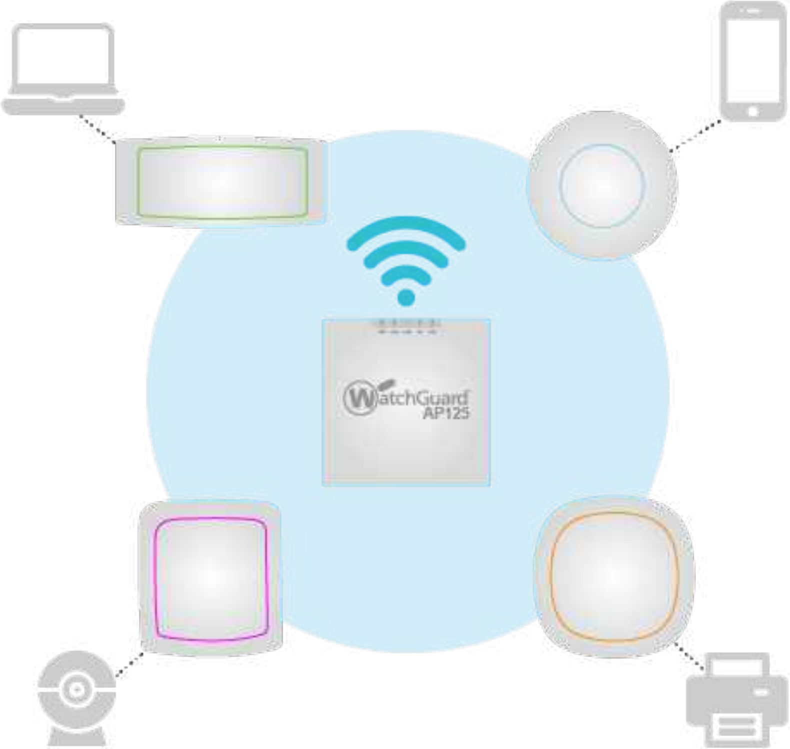
Private Wi-Fi for handheld POS, security cameras

Open, no encryption

Ooops! IT at HQ made a tiny mistake and configured the private Wi-Fi on this AP to have NO ENCRYPTION (no password on the Wi-Fi) which potentially puts credit card info, camera footage, etc. into the air in plain view for an attacker to intercept. This is a mis-configured AP that failed to adhere to the company's configurable "Authorized WLAN Policy," which states any private Wi-Fi SSID needs to be encrypted.

Schutz bestehender WLAN Netze

- WatchGuard APs als Sensor schützen bestehende WLAN Netze.



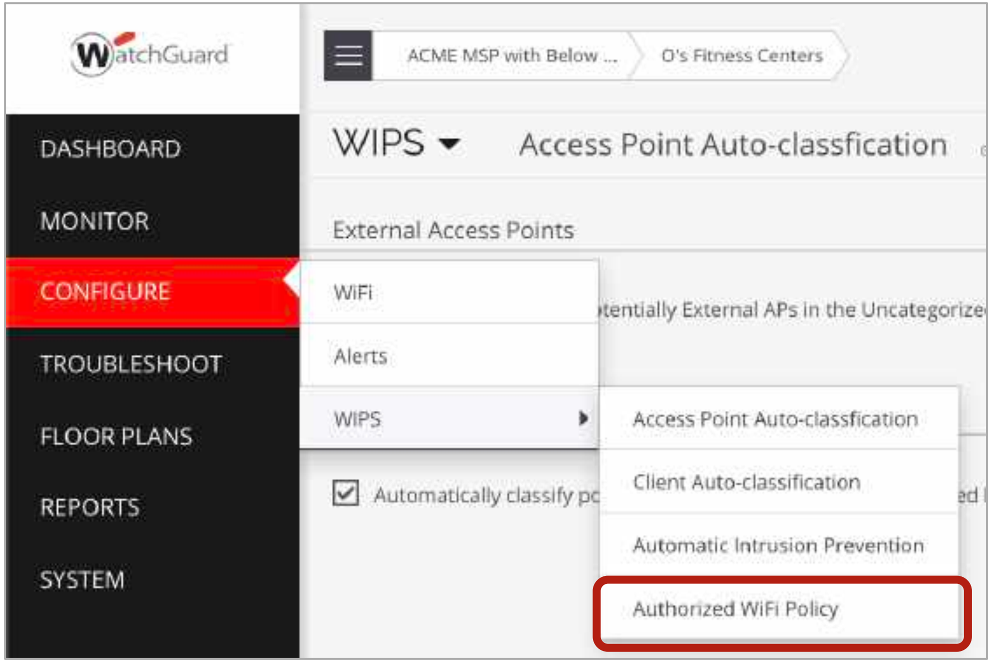
Authorized Wi-Fi Policy

Authorized WiFi Policy

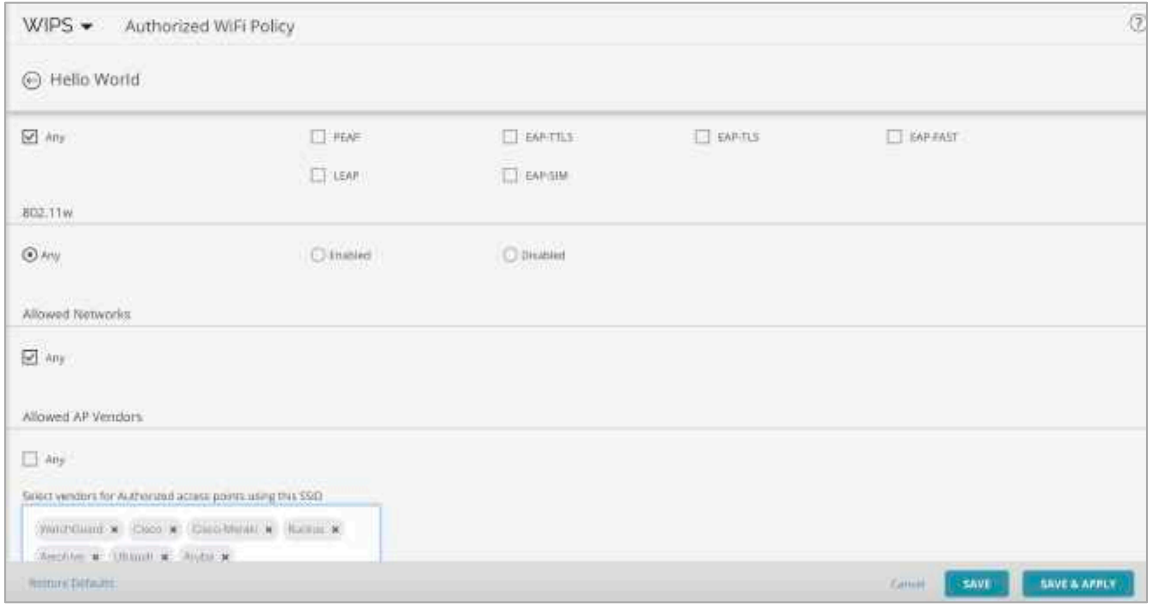
- Festlegung der WiFi Richtlinien pro Location (Vererbung in untergeordnete Locations)
  - Z.B. SSID Name, Security Parameter, Wi-Fi Vendor, etc.
- Verstößt ein Accesspoint gegen die zugewiesene Authorized WiFi Policy, so gilt dieser Accesspoint als “misconfigured”
- Ermöglicht aktive “Überprüfung” der Richtlinieneinhaltung – auch bei 3rd Party Accesspoints.

Authorized WiFi Policy

- **Configure > WIPS > Authorized WiFi Policy**


WatchGuard
ACME MSP with Below ...
O's Fitness Centers
DASHBOARD
MONITOR
CONFIGURE
TROUBLESHOOT
FLOOR PLANS
REPORTS
SYSTEM
WIPS
Access Point Auto-classfication
External Access Points
WiFi
Alerts
WIPS
tentially External APs in the Uncategorize
Access Point Auto-classfication
Client Auto-classification
Automatic Intrusion Prevention
Authorized WiFi Policy
☑ Automatically classify po

Configure > WIPS > Authorized WiFi Policy



Hello World

☑ Any　□ PEAP　□ EAP-TTLS　□ EAP-TLS　□ EAP-FAST

□ LEAP　□ EAP-SIM

802.11w

● Any　○ Enabled　○ Disabled

Allowed Networks

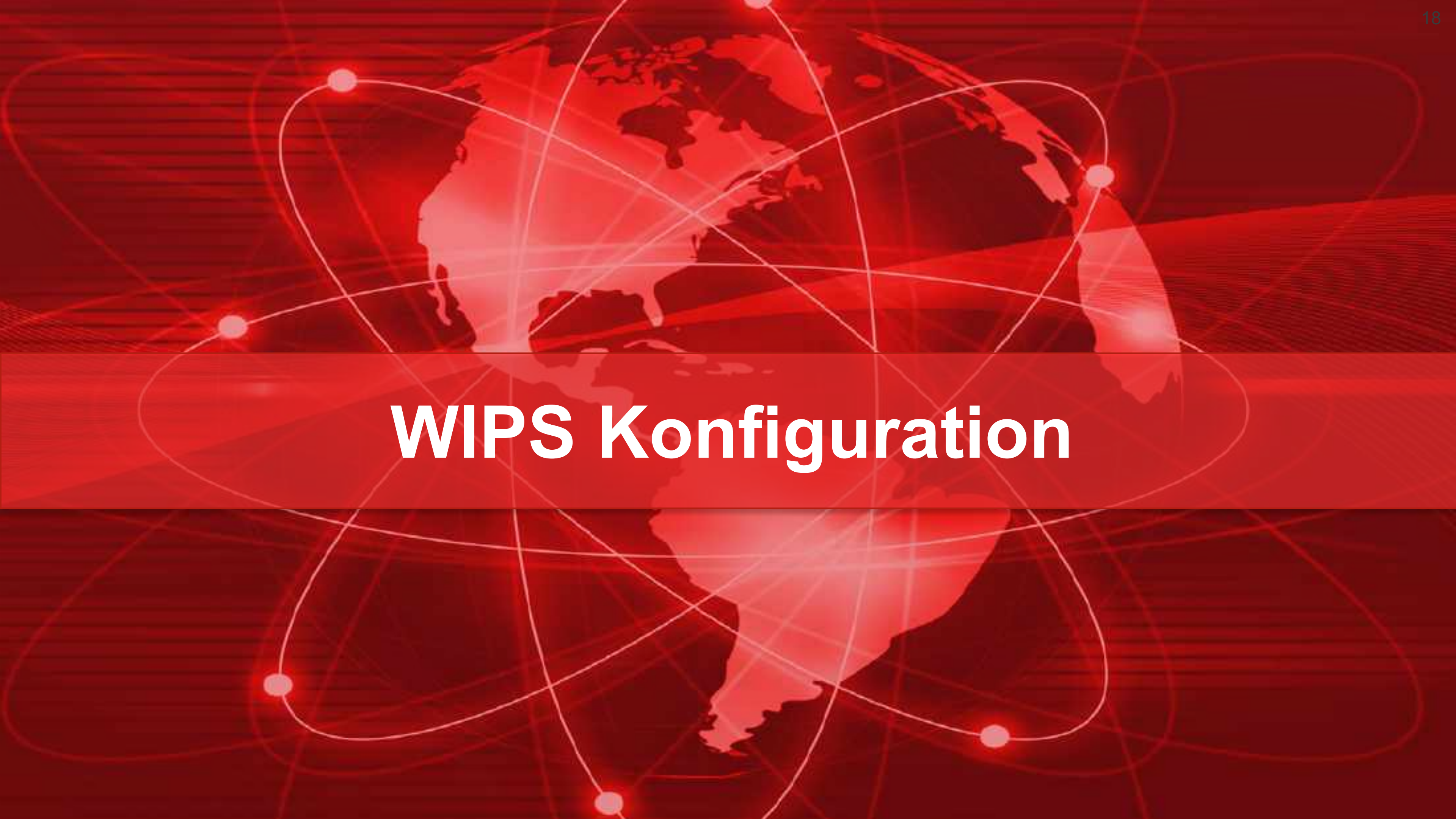
☑ Any

Allowed AP Vendors

□ Any

Select vendors for Authorized access points using this SSID

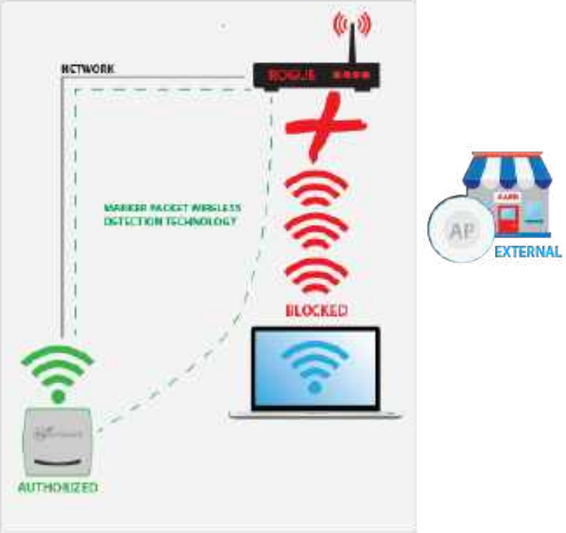
WatchGuard ✖　Cisco ✖　Cisco Meraki ✖　Ruckus ✖　Aerohive ✖　Ubiquiti ✖　Aruba ✖



WIPS Konfiguration

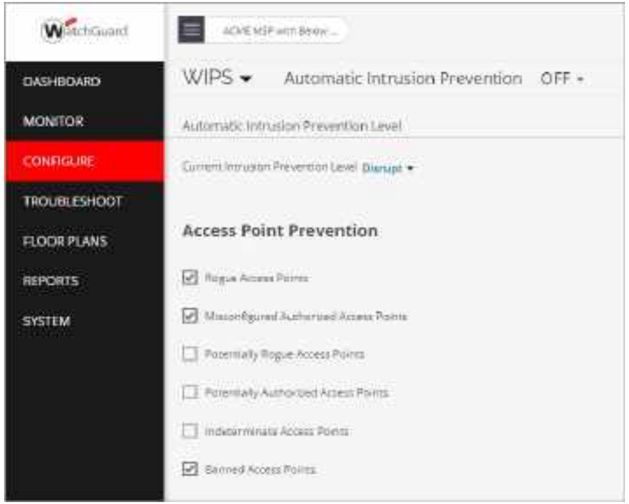
Wireless Intrusion Prevention System (WIPS)

- Access Point überwacht die Wi-Fi Umgebung auf schädliche Aktivitäten
- WIPS Technologie blockiert die Gefahr automatisch
- “Sicherheits Schild” für Ihr Unternehmen und die Nutzer



WIPS Konfiguration

- Die aktive und automatischen Abwehr von gefährlichen Aktivitäten wird hier festgelegt
- Bitte in Zusammenhang mit der geplanten Installation prüfen
- Empfohlene Anpassungen der Default Konfiguration:
  - „MAC Spoofing“ aktivieren



Automatic Intrusion Prevention OFF ▾

Automatic Intrusion Prevention Level

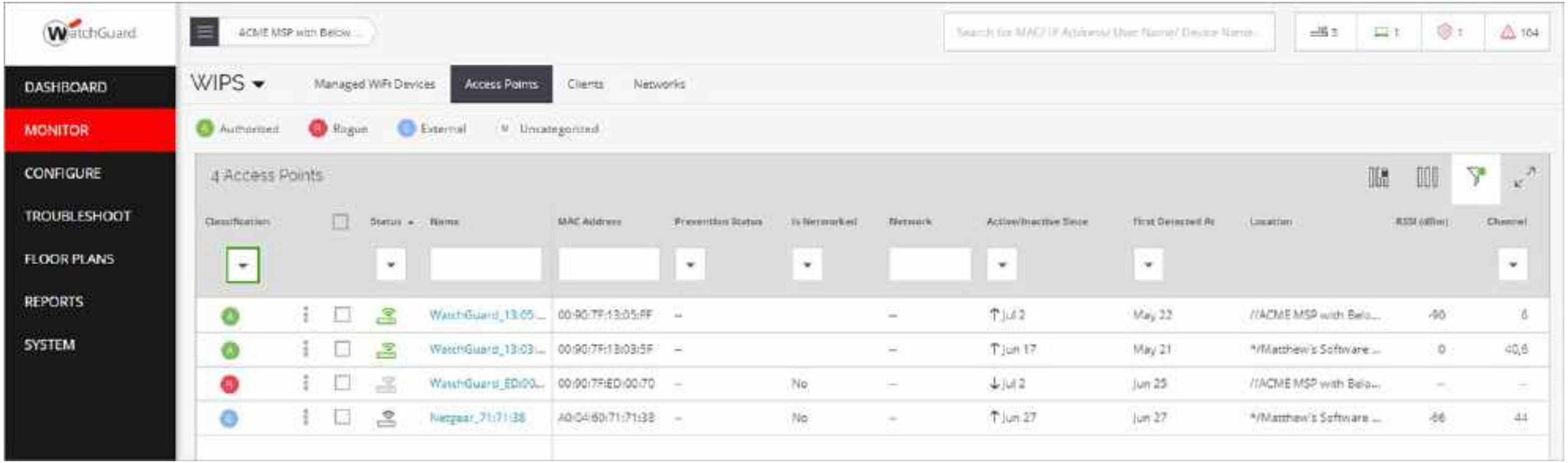
Current Intrusion Prevention Level Disrupt ▾

Access Point Prevention

☑ Rogue Access Points
☑ Misconfigured Authorized Access Points
☐ Potentially Rogue Access Points
☐ Potentially Authorized Access Points
☐ Indeterminate Access Points
☑ Banned Access Points

WIPS Klassifikation prüfen

- In Monitor WIPS sollte die Klassifikation der Accesspoints und Clients geprüft werden.

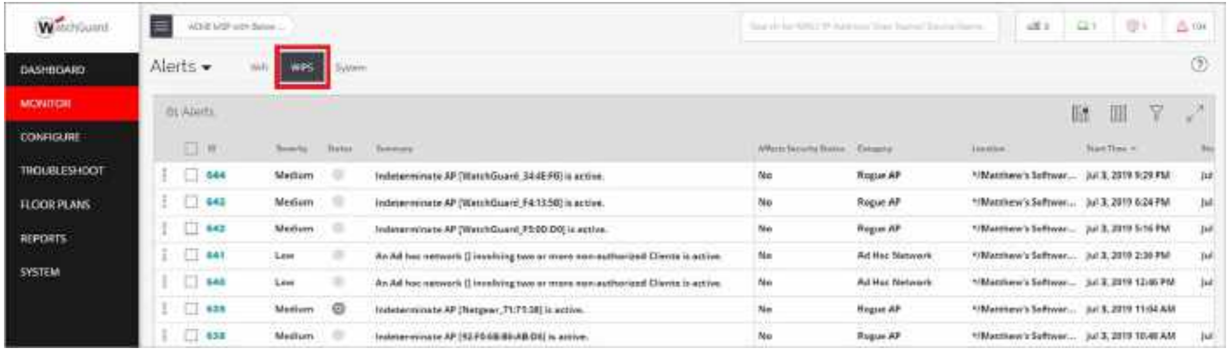


4 Access Points

Classification		□	Status	Name	MAC Address	Prevention Status	Is Networked	Network	Active/Inactive Since	First Detected At	Location	RSSI (dBm)	Channel
A	⋮	□		WatchGuard_13:05_...	00:90:7F:13:05:FF	–		–	↑Jul 2	May 22	//ACME MSP with Belo...	-90	6
A	⋮	□		WatchGuard_13:03...	00:90:7F:13:03:5F	–		–	↑Jun 17	May 21	*/Matthew's Software ...	0	40,6
R	⋮	□		WatchGuard_ED:00...	00:90:7F:ED:00:70	–	No	–	↓Jul 2	Jun 25	//ACME MSP with Belo...	–	–
E	⋮	□		Netgear_71:71:38	A0:04:60:71:71:38	–	No	–	↑Jun 27	Jun 27	*/Matthew's Software ...	-66	44

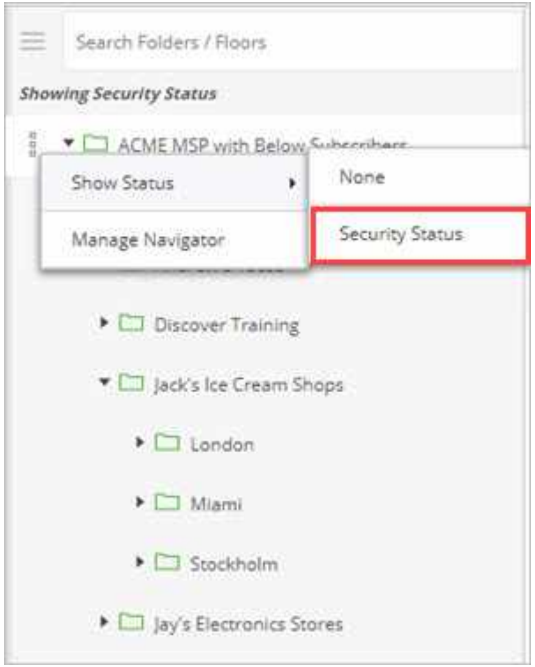
Prüfen der Alarme und des Security Status

- Überprüfen auf offene Alarme und Events im Zusammenhang mit der WIPS Funktion



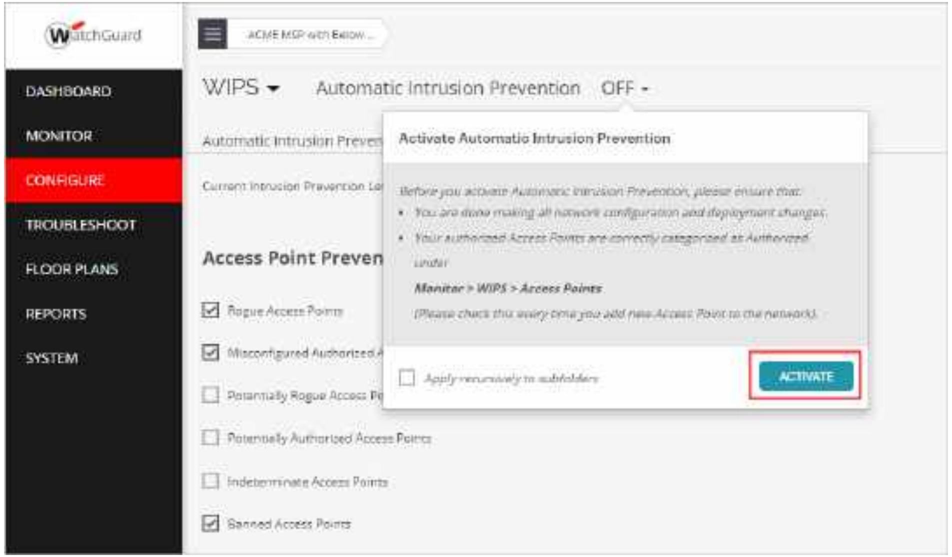
61 Alerts

	ID	Severity	Status	Summary	Affects Security Status	Category	Location	Start Time
□	644	Medium		Indeterminate AP [WatchGuard_34:4E:F6] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 9:29 PM
□	643	Medium		Indeterminate AP [WatchGuard_F4:13:58] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 6:24 PM
□	642	Medium		Indeterminate AP [WatchGuard_F5:0D:D0] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 5:16 PM
□	641	Low		An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*/Matthew's Softwar...	Jul 3, 2019 2:30 PM
□	640	Low		An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*/Matthew's Softwar...	Jul 3, 2019 12:06 PM
□	639	Medium		Indeterminate AP [Netgear_71:71:38] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 11:04 AM
□	638	Medium		Indeterminate AP [92:F6:6B:B8:AB:D8] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 10:48 AM



Aktivieren von WIPS

- „Scharfschaltung“
  - Ab jetzt werden automatische Abwehrmechanismen angewendet



Automatic Intrusion Prevention OFF

Automatic Intrusion Preven

Current Intrusion Prevention Le

Access Point Preven

☑ Rogue Access Points

☑ Misconfigured Authorized A

□ Potentially Rogue Access Po

□ Potentially Authorized Access Points

□ Indeterminate Access Points

☑ Banned Access Points

Activate Automatic Intrusion Prevention

Before you activate Automatic Intrusion Prevention, please ensure that:

- *You are done making all network configuration and deployment changes.*
- *Your authorized Access Points are correctly categorized as Authorized under*

Monitor > WIPS > Access Points

(Please check this every time you add new Access Point to the network).

□ Apply recursively to subfolders

Weitere Ressourcen – Deployment Guides

https://www.watchguard.com/help/docs/Wi-Fi_Cloud/en-US/WatchGuard_Wi-Fi-Cloud_AP-Deployment-Guide.pdf

https://www.watchguard.com/help/docs/Wi-Fi_Cloud/en-US/Wi-Fi-Cloud_WIPS_Trusted_Wireless_Environment.pdf

https://www.watchguard.com/wgrd-resource-center/wifi-wips-report

Let’s Make Wi-Fi Security a Global Standard!

www.trustedwirelessenvironment.com

Haben Sie noch Fragen?

Vielen Dank!

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.