Best Practices Wi-Fi Cloud – WIPS zur Verhinderung von ungewünschten Verbindungen

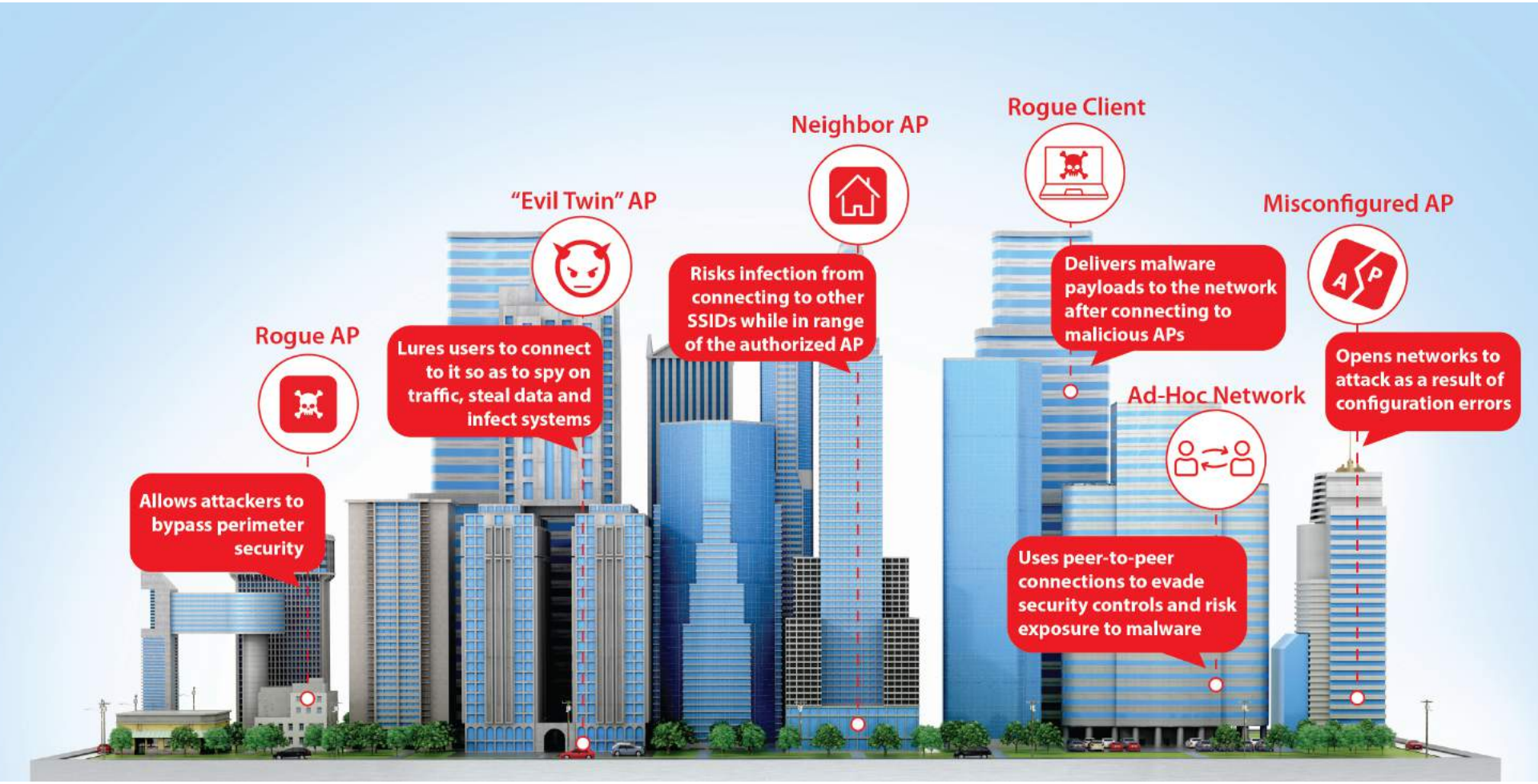
Thomas Fleischmann
Senior Sales Engineer Central Europe

Thomas.Fleischmann@watchguard.com

Agenda

- Bedrohungen im WLAN Umfeld
  - Welchen Gefahren ist ein Client ausgesetzt
- Was ist WIPS genau?
  - Wireless Intrusion Prevention erklärt
  - Wie kann man WIPS nutzen, Client Verhalten zu kontrollieren
- Demo
- Vorteile von TWE

Unternehmen bleiben gegenüber den sechs bekannten Wi-Fi-Bedrohungskategorien anfällig



Bedrohungen im WLAN Umfeld

- Ein Client im Bereich WLAN ist mehreren Bedrohungs Szenarien ausgesetzt
  - Deauthentication-Angriff
  - falsch konfigurierter Access Point
  - Evil Twin
  - Karma Attacke
- Da WLAN auf Einfachheit designe wurde, bekommt der Benutzer diese Angriffe nicht mit.
  - Auch die modernen Devices zeigen keine Warnung an.
  - Automatisches Verbinden ist Standard !

Bedrohungen im WLAN Umfeld

- Ist das nicht nur Theorie?

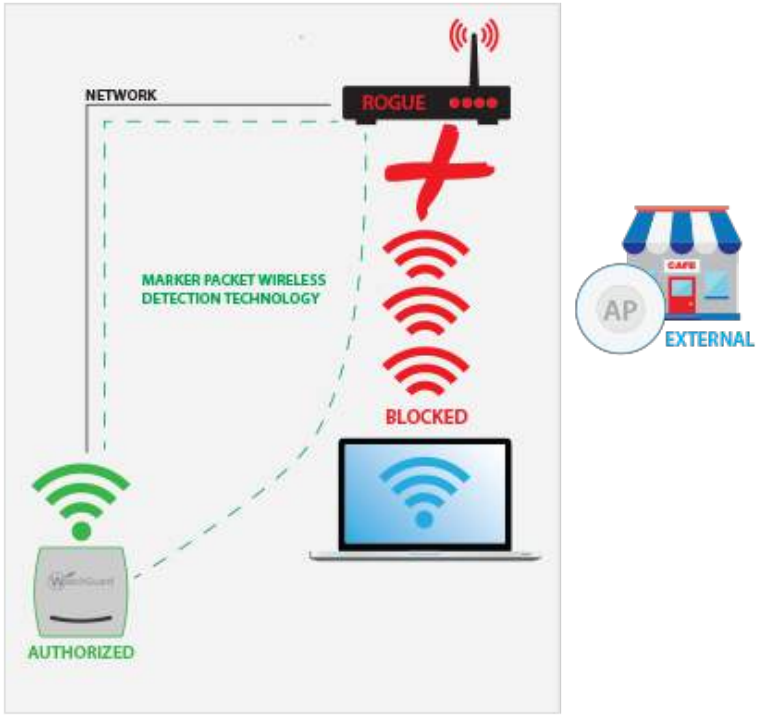
- Nein, da es viele Tools für WiFi Hacking existieren.
  - Nicht nur im Bereich WiFi, sondern in vielen anderen Bereichen. https://www.heise.de/select/ct/2017/18/1504370006723906
  - Mit einfacher Hardware und Open Source Software kann man für kaum Invest ein Angriffswerkzeug aufsetzen.
    - Kali Linux
    - Parrot OS
    - …

- Und Anleitungen in Massen
  - Ca. 10. Mio plus Einträge für Wifi Hacking auf Youtube

Was ist WIPS genau?

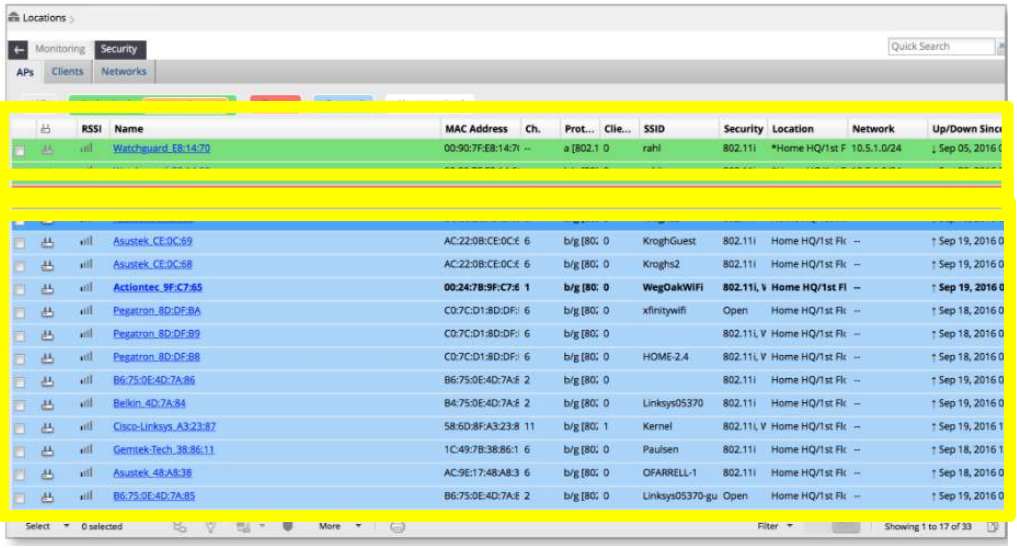
Wireless Intrusion Prevention System (WIPS)

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



Wie funktioniert WIPS?

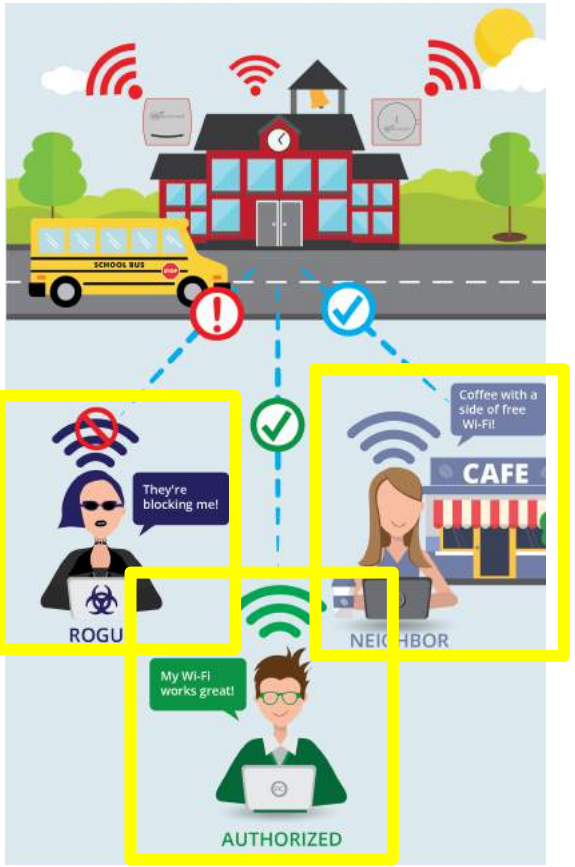
- Klassifikation der Systeme als Grundlage für WIPS



Sichert den kontinuierlichen Wi-Fi Zugriff autorisierter Systeme

Verhindert den Zugriff von Rogues (Angreifern)

Keine Auswirkungen auf Wi-Fi Netze benachbarter Unternehmen



WatchGuard Wi-Fi Cloud WIPS

WIPS

Marker Packets Method (Patented)

- Injektion ins Netzwerk und Weitergabe ins WLAN
- Versendet über WLAN und empfangen im LAN

Vorteile der Technologie:

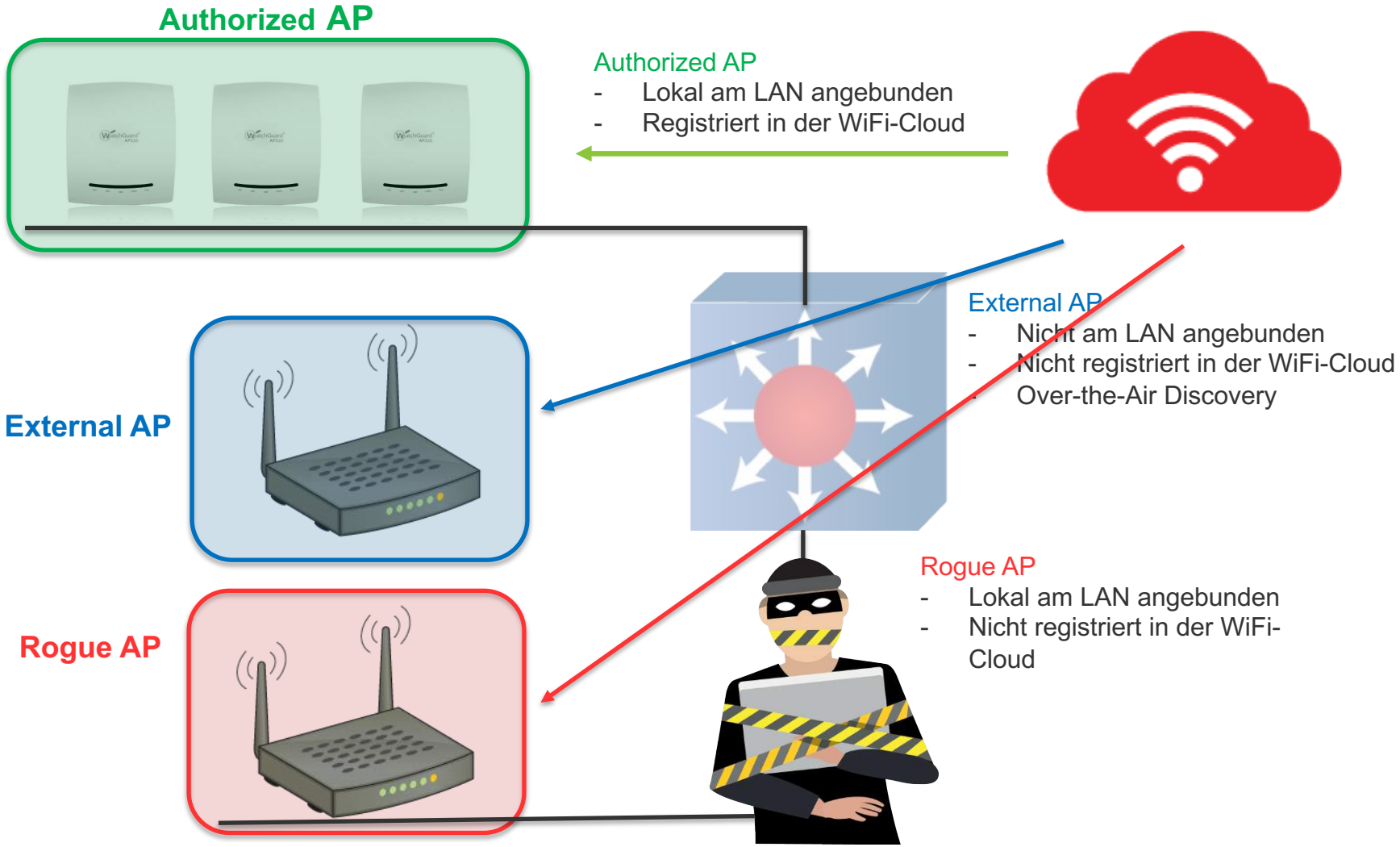
- Keine Fehlalarmierung & keine Fehleinschätzung von Rogue-APs
- Integration und Interaktion mit anderen Netzkomponenten (Switchen) ist nicht nötig
- Sofort nutzbarer und automatisierter Schutz
- Schnellste Erkennung, egal wie ”groß” das Netzwerk ist

☑ Prevent Away!

✓ The MOST Secure Wi-Fi!

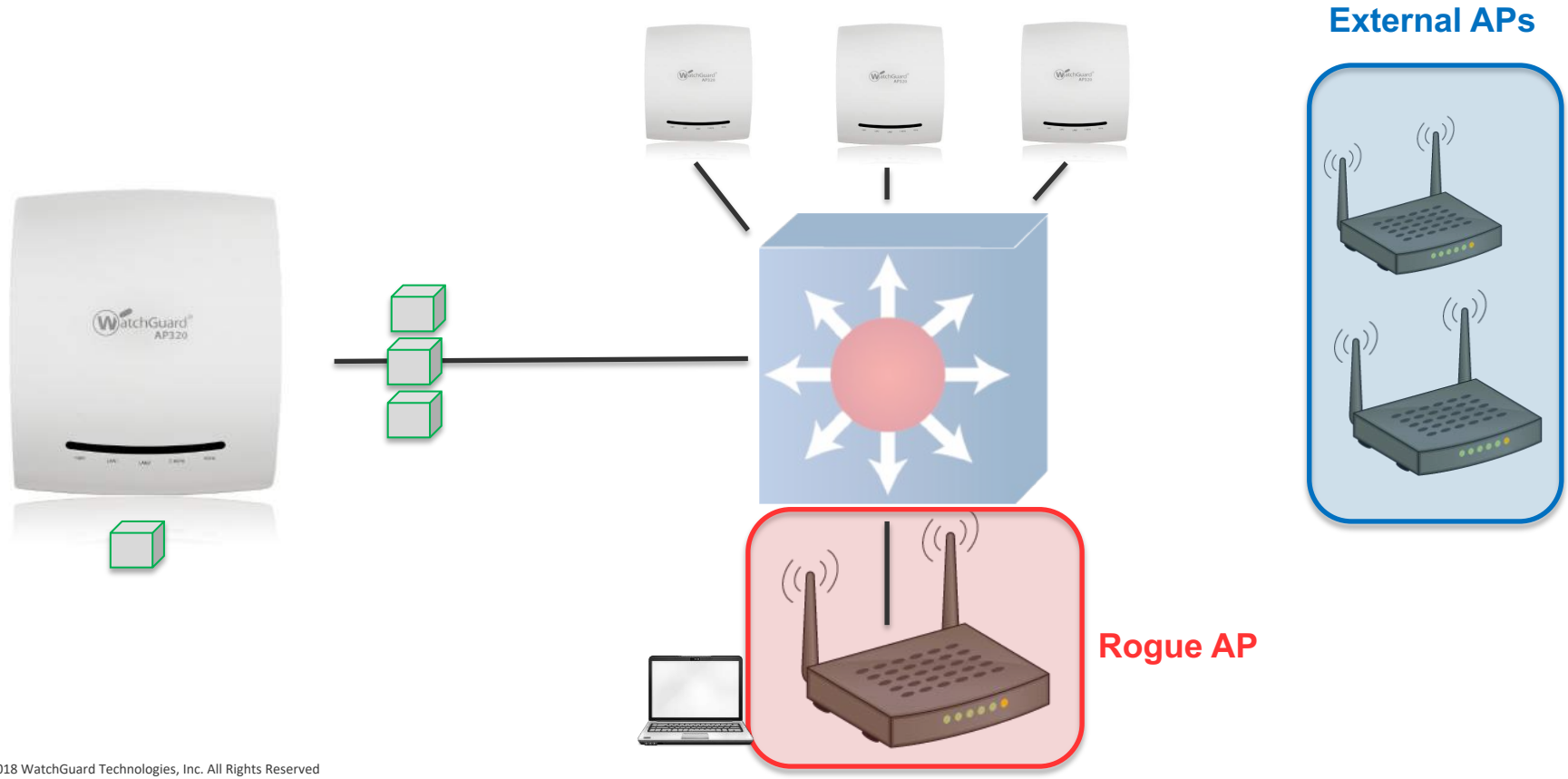
WatchGuard WIPS

- Automatische Klassifizierung der Accesspoints



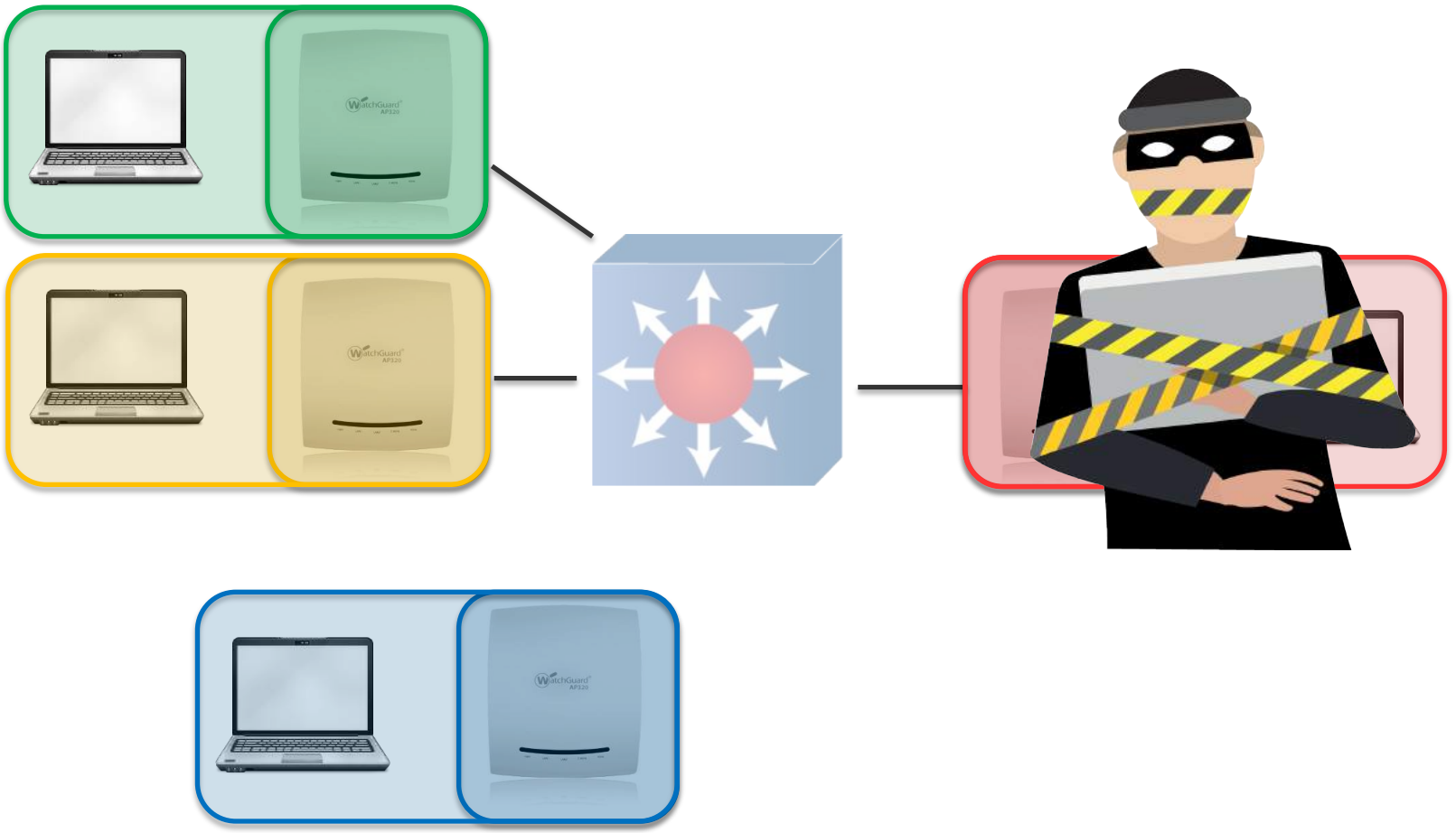
WatchGuard WIPS

- Marker Packets
  - Wired-Side Injection
  - Wireless-Side Injection



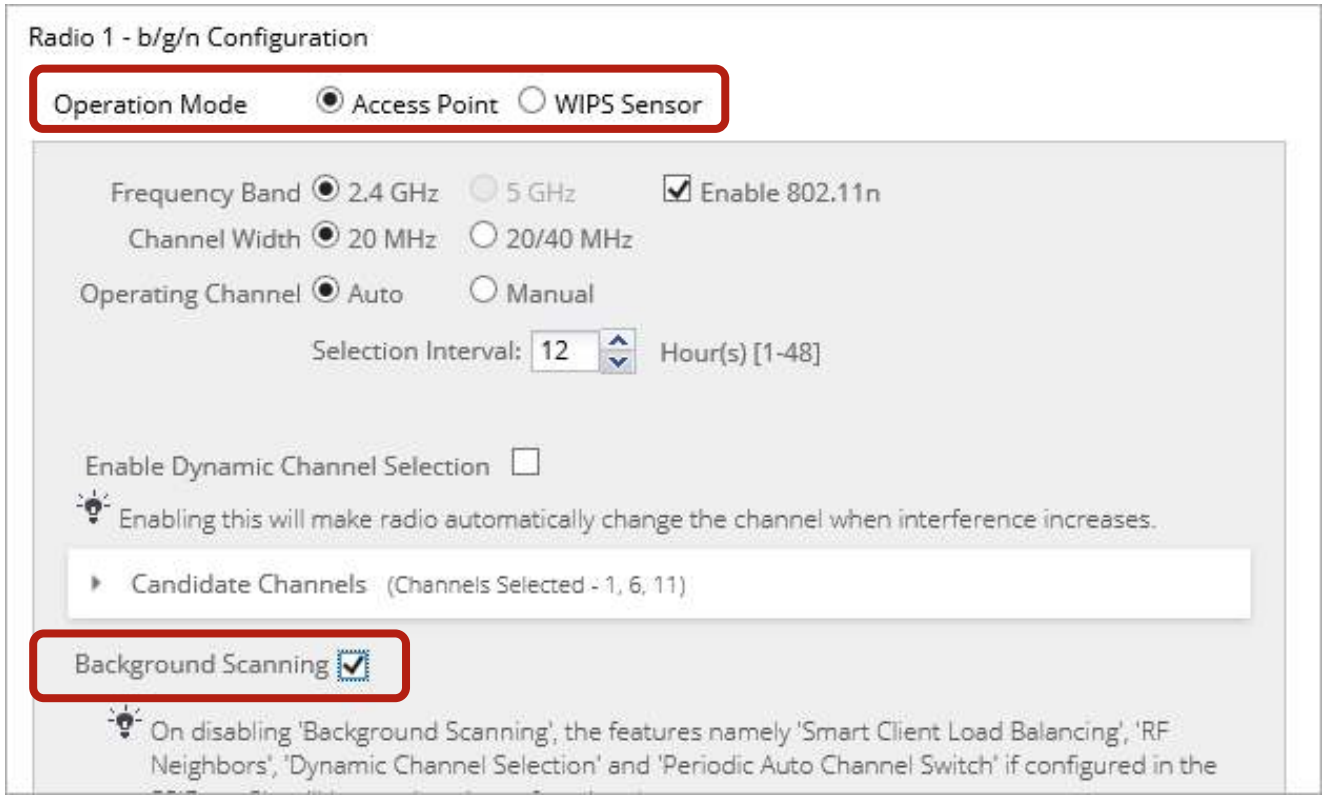
WatchGuard WIPS

- Automatische Klassifizierung der Clients
  - Bekannte Zusammenhänge werden genutzt



AP Scanning Modes

- Die Einstellungen für das Hintergrundscannen und den WIPS-Sensor werden in den Radio Settings des Device Template konfiguriert.

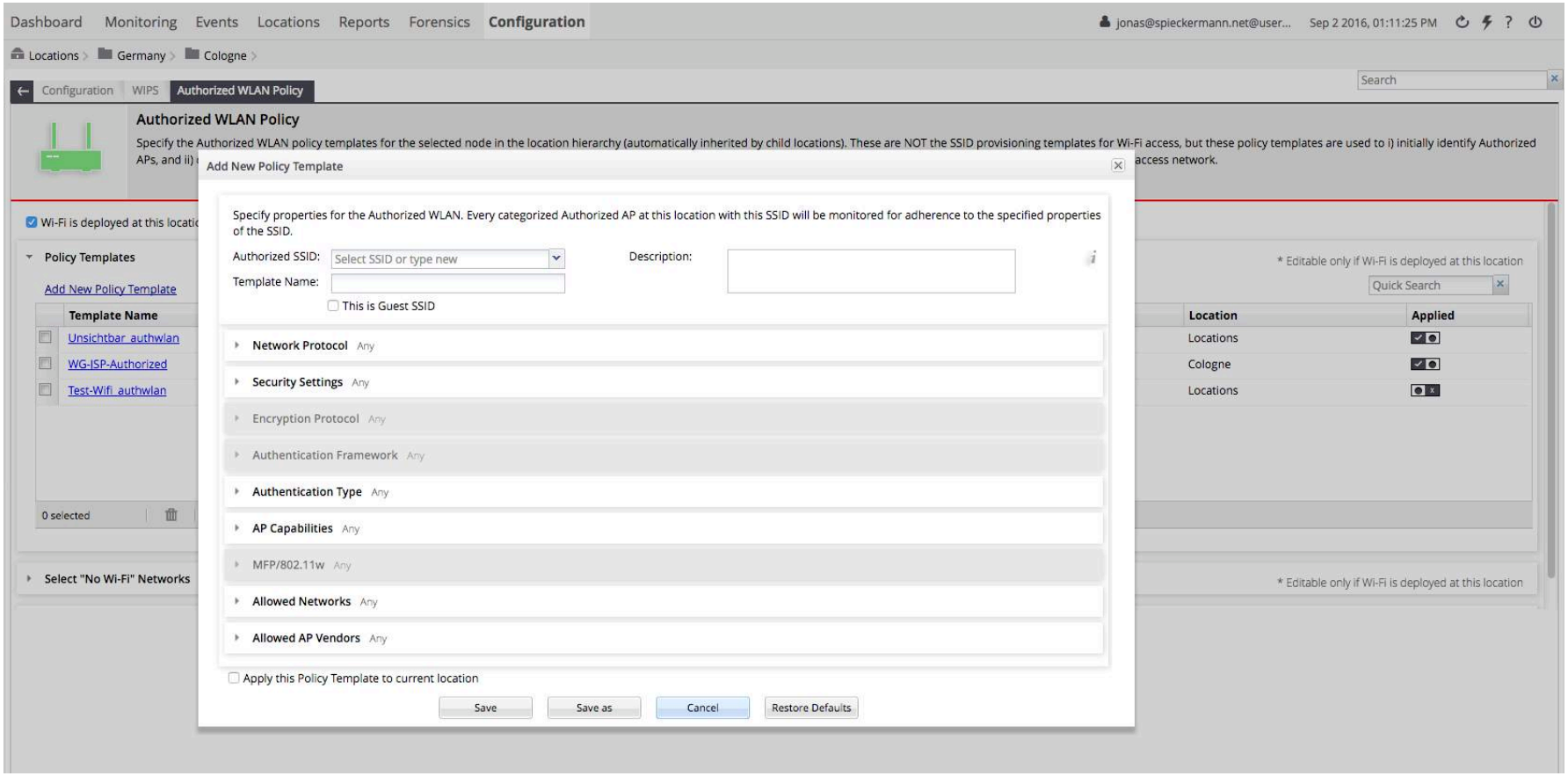


AP Scanning Modes: WIPS Sensor

- AP als dedicated WIPS Sensor
  - Keine “normale” AP Funktion und Bereitstellung einer SSID. Dedizierte Verwendung als WIPS Sensor zur Erkennung und Abwehr von Angriffen ”over-the-wire” und “over-the-air”.
  - Dual-band round-robin scanning (Jeder Kanal wird alle 5 Sekunden für 100ms geprüft)
  - AP325 und AP420 nutzen ein 3. Radio Modul zur dedizierten Anwendung der WIPS Funktion. Die beiden anderen Radio Module werden für Wi-Fi Access genutzt (SSID)
  - AP120/125, AP320, und AP322 802.11ac Wave 1 Access Points können Gefahren für 802.11ac Wave2 Netzwerke identifizieren wenn sie als WIPS Sensor genutzt werden.
  - Richtwert: 1 WIPS Sensor für alle 3-5 produktiven Accesspoints

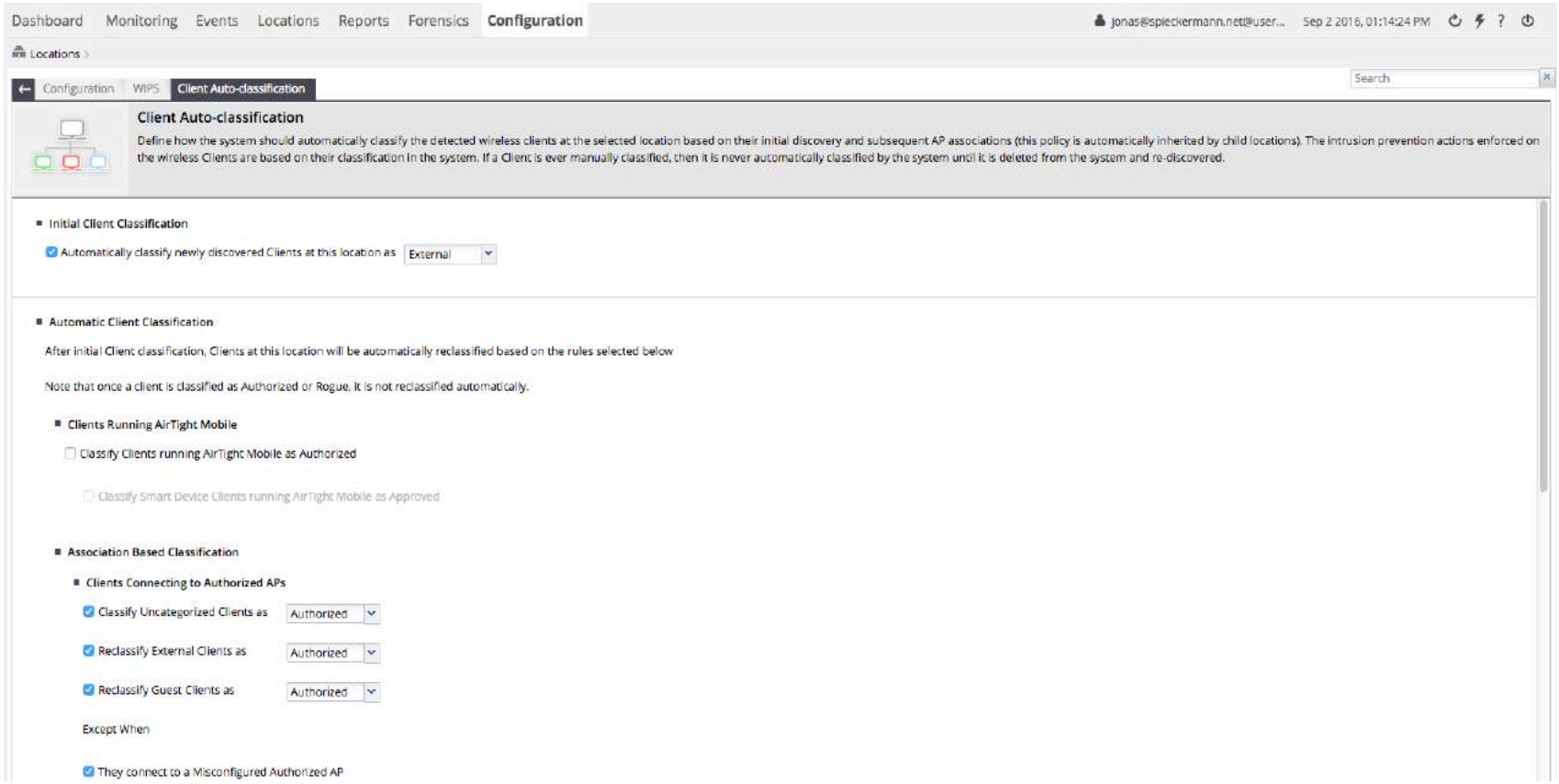
Authorized WLAN Policy

- Konfiguration der Authorized WLAN Policy
  - Welche WiFi Netze und Systeme sind autorisiert
  - Configuration > WIPS > Authorized WLAN Policy



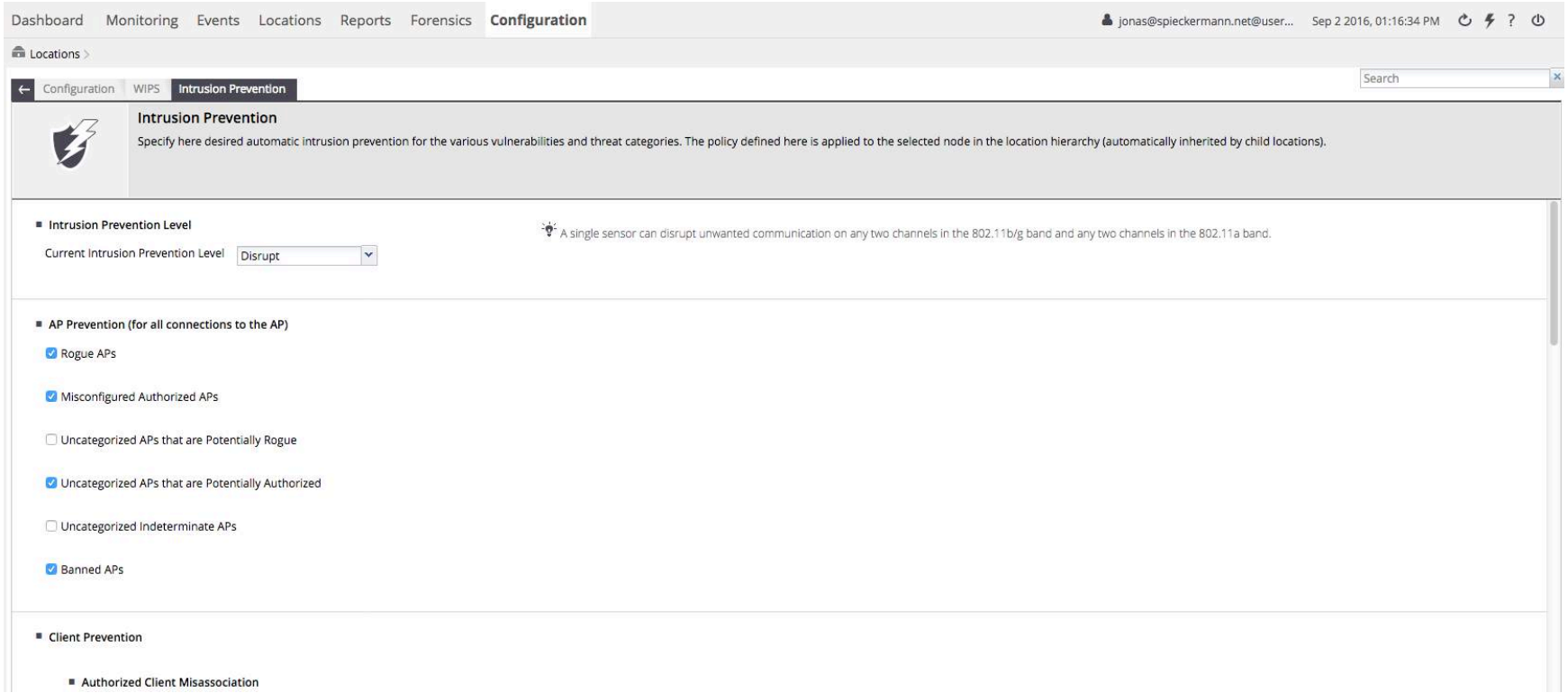
Auto-Classification

- Auto-classification anpassen
  - Configuration > WIPS > AP Auto-classification
  - Configuration > WIPS > Client Auto-classification



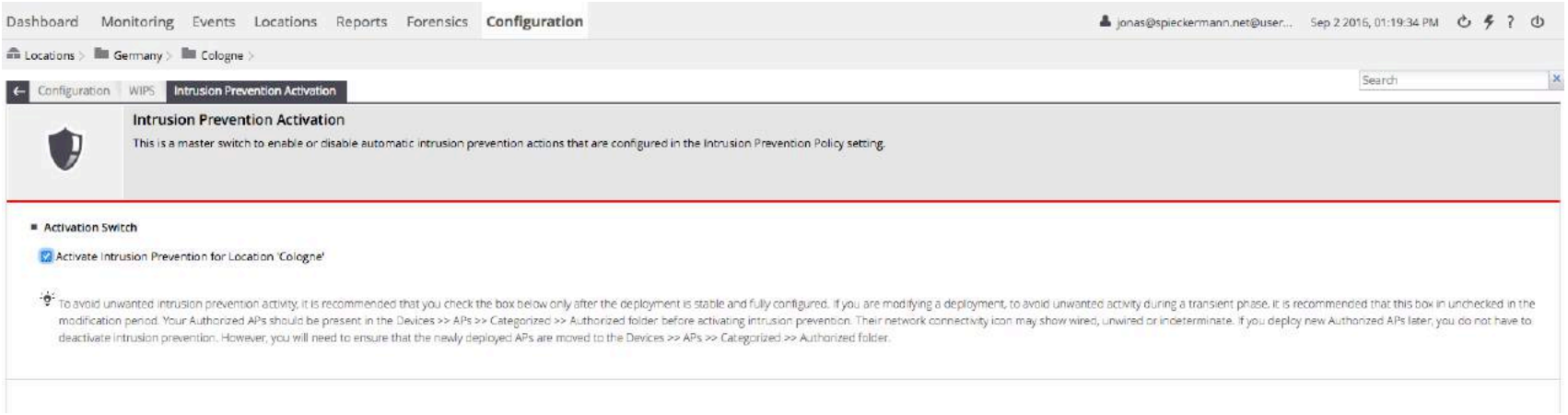
Intrusion Prevention Configuration

- Richtlinien für Intrusion Prevention definieren
  - Configuration > WIPS > Intrusion Prevention
  - Welches Verhalten soll verhindert werden
  - Welches Intrusion Prevention Level wird genutzt



Aktivierung von WIPS

- Intrusion Prevention Aktivieren
  - Configuration > WIPS > Intrusion Prevention Activation
  - „Scharfschaltung“ des Systems
  - Einstellung pro Location definierbar



Demo

Vorteile von TWE

Erstelle ein Trusted Wireless Environment

1

MARKET-LEADING PERFORMANCE

You should never be forced to compromise security to achieve adequate performance to support your environment with speed, connections and device density that it needs.

2

SCALABLE MANAGEMENT

With easy set-up and management, you should be able control your entire wireless network from a single interface and execute key processes to safeguard the environment and its users.

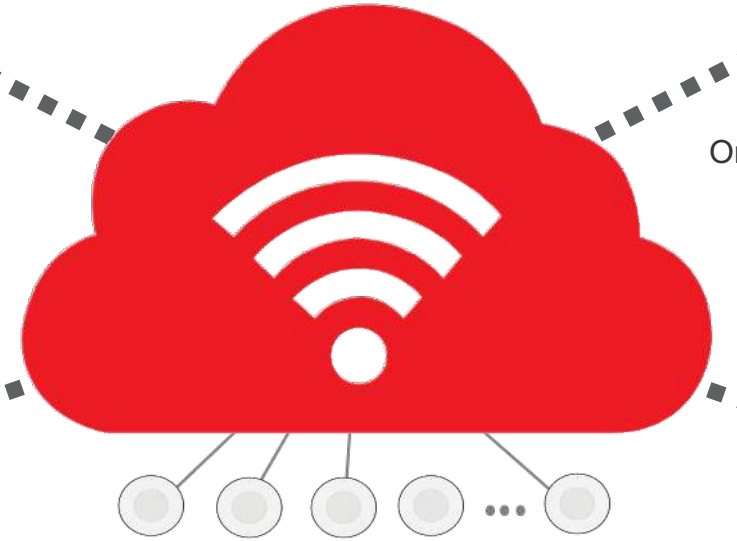
3

VERIFIED COMPREHENSIVE SECURITY

You need proof that your security solution defends your business against Wi-Fi attacks and can deliver on the following benefits:

- Provide automatic protection from the six known Wi-Fi threat categories
- Allow legitimate external access points to operate in the same airspace
- Restrict users from connecting to unsanctioned Wi-Fi access points

Mit WatchGuard's Secure, Cloud-Managed Wi-Fi



Patented Wireless Security
Only hands-off automated WIPS with low false positives on the market

Management That Scales
Only platform that easily scales from one AP to unlimited with no infrastructure

Business-Driven Analytics
Location tracking, footfall, dwell time, repeat visitors, and more at no extra cost and no third-party requirements

Powerful Engagement Tools
Captivating splash pages and campaigns to interact with visitors using social media, video, polls, and more

Verifizierte, umfassende Sicherheit mit WatchGuard

WatchGuard ist der einzige Anbieter in Miercoms Report der folgendes umsetzt:

- Erkennt automatische und verhindert die sechs bekannten Wi-Fi-Bedrohungskategorien bei gleichzeitiger Aufrechterhaltung der Leistung
- Unterstützung automatischer Erkennung und Verhinderung von Rogue-APs und Rogue-Clients
- Automatisches Blockieren von Clients bei der Kommunikation über eine Ad-hoc-Wi-Fi-Verbindung
- Verhindert automatisch die Verbindungen zu “Evil Twins“ und Verbindungen zu falsch konfigurierten Aps, wie etwa SSIDs ohne Verschlüsselung

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**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

Packaged To Meet Your Needs

Mit den WatchGuard Wifi-Paketen finden Sie schnell und einfach die richtigen Funktionen, die Ihr Unternehmen heute und morgen benötigten.

WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi *
Wi-Fi Cloud License	✓	✓	
Wireless Intrusion Prevention System (WIPS) Cloud-managed APs have built-in WIPS to help ensure you have the protection you need from malicious attacks and rogue APs	✓	✓	
GO Mobile Web App Easily set-up your network and configuration from any mobile device	✓	✓	
Customer Engagement Tools Splash pages, social media integration, surveys, coupons, videos, and so much more	✓		
Location-based Analytics Know how and when visitors are using your Wi-Fi, customizable reports and alerts for real-time and historical usage data	✓		
Firebox Gateway Wireless Controller			✓
Standard 24x7 Support Hardware warranty with advance hardware replacement, customer support, and software updates	✓	✓	✓

*Basic Wi-Fi requires a Firebox® for AP management

THANK YOU