

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

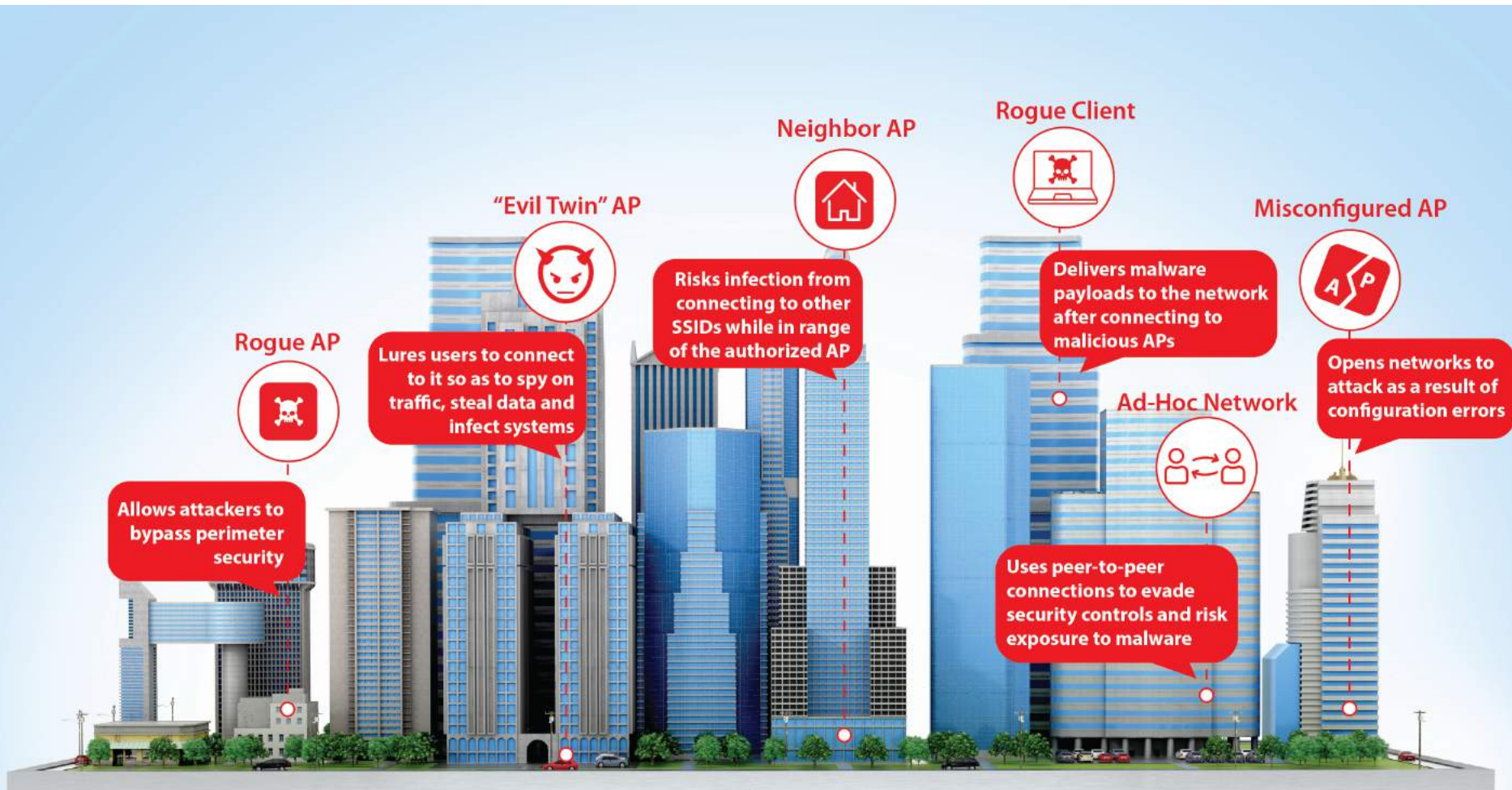
Thomas Fleischmann
Senior Sales Engineer Central Europe

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
 - ...

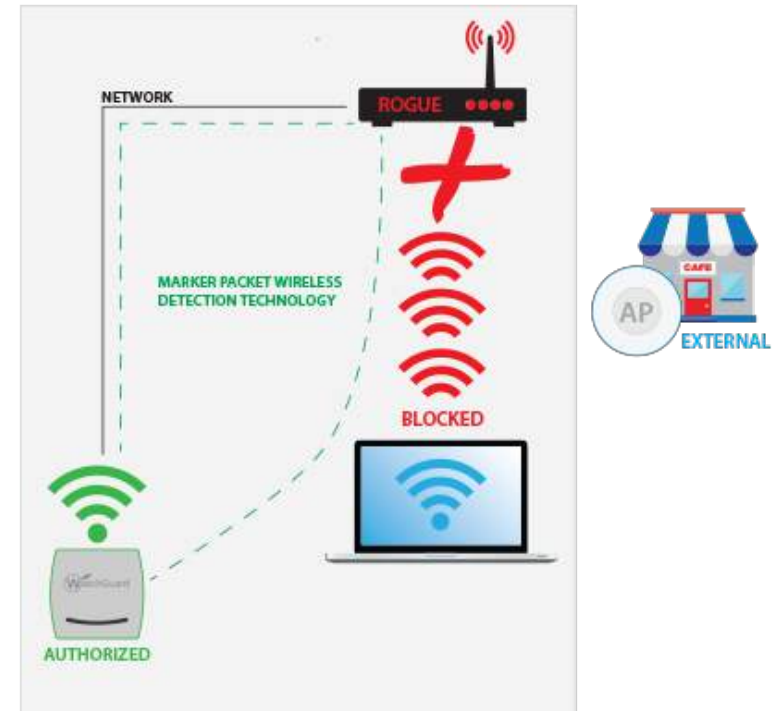
- Und Anleitungen in Massen
 - Ca. 10. Mio plus Einträge für Wifi Hacking auf Youtube

A horizontal red band across the middle of the page, filled with a repeating pattern of white Wi-Fi signal icons inside cloud shapes. The icons are of varying sizes and are scattered across the band.

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?

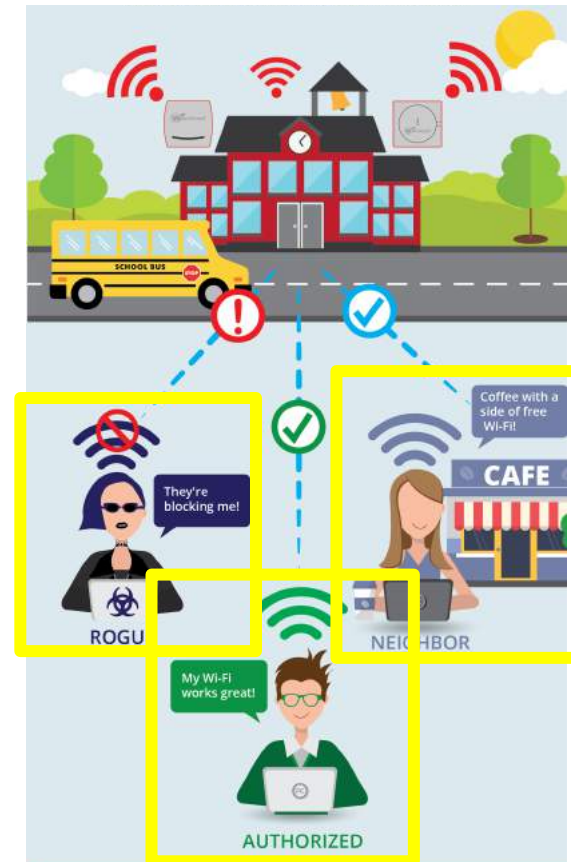
- Klassifikation der Systeme als Grundlage für WIPS

	RSSI	Name	MAC Address	Ch.	Prot...	Clien...	SSID	Security	Location	Network	Up/Down Sinc
	-71	Watchguard_E8-1470	00:90:7F:EB:14:71	11	802.11	0	rahl	802.11i	*Home HQ/1st F	10.5.1.0/24	↑ Sep 05, 2016
	-71	Asustek_CE9C-89	AC:22:0B:CE:0C:6	6	b/g	(802.11)	KrogH-Guest	802.11i	Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Asustek_CE9C-88	AC:22:0B:CE:0C:6	6	b/g	(802.11)	KrogHs2	802.11i	Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Actiontec_9F-C7-85	00:24:7B:9F:C7:85	1	b/g	(802.11)	WegOakWiFi	802.11i	V Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Pegatron_8D-DE-8A	C0:7C:D1:8D:DF:6	6	b/g	(802.11)	xfinitywifi	Open	Home HQ/1st Fl		↑ Sep 18, 2016
	-71	Pegatron_8D-DE-89	C0:7C:D1:8D:DF:6	6	b/g	(802.11)		802.11i	V Home HQ/1st Fl		↑ Sep 18, 2016
	-71	Pegatron_8D-DE-88	C0:7C:D1:8D:DF:6	6	b/g	(802.11)	HOME-2.4	802.11i	V Home HQ/1st Fl		↑ Sep 18, 2016
	-71	B6-75-0E-4D-7A-86	B6:75:0E:4D:7A:86	2	b/g	(802.11)		802.11i	Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Belkin_4D-7A-84	B4:75:0E:4D:7A:84	2	b/g	(802.11)	Linksys05370	802.11i	Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Cisco-Linksys_A3-23-87	58:6D:8FA3:23:87	11	b/g	(802.11)	Kernel	802.11i	V Home HQ/1st Fl		↑ Sep 19, 2016
	-71	Gemtek-Tech_38-86-11	1C49:7B:38:86:11	6	b/g	(802.11)	Paulsen	802.11i	Home HQ/1st Fl		↑ Sep 18, 2016
	-71	Asustek_4B-A8-38	AC:9E:17:4B:A8:38	6	b/g	(802.11)	OFARRELL-1	802.11i	Home HQ/1st Fl		↑ Sep 18, 2016
	-71	B6-75-0E-4D-7A-85	B6:75:0E:4D:7A:85	2	b/g	(802.11)	Linksys05370-gu	Open	Home HQ/1st Fl		↑ Sep 19, 2016

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



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



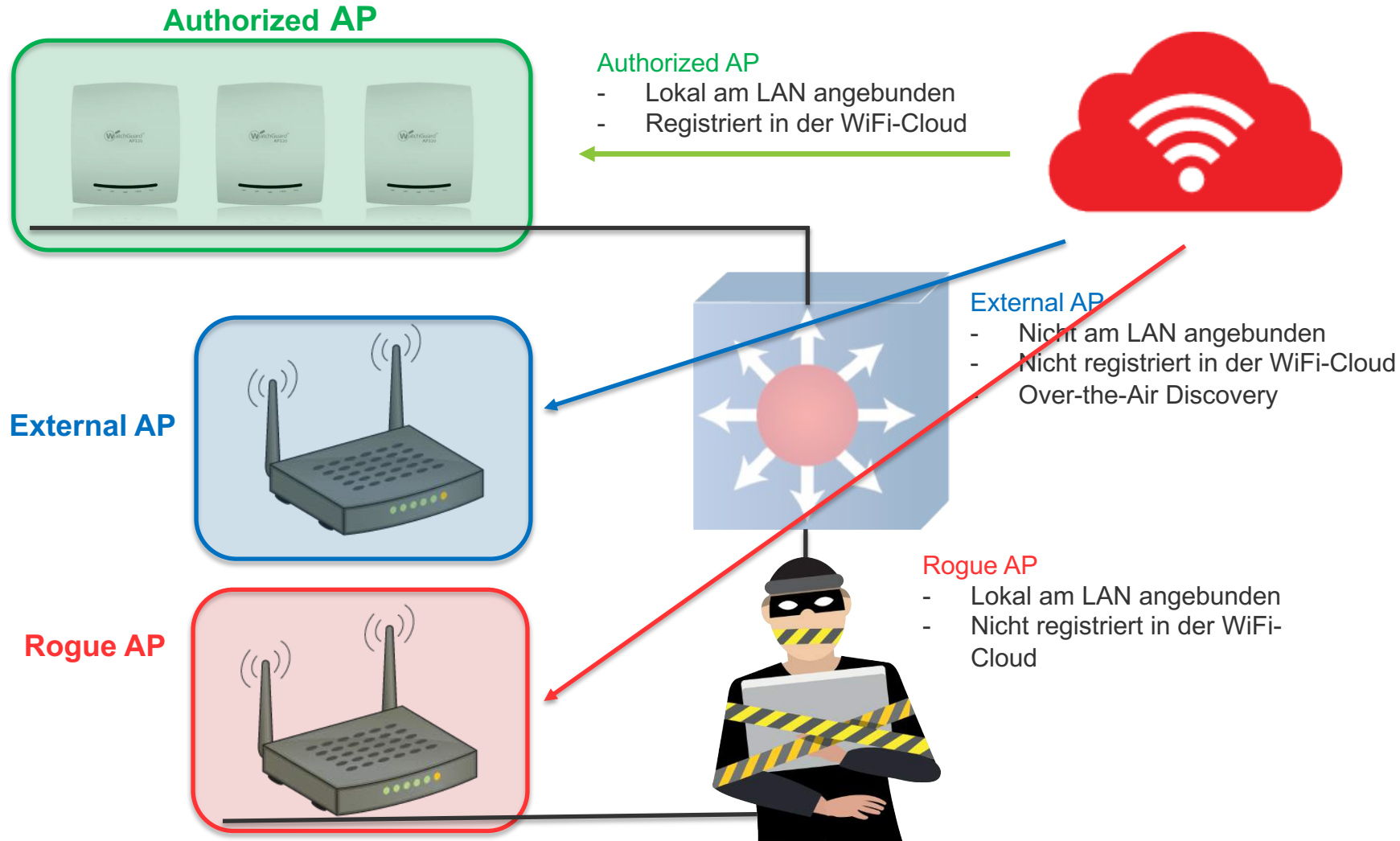
Prevent Away!



The MOST Secure Wi-Fi!

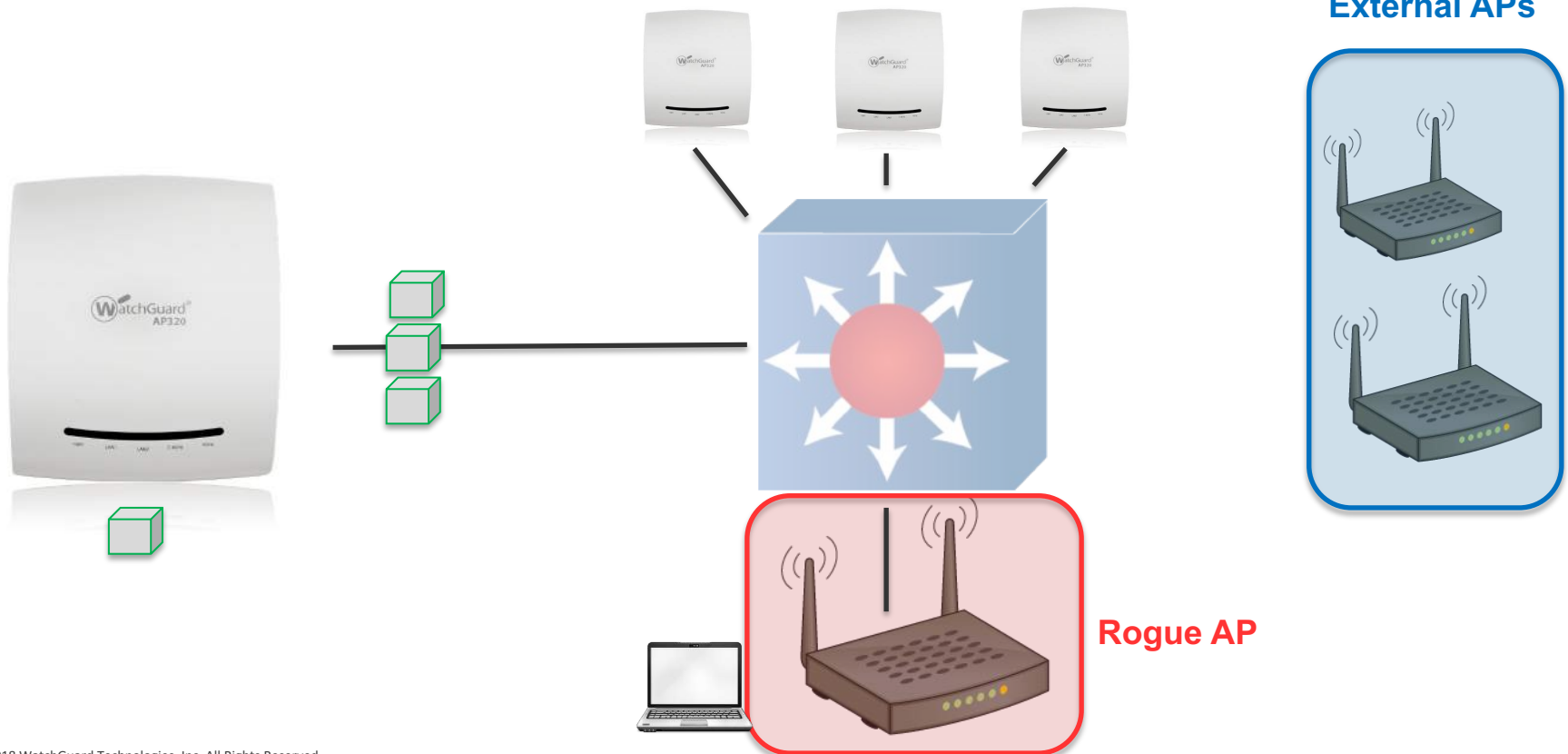
WatchGuard WIPS

■ Automatische Klassifizierung der Accesspoints



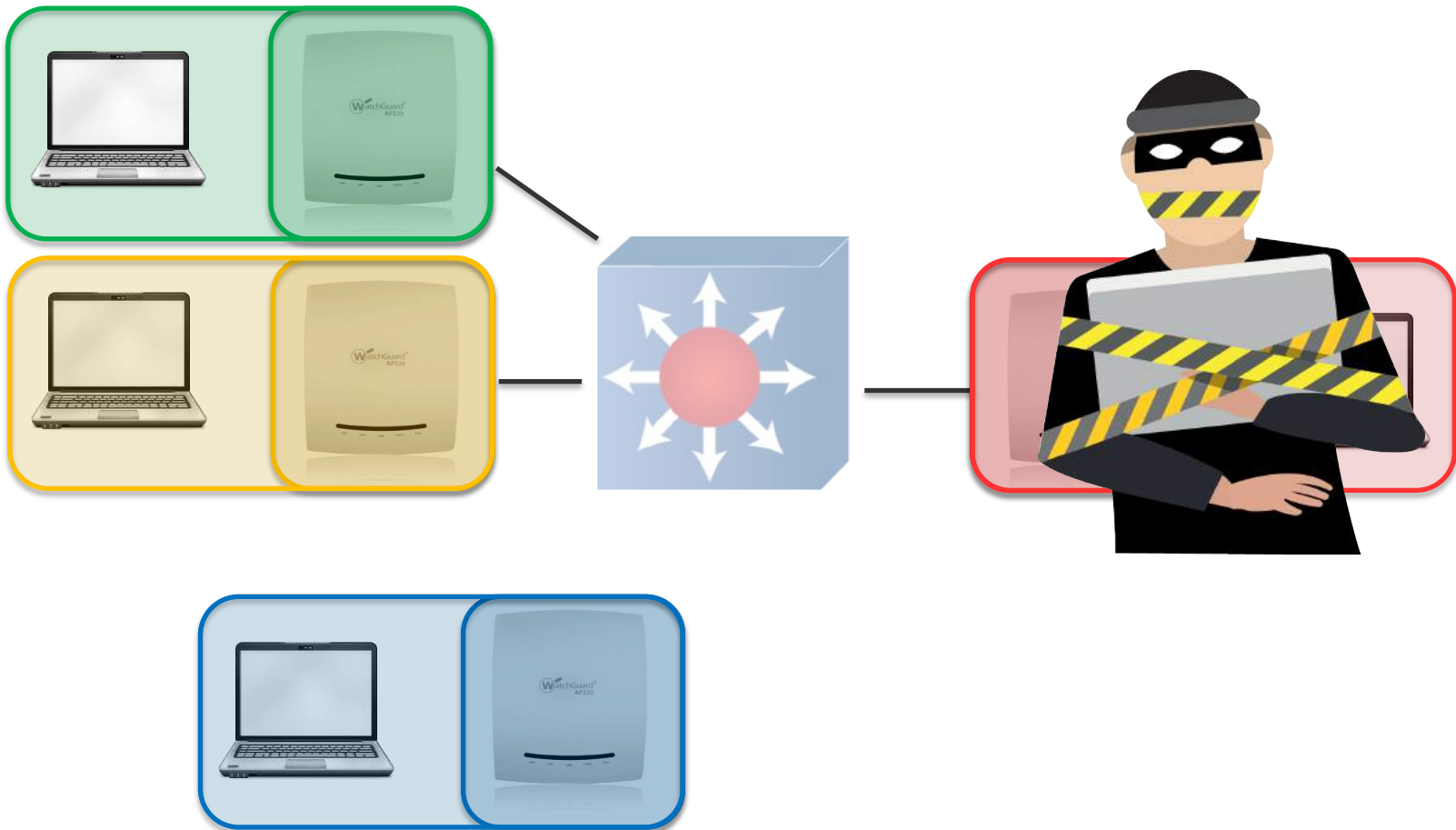
WatchGuard WIPS

- 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.

Radio 1 - b/g/n Configuration

Operation Mode Access Point WIPS Sensor


Frequency Band 2.4 GHz 5 GHz Enable 802.11n

Channel Width 20 MHz 20/40 MHz

Operating Channel Auto Manual


Selection Interval: Hour(s) [1-48]

Enable Dynamic Channel Selection

 Enabling this will make radio automatically change the channel when interference increases.

▶ Candidate Channels (Channels Selected - 1, 6, 11)

Background Scanning

 On disabling 'Background Scanning', the features namely 'Smart Client Load Balancing', 'RF Neighbors', 'Dynamic Channel Selection' and 'Periodic Auto Channel Switch' if configured in the

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

The screenshot displays the WatchGuard configuration interface. The main window is titled "Authorized WLAN Policy" and contains a dialog box for configuring a new policy template. The dialog box has the following fields and options:

- Authorized SSID:** A dropdown menu with the text "Select SSID or type new".
- Description:** A text input field.
- Template Name:** A text input field.
- This is Guest SSID
- Network Protocol:** A dropdown menu with "Any" selected.
- Security Settings:** A dropdown menu with "Any" selected.
- Encryption Protocol:** A dropdown menu with "Any" selected.
- Authentication Framework:** A dropdown menu with "Any" selected.
- Authentication Type:** A dropdown menu with "Any" selected.
- AP Capabilities:** A dropdown menu with "Any" selected.
- MFP/802.11w:** A dropdown menu with "Any" selected.
- Allowed Networks:** A dropdown menu with "Any" selected.
- Allowed AP Vendors:** A dropdown menu with "Any" selected.
- Apply this Policy Template to current location

At the bottom of the dialog box are four buttons: "Save", "Save as", "Cancel", and "Restore Defaults".

In the background, the configuration interface shows the "Configuration" tab selected, with a breadcrumb trail: "Locations > Germany > Cologne > Configuration > WIPS > Authorized WLAN Policy". A table on the right side of the interface shows the "Applied" status for various locations:

Location	Applied
Locations	<input checked="" type="checkbox"/>
Cologne	<input checked="" type="checkbox"/>
Locations	<input checked="" type="checkbox"/>

Auto-Classification

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

The screenshot shows the WatchGuard configuration interface for Client Auto-classification. The breadcrumb navigation is Configuration > WIPS > Client Auto-classification. The page title is "Client Auto-classification" with a sub-header "Define how the system should automatically classify the detected wireless clients at the selected location based on their initial discovery and subsequent AP associations (this policy is automatically inherited by child locations). The intrusion prevention actions enforced on the wireless Clients are based on their classification in the system. If a Client is ever manually classified, then it is never automatically classified by the system until it is deleted from the system and re-discovered."

Initial Client Classification

- Automatically classify newly discovered Clients at this location as External

Automatic Client Classification

After initial Client classification, Clients at this location will be automatically reclassified based on the rules selected below.

Note that once a client is classified as Authorized or Rogue, it is not reclassified automatically.

Clients Running AirTight Mobile

- Classify Clients running AirTight Mobile as Authorized
- Classify Smart Device Clients running AirTight Mobile as Approved

Association Based Classification

Clients Connecting to Authorized APs

- Classify Uncategorized Clients as Authorized
- Reclassify External Clients as Authorized
- Reclassify Guest Clients as Authorized

Except When

- They connect to a Misconfigured Authorized AP

Intrusion Prevention Configuration

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

The screenshot shows the WatchGuard configuration interface for Intrusion Prevention. The top navigation bar includes Dashboard, Monitoring, Events, Locations, Reports, Forensics, and Configuration. The user is logged in as jonas@spieckermann.net@user... on Sep 2 2016, 01:16:34 PM. The breadcrumb trail is Configuration > WIPS > Intrusion Prevention. The main heading is "Intrusion Prevention" with a lightning bolt icon. Below the heading is a description: "Specify here desired automatic intrusion prevention for the various vulnerabilities and threat categories. The policy defined here is applied to the selected node in the location hierarchy (automatically inherited by child locations)." The configuration is organized into sections:

- Intrusion Prevention Level**: A dropdown menu for "Current Intrusion Prevention Level" is set to "Disrupt". A note states: "A single sensor can disrupt unwanted communication on any two channels in the 802.11b/g band and any two channels in the 802.11a band."
- AP Prevention (for all connections to the AP)**:
 - Rogue APs
 - Misconfigured Authorized APs
 - Uncategorized APs that are Potentially Rogue
 - Uncategorized APs that are Potentially Authorized
 - Uncategorized Indeterminate APs
 - Banned APs
- Client Prevention**:
 - Authorized Client Misassociation

Aktivierung von WIPS

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

The screenshot shows the WatchGuard web interface for configuring Intrusion Prevention Activation. The breadcrumb trail is Configuration > WIPS > Intrusion Prevention Activation. The page title is "Intrusion Prevention Activation" and it includes a shield icon. The main content area features an "Activation Switch" section with a checked checkbox for "Activate Intrusion Prevention for Location 'Cologne'". Below this, a warning icon and text state: "To avoid unwanted intrusion prevention activity, it is recommended that you check the box below only after the deployment is stable and fully configured. If you are modifying a deployment, to avoid unwanted activity during a transient phase, it is recommended that this box is unchecked in the modification period. Your Authorized APs should be present in the Devices >> APs >> Categorized >> Authorized folder before activating intrusion prevention. Their network connectivity icon may show wired, unwired or indeterminate. If you deploy new Authorized APs later, you do not have to deactivate intrusion prevention. However, you will need to ensure that the newly deployed APs are moved to the Devices >> APs >> Categorized >> Authorized folder."



Demo

A horizontal red band across the middle of the page, filled with a pattern of white Wi-Fi signal icons inside cloud shapes of varying sizes.

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

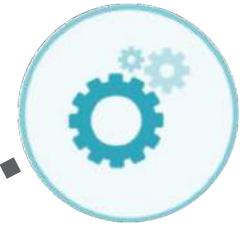


Mit WatchGuard's Secure, Cloud-Managed Wi-Fi



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

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



Packaged To Meet Your Needs

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

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