WatchGuard Wi-Fi Cloud FAQ

F1: Inwiefern unterscheidet sich die WatchGuard Wi-Fi Cloud von den Wireless-Produkten anderer Sicherheitsanbieter?

A: Die WatchGuard Wi-Fi Cloud fügt alle Teile des Puzzles zusammen: Wi-Fi-Sicherheit, vereinfachte Verwaltung, interaktives Zusammenspiel und Analysen. IT-Administratoren in mittelständischen und dezentral aufgestellten Unternehmen können nun ihre WLANs einfach bereitstellen, verwalten und skalieren, wichtige Sicherheitsfunktionen hinzufügen, den Marketingauftritt durch Auswertung neuer Daten verbessern und die Kundenerfahrung beleben.

F2: Wie funktioniert das, und was sind die Alleinstellungsmerkmale?

A: Mit der WatchGuard Wi-Fi Cloud kommen Unternehmen in den Genuss sicherer, leistungsstarker drahtloser Funktionalität, wie man sie üblicherweise nur in Fortune 100-Unternehmen findet. Das WatchGuard Wireless Intrusion Prevention System (WIPS) nutzt eine patentierte Marker-Packet-Technologie für die schnelle und automatische Identifizierung, Klassifizierung und Abwehr von Rogue-APs und -Geräten. Die Quote der False Positives ist dabei die branchenweit beste, d. h. Fehleinschätzungen kommen praktisch nicht vor, und Sie haben jederzeit einen umfassenden Überblick und auch die vollständige Kontrolle über die WLAN-Sicherheit. Mit der WatchGuard Wi-Fi Cloud können IT-Fachleute den sicheren WLAN-Zugriff einrichten, konfigurieren, überwachen, verbessern und eventuelle Störungen beseitigen. Außerdem haben sie die Möglichkeit, WLAN-Netze nach Bedarf zu skalieren. Das alles erfolgt in einem hierarchisch strukturierten, vorlagenbasierten Managementsystem über ein und dieselbe intuitive Oberfläche. Die bedarfsgerecht anpassbaren Dashboards der Lösung und Alarmfunktionen garantieren einen umfassenden Überblick über jedes Detail des drahtlosen Netzwerks. Sie sind damit für IT-Administratoren quasi eine „Goldgrube" für Marketingdaten wie Besucherzahlen und Kundendemografie, die eine direkte und persönliche Kommunikation mit einzelnen Kunden ermöglichen.

F3: Was macht die WIPS-Technologie von WatchGuard so einzigartig?

A. Die patentierte WIPS-Technologie von WatchGuard setzt sich von anderen WLAN-Sicherheitslösungen auf dem Markt ab. Sie sorgt für den realen, genauen und automatisierten WLAN-Schutz, den ein Unternehmen benötigt. WIPS von WatchGuard schützt WLAN-Umgebungen rund um die Uhr vor dem Zugriff durch unbefugte Geräte, Man-in-the-Middle(MitM)- und Denial-of-Service-Angriffen, Rogue-Access Points und vielen weiteren Bedrohungen. „False Positives" werden dabei nahezu ausgeschlossen. Einfache WIPS anderer Anbieter nutzen oft Signaturen und sind zu stark von Regeln für die MAC-Adressenkorrelation für Algorithmen zur WLAN-Bedrohungsklassifizierung abhängig. Diese generieren viele „False Positives", zu viele Alarme und einen hohen Verwaltungsoverhead. WatchGuard Wi-Fi Cloud WIPS nutzt die erweiterte patentierte Marker Packet™- Technologie, die Folgendes ermöglicht:

- Automatisches und genaues Klassifizieren von Access Points (APs) und Clientgeräten, die mit Ihrem Netzwerk verbunden sind und sich in dessen Nähe befinden
- Erkennen und Vermeiden von Rogue-APs
- Erkennen falsch konfigurierter APs im Netzwerk, die nicht den definierten Sicherheitsrichtlinien entsprechen
- Erkennen und Vermeiden gefährlicher Angriffe, wie Man-in-the-Middle, Evil Twin und SSID-Honeypots

F4: Wie einfach ist die Implementierung der cloudfähigen Access Points von WatchGuard?

A: Jede WatchGuard-Lösung ist dafür ausgelegt, in kleinen, mittleren und dezentral aufgestellten Unternehmen Sicherheit auf Enterprise-Niveau bereitzustellen. WatchGuard Wi-Fi Cloud-fähige APs können flexibel mit der Wi-Fi Cloud-Appliance (Secure Wi-Fi- oder Total Wi-Fi-Lizenz) oder der Firebox-Appliance über den Gateway

Wireless Controller (Basic Wi-Fi-Lizenz) verwaltet werden. Zusätzlich gibt es noch die cloudfähigen APs von WatchGuard, die mit einer Wi-Fi Cloud-Lizenz bereitgestellt, verwaltet und so konfiguriert werden können, dass sie den Funkverkehr über eine WatchGuard Firebox- oder XTM- oder eine sonstige UTM-Appliance routen. Die gewährleistet mehrschichtige Sicherheit und sichert die WLAN-Umgebung ganzheitlich ab. WatchGuard Access Points profitieren von absoluter Flexibilität: Sie lassen sich sowohl als APs als auch als dedizierte WIPS-Sicherheitssensoren verwenden. Werden die Geräte als dedizierte WIPS-Sensoren bereitgestellt, arbeiten sie gemeinsam mit ihren vorhandenen Access Points (Cisco, Aruba, Ruckus, Ubiquiti usw.) und erweitern Ihr Netzwerk somit um WLAN-Sicherheit auf Enterprise-Niveau. In diesem Fall sorgen die Access Points nicht für sicheren WLAN-Datenverkehr für Benutzer, sondern für die Überwachung Ihrer WLAN-Umgebung und den Schutz Ihres Unternehmens vor Wireless-Bedrohungen – für beispiellose WIPS-Sicherheit.

F5: Können Sie mir weitere Informationen über die Wi-Fi-Pakete geben?

A. WatchGuard arbeitet weiterhin an Innovationen beim WLAN-Sicherheitsangebot. Unsere Mission ist, Ihnen einen Wettbewerbsvorteil zu bieten. Mit den neuen WLAN-Paketen können unsere geschätzten Vertriebspartner schnell und einfach die richtigen Funktionen ermitteln, die ihre Kunden benötigen.

Total Wi-Fi
Verwenden Sie die WatchGuard Wi-Fi Cloud für WatchGuard AP-Management, WIPS-Sicherheit und Überwachung. Dazu erhalten Sie weitere Tools für die Benutzereinbindung von Gästen, standortbasierte Analysen, Social-Media-Integration, Captive Portals und die Erstellung von Werbeseiten.

Secure Wi-Fi
Verwenden Sie die WatchGuard Wi-Fi Cloud für WatchGuard AP-Management, WIPS-Sicherheit und Überwachung.

Basic Wi-Fi
Verwenden Sie den Gateway Wireless Controller mit einer WatchGuard Firebox, um WatchGuard APs direkt über die Firebox zu konfigurieren, zu verwalten und zu überwachen.

F6: Warum wird diese Lösung nur für KMU und dezentral aufgestellte Unternehmen angeboten?

A: Knappe Budgets und höhere Anforderungen an die Skalierbarkeit sind Herausforderungen, mit denen mittelständische und dezentral aufgestellte Unternehmen zu kämpfen haben, wenn es um die sichere und zuverlässige drahtlose Anbindung von Mitarbeitern und Kunden geht. Auch wenn sich die WatchGuard Wi-Fi Cloud vorrangig an diese Unternehmen richtet, garantiert diese leistungsstarke Lösung Unternehmen jeder Größe WLAN-Sicherheit, -Verwaltbarkeit und -Leistung auf Enterprise-Niveau.

F7: Über welche einzigartigen Sicherheitsfunktionen verfügt die WatchGuard Wi-Fi Cloud?

A: Die WatchGuard Wi-Fi Cloud bietet patentierte Technologie, mit der Aktivitäten auf drahtlosen und drahtgebundenen Netzwerken rund um die Uhr überwacht werden können. Dank des branchenweit präzisesten Algorithmus klassifiziert diese Lösung verbundene Access Points und Clients automatisch und zuverlässig als „Autorisiert", „Rogue" oder „Extern". Die Wi-Fi Cloud „lernt" das Verhalten verbundener Clients und APs und vereinfacht die automatische Prävention anhand vordefinierter Ereignisregeln. Diese Art der Automatisierung erfordert keine Eingriffe der IT-Administratoren, die sich beruhigt weiteren wichtigen Aufgaben widmen können – denn die Wi-Fi Cloud ist so programmiert, dass sie Rogue-APs und -Clients sofort blockiert, wenn diese versuchen, auf das WLAN-Netz zuzugreifen.

F8: Welche besonderen Dialog- und Analysefunktionen umfasst die WatchGuard Wi-Fi Cloud?

A: Die WatchGuard Wi-Fi Cloud bietet die Möglichkeit, Startseiten (Captive Portals) selbst zu gestalten, die beim Login und anschließend per SMS gezielte Kundenwerbung ermöglichen. Durch die Einbindung sozialer

Netzwerke erhalten Unternehmen wertvolle demografische Daten über jeden einzelnen verbundenen Kunden. Sie können Benutzern über die Wi-Fi Cloud darüber hinaus speziell auf sie zugeschnittene Nachrichten zusenden – per SMS, MMS oder über soziale Netzwerke – basierend auf vordefinierten Auslösern wie Benutzerinteraktion oder Verweilzeit im Netz. Die WLAN-Analysefunktion der Lösung generiertt auch eine visuelle Karte der Bewegungsmuster innerhalb eines Gebäudeplans und liefert informative Einblicke bietet einzigartige Einsicht in die Bewegungsmuster, das Verhalten und die demografische Entwicklung der Benutzer.

F9: Welche Managementfunktionen der WatchGuard Wi-Fi Cloud sind Alleinstellungsmerkmale?
A: Mit der Wi-Fi Cloud verwaltete Umgebungen lassen sich problemlos bis zu einer unbegrenzten Anzahl von APs über mehrere Standorte hinweg skalieren - ganz ohne Controller-Infrastruktur. Mit dem hierarchisch strukturierten, vorlagenbasierten Managementsystem der Lösung können APs nach Standort und Kunde gruppiert werden, um Richtlinien bedarfsgerecht anzupassen, Daten granular darzustellen und so eine netzwerkübergreifende Konsistenz zu gewährleisten. Über die mobile Webanwendung GO können Benutzer ihre WLAN-Umgebungen von jedem mobilen Gerät aus verwalten. Die Lösung erlaubt ferner die Einrichtung mehrerer benutzerdefinierter Werbeseiten und personalisierter Kundenwerbeaktionen.

F10: Steht die GO-App auf iOS und Android zur Verfügung?
A: GO ist eigentlich eine für Mobilgeräte optimierte Webanwendung. Deshalb muss keine App installiert werden, und die Aktualisierung erfolgt automatisch, wenn die Wi-Fi Cloud aktualisiert wird. Sowohl iOS als auch Android werden unterstützt, und die URL, über die Sie ein Symbol auf den Startbildschirm Ihres Mobilgeräts herunterladen können, lautet: http://go.watchguard.cloudwifi.com

F11: Kann der in den Firebox-/UTM-Appliances integrierte Gateway Wireless Controller über die Wi-Fi Cloud verwaltet werden?
A: Nein, der Gateway Wireless Controller (GWC) in unseren XTM- und Firebox-Appliances unterstützt lediglich grundlegende WLAN-Funktionen für APs, die über Firewalls verwaltet werden. Die Wi-Fi Cloud ist vom GWC getrennt und stellt umfassende Funktionen für eine flexibel skalierbare Verwaltung in der Cloud, WIPS, Analysen und den Kundendialog bereit.

F12: Wie lange werden die von der Wi-Fi Cloud erfassten Analysen aufbewahrt?
A: Die Daten werden 13 Monate lang in der Wi-Fi Cloud aufbewahrt.

F13: Wo werden die von diesem System erfassten Daten gespeichert? Wie werden die Daten geschützt?
A: Die WatchGuard Wi-Fi Cloud wird als VPC (Virtual Private Cloud) im Rechenzentrum von AWS (Amazon Web Services) bereitgestellt. In der VPC-Architektur ist die Wi-Fi Cloud-Umgebung logisch von Umgebungen anderer Einheiten isoliert, die ebenfalls im AWS-Rechenzentrum vorhanden sind. Weitere Informationen finden Sie in unserer technischen Kurzbeschreibung *Wi-Fi Cloud und Sicherheit*
https://p.widencdn.net/xxyazy/Tech_Brief_Secure_Wi-Fi_Cloud

F14: Was sind die Hauptunterschiede zwischen den APs von WatchGuard?
A. Der WatchGuard **AP125** ist genau die Lösung, die Sie gesucht haben. Der kompakte und kostengünstige Access Point für den Innenbereich bietet 2x2 802.11ac Wave 2 Multi-User MIMO (MU-MIMO). Dieser Access Point unterstützt außerdem zwei parallel nutzbare Funkmodule für den 5-GHz- und 2,4-GHz-Frequenzbereich mit 2 parallelen Datenströmen und damit Geschwindigkeiten von bis zu 867 Mbit/s bzw. 300 Mbit/s. Typische Einsatzgebiete für den AP125 sind Umgebungen mit geringer Dichte wie etwa kleine Schulen, verstreute Unternehmensniederlassungen und kleine Besprechungsräume.

Der **AP322** ist ein robuster 3x3 MIMO 802.11ac-Access-Point für Außenbereiche mit dualen, parallel nutzbaren Funksystemen im 5 GHz- und 2,4 GHz-Frequenzband, die 802.11a/n/ac, 802.11b/g/n, drei getrennte

Datenströme und Geschwindigkeiten von bis zu 1,3 Gbit/s und 450 Mbit/s unterstützen. Der AP322 bietet umfassende, schnelle und zuverlässige WLAN-Abdeckung. Damit ist er ideal für Stadien und Sportplätze, Schulen/Universitäten, Einkaufszentren, Parks, Hotelpoolbereiche und Straßencafés, Versandbereiche, Lagerhallen und weitere extreme Umgebungen oder Außenbereiche.

Der **AP325** schützt Ihr Unternehmen mit der neuesten 802.11 Wave 2-Technologie – passend zu Ihrem Budget. Der AP325 von WatchGuard ist ein Access Point für den Innenbereich. Dank Multi-User MIMO (MU-MIMO)-Technologie bedient er mehrere Geräte gleichzeitig – für ein noch besseres WLAN. Zum Leistungsumfang gehören außerdem zwei parallel nutzbare Funkmodule für den 5-GHz- und 2,4-GHz-Frequenzbereich, die 802.11a/n/ac Wave 2, 802.11b/g/n, zwei Spatial Streams und Geschwindigkeiten von bis zu 876 Mbit/s bzw. 300 Mbit/s unterstützen.

Der **AP420** bietet höchste WLAN-Geschwindigkeiten für die Unterstützung latenzempfindlicher Sprach- oder Videoanwendungen und Daten-Downloads über WLAN und sorgt mit einem 4x4 MU-MIMO Dualband-Funkmodul für die WLAN-Abdeckung in Räumen mit hoher Gerätedichte. Außerdem bietet dieser AP zwei parallel nutzbare Funkmodule für den 5-GHz- und 2,4-GHz-Frequenzbereich, die 802.11a/n/ac Wave 2, 802.11b/g/n, vier getrennten Datenströme und Geschwindigkeiten von bis zu 1,7 Gbit/s und 800 Mbit/s unterstützen. Eine drittes MIMO Dualband-Funkmodul für die gezielte WIPS- und Funkoptimierung (bei aktivierter Wi-Fi Cloud) sorgt dafür, dass Leistung nicht auf Kosten der Sicherheit geht. Ideal für Messen, Vortragssäle, Besprechungsräume und Einkaufszentren.

Sämtliche APs von WatchGuard bieten marktweit die beste Kombination aus Sicherheit, Leistung und Handhabbarkeit. Anwender können nur gewinnen: Sobald das Management über die WatchGuard Wi-Fi Cloud erfolgt, bieten die APs nicht nur schnellen, zuverlässigen WLAN-Zugang, sondern auch eine umfassende Sicherheit. Darüber hinaus ergeben sich ganz neue Möglichkeiten für den Dialog mit Gästen sowie zahlreiche Analysemöglichkeiten.

F15: Wenn sich APs von WatchGuard im selben Netzwerk befinden wie eine WatchGuard Firebox-/UTM-Appliance, kommen dann die UTM-Sicherheitsdienste wie Gateway AntiVirus und APT Blocker von der Firewall?
A: Ja. Wenn sie über die Wi-Fi Cloud verwaltet werden, unterstützen die APs zwar die grundlegende Content-Filterung, aber die Firebox stellt die UTM-Sicherheitsfunktionen wie Gateway AntiVirus, Intrusion Prevention und APT Blocker für den Schutz vor Zero-Day-Schadsoftware bereit.

F16: Können vorhandene APs für die Verwaltung in der Cloud aufgerüstet werden?
A: Nur die neuesten Access-Point-Modelle (AP120, AP125, AP320, AP322, AP325 und AP420) können von der Verwaltung über den GWC der Firebox auf Wi-Fi Cloud-Verwaltung umgestellt werden. Für AP100, AP102, AP200 und AP300 bieten wir als Anreiz für das Upgrade Trade-Up-SKUs mit Sonderrabatten an.

F17: Sind die APs von WatchGuard kompatibel mit der XTM-Serie?
A: Ja. Im Basic Wi-Fi Management Mode können die APs über Firebox-Appliances mit der aktuellen Firmwareversion verwaltet werden.

F18: Ist es möglich, mehrere Clients im selben Wi-Fi Cloud-Portal zu verwalten?
A: Ja. Dank der hierarchischen Baumstruktur der Wi-Fi Cloud können Managed Service Provider Kunden problemlos Ordner zuweisen und für jeden Kunden Konfigurationen, Berichte, WIPS-Sicherheit und Analysen verwalten.

F19: Bietet WatchGuard seinen Vertriebspartnern Unterstützung bei der WLAN-Ausleuchtung?

A: WatchGuardONE-Vertriebspartner haben Anspruch auf unseren Wi-Fi Design Support. Unsere Experten unterstützen Sie im Vorfeld mit Simulationen von Gebäudeplänen, aus denen die Anzahl empfohlener APs und Installationsorte hervorgeht. Der Zugang zum Wi-Fi Deployment Support erfolgt über das Partner-Portal. Melden Sie sich bei diesem Portal an, und gehen Sie zu watchguard.com/sellingsecurewifi.

F20: Steht die WIPS-Funktion nur in der Wi-Fi Cloud zur Verfügung?

A: Ja, ein Wi-Fi Cloud-Abonnement mit einer Total Wi-Fi- oder Secure Wi-Fi-Lizenz ist Voraussetzung für den Zugang zu WIPS-Funktionen.

F21: Was geschieht, wenn die Wi-Fi Cloud-Lizenz ausläuft?

A: Der AP funktioniert weiterhin mit der letzten bekannten Konfiguration. Allerdings wird er weder in der Wi-Fi Cloud angezeigt noch stehen die von diesem AP generierten Analysen in Berichten zur Verfügung.

F22: Wird es Firmware-Updates für die Nutzung der AP-Modelle AP100/AP102/AP200/AP300 in der neuen Wi-Fi Cloud geben?

A: Nein. Kunden, die zur neuen Wi-Fi Cloud aufrüsten möchten und derzeit AP100-, AP102-, AP200- oder AP300-Access-Points nutzen, bieten wir als Anreiz für das Upgrade Trade-Up-SKUs mit Sonderrabatten an.

F23: Wenn WIPS einen anderen AP sperrt, ist dann aus den Protokollen des gesperrten AP ersichtlich, warum er blockiert wurde?

A: Selbstverständlich. Die Ereignisprotokollierung in der Wi-Fi Cloud liefert eine genaue Übersicht über derartige Ereignisse – und verbindet sie sogar grafisch in einer virtuellen Kette – sodass Administratoren den zugrunde liegenden Verlauf einfach nachvollziehen können.

F24: Kann ein AP von WatchGuard in einer Umgebung mit Fremdherstellern als Sensor eingesetzt werden, ohne dass dies zu Konfigurationsproblemen führt?

A: Ja. Die Access Points AP125, AP320, AP322, AP325 und AP420 können in WLAN-Umgebungen mit Drittanbietern eingebunden werden und aussagekräftige Berichte über WLAN-Sicherheitsereignisse, Analysen und Compliance liefern – was sie zu hervorragenden Vertriebswerkzeugen macht.

F25: Wo kann ich mich darüber informieren, wie ich die Wi-Fi Cloud am besten positioniere und verkaufe?

A: Sehen Sie sich die On-Demand-Schulung zur Wi-Fi Cloud im Learning Center des Partner-Portals an.

F26: Was ist bei dem Design eines WLAN-Netzes zu beachten, wenn eine Mischung von dedizierten Access Points und dedizierten WIPS-Sensoren geplant ist?

A: Jeder cloudfähige AP kann in einem gemischten Modus als Access Point und WIPS-Sensor arbeiten. Die WLAN-seitigen WIPS-Funktionen sind in diesem gemischten Modus allerdings deaktiviert. Als Best Practice zur Gewährleistung der Sicherheit empfehlen wir einen dedizierten WIPS-Sensor für jeweils vier dezidierte APs.

F27: Können zusätzliche APs als Mesh Extender für einen primären Access Point fungieren?

A: Ja, man spricht von „Meshing", wenn ein „Root"-Access-Point mit einem Ethernet verbunden ist und „Leaf"-Access-Points nur drahtlos mit diesem Root-AP verbunden sind. Verfügbar für spezielle AP-Modelle.

F28: Wie werden cloudfähige APs von WatchGuard mit konkurrierenden APs von Drittanbietern implementiert?

A: Die WIPS-Technologie von WatchGuard ist einzigartig, und die APs von WatchGuard können als dedizierte WIPS-Sensoren parallel zu APs von Drittanbietern implementiert werden, um in einer WLAN-Umgebung WIPS-Sicherheitsfunktionen bereitzustellen. Der AP420 verfügt über ein drittes Funkmodul für gezielte WIPS- und Frequenzoptimierung.

F29: Bisher musste ich eine Liste benachbarter Geräte erstellen und diese JEDEM WIDS-/WIPS-System zuweisen. Wie kann ich automatisch feststellen, ob es sich um einen Rogue-AP bzw. -Client handelt?

A: WatchGuard verwendet ein patentiertes Verfahren für die Klassifizierung von APs und Clients, das ohne eine manuell erstellte Liste auskommt. Stattdessen sendet jeder WatchGuard-AP – wenn er über die Wi-Fi Cloud verwaltet wird – Marker Packets an den Ethernet-Port und wartet darauf, dass ein beliebiger AP bzw. Client diese Pakete zurücküberträgt, wobei durch Fingerprinting von jedem Gerät auf diesem Weg ein „Fingerabdruck" genommen wird. Der gleiche Vorgang wird funkseitig ausgeführt. WatchGuard-APs versenden Market Packets, und mithilfe von Fingerprinting wird ermittelt, welches Gerät diese Pakete berechtigter- oder unberechtigterweise erhalten hat. Die Geräte werden automatisch als Rogue-, externe, autorisierte oder Gast-Clients klassifiziert.

F30: Wie sollten die Vorteile der erweiterten WLAN-Funktionen, die im Manage-Modul der Wi-Fi Cloud verfügbar sind, positioniert werden?

A:

Name	Beschreibung	Vorteil(e)
Intelligentes Client-Load Balancing	Diese Funktion sorgt für die effiziente Verwaltung und Verteilung der Clients auf die APs innerhalb eines Frequenzbands.	Finden Clients in der Nachbarschaft mehr als einen AP mit einer guten Signalstärke, stellen unter Umständen mehrere Clients eine Verbindung zu demselben AP her, sodass Leistungsprobleme und eine Beeinträchtigung des WLAN die Folge sind.
Verbessertes Fast Roaming	Clients können von einem AP zu einem anderen wechseln, was in WLAN-Umgebungen ein nahtloses Hand-off ermöglicht.	Ist die 802.1x Enterprise-Authentifizierung aktiviert und Fast Roaming eingeschaltet, verkürzt sich dank einer Liste benachbarter 802.1 1k-Standards und der 802.11v BSS-Transition die Zeit, die Clients für das nahtlose Roaming zwischen APs benötigen.
Abwicklung des Multicast-Verkehrs	Diese Funktion ermöglicht eine erhebliche Bandbreiteneinsparung, wenn zur Optimierung des Netzwerkverkehrs Multicast-Daten in Unicast-Daten umgewandelt werden.	Der Multicast-Verkehr wird nun in Unicast umgewandelt, wenn IGMP-Snooping für ein SSID-Profil aktiviert ist. Dabei werden zur Optimierung des Multicast-Verkehrs Multicast-MAC-Adressen des Netzwerk-Layers 2 in zugehörige Unicast-MAC-Adressen umgewandelt.
Integration mit Google for Education	Diese einzigartige Integration optimiert die Kontrolle, Bedienbarkeit und Benutzerfreundlichkeit in Schulbezirken.	Dank der Integration mit Google for Education können Administratoren gezielt steuern, wer sich in das Netzwerk einer Schule einklinkt, und damit den Netzwerkzugriff für Schüler und Lehrkräfte in der gesamten Schule optimal absichern.
Rollenprofile	Durch Zuweisung bestimmter Attribute wie Firewall-Regeln, VLAN-Richtlinien und weiterer Optionen kann jede Rolle genauer definiert werden.	Außerdem besteht nun die Möglichkeit, den WLAN-Zugriff basierend auf der Rolle einzuschränken bzw. zu steuern, die Clients oder Benutzer zugewiesen ist, welche eine Verbindung zum selben WLAN-Netz herstellen. Anhand einer vordefinierten Richtlinie für Benutzerrollen können Benutzern bestimmte Rollen zugewiesen werden.
Client-bezogene Anwendungstransparenz	Ermöglicht die Visualisierung der Anwendungen, die im WLAN-Netz im Einsatz sind.	Unsere Manage-Anwendung überwacht und erstattet über mehr als 1.300 Anwendungen auf Netzwerk-Layer 2 und höher Bericht. Administratoren können den Netzwerkverkehr visualisieren und haben für Analysen und Berichterstattung auf Anwendungsebene Einblick in die Nutzung von Anwendungen und die Bandbreitenbelegung von Netzwerkressourcen. Anhand von Berichten können Abweichungen überwacht und Fair-Use-Richtlinien durchgesetzt werden, um Netzwerküberlastungen durch hohen Datenverkehr auf der Anwendungsebene möglichst zu vermeiden.
Application Firewall	Anwendungsbezogene Sperrung oder Freigabe des Datenverkehrs	Application Firewall und Application Visibility ermöglichen das anwendungsbezogene Sperren bzw. die Freigabe des Datenverkehrs. Zusätzlich zur Sperrung und Freigabe kann das DSCP-Byte (Diffserver Codepoint) im IP-Header markiert werden.

F31: Wie funktioniert das dritte Funkmodul des Access Point AP420?

A: Der Access Point AP420 verfügt über ein drittes 2x2 MIMO Dualband-Funkmodul für gezielte WIPS- und Frequenzoptimierung, wenn es über die Wi-Fi Cloud gemanagt wird. Mit dieser Funktion können Unternehmen viel Geld sparen – sie müssen nicht in zusätzliche APs investieren, die ausschließlich für das WIPS-Scannen genutzt werden. Das im AP420 integrierte, zusätzliche Funkmodul ist nicht auf den WLAN-Zugang beschränkt, sondern sorgt gezielt für zusätzliche Sicherheit.

F32: WatchGuard bietet nun drei Wave 2-AP-Modelle. Wie unterscheiden sich diese?

	AP125	AP325	AP420
Empfohlene Anwendungsfälle	Niedrige Dichte	Mittlere Dichte	Hohe Dichte
Funkmodule und Streams	2x2:2 MU-MIMO Wave 2	2x2:2 MU-MIMO Wave 2	4x4:4 MU-MIMO Wave 2 Drittes WIPS-Funksystem
Bereitstellung	Innenbereich	Innenbereich	Innenbereich
Anzahl Antennen	4 intern	6 intern	10 intern
Maximale TX-Leistung	20 dBm	20 dBm	27 dBm
Maximale Datenrate (5/2,4 GHz)	867 Mbit/s/300 Mbit/s	867 Mbit/s/300 Mbit/s	1,7 Gbit/s/800 Gbit/s
Ports	2 ports GbE	2 ports GbE	2 ports GbE
Power over Ethernet (PoE)	802.3af (PoE)	802.3at (PoE+)	802.3at (PoE+)

F33: Wie unterscheidet sich Wave 1-Technologie von Wave 2?

Angesichts des heute so beliebten Streamens von Videos, Musik, Fotos und Spielen sind die aktuellen digitalen Inhalte umfangreicher und besser denn je.

Immer mehr Menschen sind gleichzeitig mit mehreren Geräten wie Smartphones, Tablets und Laptops online. Wen wundert es da, dass WLAN-Netze häufig überlastet sind und mit den Anforderungen nicht Schritt halten können? Mit der Einführung des 802.11ac Wave 2-Standards kommt das WLAN jetzt auf Touren und kann auch die Anforderungen durchsatzstarker Umgebungen mit hoher Gerätedichte wie ausgelastete Besprechungsräume, Schulen und Messen erfüllen. Wave 2 bietet ultraschnelle Geschwindigkeiten, eine noch bessere Abdeckung und die höchste Client-Dichte. Die fünf wichtigsten Verbesserungen der Wave 2-Technologie:

1. Gleichzeitige Unterstützung einer größeren Anzahl verbundener Geräte dank MU-MIMO-Funktionalität. Client-Geräte können schneller auf das Netzwerk zugreifen und es wieder verlassen, sodass sich die Qualität der Benutzererfahrung für alle verbessert.

2. Die höhere Leistung vereinfacht das Aufrufen und Übertragen großer Dateien wie beispielsweise Videos und die Unterstützung latenzempfindlicher Anwendungen wie VoIP.

3. Eine größere Bandbreite durch zusätzliche Kanäle im 5-GHz-Frequenzband, damit eine größeren Anzahl von Clients bedient werden kann.

4. Weiträumigere Abdeckung, wenn 4x4 Access Points in denselben Abständen platziert werden wie 2x2 oder 3x3 Wave 1-Access-Points.

5. Schnelleres und zuverlässigeres WLAN, das dreimal so schnell ist wie seine Vorgänger. Aber nur weil Wave 2 als neueste und leistungsstärkste Technologie gilt, heißt das noch lange nicht, dass es auch die richtige Technologie für Ihr Unternehmen ist. Überlegen Sie, was für Sie, Ihre Mitarbeiter, Verkäufer und Kunden wichtig ist. Wählen Sie dann eine Lösung aus, die die Produktivität Ihres Unternehmen steigert und Ihnen zu Einsparungen verhilft.