Drei wichtige Gründe zum Trade-up von Wi-Fi Access Points!

Die durchschnittliche Lebensdauer eines Wi-Fi Access Points beträgt fünf bis acht Jahre. Bei WatchGuard empfehlen wir, Audits für Kundenumgebungen durchzuführen, um gegebenenfalls Hardware alle drei bis fünf Jahre hinzuzufügen oder zu ersetzen, um den selbst den ausgeklügeltsten WLAN-Bedrohungen der heutigen Zeit die Stirn bieten zu können. Nachfolgend finden Sie die Informationen, die Sie mit Ihren Kunden teilen sollten, bevor Sie zulassen, dass Kunden die Möglichkeit für ein Trade-up auslassen:

GRUND 1: Leistung

Ein Upgrade von WLAN-Access Points liefert die Leistung, die ein wachsendes Unternehmen braucht.

Die neuste Hardware für Wi-Fi 6 Access Points bietet Folgendes:

- Wi-Fi 6-Technologie für den Kampf gegen Netzwerküberlastungen mit einer besseren Leistung in Bereichen mit hohem Datenverkehr
- Verbesserte Sicherheit mit WPA3-Verschlüsselung
- Schnellere Durchsatzgeschwindigkeiten mit einer höheren maximalen Datenübertragungsrate für Wi-Fi 6 (bis zu 2402/574 Mbit/s*) im Vergleich zu Wi-Fi 5 (bis zu 867/300 Mbit/s)
- Erweiterter Bereich für WLAN-Anwendungen im 2,4- und 5 Ghz-Bereich mit mehreren verfügbaren Kanälen
- Der Wi-Fi 6-Standard, einschließlich OFDMA-Funktechnik für Uplinks und Downlinks, verbessert die WLAN-Netzwerkleistung durch gleichzeitige Übertragungen zwischen mehreren Clients, die mit dem Access Point verbunden sind. Mit der Wi-Fi 5-Technologie konnten Kanäle Verbindungen nur zu einem einzelnen Client herstellen. OFDMA ist eine der wichtigsten Wi-Fi 6-Technologien und bietet zahlreiche Netzwerkvorteile, wie höheren Datendurchsatz, niedrigere Latenz, IoT-Optimierung und effizienteren Stromverbrauch.
- Die Target Wake Time (TWT), eine von Wi-Fi 6 unterstützte Funktion, gibt an, wie oft ein Access Point mit der OFDMA-Funktechnik kommuniziert, um Akku zu sparen und Datenstau zu vermeiden. Dies bietet eine riesige Chance für die Einführung von IoT-Geräten (IoT, Internet of Things).

**Diese max. Datenübertragungsrate bezieht sich auf den AP430CR. Die maximale Datenübertragungsrate variiert je nach Access Point-Modell.*

GRUND 2: Einfaches Management

WatchGuards Unified Security Platform™ liefert eine neue Vision von Managed Security, die unseren MSPs ermöglicht, erweiterte, anwenderzentrierte Sicherheitsmodelle schnell und einfach umzusetzen. Grundlage hierbei ist die WatchGuard Cloud-Plattform, mit der MSPs über eine zentrale Oberfläche alle Aspekte der Verwaltung, Automatisierung von Betriebsabläufen, Transparenz und des erweiterten Reportings übersichtlich im Blick und unter Kontrolle haben.

Genießen Sie eine einfache Bereitstellung, Verwaltung und problemloses Reporting auf Wi-Fi 6 Access Points in WatchGuard Cloud, einem intelligenten und zentralen Verwaltungsbereich.

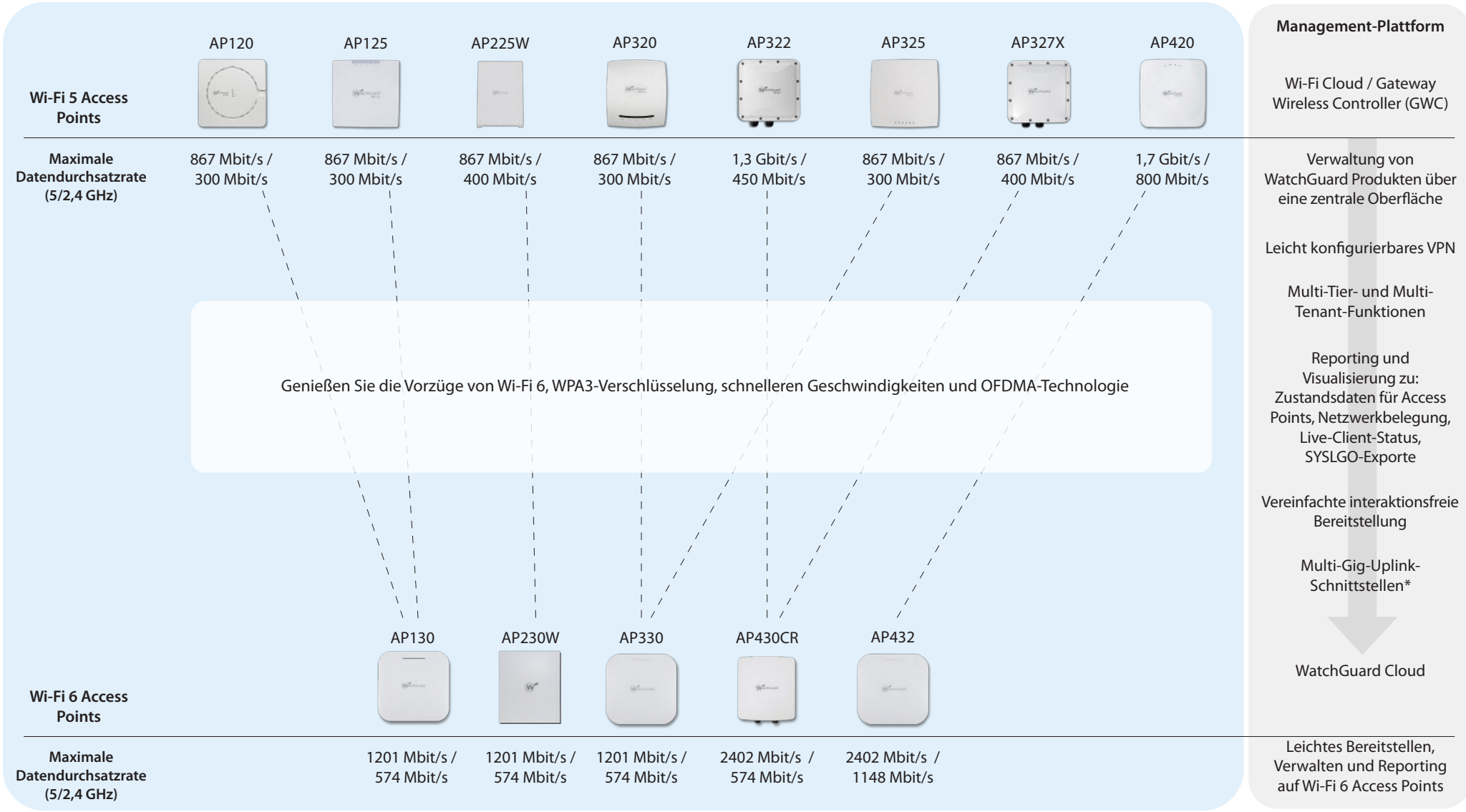
- Die WatchGuard Cloud-Plattform ist eine zentrale Oberfläche für alle Aspekte der Verwaltung, Automatisierung von Betriebsabläufen, Transparenz und des erweiterten Reportings.
- Nutzen Sie mehr als 100 Dashboards und Berichte aus der Cloud, mit denen schnell allgemeine Trends und Anomalien erkannt und zugehörige detaillierte Informationen angezeigt werden können.
- Erstellen Sie ein sicheres VPN zwischen einer WatchGuard Firebox und einem Wi-Fi 6 Access Point mit der Remote Access Point-Lösung (RAP), mit der Unternehmen Unternehmens-SSIDs flexibel auf einen Remote-Arbeitsplatz (wie das Home Office eines Remote-Mitarbeiters oder ein kleines Büro) ausweiten können.
- Die interaktionsfreie Bereitstellung ist vollständig in WatchGuard Cloud integriert; daher können Sie Ihre Fireboxes und Access Points in Minutenschnelle in Betrieb nehmen und verlieren keine wertvolle Zeit. Sie können sogar die neuesten Firmware-Updates außerhalb der normalen Geschäftszeiten planen und so mögliche Unterbrechungen für Ihre Kunden auf ein Minimum beschränken.

GRUND 3: Schwachstellen

Stellen Sie mit den Sicherheitsdiensten von WatchGuard sicher, dass Kunden Zugang zu den neuesten Sicherheitsentwicklungen zum Schutz vor den versteckten Bedrohungen unserer heutigen Zeit haben.

- Nutzen Sie plattformübergreifende Funktionen wie die Remote Access Point-Lösung, mit der Sie einen IPSec-VPN-Tunnel zwischen der Firebox und Access Points erstellen können, die im Home Office eines Remote-Mitarbeiters oder in einem kleinen Büro bereitgestellt werden.
- Wi-Fi 6 Access Points können die WPA3-Verschlüsselung nutzen, ein Sicherheitsprotokoll, das das Hacken von Passwörtern erschwert und so Daten schützt.
- Die OFDMA-Technologie in Kombination mit der WPA3-Verschlüsselung stellt sicher, dass IoT-Geräte sicher sind und die geeigneten Netzwerkressourcen genutzt werden, ohne dass sich dies auf die Leistung anderer WLAN-Geräte auswirkt, die mit demselben Access Point verbunden sind.
- Nutzen Sie Access Points mit dedizierten Funksystemen für Sicherheitsteams zur Überwachung der WLAN-Umgebung – mit Scans auf bösartige APs im selben Netzwerk.

UPGRADE-PFAD



** Dieser Funktionsumfang gilt nicht für AP130*