KURZBESCHREIBUNG DER LÖSUNG

Trusted Wireless Environment

Werden Sie aktiv, damit Ihr WLAN nicht zu Ihrem größten Sicherheitsrisiko wird. Hacker suchen sich bevorzugt das schwächste Glied der Sicherheitskette aus und können sich mithilfe leicht zugänglicher Werkzeuge und unzähliger Online-Anleitungsvideos ohne großen Aufwand in das WLAN einhacken. Schlimmer noch: Beim Eindringen in Ihr WLAN werden Ihre Unternehmensnetzwerke durch eingeschleuste Malware beschädigt und Anmeldedaten gestohlen. Dabei kann eine Summe von mehreren Millionen für Geldbußen und die Beseitigung von Schäden zusammenkommen.

Sie benötigen ein **Trusted Wireless Environment** – ein Konzept für den Aufbau eines WLAN, das schnell, leicht zu verwalten und vor allem sicher ist. Ihre Mitarbeiter, Lieferanten und Gäste verlassen sich darauf, dass Sie für ihre Sicherheit sorgen. Und Sie sind dafür verantwortlich, dass Sie die WLAN-spezifischen Sicherheitsrisiken und deren Auswirkungen auf Ihr Unternehmen kennen. Sie benötigen eine Lösung, die sich durch drei wesentliche Eigenschaften auszeichnet:

1 MARKTFÜHRENDE PERFORMANCE

Damit Ihre Umgebung mit der erforderlichen Geschwindigkeit, Vernetzung und Gerätedichte unterstützt werden kann, sind Sie auf eine den Anforderungen entsprechende Leistung angewiesen. Dabei sollten Sie jedoch in keinem Fall Einbußen bei der Sicherheit hinnehmen.

2 SKALIERBARES MANAGEMENT

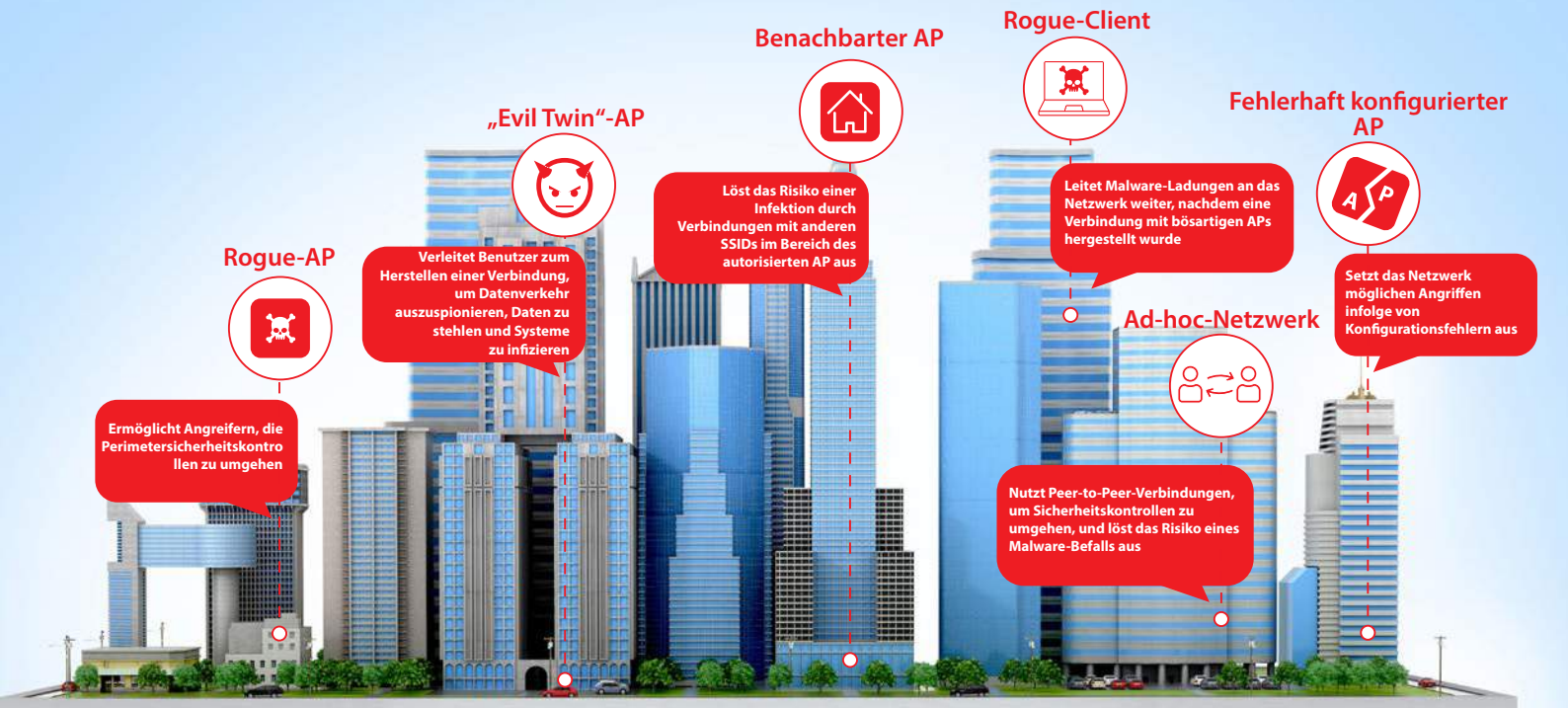
Aufgrund der einfachen Einrichtung und Verwaltung sollten Sie in der Lage sein, Ihr gesamtes WLAN über eine einzige Schnittstelle zu steuern und wichtige Prozesse zum Schutz Ihrer Umgebung und Ihrer Benutzer auszuführen.

3 VERIFIZIERTE UMFASSENDE SICHERHEIT

Sie müssen die Gewissheit haben, dass Ihre Sicherheitslösung Ihr Unternehmen vor Angriffen auf das WLAN schützt und die folgenden Vorteile bietet:

- Automatischer Schutz vor den sechs bekannten Kategorien von WLAN-Bedrohungen
- Möglichkeit, dass legitime externe Access Points in derselben Umgebung betrieben werden können
- Beschränkung der Möglichkeit, dass Benutzer eine Verbindung zu nicht zugelassenen WLAN Access Points herstellen können

Die sechs bekannten Kategorien von WLAN-Bedrohungen



Miercom-Bericht zur WLAN-Sicherheit

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	Erkennung	Prävention	Erkennung	Prävention	Erkennung	Prävention	Erkennung	Prävention
Rogue-AP	P	P	F	–	F	MP	F	–
Rogue-Client	P	P	F	–	F	MP	–	MP
Benachbarter AP	P	P	P	P	F	–	F	–
Ad-hoc-Netzwerk	P	P	F	–	F	–	P	–
„Evil Twin“ AP	P	P	P	F	P	MP	P	F
Fehlerhaft konfigurierter AP	P	P	P	–	–	–	–	–
Gleichzeitige Bedrohungen	P	P	F	F	F	F	F	F

- P = Pass (Bestanden)
- F = Fail (Nicht bestanden)
- MP = Marginal Pass (Knapp bestanden)
- N/A = Funktion nicht unterstützt

Den vollständigen Miercom-Bericht finden Sie hier:
www.watchguard.com/wifi-security-report

Sicheres, in der Cloud verwaltetes WLAN

Wir nutzen das WatchGuard-WLAN in unseren Lösungen, da es patentierte **Sicherheit**, gesteigerte **Produktivität** und höhere **Kundenzufriedenheit** ermöglicht. Wenn Sie unseren Access Point mit WatchGuard Wi-Fi Cloud bereitstellen, haben Sie Zugriff auf wertvolle Tools, mit denen Sie Ihr Unternehmen auf die nächste Stufe heben – durch branchenführende WLAN-Sicherheit, spezielle Zugangsportalseiten, standortbasierte Analysemodule und zentrale Verwaltung.

Miercom bestätigt, dass WatchGuard als einziges Unternehmen die sechs bekannten Kategorien von WLAN-Bedrohungen **automatisch erkennt und bekämpft**.

BOC IT-Security GmbH

+49 661 9440440

https://www.boc.de

Unsere Produkte nutzen WatchGuard-Technologie

WatchGuard® gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Es bietet die zentralen Technologien, um sich gegen die heutigen aggressiven Bedrohungen zu wehren.

®2019 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. Teilenr. WGPP67128_042219