













## COMPETITIVE LANDSCAPE

# ZERO-TRUST SECURITY FOR TODAY'S MIDSIZED BUSINESSES

## Industry-Leading Network Security

The Aruba Edge Services Platform (Aruba ESP) with Zero Trust Security natively applies a more rigorous set of security best practices and controls to network resources than any other cloud-networking solution on the market.

Feature	Aruba	Competitive Differentiator	Other Vendors	Their Weakness
Full-Time Security Monitoring	Yes 	With dedicated dual-radio access points as sensors, Aruba supports full time security scanning on both bands, providing effective detection and mitigation against network attacks.	Limited 	Other leading cloud vendors use a dedicated third radio, which by design only scans each band 50% of time. Third radios are typically 1x1 MIMO, and only see a portion of the threat landscape and take longer to identify attacks (if at all).
Embedded Policy Enforcement Firewall (PEF)	Yes 	Aruba's <b>Cyber Catalyst™</b> designated-multi-tiered <b>policy enforcement</b> firewall applies security, traffic forwarding, and network performance policies to wireless clients and applications for secure high-quality communications.	No 	Others lack a built-in policy enforcement firewall. They require dedicated hardware, licensing and support.
Built-in Web Content Filtering	Yes 	Aruba Central, our cloud-native network management platform, includes web content filtering without requiring additional hardware or licensing.	No 	Web content filtering solutions reside on a hardware appliance, which is offered at an additional cost and requires additional licensing.
On-board Wireless Intrusion and Rogue Mitigation	Yes 	Aruba's built-in wireless intrusion protection is tested to perform at scale, consistently identifying rogue devices quickly and mitigating threats.	Limited 	Standard wireless intrusion offerings are slow to identify rogue devices and fail at containing threats. Suitable wireless intrusion protection requires additional hardware and licensing.
WPA3 and Enhanced Open Support	Yes 	Aruba security experts were instrumental in developing the encryption protocols used in WPA3 and Enhanced Open and was the first vendor to incorporate the standard into shipping products.	Yes 	Though the standard was announced in October 2018, it took other leading networking vendors well over a year to support the new standard - demonstrating their lack of focus and commitment to the safety and security of their customer's networks.
User/Device visibility and policy enforcement	Yes 	Aruba's award-winning, Cyber Catalyst designated security suite, including <b>ClearPass Device Insight</b> and <b>ClearPass Policy Manager</b> , is the industry's best-in-class solution for device profiling and classification, automated, policy enforcement, and vulnerability response.	Limited 	While there are other advanced security platforms out there, they are complex to deploy, require additional licensing and/or subscriptions for basic services, and have limited multi-vendor support.

Want to learn more about Aruba's Midsized Business Solutions? [Click here.](#)

1