FORTINET VS. CISCO

TOP FIVE CISCO BEATERS

1. EXPENSIVE SOLUTION

Cisco products require a lot of operational overhead and numerous licenses. Cisco requires licenses to manage their AP with any of their controllers and even licenses individual features in some cases. Therefore, ASPs of wireless solutions have been about 20-30% higher than a competitive Fortinet bid. This can lead to sticker shock for customers who only compare prices at the hardware level.

2. BOLT-ON SECURITY

Cisco is not a security company and most of their security solutions come via acquisition and are "bolted on" to their core networking offering. This leads to less integration and protection than the Fortinet solution.

3. INCREASED MANAGEMENT OVERHEAD

Cisco does not offer an easy way to manage all the pieces of their solution. While they have introduced Digital Network Architecture (DNA) to try and address this, it comes with additional costs and (at least today) limited support for the full portfolio. Fortinet's FortiGate UI handles all the access layer plus security in a single interface for quicker ramp time and lower TCO.

4. LIMITED DEPLOYMENT FLEXIBILITY

While Cisco does offer a cloud controller via Meraki and standalone management, customers need to choose up front which is right for them and then are solidly locked into that choice. Moving to or from their cloud architecture down the line is costly, requiring all new AP SKUs. Fortinet offers a universal line of APs that can be used with any of our management options. With no license cost or reconfiguration necessary, a customer who decides to switch management options has no additional cost or hassle.

5. NO FREE LOCATION ANALYTICS

Cisco has their own location analytics platform, but they do not offer a free tier to customers. This prevents most customers from getting a chance to see what value location analytics can offer them.

WHY FORTINET?

1. FORTINET SECURE UNIFIED ACCESS

Fortinet invented the Secure Unified Access Solution to deal with security protection against data breaches and cybersecurity threats, specifically at the access layer.

2. FORTINET SECURITY FABRIC

Fortinet's Security Fabric provides a complete solution that delivers:

- **Broad visibility and protection across the digital attack surface.** Siloed apps in multi-cloud environments make it even harder to respond to threats. The Security Fabric delivers real-time visibility across all devices and applications.
- **Integrated detection and response to advanced threats.** The Security Fabric streamlines communications among all the organization's different security solutions, shrinking detection and remediation windows.
- **Automated operations and analytics via a single console.** With today's sophisticated threats, firms need to detect attacks faster. With the Security Fabric, you can coordinate automated responses and remediation to threats detected anywhere across your extended network.

CISCO BACKGROUND

- Cisco Systems was founded in 1984 and went public in 1990.
- Cisco reported Q3 2018 Revenue of $15.5 billion.
- Cisco has a multitude of product lines across the networking space, many from a variety of acquisitions over the years.
- Cisco's security features include Identity Services Engine (ISE), their various firewall offerings, wireless intrusion prevention (WIPS), and VPN solution.
- The Cisco APs can either be configured for standalone deployment or for use with a controller. Cloud is offered via the Meraki product line.

CISCO TARGET ACCOUNT PRIORITIES (WHO THEY TARGET)

- Cisco horizontally targets both large enterprises and small businesses, along with service providers, for wireless LAN.
- They are able to sell most successfully into accounts that are not price-sensitive and who are receptive to Cisco's one-stop-shop message.
- Beware that you may not be facing just one Cisco, but multiple parallel product portfolios. Meraki, SMB products, Mobility Express with embedded controller functions, or the enterprise solution with a separate physical or virtual WLC. All have very different features and price points.

3. WIDE RANGE OF SECURE SOLUTIONS:

Universal APs: This range of access points works with any management architecture.

- FortiGate Integrated Wireless: consolidated solution with security and wireless LAN management integrated with FortiGate
- Cloud Managed: wireless management from anywhere using the Fortinet cloud
- Dedicated Controller Wireless: wireless network solution using dedicated WLAN controller with flexible deployment options and unique RF capabilities.

TAKING THE OFFENSIVE AGAINST CISCO WEAKNESSES

To cope with higher bandwidth and features, Cisco had to throw away IOS® code of the access points, resulting in tremendous efforts to rewrite from scratch and stabilize the new code. It still has a huge number of unfixed bugs and lacks feature parity in all modes including FlexConnect and Mobility Express. The next phase of controllers is also based on totally new code (APIC-EM and elastic controllers) that will take years to get stable. Customers know and fear this.

Cisco Weakness	How to Attack It
Cisco security for access includes various other products or solutions, such as Stealthwatch, TrustSec, ISE, and Talos for protection against emerging threats.	Position Fortinet Secure WLAN as a premier wireless solution integrated into an industry-leading security fabric.
Cisco Aironet does not extend to branch. They position Meraki solution for small medium branch locations. Meraki cloud solution is a subscription model, where your devices will not work if not renewed.	State the obvious to the customers that Cisco and Meraki offer two different product sets with non-unified management.
Cisco architecture limits flexibility by requiring customers to pick a management topology up front. Obtaining a full feature set for guest management requires Cisco infrastructure, including large CAPEX investments or expensive upgrades.	Emphasize the flexibility of Fortinet's portfolio in the access, control, policy, and application layers.

DEFENDING AGAINST CISCO SALES TACTICS

What They Will Do	How to Respond
Claim that Fortinet's technology is proprietary technology that is costly to deploy and complex to manage.	All Fortinet infrastructure products are Wi-Fi Alliance certified and industry standard. All standard enterprise configurations are available on Fortinet APs. Our Virtual Cell mechanism is an option (something that Cisco does not offer) which does not impact clients nor increase management complexity.
Position security as a key attribute and differentiator of Cisco's WLAN solution.	Only Fortinet has an established security pedigree and delivers enterprise-grade encryption and authentication, per-user and per-application security policies, VPN for remote offices, threat and rogue detection and mitigation, and wireless intrusion detection.
Push full-blown network access control with posture assessment, including the capability to deny access based on characteristics of the device.	NAC posture assessment is a heavier version of NAC that most customers will find hard to deploy, and adoption rates are low because it is labor-intensive and expensive with ISE. Cisco knows that most customers want simple guest access and BYOD on-boarding, which is exactly what FortiNAC offers with full third-party support, including Cisco.
State that they have the largest wireless portfolio on the market for any wireless use.	Fortinet's portfolio covers just as many use cases without the need to have separate SKUs for cloud vs. standalone management. In addition, FortiPresence is now providing many more features than CMX, and virtual wireless LAN controllers and cloud are a reality at Fortinet.

FEATURE COMPARISON CHART

Capability	Fortinet	Cisco
Provides Wi-Fi infrastructure for multivendor client environments.	Yes	Yes
BYOD security: market-proven, competitively priced, connectivity solution with no bloat-ware. E.g., NAC, MDM, endpoint policy enforcement, multiple subscription licenses.	FortiNAC	Cumbersome and expensive ISE
Wireless virtualization manages co-channel interference and also supports channel layering, providing higher client capacities.	Yes	No
Virtualized controller and management suite options (private cloud solutions).	Yes	Yes
Ultra-high density design with a 160 MHz channel everywhere.	Yes	Yes
RF management.	Yes (ARRP)	Yes (RRM)
Wireless service assurance for onsite and remote network health proactive visibility, analytics, and synthetic tests.	Yes FortiWLM	Future, cloud-based only
Enhanced location and analytics, integrating with social Wi-Fi.	Yes (FortiPresence)	Yes (CMX)
Spectrum intelligence with Wi-Fi and non-Wi-Fi interferers' visibility.	Yes	Yes