PARTNER SELL SHEET

Zero Trust Access (ZTA)

Market Opportunity

Organizations face an expanding attack surface with all the people and devices that connect to or exist on their network. With Internet-of-Things (IoT) trends, more and more devices are showing up on networks. The result is that network owners need help to regain control of their network. The first step of that process begins with knowing who and what is on your network. Businesses of all types and sizes are grappling with this issue and are looking for solutions that they can manage with their IT staff. The ZTA solution enables companies to know and control both who and what is on their network. Additionally, ZTA solutions can also provide control for managed devices (company laptops and managed mobile devices) when they are off the network.

The endpoint protection (EPP) market, including identity and access management and network access control, is estimated to be $17 billion in 2023.

Why Fortinet

Fortinet solutions offer the only integrated solution to support the ZTA solution. Unlike point solutions from multiple vendors, Fortinet offers all the elements to deploy the entire ZTA solution today. Fortinet has field-tested products that work together for a cohesive solution addressing several use cases, simplifying deployment, operation, and management. Use cases include: understanding and controlling *who* is on the network; knowing and controlling *what* is on the network; and protecting managed devices when they are off the network.

Addressing Business Challenges

Customer Challenge	How Fortinet Addresses Challenge
Easy integration into existing infrastructure	The Fortinet ZTA solution is flexible and can work with many other vendor products and even incorporate products from other vendors into the ZTA solution.

Target Companies and Personas

Organization Size

- Mid-market and larger organizations with a wallet spend of $249 million and above. ZTA requires some expertise to deploy, so the company must have an in-house security team.

Personas

- **Primary audience:** CISO
- **Technical buyers/influencers:** Security Architect, Network Engineer, VP of Networking
- **Business buyers/influencers:** CFO, Finance/Procurement

Key Differentiators

The ZTA concept has proven popular and many companies talk of the solution. However, only Fortinet provides all the elements of ZTA in shipping products. Furthermore, the Fortinet ZTA solution integrates into the Fortinet Security Fabric, providing visibility and control across the platform. This integration delivers broader coverage and simpler management across the entire solution.

Qualifying Questions

- Do you know everything connected to your network? At all times?
- Can you control where the devices that are on your network go? Even if they physically roam?
- Do you have a centralized authentication capability for your employees? That also includes SaaS applications?
- Are you enforcing a least privilege access policy for employees, contractors, and vendors?
- Are you controlling corporate-managed devices when they are off-network?

Overcoming Objections

We already have an authentication solution (Okta, Ping, Duo, etc.).

The Fortinet ZTA solution is flexible and can work alongside other products providing individual elements of the overall solution. Do you have complete visibility of all devices on your network? Perhaps you need to look at FortiNAC.

We already have a NAC solution (Cisco ISE, Forescout, Aruba ClearPass, etc.).

Is your current solution working well across both wired and wireless networks? Is your current solution providing both visibility and enforcement? If not, perhaps you should look at how the technology in FortiNAC has made it the fastest-growing NAC product on the market.

Competitive Landscape

Note: There are only two vendors that offer the complete elements of ZTA: Fortinet and Cisco. However, Fortinet's solution is an integrated, platform-focused solution while Cisco's is a collection of point products. Other vendors talk about ZTA but only offer elements of the solution, thereby requiring multiple management tools and manual information sharing.

	FORTINET	CISCO	aruba NETWORKS	FORESCOUT	okta	paloalto NETWORKS
User authentication	Yes	Yes	No	No	Yes	No
SAML support for SaaS	Yes	Yes	No	No	Yes	No
Multi-factor authentication	Yes	Yes	No	No	Yes	No
Device visibility	Yes	Yes	Yes	Yes	No	Yes
Device control	Yes	Yes	Yes	Yes	No	No
Off-network control	Yes	Yes	No	No	No	Yes
VPN agent	Yes	Yes	Yes	Yes	No	Yes