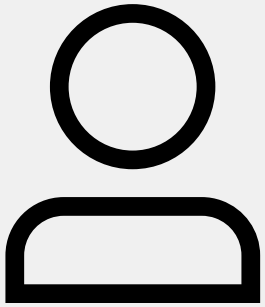
Why You Should Sell EndPoint Security?

ZTNA Business Drivers

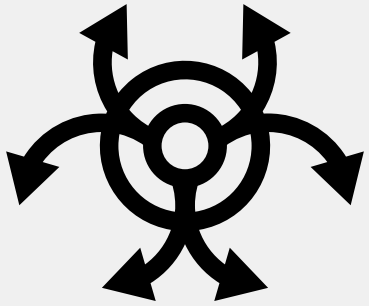
Work From Anywhere (WFA)



Users **Access** unaffected by Location

Improved User Experience

Malicious Attacks



Granular **Application** Access

Reduced Attack Surface

Cloud Journey

Applications unaffected by **Location**

Flexible Administration

© Fortinet Inc. All Rights Reserved.

Your ZTNA Opportunity

Market Forecast, Size and Growth, Trends

ZTNA OPPORTUNITY

BIG
market opportunity

85%

of enterprises
plan to adopt
by 2024

HIGH GROWTH
vendor

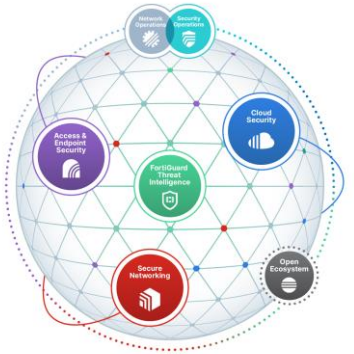
Fastest Growing
ZTNA Vendor

EASY
To deploy

Easy Transition from VPN

FortiClient

SECURITY FABRIC
integration



© Fortinet Inc. All Rights Reserved.

Want Help with ZTNA? Try Our Services

A variety of assistance options

FortiClient

Best Practice Service (BPS)

- Phone-based consultation
- Fortinet experts learn about the customers requirements and provide tailored recommendations
  - Sample code
  - Links to tools
  - Recommended technical documentation
  - Sample configurations
- Annual subscription (account-based)

Managed Services (MS)

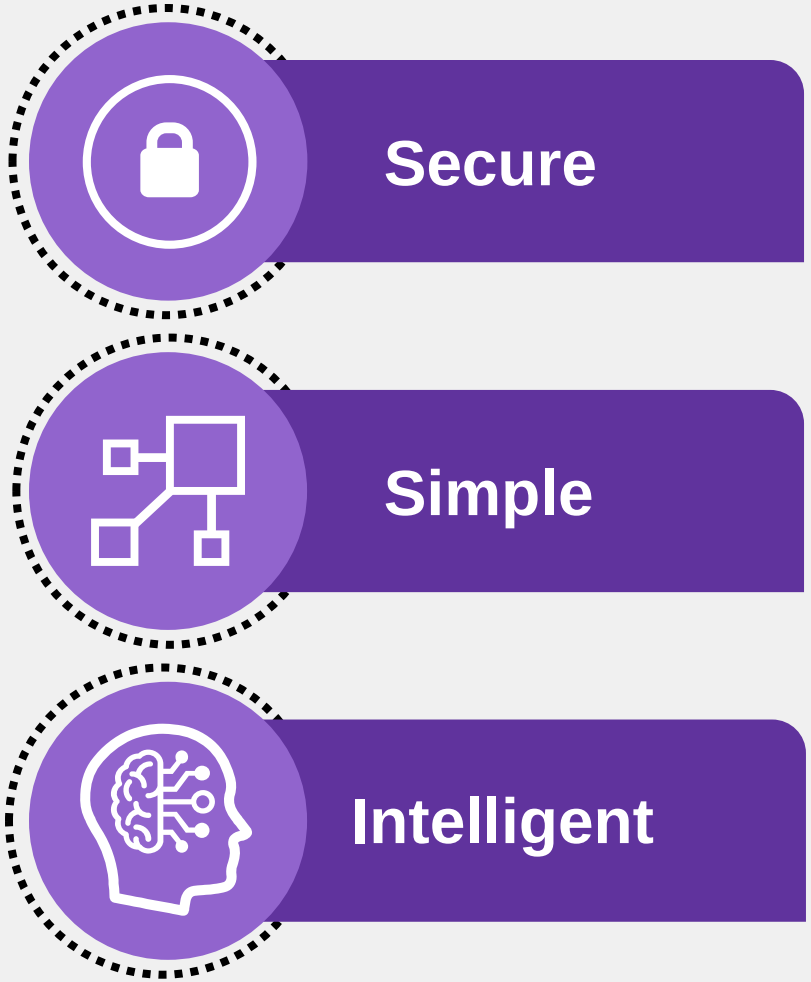
- Fortinet professionals actively assisting with:
  - Deployment
  - Configuration
  - Management
  - Analysis
- Vulnerability monitoring and reporting (with recommendations)
- Requires Cloud-based EMS
- Annual subscription (account-based)

Fortinet Professional Services

- Assistance across all products, including FortiGate NGFW
- Fortinet professionals actively assisting with:
  - Design
  - Deployment/Migration
  - Optimization
  - Management/Analysis
  - Evolve/Upgrade
- Flexible Engagements from 1 day to annual subscription

© Fortinet Inc. All Rights Reserved.

Delivering on Fortinet's Endpoint Security Vision



VPN included with an ability to upgrade and deploy a ZTNA framework

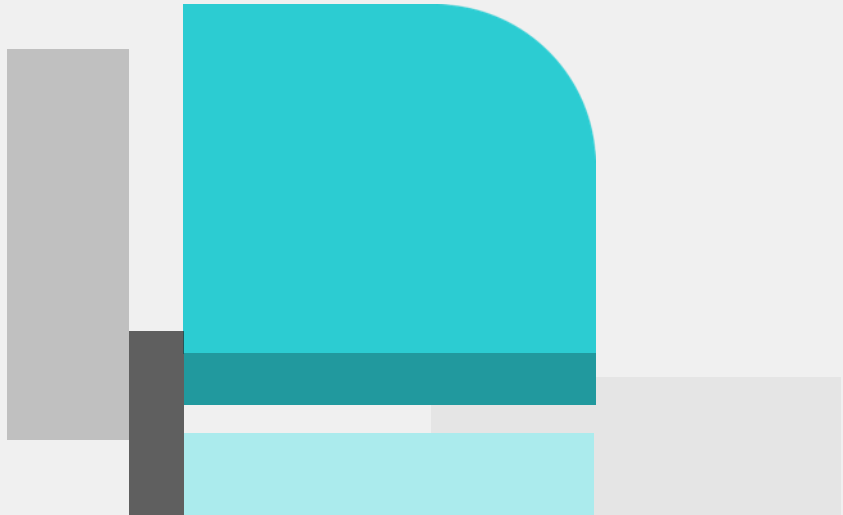
Endpoint and Network security policies managed from a single point

Automated endpoint patching and vulnerability scanning

© Fortinet Inc. All Rights Reserved.

Customer pitch

Endpoint Security



Endpoint Security – Challenges

Secure Remote Access

Simple VPN username & password simplify access to the network for hackers

Hight Total Cost of Ownership

Additional licenses for nonintegrated solutions

Lack of Visibility and Control

Unsanctioned apps installed on endpoints

Users ignoring critical system updates

© Fortinet Inc. All Rights Reserved.

Zero Trust Mindset

As defined by National Institute of Standards and Technology (NIST)

NIST

Zero trust is a **cybersecurity paradigm** focused on resource protection and the premise that trust is **never granted implicitly** but must be **continually evaluated**.

© Fortinet Inc. All Rights Reserved.

Supporting Work From Anywhere

- User-based Security
- Consistent Experience in all locations
- Automatic, Secure Tunnels
- Continuous verification with Single Sign-on (SSO) Support

Endpoint Security

Components:

FortiGate

NGFW

FortiClient EMS

ZTNA Agent

FortiToken

Multi-Factor Authentication

Powered by the same OS

Fortinet's Endpoint security solution offers:

Full protection

Always-on, auto-connect VPN and multi-factor authentication

Reduced costs

Free VPN with the purchase of endpoint protection

Visibility

Easy, cloud-based management solution, ensuring total visibility

© Fortinet Inc. All Rights Reserved.

Fortinet ZTNA

What's it made of? Existing Fortinet security fabric products that many customers already have

Core Elements

ZTNA Application Gateway

FortiOS

FortiOS performs access checks, maintains user group/application access table, proxies application (FOS 7.0+)

ZTNA Agent and Policy Orchestration

FortiClient/Central Management

FortiClient Central Management configures the ZTNA agent; FortiClient for ZTNA agent (FortiClient 7.0+)

Optional

Identity Solution

FortiAuthenticator

FortiToken

FortiTrust Identity

any 3rd party ID providers supported by the Security Fabric

© Fortinet Inc. All Rights Reserved.

ZTNA–The Evolution of Application Access

Bringing zero trust principles to application access

Per Session Verification

User identity checks

- MFA
- Passwordless
- SSO

Device checks

- Identity
- OS version
- A/V status
- Vulnerability assessment

Continuous verification

- Device Posture
- User Behavior

Granular control

Access granted only to specific application

© Fortinet Inc. All Rights Reserved.

Reducing the Attack Surface

Granular control to applications

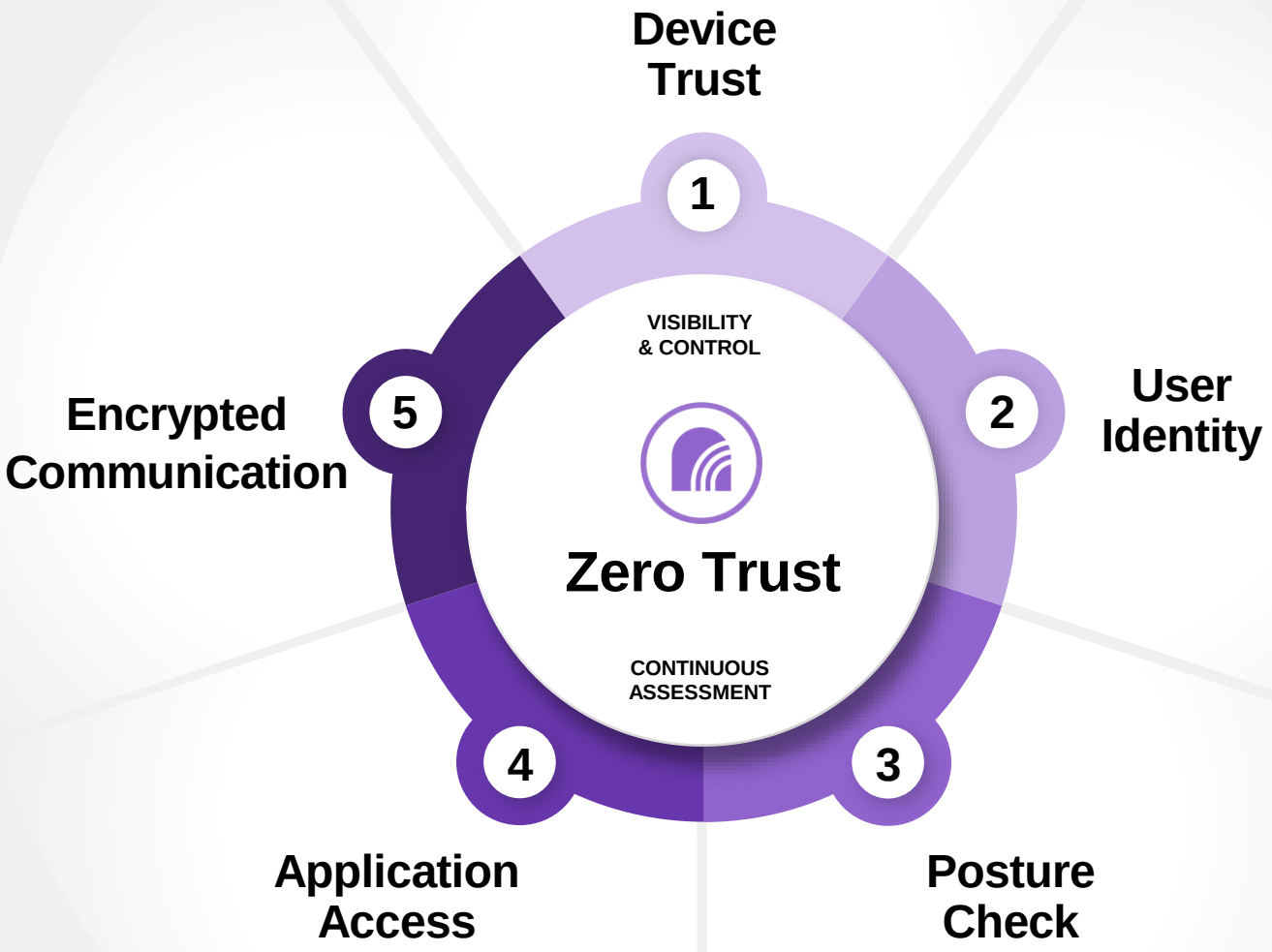
1
- Identify and Authenticate device
- Authorized device or BYOD?
- Approved for access? revoked?

2
- User identity should be verified
- Strong MFA
- Role-based access controls

3
- Adaptive and conditional access
- Security Compliance
- Device Vulnerabilities

4
- Verify Application Access Rights
- Application Specific Access
- Application not available to internet

5
- End-to-end encryption- even on-prem
- Data protection
- All communication is logged

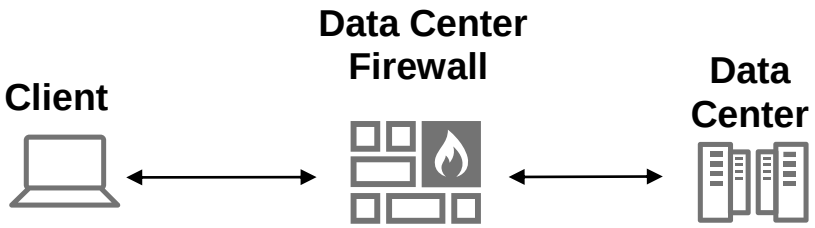


© Fortinet Inc. All Rights Reserved.

Fortinet ZTNA

Traditional VPN

- One Time Trust Check
- Access Entire Network
- Generic Rule Set
- Static Password

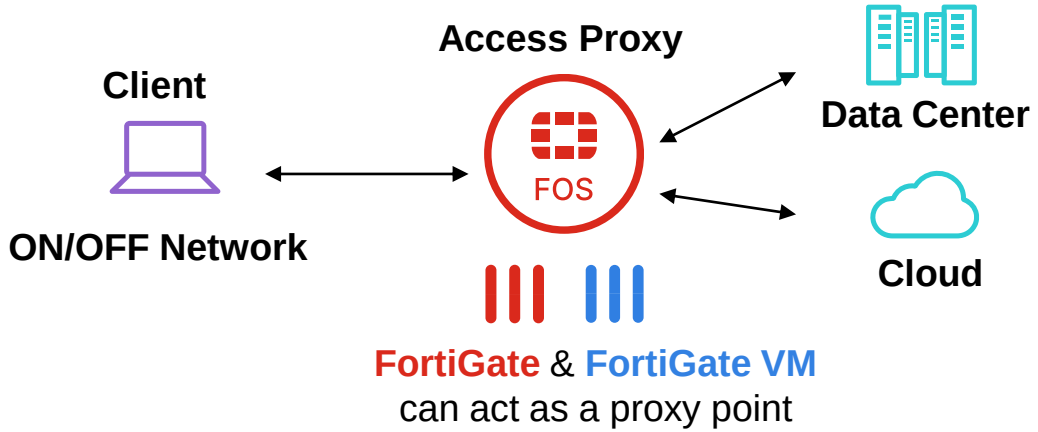


ZTNA

- Continuous Trust Check
- Access Specific Applications
- User Contextual Rule Set
- Multi-factor authentication

Existing FortiGate and FortiClient customers can use ZTNA as soon as they upgrade to FortiOS 7.0.

No additional licensing fees



© Fortinet Inc. All Rights Reserved.

Remote User Protection

3 Use Cases to Support Remote Work

General User

Need access to email, data and applications to do their job

FortiClient
Free VPN Client

+

FortiToken
Multifactor Authentication

Power User

Need more consistent secure connectivity for multiple devices

FortiClient
Free VPN Client

+

FortiAP
Secure Wireless Access at remote work locations

+

FortiToken
Multifactor Authentication

Super User

Need access to the most sensitive company information

FortiClient
Free VPN Client

+

FortiGate
High level of security at home

+

FortiAP
Secure Wireless Access at remote work locations

+

FortiFone
Secure, voice over IP (VoIP telephony solution)

+

FortiToken
Multifactor Authentication

© Fortinet Inc. All Rights Reserved.

Fortinet ZTNA Advantages

Convergence of capabilities, complete coverage, and cost

FOS-based ZTNA	• Leveraging existing infrastructure • Complete WFA coverage, including campus • Traffic Security Inspection • Operate at Scale • Leverage SD-WAN capabilities
ZTNA Client also VPN client	• Transition to ZTNA simplified • Shift to ZTNA at customer's pace • Optional EPP Protection in Unified Agent
No Licenses Required	• Simply a feature in FOS & FortiClient to turn on!

Fortinet Championship Trophy

© Fortinet Inc. All Rights Reserved.

FORTINET