



Partner Enablement Playbook

Fortify Your Partnership

Let's Engage



Contents:

> 1. Introduction

> 2. Selling Fortinet

> 3. SMB solutions

- > 3.1 SMB solutions overview
- > 3.2 The SMB Hub
- > 3.3 Fortinet Product Matrix
- > 3.4 Zoom in

> 4. The Target Audience

> 5. Engage: Partner Program Requirements & Benefits

> 6. Support and tools

- > 6.1 Exclusive Networks
- > 6.2 CTAP
- > 6.3 Fortinet NSE Training
- > 6.4 Marketing Centre

> 7. Fortinet as a subscription

- > 7.1 X-OD
- > 7.2 Why is it worth it?

> 8. Getting started in 5 Steps

> 9. Contact Us

**Let's
Engage**

1. Introduction

Your knowledge and support is vital for the SMB market

The SMB market is actively seeking to increase its level of cybersecurity, and needs a knowledgeable, reliable partner to help them evaluate their security requirements and determine which controls they need to invest in to maximize the value of the limited budget they have to spend. Many SMBs struggle to implement strong, holistic security across their business for a variety of reasons and too often rely on piecemeal security cobbled together with multiple vendor point products that don't operate cohesively.

Fortinet offers a variety of security solutions that are specifically designed for SMBs and their main concerns of losing consumer data, losing consumer trust, suffering reputational damage, and being out of compliance with regulatory standards due to a successful cyberattack—and with the best price/performance and functionality value in the market.

Let's discover together your target audience, the solutions portfolio, the supporting tools you have available and how to get your started!



2. Selling Fortinet

Two decades of cybersecurity experience!

Fortinet's mission is to deliver the most innovative, highest-performing network security fabric to secure and simplify your IT infrastructure.

We are a leading global provider of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centres, enterprises, and distributed offices.



Headquarters: Sunnyvale, California

Employees: 8,238

Founded: Nov. 2000

First Product Release: May 2002

Fortinet IPO: Nov. 2009

NASDAQ: FTNT

FY 2020 revenue: \$2.59B

FY 2020 billings: \$3.09B

Q4 2020 revenue: \$748M

Q4 2020 billings: \$961M

Q4 2020 EPS (GAAP): \$0.89/share

Q4 2020 EPS (non-GAAP): \$1.06/share

Market Cap (Dec. 31 2020): \$24.1B

\$1.96B cash+investments and no debt

Units Shipped to date: 6.5m+

Total Customers: 500,000+

Global Patents (as of Dec. 31 2020): Issued: 716 / Pending: 194

You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

Most Deployed Network Security

~30% of all FW/UTM appliance shipments

Source: IDC Worldwide Security Appliance Tracker, April 2020
(based on annual unit shipments of Firewall, UTM and VPN appliances)

Top network security innovator

3x more patents than comparable network security companies

Source: US Patent Office, As of December 31 2020

Broadest security protection

From IoT to the Cloud

Source: Fortinet estimates based on recent analyst research. 2024 opportunity shown.

Most 3rd party validations

NSS Labs, ICASA, VB and more

Source: NSS Labs most recent test results, as of December 2020.

The only company to excel at all key stages of network security

Discover the leading Fortinet Security Fabric

The Fortinet Security Fabric is the industry's highest-performing cybersecurity platform, powered by FortiOS, designed to span the extended digital attack surface to enable broad, integrated, and automated security protecting devices, data, and applications. Empowering organizations of any size to secure and simplify their IT infrastructure on the journey to digital innovation.



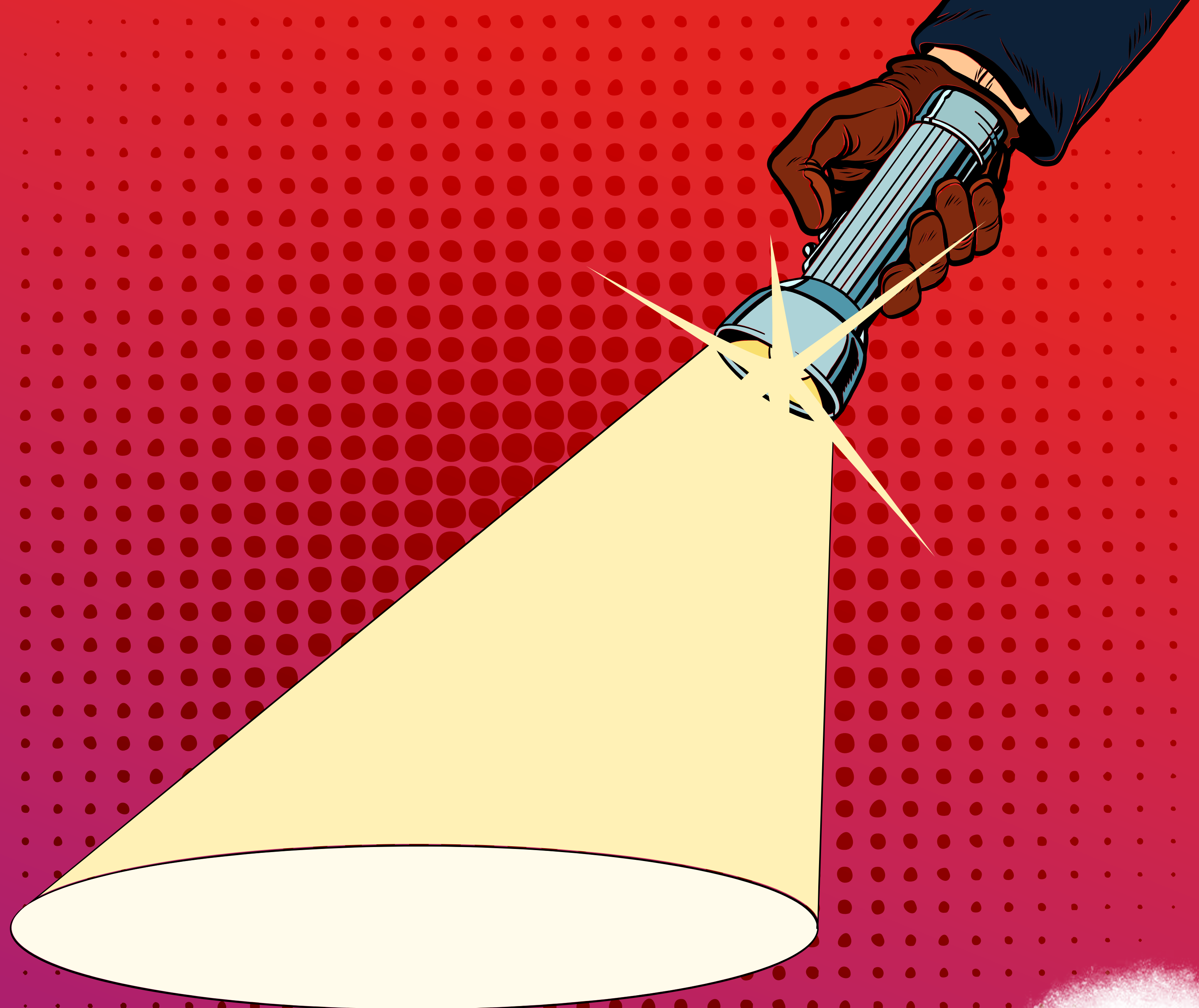
Get comfortable talking about the Fortinet Security Fabric:

Resources available:

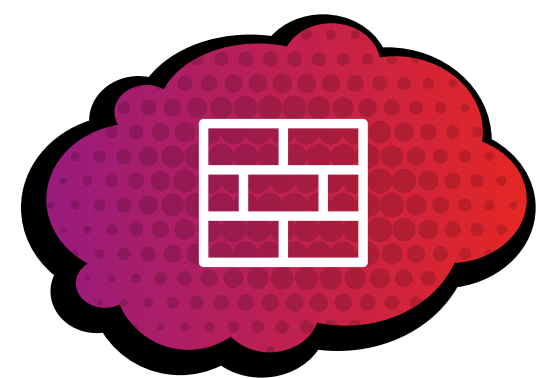
You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

3. SMB solutions

- > **3.1 SMB solutions overview**
- > **3.2 The SMB Hub**
- > **3.3 Fortinet Product Matrix**
- > **3.4 Zoom in**



SMB solutions overview



Network security

FortiGate



Multi Cloud security

FortiGate Vm

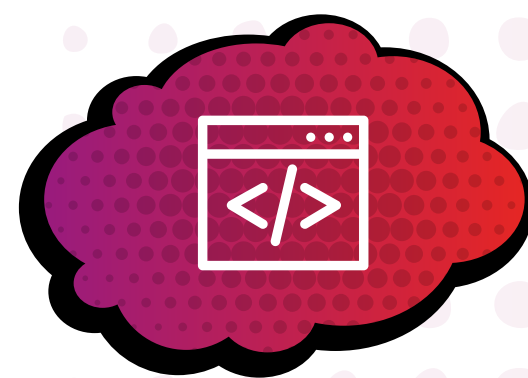
FortiCASB



Endpoint protection

FortiClient

FortiNAC



App & Email protection

FortiMail

FortiWeb

FortiADC



Access security

FortiWiFi

FortiAP

FortiSwitch

FortiToken



Security operation

FortiSandbox

FortiAnalyser

FortiSIEM



Network operation

FortiManager



Open Fabric Ecosystem

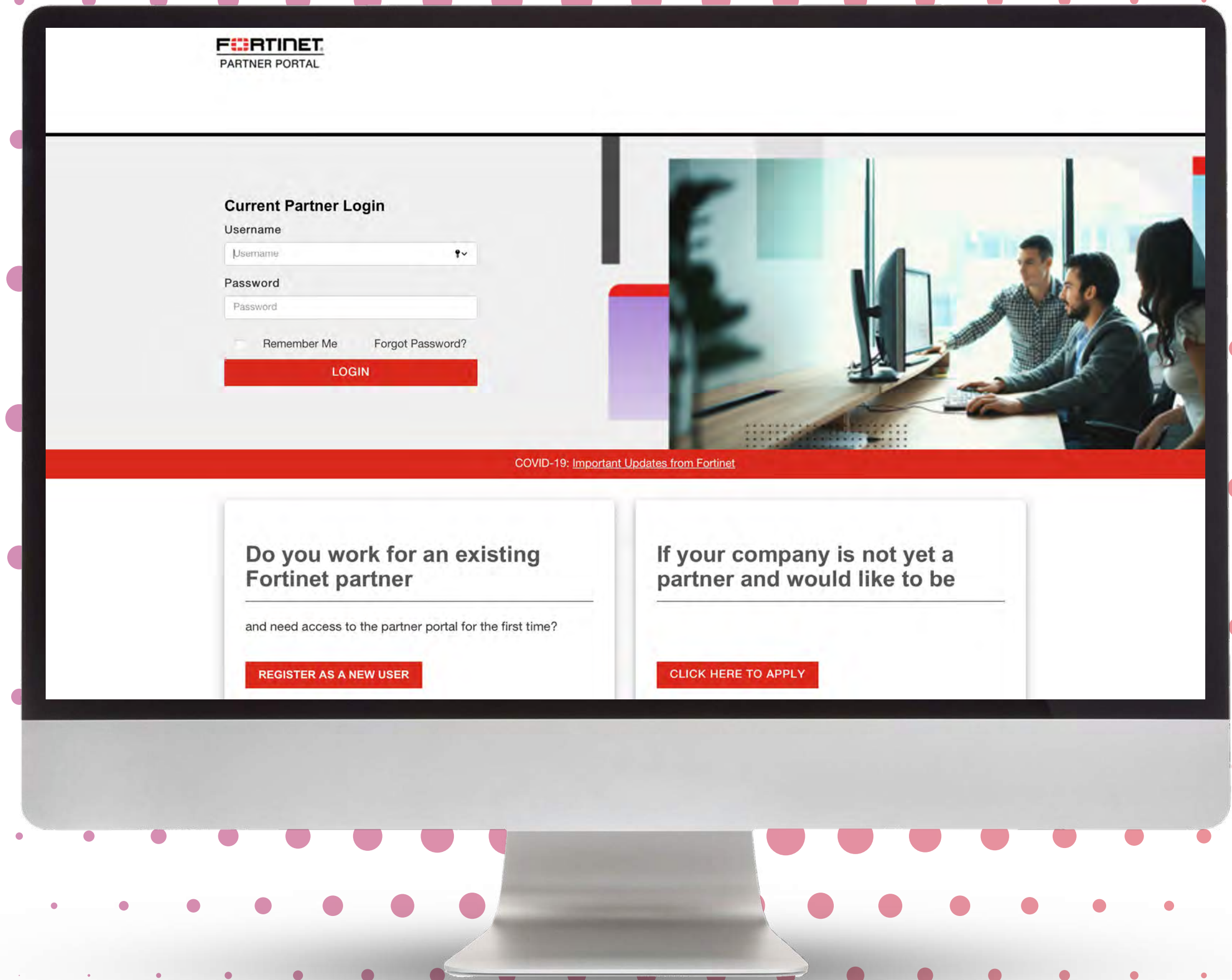
Fabric API's

Fabric Connectors

The SMB Hub

Discover and visit the Fortinet SMB Hub on the partner portal

3 steps to success:



You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

Fortinet Product Matrix

Fortinet delivers high-performance network security solutions that protect your network, users, and data from continually evolving threats. Our broad portfolio of top-rated solutions and centralized management enables security consolidation and delivers a simplified, end-to-end security infrastructure.



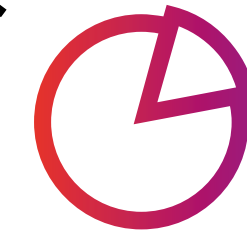
FortiGate



FortiManager



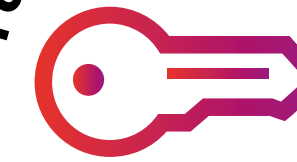
FortiAnalyser



FortiSIEM



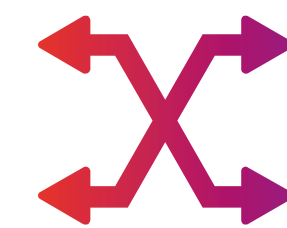
FortiAuthenticator



FortiAP



FortiSwitch



FortiNAC



FortiSandbox



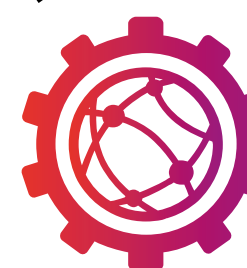
FortiClient



FortiMail



FortiWeb



You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

3.4 Zoom in

- **3.4.1 Fortinet Secure Office Networking**
- **3.4.2 Discovery Questions and Answers**
- **3.4.3 FortiManager**
- **3.4.4 Fortinet SD-Branch**
- **3.4.5 Zero-Trust Access**



Fortinet Secure Office Networking

Market Opportunity

According to customer surveys, despite many employees working remotely, many companies are taking this opportunity to upgrade their existing network infrastructure.

Remote employees place a unique demand on next-generation firewalls (NGFWs) requiring much more effective and efficient virtual private network (VPN) throughput and high-speed decryption performance without performance impact. Without a holistic strategy for security that automatically protects technology as it's added, growth will slow as each new technology requires its own security strategy.

Why Fortinet Secure Office Networking?

Fortinet's dedication to research and development (R&D) has resulted in a faster, more intuitive way of delivering network security that uses technology and automation to reduce cycles and combat the modern tools attackers use to target companies with weak security. Simplified management consolidates visibility and control and enables lean IT teams to maintain consistency across key networking devices such as firewalls, switches, and wireless access points (APs) wherever they are physically located.

Discovery Question...

Get selling Fortinet Secure Office Networking.

Have you expanded recently or moved to a remote-based environment? More employees, more applications, or updates? When was the last time you updated your firewalls?

Are you running any threat functions like web filtering, AV, or IPS as a point solution?

How many different platforms do you have to use to oversee your entire network security as well as your core networking capabilities? Are there ever conflicts or visibility and control you wish you had?

How can I get an overview of Fortinet's Secure Office Networking Solution?

and answers.

Click  to view Answers

FortiManager

Simplify Operations with Single-Pane Automation Orchestration & Response.



1 Single Pane of Glass Management & Visibility

Challenges:

Human Errors and Misconfigurations are the leading cause of security breaches and/or network outages.

Solutions:

Centralized security management and visibility helps multiple complex management consoles and enables true Automation

- Single Pane of Glass Management
- Zero Touch Deployment
- Single Console Visibility
- Configuration Management
- Multi Factor Authentication
- High Availability



2 Workflow Optimization

Challenges:

Staff Shortage. Enterprises don't have the resources to staff the detection and response of Anomalies. Leverage Workflow Optimization technology to reduce the time to detect and respond to threats or operational anomalies.

Solutions:

- Incident Detection & Response
- ITSM Workflow Applications
- SIEM Integration
- Webhook Integration
- Automation Stitches



3 Advanced Threat Detection

Challenges:

Advanced Threats: Attacks are getting complex and very hard to detect and that coupled with lack of skilled staff. It's challenging to protect the modern enterprise.

Solutions:

- Analytics Driven threat detection that can detect any threats and identify them as High, Med or Low risks for the enterprise
- IoC Detection & Correlation
- Fabric Integrated Detection
- SIEM Integration



4 Audit & Compliance

Challenges:

Regulation: Compliance Management is usually a very manual and inefficient process that involves multiple full time staff and involves months to get right.

Solutions:

- Simple Reporting and Compliance Controls
- Management to enables proving Compliance pro-actively
- NIST, CIS Frameworks
- Reports on PCI DSS, SAR etc.
- Audit Logging & RBAC
- Integrated Workflow for Security & Operations

Fortinet SD-Branch

Fortinet SD-Branch Secures the Network Edge at the Branch.

Digital transformation (DX) has made branch networks much more complex—and therefore vulnerable to attack. In response, many organizations have deployed multiple point products to address new threat exposures as they appear. But this approach further complicates branch infrastructures—adding greater cost, complexity, and vulnerability. To address these issues, branches should integrate networking and security capabilities across the WAN edge, access layer, and endpoints.

The solution, Fortinet SD-Branch, consolidates the network access layer within a secure platform that provides visibility and security to the network and all devices that connect to it.

Addressing an Expanding Attack Surface

Rapid adoption of DX technologies—including Internet-of-Things (IoT) devices, Software-as-a-Service (SaaS) applications, digital voice/video tools, and bring-your-own-device (BYOD) endpoints—has caused an increase in the number of network edges that need to be secured at a given branch. Both the networks themselves and the point solution security products used to protect branch infrastructure have become difficult and costly to manage.

The rise of IoT in particular—from connected office appliances, to efficient lighting and climate controls, to employee-owned personal fitness products—represents many more devices coming onto the network, often with questionable security and unreliable visibility.

Benefits for Network Engineering and Operations Leaders

- Improving security at the branch.
- Global policies are enforced at all WAN edges, at the branch access layer, and across all endpoint devices.
- Extends both security and network performance to the access layer by unifying WAN and LAN environments.
- Automates discovery, classification, and security of IoT devices when they seek network access.
- Automatically provides anomaly detection and remediation processes based on defined business logic.
- Allows distributed organizations to rapidly scale their operations across new offices and geographic locations.
- Reduce the need for on-site resources, which lower TCO.
- SD-Branch integrates firewalls, switches, and APs into a single, consolidated solution.
- Its single-pane-of-glass management capabilities combine security and network layer visibility to optimize staff efficiency while enabling proactive risk management.
- Zero-touch deployment features reduce the burdens associated with initial setup and business growth over time.

You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

Zero-Trust Access.

Why ZTA?

The Market Opportunity...

Organizations face an expanding attack surface with all the people and devices that connect to or exist on their network. With 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.

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.

Click below to learn more about: "Securing Digital Innovation Demands Zero-trust Access" and how CISOs Face New Risks as the Attack Surface Expands

4. The SMB Audience

Maximise the Opportunity



Target Keywords and Personas

Organisation Size

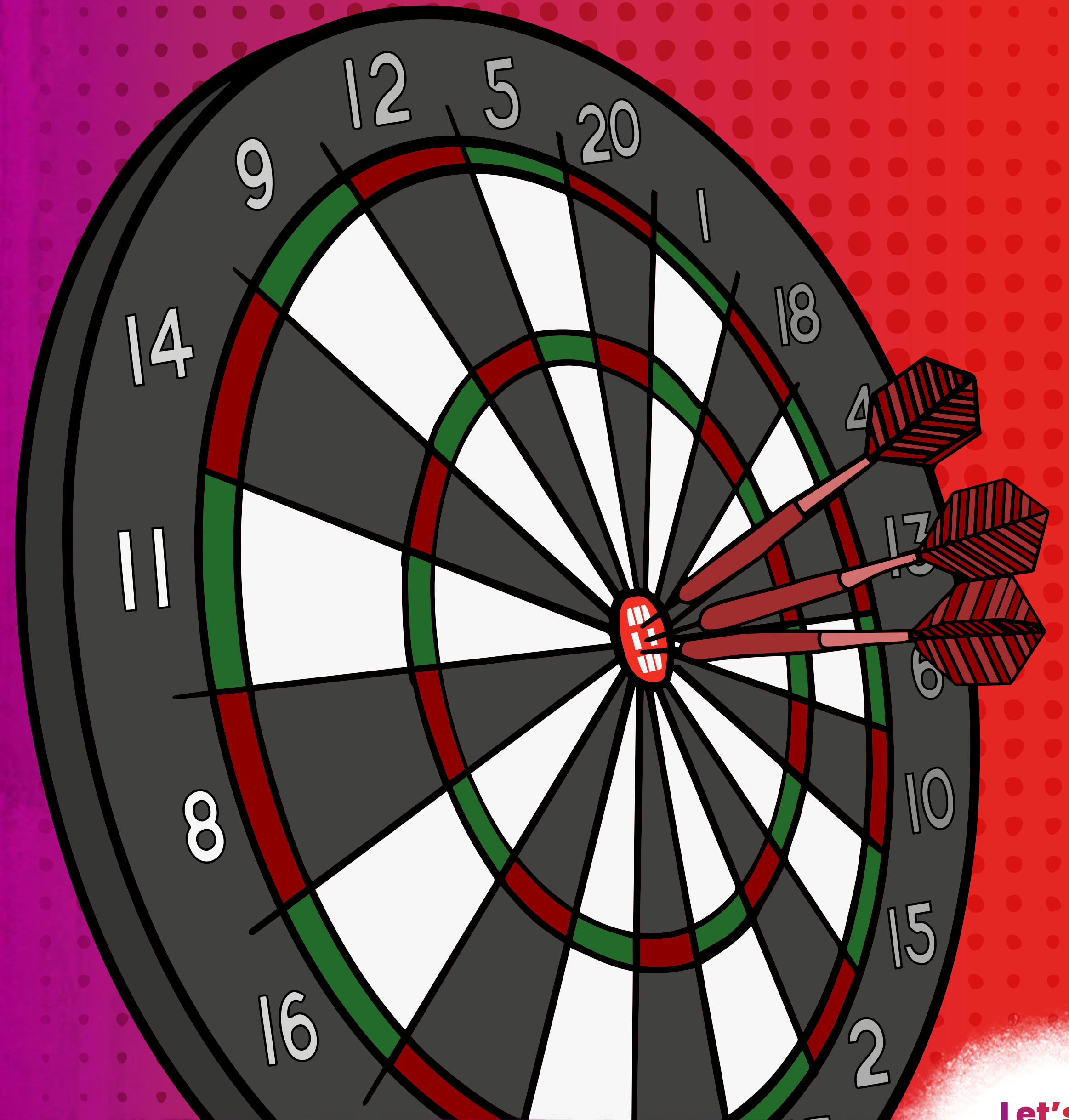
- Small and Medium Enterprise - 50 - 250 employees

Personas:

- IT Directors/Managers or higher
- System Administrators

Keywords—What To Listen For?

- Lack of staff/budget to maintain security
- Any kind of expansion, people, or digital transformation
- Phishing, ransomware, advanced/zero-day threats
- Technology refresh or new IT projects—how will they be secured?



Fortinet for SMBs: Engineered for Complete Protection

Intuitive Security. Simplified Management. Maximum Value.

Market Opportunity

- Small and midsize businesses (SMBs) are consuming technology at a rapid pace to gain competitive advantage and increase employee productivity, but this also increases their attack surface and risk.
- Many SMBs have similar cybersecurity needs to larger enterprises, but they simply don't have as many staff to implement and maintain nor the budget to afford the amount of protection they would like.
- 89% of SMBs consider cybersecurity a top priority.

Why Fortinet for SMB?

Fortinet SMB Security Solutions provide a path to complete protection that delivers clear return on investment (ROI) without sacrificing security.

SMBs can take advantage of tight integration, automation, and visibility across the entire cybersecurity footprint to improve effectiveness, reduce cycles, and scale as the company grows.

Addressing Business Challenges

Business Challenges	Fortinet Solutions
<p>Lack of Automation and Integration</p> <ul style="list-style-type: none"> • Ranks as the second-highest concern (after resources) when it comes to implementing and maintaining security. • Point products with separate management, policies, and/or configurations cause gaps in security from misconfiguration and are further complicated when tight integration and automation are lacking. 	<p>Whenever a new threat is first encountered, Fortinet offers a tightly integrated and automated security platform that uses technology to reduce cycles and combat the modern tools attackers use to penetrate companies.</p> <p>Whenever a threat is first encountered, anywhere in the world, your entire platform can be protected in minutes, not hours or days, without human intervention.</p>
<p>Lack of Visibility and Control</p> <ul style="list-style-type: none"> • Understanding the number of users, devices, applications, what’s running where, and controlling the above becomes daunting when platforms weren’t meant to work together. • Lack of central visibility complicates, especially with multiple sites when management requires on-site staff. 	<p>Fortinet boasts the broadest, most integrated platform on the market—built from the ground up to work together and provide superior protection. Cloud-delivered management centralizes visibility and control and brings consistent security across network, endpoint, and cloud deployment.</p>
<p>Resources—Budget and Workforce</p> <ul style="list-style-type: none"> • Even large SMBs (over £20m+) only have on average six IT members responsible for general IT as well as security. • Despite budget constraints, SMBs still understand the value of security and struggle to find a solution that fits their means without sacrificing the security they need 	<p>Fortinet’s focus on R&D has enabled us to engineer technology capable of significantly higher performance than similarly priced competitor devices, regardless how much security is enabled. It’s why Fortinet is consistently recognized by industry leaders and analysts including Gartner and NSS Labs as a leader in cybersecurity.</p>

Key Differentiators

Networking and Security Converged

The FortiGate next-generation firewall (NGFW) brings advanced threat protection, intrusion prevention system (IPS), web filtering, and more in a single device. Security policies extend through Switching and Wireless Access Points, consolidating visibility, control, and maintaining consistency across key networking components. Finally, Fortinet pioneered combining NGFW and software-defined wide-area networking (SD-WAN) into a single solution that leads the market in application performance and experience without sacrificing security or adding complexity.

Automated Security

FortiSandbox Cloud is an as-a-service Sandbox that simplifies deployments and maintenance, and reduces risk. Customers' entire Fortinet deployment and third-party solutions across network, endpoint, and cloud security are updated with the latest threat intelligence against new, never-before-seen threats automatically—in minutes, not hours or days.

Broadest Integrated Platform

Fortinet prides itself on limited acquisitions to grow our capabilities and continues to boast the broadest offering in the industry. Products are designed to work together, maintain consistency, and offer superior integration.

Industry-leading Price to Performance

Fortinet consistently delivers multiple times better performance than similarly priced competitors regardless what mix of security and decryption analysis is being used, and our security bundle pricing is significantly less expensive, leading to greater total cost of ownership (TCO) over multiple years.

Smarter Long-term Investment

Fortinet offers right-sized options and growth paths for small businesses and large enterprises alike, including an extensive security and management-as-a-service offering for those looking to take advantage of cloud security and flexibility from a single vendor, eliminating the need to rip and replace solutions and retrain staff.

Most Deployed NGFW in the World

Fortinet has over 465,000 customers and the FortiGate is the most deployed NGFW on the market—With more third-party validations than any other network security vendor, including from Gartner and NSS Labs.



5. Engage

Partner program Requirements and Benefits.



[Introduction](#)

[Selling Fortinet](#)

[SMB solutions](#)

[The Target Audience](#)

[Engage: Partner Program Requirements & Benefits](#)

[Support & tools](#)









[Fortinet as a subscription](#)

[Getting started in 5 Steps](#)

[Contact Us](#)

Let's Engage

Requirements:

		INTEGRATOR	MSSP	CLOUD
ADVOCATE	 Business Requirements	<ul style="list-style-type: none"> Fortinet Integrator questionnaire Valid partner agreement Primary Business Face-to-Face selling model 	<ul style="list-style-type: none"> Fortinet MSSP questionnaire Valid partner agreement 	<ul style="list-style-type: none"> Fortinet Cloud questionnaire Valid partner agreement Proof of existing relationship with: <ul style="list-style-type: none"> Microsoft Registered AWS Registered
	 Training Requirements	1 NSE 1, 1 NSE 2	1 NSE 1, 1 NSE 2	1 Adaptive Cloud Sales Training
SELECT	 Business Requirements	<i>All ADVOCATE requirements, plus...</i> <ul style="list-style-type: none"> Sales volume requirement¹ Provide Level 1 support 	<i>All ADVOCATE requirements, plus...</i> <ul style="list-style-type: none"> Minimum 8x5 Security Operations Centre Test lab environment Annual Sell To and Sell Through revenue¹ 12 Month business plan review POS reporting Annual support ticket review Business Review, 3 months prior to contract renewal 	<ul style="list-style-type: none"> Fortinet Cloud questionnaire Valid partner agreement Proof of existing relationship with: <ul style="list-style-type: none"> Microsoft Cloud Service Provider AWS Select Partner Sales Volume Requirement¹
	 Training Requirements	1 NSE 1, 1 NSE 2, 1 NSE 4	1 NSE 1, 1 NSE 2, 1 NSE 3, 1 NSE 4, 1 NSE 5 (exam)	1 Adaptive Cloud Sales Training, 1 NSE 4 (recommended), 1 NSE 6 (exam, FortiMail/FortiWeb*), 1 NSE 7 (Cloud)
ADVANCED	 Business Requirements	<i>All SELECT requirements, plus...</i> <ul style="list-style-type: none"> Sales forecasting Lead follow up and reporting Quarterly business plan review Hold co-marketing end-user events 	<i>All SELECT requirements</i>	Business Requirements <i>All SELECT requirements</i>
	 Training Requirements	2 NSE 1, 2 NSE 2, 2 NSE 4, 1 NSE 5 (exam), 1 NSE 7	2 NSE 1, 2 NSE 2, 1 NSE 3, 2 NSE 4, 1 NSE 5 (exam), 1 NSE 6 (exam), 1 NSE 7	
EXPERT	 Business Requirements	<i>All ADVANCED requirements, plus...</i> <ul style="list-style-type: none"> Provide Level 2 support 	<i>All ADVANCED requirements, plus...</i> <ul style="list-style-type: none"> 24x7 Security Operations Centre Certain % of revenue from services <ul style="list-style-type: none"> Determined in region Semi-annual support ticket review 	Business Requirements 1 Adaptive Cloud Sales Training, 1 NSE 4 (recommended), 1 NSE 5 (exam, FortiSIEM/FortiManager, FortiAnalyzer, FortiEMS*), 2 NSE 6 (unique exams, FortiMail/FortiWeb*), 2 NSE 7 (Cloud)
	 Training Requirements	2 NSE 1, 2 NSE 2, 2 NSE 4, 1 NSE 5 (exam), 1 NSE 7	2 NSE 1, 2 NSE 2, 1 NSE 3, 2 NSE 4, 1 NSE 5 (exam), 2 NSE 6 (unique exam), 2 NSE 7	

ADVANCED / EXPERT

* Suggested exams

Benefits:

		INTEGRATOR	MSSP <small>All INTEGRATOR benefits, plus...</small>	CLOUD <small>All MSSP benefits, plus...</small>
ADVOCATE	Sales Support	<ul style="list-style-type: none"> Authorized to resell Fortinet solutions Access to Deal Registration Program Access to renewal assets Eligible for Not For Resale demo (NFR¹) Eligible for FortiRewards Program¹ 	<ul style="list-style-type: none"> Exclusive access to Fortinet MSSP Portfolio 	<ul style="list-style-type: none"> Ability to purchase VM Solutions via distribution which can be installed in a public cloud (BYOL)
	Technical Support	<ul style="list-style-type: none"> Fortinet Support Portal access 	<ul style="list-style-type: none"> On-premise hardware Virtual machines SAAS Solution 	
	Marketing & Communications	<ul style="list-style-type: none"> Access to Partner Portal, webinars, newsletters 		
		<i>All ADVOCATE benefits, plus...</i>	<i>All ADVOCATE benefits, plus...</i>	<i>All ADVOCATE benefits, plus...</i>
SELECT	Sales Support	<ul style="list-style-type: none"> Eligible for specialization 	<ul style="list-style-type: none"> "Sell-to" specific discounting (for internal needs) 	<ul style="list-style-type: none"> Ability to purchase directly from public cloud/ private cloud provider or distributor cloud PayG discount: <ul style="list-style-type: none"> - 15%: AWS CPPO, Azure, GCP, OCI, AliCloud - 20%: AWS SPPO
	Technical Support	<ul style="list-style-type: none"> Direct access to Fortinet support 		
	Marketing & Communications	<ul style="list-style-type: none"> Preferential access to joint marketing funds 		
		<i>All SELECT benefits, plus...</i>	<i>All SELECT benefits, plus...</i>	<i>All SELECT benefits, plus...</i>
ADVANCED	Sales Support	<ul style="list-style-type: none"> Fortinet channel account manager Fortinet channel marketing manager 		
	Technical Support			
		<i>All ADVANCED benefits, plus...</i>	<i>All ADVANCED benefits, plus...</i>	
EXPERT	Sales Support			
	Technical Support	<ul style="list-style-type: none"> Exclusive invitations to Fortinet technical events 	<ul style="list-style-type: none"> Free yearly subscription to: FortiConverter License, a multi-vendor configuration migration tool for building FortiOS configurations. FortiDeploy License: Enable zero-touch bulk provisioning for your FortiGate, FortiWiFi or FortiAp products. FortiPortal VM License: Virtual machine which includes both wireless and security features of FortiPortal, includes management of 10 FortiGates and 100 FortiAPs. Requires FortiGate as a wireless controller, FortiAnalyzer and FortiManager. 	

ADVANCED / EXPERT

- Access to Pay-as-you-go
- Direct purchase from cloud marketplace (AWS, Azure, GCP, OCI, AliCloud)
- BYOL discount: Same as INTEGRATOR
- Dedicated cloud expert
- VM solutions available

Engage Partner Specializations:

Designed to help your organization gain the knowledge and skills necessary to become a partner of distinction in one of several high-business demand areas. When individuals from your organization complete the training, your organization becomes eligible for designation. Once Specialized, you will receive a badge, official recognition on the Partner Locator, discounted not-for-resale kits designed for each Specialization, and exclusive access to events. Partners will also gain access to our communities where you can engage, learn, and network with other Fortinet enthusiasts. Each Specialization has customized Sales Training and Technical Exam requirements that must be completed before a partner organization becomes eligible for designation.



- Specialization badge and featured on Partner locator
- Discounted specialization-specific Not For Resale (NFR) kit
- Access to communities



- Eligible for 1 Exclusive Accelerate Pass1



- Eligible for 1 Exclusive Xperts Academy Pass1
- Eligible for joint PR Activity

	SPECIALIZATION SD-WAN	SPECIALIZATION LAN Edge and SD-Branch	SPECIALIZATION Data Center	SPECIALIZATION Adaptive Cloud Security	SPECIALIZATION Zero Trust Access	SPECIALIZATION Operational Technology	SPECIALIZATION Security Operations
Sales Training	SD-WAN Sales Training (1)* SD-WAN MSSP Sales Training (1)*	Secure access Sales Training (1)	Data Centre Sales Training (1)	Dynamic Cloud Sales Training (1)	Zero Trust Sales Training (1)	OT Security Training (1)	Security Operations Training (1)
Technical Exams	NSE 7 SD-WAN (1)	NSE 7 Secure Access (1)	Select: NSE 7 (any) (1) Advanced: NSE 7 (any) (1) Expert: NSE 8 (1)	NSE 4 (1) NSE 7 Cloud (1)	NSE 5 FortiClient(1) NSE 6 FortiNAC (1) ENSE 6 FortiAuthenticator (1)	NSE 7 OT Security (1)	NSE 5 FortiEDR (1) NSE 7 Advanced Analytics (1) NSE 7 FortiSOAR Design and Development (1)

Engage Requirements & Benefits Matrix



You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

6. Support & Tools

- > **6.1 Exclusive Networks Support**
- > **6.2 CTAP**
- > **6.3 Fortinet NSE Training**
- > **6.4 Marketing Centre**

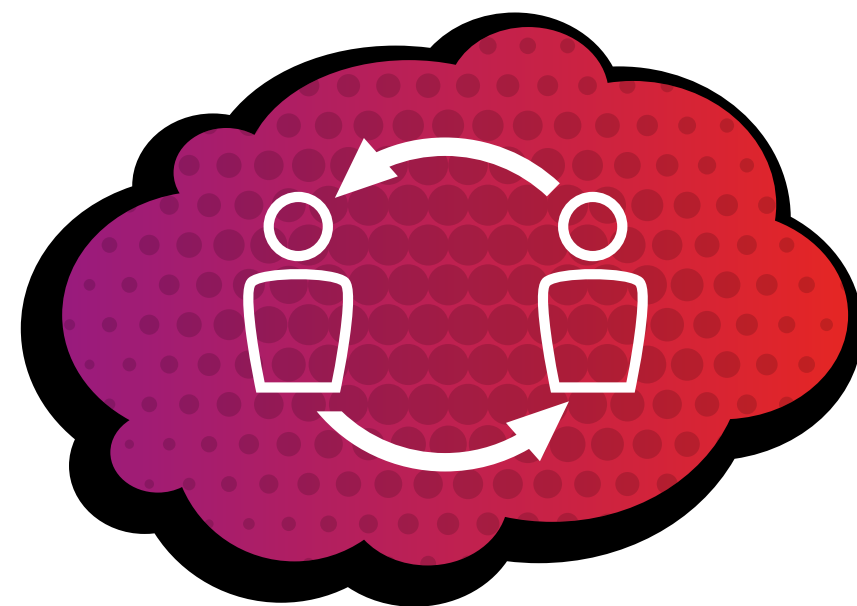


Exclusive Networks Support

Value Add from Exclusive Networks, the global trusted digital infrastructure specialist you deserve:

By partnering with Exclusive Networks, we will be on hand to help you navigate your Fortinet journey

With a Fortinet partnership spanning more than a decade, we offer unrivalled experience on Fortinet solutions with 38 people aligned to Fortinet including 10 Fortinet dedicated Team Members across Commercial, Pre Sales & Marketing. Our global 'services first' ideology offers an orchestrated array of global services that focus on delivering the best outcomes for you and your customers.



End to End Partner Support

Our end to end support offers you the power to sell, implement, and support Fortinet projects on the scale of a major 24/7 value-added service and technology operation, without the time and operating cost overhead.



2:1 Certified Technical Resource

Need help to scope, design and install your customer projects, manage configuration, health checks or proposals? Our Professional Services team operate as an extension of your teams with the expert product and integrated solutions knowledge you need.



Omnichannel Consumption

With our 5 ways to buy, we offer a broad range of consumptions models – from traditional procurement, finance and leasing to subscription based services with X-OD and even As a Service or Managed Services..



Global Reach

If your customer project involves international roll-out or requires in-country support or deployment, our Global Services Operations (GSO) team can provide logistics and professional services to over 150 countries worldwide.

The Cyber Threat Assessment Program (CTAP) Sales Methodology

- Designed to help you during greenfield and renewal opportunities to convert prospects and expand your business by giving customers an in-depth view of the current state of their network.
- After deploying a FortiGate to monitor your prospect's network for a short period of time, a report is generated that provides visibility into their network risks, and allows you to position a clear path forward that will quickly gain buy-in from key technical and business decision makers.

Learn more about CTAP:

When to use CTAP:

There are four key times to put CTAP into play with your prospects and customers...

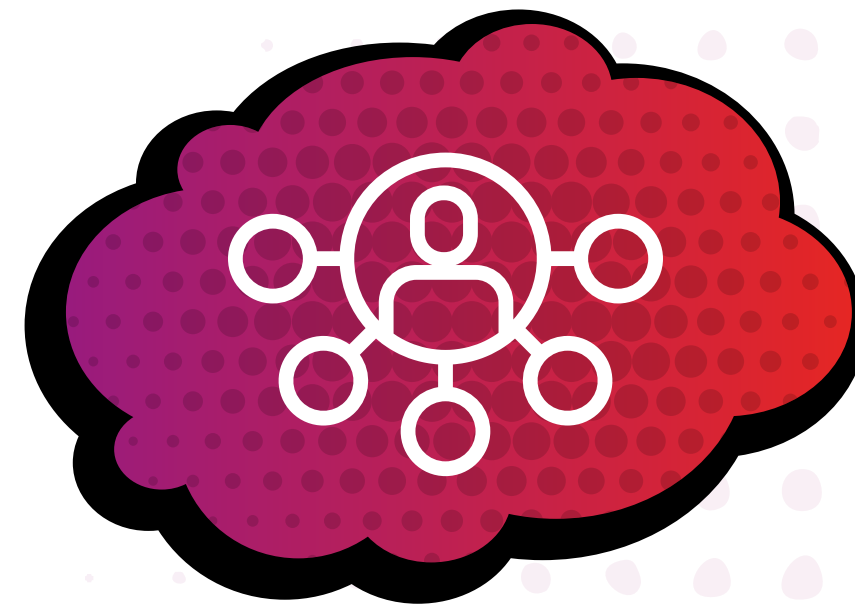
- 1 Land:**
Use it as a pre-sales tool to generate interest and begin an impactful dialogue with prospects.
- 2 Compete:**
Use assessments as a displacement tool to highlight areas where an incumbent is ineffective.
- 3 Renew:**
Use an assessment to substantiate the need for additional features or FortiGuard services.
- 4 Expand:**
Expand your account footprint and cross-sell more Security Fabric solutions.

The Fortinet CTAP Difference



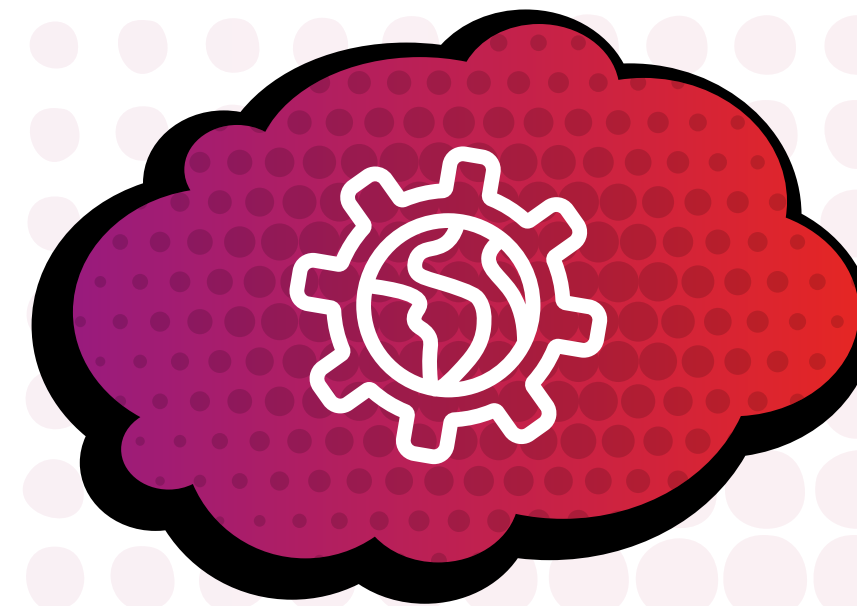
Superior Visibility

Fortinet solutions are powered by content security and threat intelligence from FortiGuard Labs, who work constantly to identify emerging applications and protect enterprises against new threats.



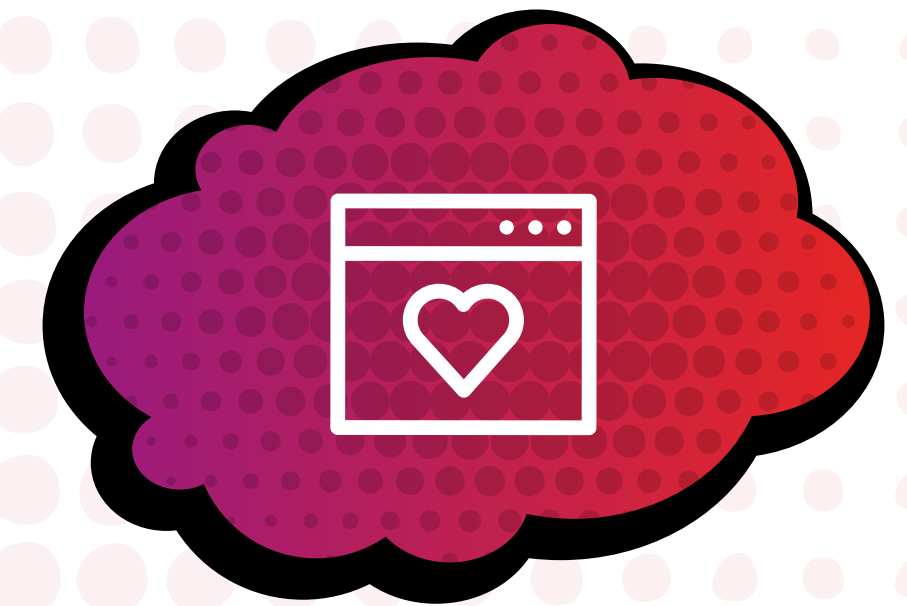
Deployment Flexibility

CTAPs allow multiple deployment options in order to minimize network disruption. This allows you flexibility to meet your customer needs while demonstrating real value to their organization.



Fortinet Security Fabric Cross Selling Opportunities

The CTAP can uncover additional opportunities where the broad and integrated Security Fabric comes into play – analytics, sandboxing, and more.



Actionable Recommendations

Each assessment report includes a set of actionable recommendations that technical staff can use to refine their security and network utilization.

FORTINET NSE Training Institute

What is it?

The Fortinet Network Security Expert (NSE) program guides Partners through 8 levels of training and assessment in network security. A wide variety of courses and practical exercises are available that demonstrate mastery of complex network security concepts.

NSE certification enables you to:

- Validate your network security skills and experience
- Demonstrate value
- Leverage Fortinet's full range of network security products, consolidate solutions, and reduce risks
- Accelerate sales and offer new services

For a detailed overview on the NSE Program visit the NSE Training Institute homepage. Here you will find the latest updated new courses, updated exams and more resources.



You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

Additional Training Services

Exclusive Networks Training Services

A Fortinet Authorised Training Centre, Exclusive Networks' certified trainers offer the highest standard of accredited technical education on Fortinet products and solutions. Courses can be provided either from Exclusive Networks' training suites, at the customer's premises or a suitable location for all parties. Alternatively, bespoke training courses using selected material from the vendor courseware can be provided where necessary.

Both accredited training and bespoke training include instructor led training and hands-on labs. Knowledge transfer sessions are also available which provide instruction and demonstration of customer selected topics (but without courseware or hands-on labs). All of Exclusive Networks' trainers adopt a 'hands-on' approach, which means they teach course content with real-world practical experience, rather than simply facilitate how to achieve accreditation.

Fortinet Fast Track Training

Fortinet created the Fast Track Training to support your pursuit of the technical expertise and knowledge required to take full advantage of the Fortinet Security Fabric and protect your network against all current and future security threats. Contact your Fortinet Channel Account Manager or check out the Exclusive Networks Fast Track sessions on our events page.

NSE 4 Technical Bootcamps

Created specifically as a value add service from Exclusive Networks for those partners whose NSE4 certification has lapsed or who already have an in-depth knowledge and experience of the configuration and day to day management of FortiGates. Suitable only for technical engineers with that experience, these one day intense revision workshops work as a refresh session of the FortiGate Security and Infrastructure courses and are designed to remind you of the information needed to take the NSE4 exam. Those who attend and complete the bootcamps will be provided with an NSE 4 exam voucher.

Fortinet Marketing Support

The Fortinet Partner portal is the place to go for easy access to the latest marketing campaigns for partners.

You can also find a wealth of supporting content in the asset library

Other useful information:

You need to be logged into the Fortinet Partner Portal at <https://partnerportal.fortinet.com/> for this link to work.

Start Building Your Pipeline

You can find more assets and tools on our Exclusively Fortinet Microsite including CTAP & SD-WAN assessment playbooks, end user facing videos, infographics and quick links to co-brandable campaigns to save you time.

We are also available to consult with you on your marketing campaigns if you're unsure where to start.



7. Fortinet as a subscription

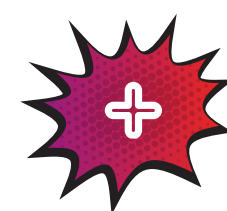
- 7.1 X-OD
- 7.2 Why is it worth it?



X-OD

What is X-OD?

X-OD is an on-demand platform designed to simplify technology consumption and drive growth by fast forwarding your evolution to the subscription economy.



Key Benefits:

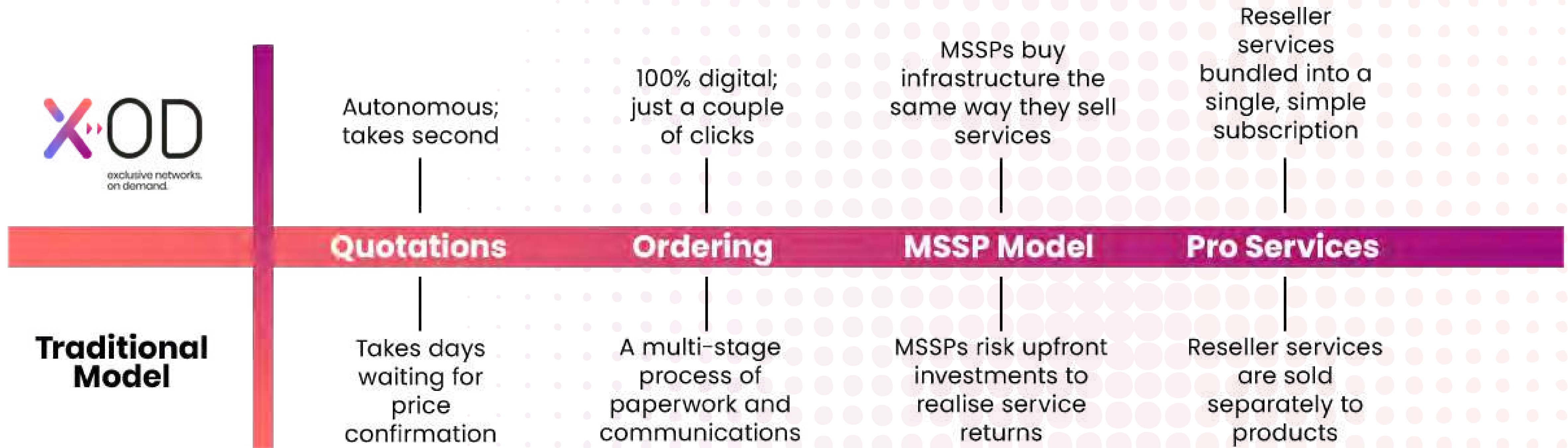
X-OD has the power to transform your business into a customer-centric operation that can thrive in the on-demand world. By fast forwarding your evolution to the subscription economy, digitalising your value chain and enabling you to convert customer insight into customer success, X-OD can help you win now and drive your business forward.

- Focus your offering on technical expertise and customer intimacy
- Reduce workload and operating cost
- Fast forward your transition to the subscription economy
- Develop a predictable revenue stream



Key Features:

- Autonomous quoting & billing
- Quote management
- Renewal management
- White labelling



Why is it worth it?

Use Case 1: Security Fabric – Increase deal size thanks to predictable spends

End-users requirements:

- Increase security level.
- Secure external devices connections to company network.

End-users challenge:

- Budget is negotiated in OPEX, CAPEX has longer validation process.
- Client willing to get additional options but total price does not fit into this years budget.

Win the deal with X-OD by removing complexity and offering perspective



Offer customer off the shelf X-OD solutions for different level of security with monthly, quarterly or yearly subscriptions.



Speed up sales cycle, unlock budget with flexible payments.



Provide different offers and agility on the way security is consumed and operated.

Why is it worth it?

Use Case 2: Secure Access – Business Continuity Controlling IT spends

End-users requirements:

- Converged network enabling voice, data and wireless traffic.
- Safe extension of corporate development.
- Scalable solution and easy to deploy.

End-users challenge:

- Cash available is limited with COVID, already unexpected expenses to implement work from home at scale.
- Customer doesn't want complexity associated with leasing as time is of the essence.

Win the deal with X-OD by removing complexity and offering perspective



Off the shelf X-OD offering flexibility to choose and build configurations.



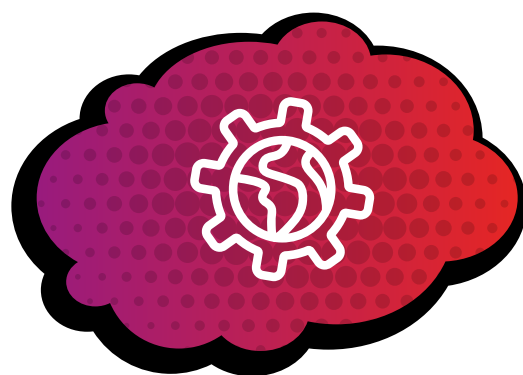
Speed up sales cycle, unlock budget for better features and best security level.



Limited financial impact while removing complexity tied to leasing contracts.

Why is it worth it?

**X-OD value proposal is different by reseller type.
Our primary reseller targets are MSSPs and specialist resellers**



MID-SIZE TRADITIONAL RESELLERS

FIT WITH X-OD

Tactical engagement (could take more time to convert)

- Transformative approach
- Impact on revenue recognition and sales model

VALUE PROPOSAL

- ✓ Answer to changing end users needs towards subscription
- ✓ Transition towards MPs/MSSP model
- ✓ Transition from MPLS to SD WAN



SMB RESELLERS

Primary Target with SMB offers

- Easy Answer to client needs
- Financial transformation for smaller end users

- ✓ Pre packaged offers to help selling Fabric
- ✓ Digitize and simplify operations
- ✓ Easy Financing already designed monthly offers

8. Getting started in 5 Steps

Your first 90 day journey.

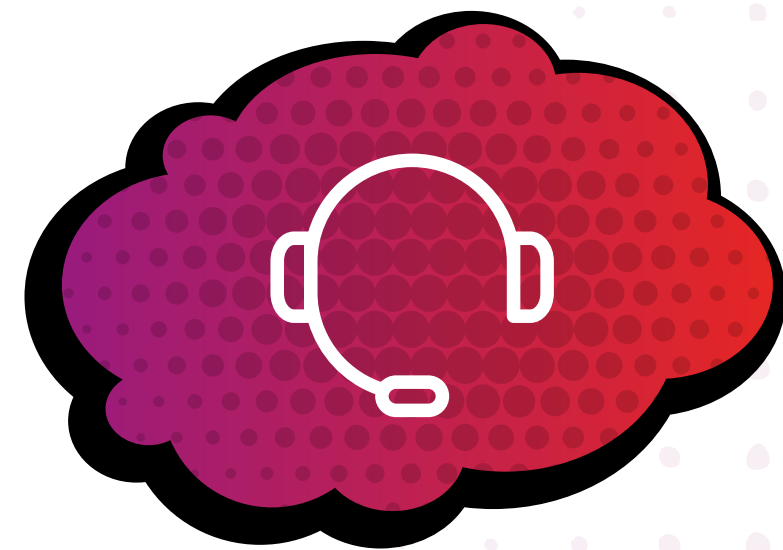


Your first 90 day journey



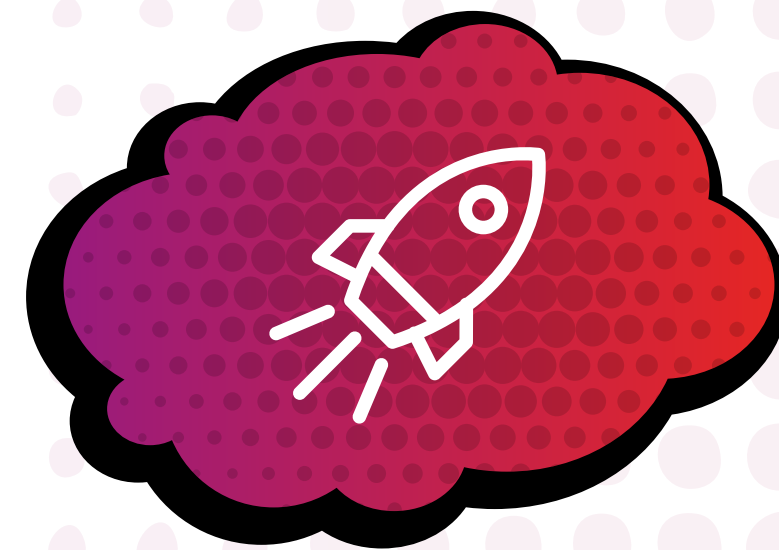
Partnership

Get started with your access to the partner portal, Exclusive Networks introduction, Fortinet Partner strategy.



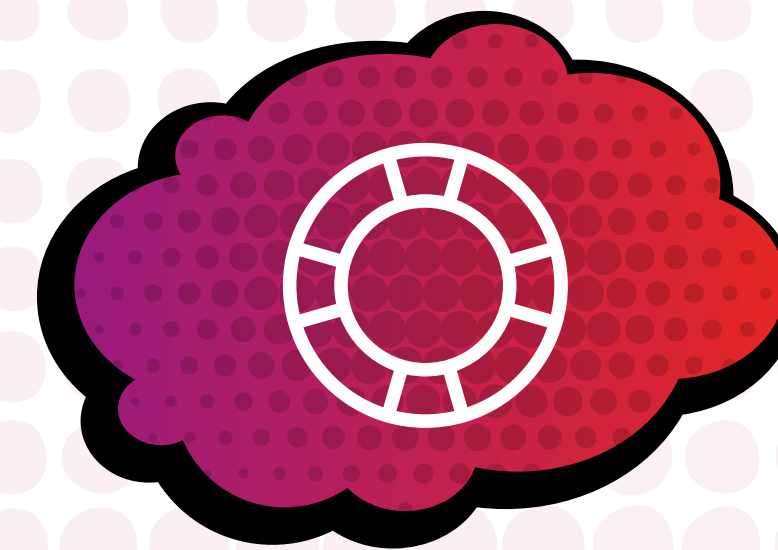
Support

30 days support call.



Launch

Technical training recommended, test/demo assets, SMB experts, Fortinet program.



1st sales

90 days objectives review and refine, marketing campaign kick off.



Follow up

Commercial follow up of first sales, sales support/post sales support.

Contact Us

Please contact the Exclusively Fortinet team for more information or support

EMAIL US



**Let's
Engage**