

Discover the Opportunities for

Growth

Engage with us to evolve and succeed
in today's new security environment



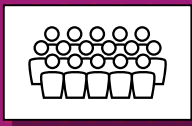
Secure remote working



The transition to remote working opens users and companies up to a myriad of security threats including malware, all forms of phishing attacks and many more.

Fortinet has identified remote worker scenarios with three primary levels of connectivity.

Remote users



Applies to most people in the company.

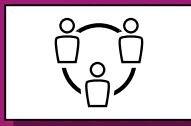


Need access to Email, Data & Applications whilst connecting remotely.

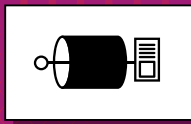


For Remote Users, a Virtual Private Network or VPN tunnel is needed to connect to the firewall back at the office. FortiGate customers already have high-performance VPN at their fingertips and can download FortiClient VPN agent for end points. The VPN client can be coupled with Fortinet's FortiToken providing additional security with two factor authentication.

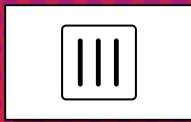
Power users



Applies to specific roles who spend extended periods of time on the corporate network.

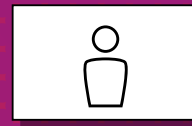


Need a consistent, secure always-on connection to the head-end firewall for multiple devices.

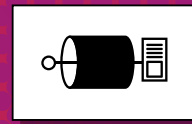


For Power Users, FortiAP can establish a secure connection back to the office and can be set up at home. While the traffic from that wi-fi connection can get the same security policies that the FortiGate provides. Wireless networks can be configured exactly as they are in the office, so that devices can be securely connected just as easily.

Super users



An executive or user with access to the most sensitive company information.



Need highest levels of security or application performance for their work.



For this user a small FortiGate will provide the highest level of security, whilst also enabling the deployment of additional hardware like FortiAP. This effectively creates a small branch office for the employee. The FortiAPs and FortiGates can be delivered straight to the user and the configuration pushed directly to the units.



To support all users

The office users are connecting to needs a VPN Concentrator. Fortinet customers have this available for free as part of the FortiOS operating system. To help manage the many VPN clients deployed, FortiClient EMS – an endpoint management system, can simplify larger deployments. For two-factor authentication the office could use a FortiAuthenticator to coordinate this across all the FortiGates in the company.

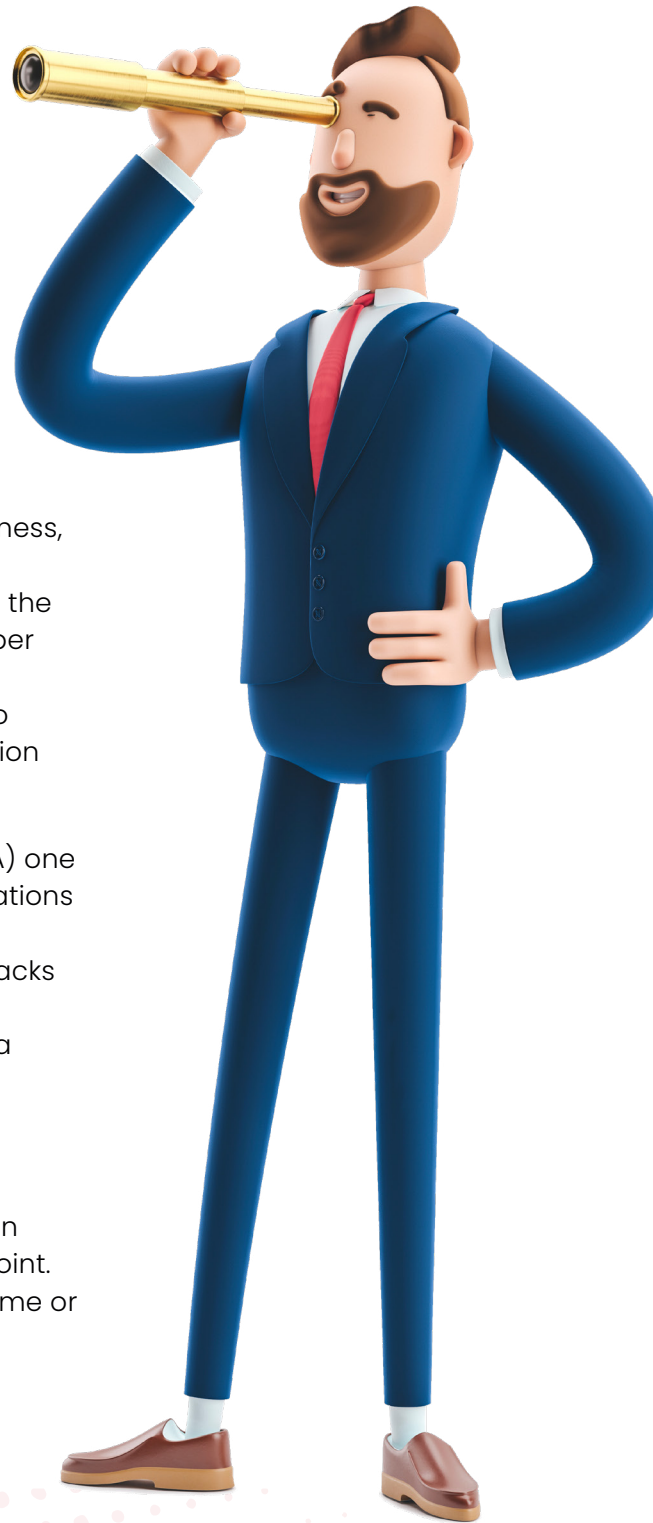


For more information about Fortinet solutions for remote working

[Click here](#)



Opportunities for Partners



Opportunities for partners

Digital acceleration is transforming how organisations do business, allowing them to remain competitive in today's market, it also impacts their ability to manage and secure their networks. As the attack surface expands, network complexity increases and cyber threats are simultaneously becoming increasingly automated and innovative. Today's organizations need a new approach to deliver the expected secure high-performing user-to-application connection.

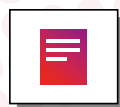
Gartner has named its cybersecurity mesh architecture (CSMA) one of the top strategic technology trends for 2022. It says organizations adopting cybersecurity mesh as part of their collaborative ecosystems will reduce financial losses from cybersecurity attacks by 90%. Gartner's insight around CSMA may sound like a new initiative, but this type of protection has existed for more than a decade through the Fortinet Security Fabric

Solution sprawl, an explosion of new edges and devices, and a work-from-anywhere workforce - coupled with the growing cybersecurity skills gap and the evolving sophistication of cyber threats - means IT teams are stretched to breaking point. Organisations are therefore turning to partners to take over some or all of their IT security infrastructure.

For partners, evolving service offerings or cloud capabilities to keep up with the changing digital landscape and diversifying their business model will perfectly position them to address the new opportunities, successfully differentiate themselves from their competitors and grow their business.



[View fabric video](#)



[Visit Fortinet blog](#)

 <p>Profitability through Technology Differentiation</p>	 <p>Business Success with Proven Credibility</p>	 <p>Long-Term, Sustained Growth</p>
<p>Fortinet's breadth of products are tightly integrated into one highly-automated, high-performing platform that spans endpoint, network and cloud, and includes tools to easily connect with adjacent technologies</p>	<p>Fortinet's innovation superiority with hundreds of patents and industry-leading threat intelligence, alongside customer ratings and independent analyst reports validates and differentiates your offerings.</p>	<p>Fortinet are 100% channel focused. And with value add and end-to-end support from Exclusive Networks you can grow productive, predictable and profitable relationships.</p>

Learn more about Fortinet's Engage Partner Program and how your organisation can benefit by joining

 Watch the Partner Program video





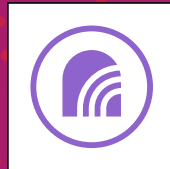


Expand your business through the Fortinet Engage Partner Program

Designed to help partners grow their business with a profitable and highly differentiated security practice, the Fortinet Engage Partner Program does this in three ways.

- 1** Fortinet's unique security solutions, built around the Fortinet Security Fabric—the industry's first and truly converged security platform—ensure profitability through technology differentiation.
- 2** Fortinet's commitment to innovation, boasting more patents than most competitors combined, and ongoing industry and customer accolades mean that your business immediately enjoys proven credibility.
- 3** Finally, Fortinet and Exclusive's sales, marketing, and executive support enable long-term sustainable growth through productive, predictable, and profitable relationships.

Diversify and differentiate yourselves

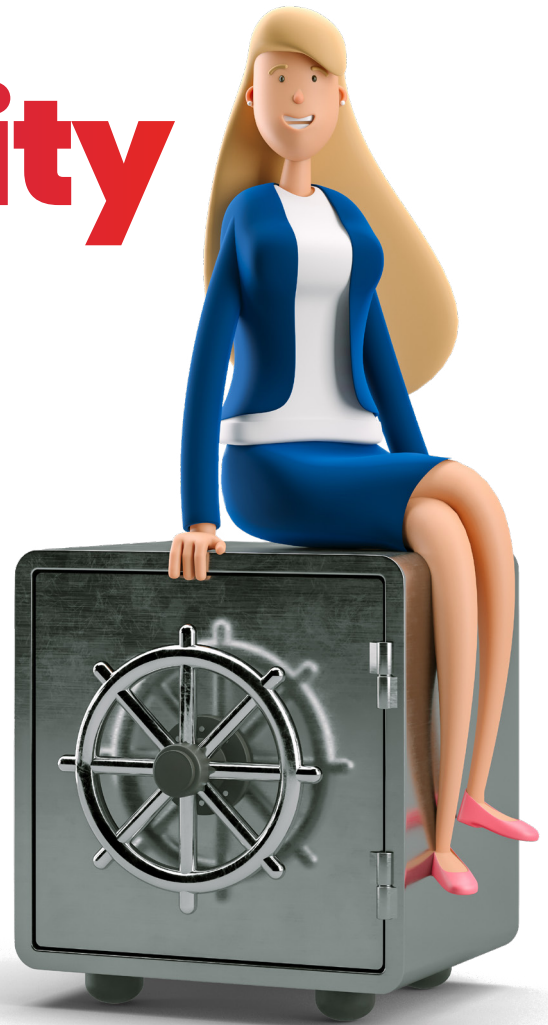
By partnering with Fortinet and Exclusive Networks, we can help you diversify – whether that's with an MSSP, Cloud Partner or Value Add Reseller business model, and you can differentiate yourselves with specialisations in key areas like:

-  SD-WAN
-  LAN Edge & SD-Branch
-  Data Centre
-  Zero Trust Access
-  Operational Technology
-  Cloud Security
-  Security Operations

The importance of Cybersecurity

Triggered by the global pandemic, the rapid transition to working from home forced businesses to scramble to support a larger remote workforce. The speed at which this was executed means that certain security measures and requirements inevitably fell by the wayside.

At the same time, cybercriminals found a new opportunity for attack with remote workers and improperly secured connections and technologies. Together, these trends created a more vulnerable environment affecting the cybersecurity defences of many organisations.



1/3

Around **1/3** companies transitioned **81-100%** of their employees to remote working

2/3

More than **2/3** companies moved **61%** or more of their workforce to a work from home environment

44%

44% admit they haven't provided cybersecurity training focused on the potential threats of working from home

68%

68% have not deployed a new antivirus solution for work-issued devices

45%

45% have not analysed the security or privacy features in the software tools considered necessary for remote working

However, IT leaders acknowledge the number of challenges of cybersecurity in the move to working from home.

55%

55% see the need to train employees on how to securely and compliantly work at home as a priority

53%

53% acknowledge that setting up work or personal devices with new software for employees to work remotely is a challenge

1/2

Over 1/2 cited the need to shift to a new, remote model of communication and/or collaboration among employees

47.5%

47.5% companies are struggling with limited IT resources to serve employees working from home

45%

More than 45% see finding the right cybersecurity tools to support home workers as a key challenge

36.6

36.6% are concerned about how to enable their staff to achieve a work/life balance



Since the shift to remote working, businesses have encountered a range of security issues.

1/5

Around 1/5 companies have faced a security breach caused unintentionally by a remote worker

24%

24% have had to spend money unexpectedly to resolve a security breach or malware

1/3

Around 1/3 admitted to using personal devices rather than company devices leaving them more vulnerable to breaches

Meet the Team



“Let’s talk about the value add Exclusive Networks offer”

Neil Brosnan,
Fortinet Business Unit Director



“Find out about Cloud Opportunities”

Charlotte Skevington,
Internal Product Specialist



“Interested in growing your Fortinet business? Let’s chat.”

Tom Usher & Rhea Skelton,
Strategic Team



“We’ll share marketing tools to help you generate leads”

Sarah Duce,
Fortinet Marketing Manager



“Let’s discuss how to build profitable managed services”

Jake Huckle, Paul Araujo &
Bryony Swanston, MSSP team



“Our services can help you scope, design and install projects to win more business”

Chris Pritchard, Technical Unit
Manager, Fortinet



“Tap into the SMB opportunity, the fastest growing sector of Fortinet’s business”

Jess Kok, Ryan Boyle & Tim Wiggins,
SMB team

