



#WeAreExclusive

SD-WAN Accelerator

In partnership with
FORTINET[®]



Agenda

- › Overview
- › Key Considerations
- › Service Blue Prints
- › Training Plans
- › Recruitment Role Descriptions
- › Service Definition
- › Go to Market Tools
 - › Datasheet
 - › Battlecard
 - › Pitch Deck
- › Marketing Guidance
- › Exclusive Networks Services



Overview

Our SDWAN Accelerator process is designed to help kickstart your SDWAN product launch. Our structured approach helps you consider all the factors needed to develop a profitable SD-WAN service for your MSP and highlight the key considerations and decisions you need to make along the way.



Business Case

Identify your key stakeholders and sponsors
Profile your customers and identify likely targets



Service Design

Agree MSP infrastructure and customer devices
Agree the scope for managed services



Review Current Systems

Do monitoring, ticketing and customer portals
need upgrades or investment to support SDWAN?



Build Training Plans

Undertake a skills assessment of your team and
build a training plan for Operations and Sales



Identify Costs

Identify all burden costs for the MSP and any Cost of
Sales which should be in the commercial model



Build Contracts

Agree target margins and charges for Setup and
ongoing managed services; create SLAs and terms



Build Sales Materials

Create Customer Pitch Decks, Datasheets and
Battlecards. Build Website landing page content



Marketing Plan

Plan your 30-60-90 day Marketing Launch and
social media content
Plan your mailing campaigns and record your
webinar content



#WeAreExclusive

In partnership with
FORTINET[®]

Key Considerations



Key Considerations

The SDWAN accelerator program is designed to provide a springboard for MSPs to bring a managed SDWAN service to market. Here we offer a structured approach which aims to remove a number of the typical roadblocks which MSPs face when pulling together a new service offering.

We'll cover customers, technology, people, systems, time, service descriptions, sales and marketing.

Along the way we will highlight the key areas you need to consider when bringing this service to market. Some you will know, some will be a good prompt to go an do some internal discovery to come out with the answers.

All of the advice around the specific technology to use is taken from the Fortinet Reference Architecture Guide for SDWAN which we encourage you to read. It's available on request from your Fortinet Account Manager.



Why SD-WAN? Why Now?

What are your drivers for creating and selling an SD-WAN Service?

- › Provide an additional Revenue Stream
- › Protect your customer base
- › Stay competitive in the market
- › Increase revenues from standard network access services
- › Simply to control the conversation with the client

It's important to understand WHY we want to bring SD-WAN to market as it will guide the amount of time, effort, investment, staff resources and everything else that you are prepared to invest in the development of this service



Why SD-WAN? Why Now?

Next you need to identify and get a size of the real opportunity within your customer base for SD-WAN. It's always easier to sell to existing clients than attain new ones.

Don't just take the market view for SD-WAN in Billions of dollars and look to close a percentage of that. You need to be realistic and review your current clients.

- › What clients do you have who would be interested in SD-WAN?
- › How many of those are at a stage in their contract where they could upgrade?
- › Track the renewal dates for customers whose contracts are due to renew in the next 6 – 12 months. Are they interested in SD-WAN, can we start campaigning to them now and gauging interest?
- › What is the annual / total contract value for each client? What is the margin?
- › Notionally how much do we expect to charge for Managed SD-WAN for each of these clients? At what margin levels?
- › Realistically, how many of those clients do you think you can convert to SD-WAN?

It's important to understand WHY we want to bring SD-WAN to market as it will guide the amount of time, effort, investment, staff resources and everything else that you are prepared to invest in the development of this service



Identify Stakeholders

New product launches need involvement from multiple people across the MSP organisation and we would encourage you to recruit as many of these stakeholders early on in the process. They will not all be needed for the entire time but if we can at least identify these key individuals it will smooth the launch process.

- › Commercial Finance
- › Delivery Lead
- › Field Engineering Lead
- › Legal
- › Marketing Lead
- › Operational Lead
- › Product Manager
- › Project Manager
- › Sales Representative
- › Support Desk Lead
- › Systems and Development Lead



Choose your SD-WAN Model

Choosing your overlay model is key to understanding operational and commercial factors, as well the service revenue opportunities each model brings. The first major decision factors is whether or not SD-WAN is an overlay upon your existing MPLS core network service? If so, do you want to maintain the traditional centralized Internet breakout model. Typically, we see three main deployment models;

SDWAN Overlay for MPLS

Existing MPLS Core is used to provide the underlying connectivity for Private and Internet Traffic.

Branches are equipped with NGFW and SD-WAN capabilities.

Centralised Firewalls are used for Internet Breakout, Content Filtering and Protection Services.

Application Priority policies are applied centrally at the Internet access point.

Security Policies are applied and enforced centrally at the Internet access point.

SDWAN Overlay with Hybrid Direct Internet

Existing MPLS Core is used to provide the underlying connectivity for Private and Internet Traffic.

Internet Access is also available at selected Branch sites

Branches are equipped with NGFW and SD-WAN capabilities

Distributed Firewalls are used for Internet Breakout, Content Filtering and Protection Services.

Application Priority policies are applied **at each** Internet access point.

Security Policies are applied and enforced **at each** Internet access point.

Direct Internet Access Only

Internet Access is provided to all Branches

Branches are equipped with NGFW and SD-WAN capabilities

Distributed Firewalls are used for Internet Breakout, Content Filtering and Protection Services.

Application Priority policies are applied **at each** Internet access point.

Security Policies are applied and enforced **at each** Internet access point.



How Do You Plan to Monitor and Report?

A core aspect of the SDWAN service is providing insight for your clients on how the service is supporting their business. Real-time and scheduled reporting requires infrastructure which can be deployed in multi-tenant and customer-dedicated models.

Multi-Tenant Model

FortiManager is deployed in a centralized location, usually the MSP Datacentre or a Cloud Service. All customer devices will be managed from here.

FortiAnalyzer is deployed centrally collecting data from customer appliances. Usually within the MSP Datacentre or a Public Cloud Service. Administrative Domains (ADOMS) are used to separate customers, devices and enabling delegated administration.

Platform infrastructure and cost scaling impact the MSP directly whilst being recovered from the clients indirectly.

Multi-Tenant Model AND Customer Dedicated

FortiManager is deployed in a centralized location, usually the MSP Datacentre or a Cloud Service. All customer devices will be managed from here. For large clients a dedicated FortiManager deployment could be considered.

FortiAnalyzer is deployed on a per customer basis. Typically this will be run on a virtual machine in the MSP Datacentre or a Public Cloud service.

FortiManager infrastructure and cost scale will directly impact the MSP whilst being recovered from the clients indirectly. FortiAnalyzer become Cost of Sale.

Custom Experience

FortiManager and **FortiAnalyzer** support the use of API access enabling data and configuration to be accessible to the client within an MSP's own portal.

Here the MSP can fully decide which pieces of information to surface to the client, what changes can be made and control the entire user experience.

The two primary choices here are 'buy' and 'build'. Where the MSP has access to Dev teams and an existing customer portal, there is the option to integrate Fortinet technologies. Alternatively they can purchase **FortiPortal** which provides an off-the-shelf customer reporting and management portal experience.



Does the Customer have Access to Make Changes?

Granting customer access to the SDWAN configuration elements is a popular consideration. Customers sometimes require read-only access to the configuration for compliance purposes. In other cases, MSPs may offer a co-managed service where clients are able to make changes to a subset of configuration items.

Fully Managed by MSP

Customer Profile: Organisations with limited or no networking skills in-house. Clients who want the MSP to take full responsibility for the service performance and security.

FortiManager enables the client to review reports and current activity.

Role Based Access is used to decide which devices they can view.

Application Priority policies are viewable by the client.

Security Policies are viewable by the client.

Standard Reports are available to the client.

Custom Reports are not available to the client.

Co-Managed with MSP

Customer Profile: Organisations with Fortinet skills in-house. Clients who have the capability to manage day-to-day policy changes but rely on their MSP to maintain ownership of the overall service performance and security.

FortiManager enables client to review reports, activity, make **limited** changes

Role Based Access is used to decide which devices and elements they can change

Application Priority policies are viewable by the client and a **subset of elements are changeable**

Security Policies are viewable by the client and a **subset of elements are changeable**

Standard Reports are available to the client

Custom Reports are not available to the client

Custom Experience

FortiManager access is not provided to the client. All access to any information regarding the SDWAN service is centralised within the MSP's own portal. This requires API integration between the FortiManager, FortiAnalyzer and the MSP portal.

Here the MSP decides which information are surfaced to the client and which elements are available for Moves, Adds and Changes.

In addition to the MSP's portal, standard elements of the Fortinet SD WAN platform can still be used to provide information to the client.

Standard Reports may still be run and emailed to the client

Custom Reports may still be run and emailed to the client



Systems Integration

One of the key considerations you need to make is to understand how your Managed SD-WAN service and appliances will interact with your Alerting, Monitoring, Management, Reporting and Billing systems.

- ▶ Do the existing systems require upgrades, investment, licensing?
- ▶ Do you need new platforms or systems?
- ▶ Have you looked at Fortinet's offerings such as Forti-Portal, Forti-Monitor?
- ▶ Are they able to effectively monitor and report on Fortinet SD-WAN?
- ▶ How do you plan to re-coup the costs of any investment here? Cost of sale to the customer?

Although we can't provide you with all the answers here, this is a set of questions which you need to consider internally as part of your operational thoughts for SD-WAN. Although Fortinet SDWAN is based on the Fortigate NGFW, the reporting and analytics on a per application basis are far more granular and detailed. So if you have an effective way to monitor Fortigate's today, don't assume that this will do the job for SDWAN as well.

We can absolutely help when it comes to showcasing how Forti-Portal and Forti-Monitor would work here as well as engaging a Fortinet SE if you want to consider a custom integration using the Fortinet API





#WeAreExclusive

In partnership with
FORTINET®

Service Blueprints



Service Bundles

Providing standardised offers to your customers makes the sales process simpler. Recommended configurations assures clients that you have ready-made, proven solutions to their network challenges.

	Branch Office	Small Office	Medium Office	Large Office
Size	Basic guidance around number of people or site connectivity speed to help with selecting the scale of the device 1 – 25 People Site Connectivity Up to 80Mbps	10 – 50 People Site Connectivity Up to 250Mbps	50 – 150 People Site Connectivity Up to 500Mbps	150 – 500 People Site Connectivity Up to 1Gbps
Device	With UTP licence applied, the device here should be appropriate for the size of site / bandwidth Fortigate FG-30E	Fortigate FG-40F	Fortigate FG-60F	Fortigate FG-60F or FG-100F

At critical branches, dual firewalls and switching is recommended

You can have as many bundles as you like. It's recommended to keep to a small number. These are four of the most common deployment scenarios.

MSSP Benefits:

- › Faster sales quotes
- › Standardised orders from distribution
- › Faster to deploy with standardised configurations
- › Easy for all levels of support within your organisation

Please note that all configurations are suggested examples. Be sure to speak with your Fortinet Account Manager and Solutions Engineer to ensure that you create configuration bundles to suit your specific requirements.

IMPORTANT: Enabling multiple UTM features impacts resources on the Fortigate appliance. Ensure you work with the Fortinet team to size your appliances correctly for the bandwidth and intended UTM feature set.



Pricing Model Guidance

Once you've standardised the hardware configurations in each bundle with your Fortinet SE. You can now create standardised pricing options for each bundle. These fixed price configurations will decrease Pre-sales burden and increase Sales independence to provide quick quotes.

	CAPEX Model <i>Customer purchases the hardware</i>	OPEX MODEL <i>Customer rents a full service</i>
Costs	What do you need to consider as an MSP for providing either a CAPEX or OPEX version of Managed SDWAN? Staff costs for Level 1,2,3 Support Hosting costs for centralised FortiManager	Staff costs for Level 1,2,3 Support Hosting costs for centralised FortiManager Hardware and UTM licence costs (per bundle)
Billable Items	<p>What are the billable line items to cover the cost and provide margin on the service?</p> <p>ONE OFF</p> <ul style="list-style-type: none"> • SDWAN Assessment (pre-sale) • SDWAN Core Setup Fee • Branch Setup Fee (per site) • Hardware Purchase and 3 Years UTM <p>RECURRING</p> <ul style="list-style-type: none"> • Monthly SDWAN Service Charge <ul style="list-style-type: none"> • Management Costs • Contribution to centralised FortiManager 	<p>ONE OFF</p> <ul style="list-style-type: none"> • SDWAN Assessment (pre-sale) • SDWAN Setup Fee • Setup Fee (per site) <p>RECURRING</p> <p>Monthly SDWAN Service Charge</p> <ul style="list-style-type: none"> • Amortised Hardware (contract term) • Amortised UTM (<i>contract term</i>) • Management Costs • Contribution to centralised FortiManager

Standardised Pricing

Pre-Sales spend more time looking at customer outcomes and less time on pricing exercises.

Sales teams can rapidly quote a client based on the number of branches and which bundle each branch requires.

Please note that all configurations are suggested examples. Be sure to speak with your Fortinet Account Manager and Solutions Engineer to ensure that you create configuration bundles to suit your specific requirements.



#WeAreExclusive

In partnership with
FORTINET®

Training Plans



Training Plans

Ensuring that your MSP teams are fully trained is a key stage in successfully selling, deploying and managing your Secure SD-WAN solution.

Fortinet have a full range of training options and certification levels for their partners which covers the entire spectrum of their products and services.

Fast Track Workshops

The Fast Track Program is not targeted at certification. It is not a demo. It implements an active learning approach, using hands-on labs, real-life use-cases and lectures to provide experience and build competence. You will learn how Fortinet products and solutions work and perform by actually working with them.

Each workshop focuses on a specific product, technology or benefit of using Fortinet within your MSP and typically takes around four hours.

Fortinet NSE Certification

Formal certified training options are specifically designed to build deep knowledge and confidence in Fortinet technologies. There are courses for every person involved in the Sales, Planning, Delivery, Support and ongoing Management of SD-WAN within your MSP from Awareness level through to Expert.



We have identified the key courses and programs which will put you in a great position to start offering Secure SD-WAN.



Fast Track Schedule

Fortinet provide free Fast Track training workshops to their partners. These workshops are designed for attendees of any experience level to get an overview of how the product or service works and how it can benefit their MSP business.

Recommended workshops for a Managed SD-WAN Service

- › Getting Started With the FortiGate Firewall
- › Fortifying the Enterprise Network (NGFW Solution)
- › Constructing a Secure SD-WAN Architecture
- › Reducing Complexity of Operations with the Fabric Management Center
- › Simplify SOC Operations for the Security Fabric with FortiAnalyser
- › SD-Branch: Securing Your Ethernet Switching Infrastructure with FortiSwitch, FortiAP and FortiLink


Add in here that EXN can run partner specific Fast Tracks on request





SD-WAN Formal Certification Plan

Here we outline the key job roles in your organization and the recommended training plan for each person.

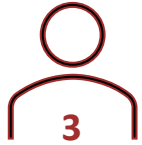



Sales & Pre-Sales

Scope, Assess, Engage, Discuss

NSE 3

- 2 Days Online Training

Initial Headcount 

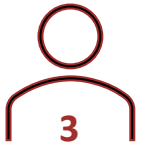



Service Desk

24x7 Monitoring
Adds Moves and Changes
Incident triage

NSE 4

- 3 Days Forti Security
- 2 Days Forti Infrastructure

Initial Headcount 



SD-WAN Engineer

Deploy and manage
Standard Customer design and implementation
Build maintenance plans

NSE 4

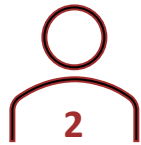
- 3 Days Forti Security
- 2 Days Forti Infrastructure


Plus NSE 5

- 3 Days Forti Manager
- 1 Day Forti Analyser

Plus SD-WAN Specialism

- 2 Days SD-WAN

Initial Headcount 



Specialist

Advanced Customer design & implementation
Core Services design & implementation

NSE 4

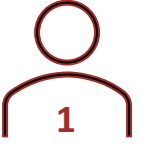
- 3 Days Forti Security
- 2 Days Forti Infrastructure

Plus NSE 5

- 3 Days Forti Manager
- 1 Day Forti Analyser

Plus NSE 7

- 2 Days SD-WAN


Initial Headcount 





Skills Matrix

Here we outline the key job roles in your organization and the recommended training plan for each person.

Name	Team	NGFW	UTM	SD WAN	Forti Portal	Forti Manager	Forti Analyzer	Req. Training	#Days	Cost
A Sample	Sales									
A Sample	Sales									
A Sample	Pre-Sales									
A Sample	Pre-Sales									
A Sample	Service Desk									
A Sample	Service Desk									
A Sample	Service Desk									
A Sample	Service Desk									
A Sample	Core Network									
A Sample	Core Network									
A Sample	Core Network									
A Sample	Core Network									
A Sample	Product Management									

 Limited / no experience of the technology

 Able to support an existing configuration

 Able to plan, deploy and manage a configuration



An editable Excel version of this table is in your Accelerator Pack



#WeAreExclusive

In partnership with
FORTINET®

Recruitment Role Descriptions



Recruitment and Role Descriptions

As well as your comprehensive training plan for the existing team, you might need to bring in some experienced technical team members to accelerate your service offerings around SD-WAN.

One of the key tasks here is to quickly get together role descriptions for the people you need to hire. Most MSP's will already have an approach to hiring Sales and Marketing staff members so we've focused on the technical team members you might want to hire.

Here we've provided descriptions for two technical roles. A Security Engineer and a Senior Security Engineer. You'll notice that we've called them both 'Security' engineers. That's because the Fortigate NGFW appliance is at the heart of the SD-WAN solutions so we believe that this is the firm foundation that we need in the candidates. On top of that we can then look for those people with SDWAN experience.

Security Engineer (SDWAN)

This position looks for a candidate who has solid experience in managing and maintaining secure network infrastructure at the core and on customer premise. They are able to optimally manage existing deployments and troubleshoot, recommend areas of improvement.

Senior Security Engineer (Fortinet SDWAN)

The senior engineer role is an escalation path for the standard engineer. Here we are looking for candidates who can do everything the standard engineer can do but also plan, design and implement new infrastructure models at the core and on customer premise.



Security Engineer (Fortinet SDWAN)

Role Description:

This position looks for a candidate who has solid experience in managing and maintaining secure network infrastructure at the core and on customer premise. They are able to optimally manage existing deployments and troubleshoot, recommend areas of improvement.

Experience:

- ▶ Advanced Security/Firewall management background in working for large enterprise
- ▶ In-depth knowledge and proven expert proficiency in configuring and maintaining of large enterprise firewalls such as Fortinet UTMs
- ▶ Support of firewall technologies includes Fortinet firewalls. Administration, troubleshooting and engineering background is required.
- ▶ Must have experience analysing and implementing firewall rules on FortiGate security devices.
- ▶ Demonstrated ability to analyse network traffic flows to reverse-engineer the required firewall ports and rules to allow secure access of applications
- ▶ Strong technical ability to troubleshoot firewall problems in a large enterprise involving complex network application flows between multiple hosts spanning multiple firewalls/security zones and different geographic locations
- ▶ Proven hands-on experience with firewalls and a comprehensive knowledge of IP networking and network security including Intrusion Detection, DMZ, encryption, IPSec, PKI, VPNs, MPLS/VPN, Site to Site VPN tunnels, SSL/VPN, proxy services, and DNS
- ▶ Experience with routers and switches, and a good understanding of IP sub netting and routing such OSPF and BGP
- ▶ Must have strong analytical and problem -solving skills and a solid understanding of how to troubleshoot connectivity and performance issues that involve firewalls, network, and applications

Required Skills:

- ▶ Min 3 years of experience in an IT role & 2 years in a Network Engineering role
- ▶ Min 1 years of experience working with FortiGate firewall technologies
- ▶ Min 1 year of experience running mid to large scale network implementations and implementations of firewall technologies both on the edge and internally
- ▶ Min 1 years of experience running small to mid scale SDWAN implementations
- ▶ Min 1 year of experience with some of the following: FortiOS, Juniper OS, Cisco IOS, Microsoft Windows Server

Desired Skills:

- ▶ Working experience of SDWAN technologies and principles
- ▶ Working in a changeable environment
- ▶ Good communication and writing skills (customers, management, and peers)
- ▶ Detail and Process oriented person working in ITIL organisation
- ▶ Good documentation skills

Education:

Windows or Unix Technology certification a plus (MCSE, Redhat Certified etc.)



Senior Security Engineer (Fortinet SDWAN)

Role Description:

As a senior member of the Security Services, this role will be responsible design, product selection and recommendation, implementing and managing security devices for customer and core networking projects. This position requires excellent security/firewall management background in large organization or MSP. The position is a hands-on role to design and implement the security using Fortinet UTM.

Experience:

- ▶ Advanced Security/Firewall management background in working for large enterprise
- ▶ In-depth knowledge and proven expert proficiency in configuring and maintaining of large enterprise firewalls such as Fortinet UTMs
- ▶ Support of firewall technologies includes Fortinet firewalls. Administration, troubleshooting and engineering background is required.
- ▶ Must have experience analysing and implementing firewall rules on FortiGate security devices.
- ▶ Demonstrated ability to analyse network traffic flows to reverse-engineer the required firewall ports and rules to allow secure access of applications
- ▶ Strong technical ability to troubleshoot firewall problems in a large enterprise involving complex network application flows between multiple hosts spanning multiple firewalls/security zones and different geographic locations
- ▶ Proven hands-on experience with firewalls and a comprehensive knowledge of IP networking and network security including Intrusion Detection, DMZ, encryption, IPSec, PKI, VPNs, MPLS/VPN, Site to Site VPN tunnels, SSL/VPN, proxy services, and DNS
- ▶ Experience with routers and switches, and a good understanding of IP sub netting and routing such OSPF and BGP
- ▶ Must have strong analytical and problem -solving skills and a solid understanding of how to troubleshoot connectivity and performance issues that involve firewalls, network, and applications

Required Skills:

- ▶ Min 5 years of experience in an IT role & 2 years in a Network Engineering role
- ▶ Min 3 years of experience working with FortiGate firewall technologies
- ▶ Min 2 years of experience running mid to large scale network implementations and implementations of firewall technologies both on the edge and internally
- ▶ Min 2 years of experience running small to mid scale SDWAN implementations
- ▶ Min 3 years of experience with some of the following: FortiOS, Juniper OS, Cisco IOS, Microsoft Windows Server

Desired Skills:

- ▶ Working experience of SDWAN technologies and principles
- ▶ Working in a changeable environment
- ▶ Good communication and writing skills (customers, management, and peers)
- ▶ Detail and Process oriented person working in ITIL organisation
- ▶ Good documentation skills

Education:

Windows or Unix Technology certification a plus (MCSE, Redhat Certified etc.)



#WeAreExclusive

In partnership with
FORTINET®

Service Definitions



SD-WAN Service Definition Matrix

Key considerations when building your service definition matrix

- ✓ Ensure all stakeholders are involved in the process across product management, operations, technical support, service delivery, pre-sales and sales.
- ✓ Take the time to decide how many levels of service will be published initially at point of launch and then potentially later subject to demand. Starting with one service offering is not uncommon and in most cases makes a lot of sense if the target audience has been well profiled. You should aim to have no more than three levels to reduce complexity of positioning and service delivery.
- ✓ Ensure the levels of service align to the target customer profiles (As per the sponsorship and profiling phase), taking into account the required simplicity or complexity with how the customer will consume the service and engage with you as their provider.
- ✓ Build in frequent levels of engagement on upper levels of service such as account reviews, service reviews, reporting analysis workshops) to ensure customer satisfaction and enable you to regularly demonstrate added value.

EXCLUSIVE NETWORKS **SD-WAN**
Service Definition Matrix

	Standard	Enhanced
Management and Support Services		
Support SLA	24x7 – 1 hour response	24x7 – 1 Hour response
Support Type	Proactive Management	Proactive Management
Incidents/Events	10 incidents per month	Unlimited
Change Request SLA	Business Hours 24 hour notice	24x7 4 Hour notice
MSSP Managed	Fully Managed	Fully Managed / Co-Managed
Customer Management	Read Only	Restricted Changes
Network Services		
DSL	Supported	Supported
Ethernet(UTP or Fibre) up to 10Gb	Supported	Supported
4G/5G Capable	Supported	Supported
Security Services		
Firewall	o	o
SSL VPN (Client and Site to Site)	o	o
URL Filtering	o	o
Web Content Filter	o	o
Intrusion Prevention	o	o
Anti-Botnet	o	o
Anti-Spam	o	o
IP Domain Reputation	o	o
SSL Inspection	o	o
Data Leakage Protection	o	o
Policy Creation	Standard Policies	Bespoke Policies
Application Services		
Detect and prioritise Applications	Up to 100 Applications	All applications (currently over 3,000)
WAN Path Control and Remediation	o	o
Cloud Optimisation for IaaS and SaaS	o	o
Reporting Services		
Monthly Reporting	Standard Template Reports	Bespoke Reporting



An editable Excel version of this document is in your Accelerator Pack



#WeAreExclusive

In partnership with
FORTINET®

Go to Market Tools



Service Overview: Value Proposition

Products and Services

Fortinet Fortigate Appliances, MSP Partners' vertical experience and expertise

Gain Creators

Flexible adaptable networking, ubiquitous security, SaaS optimisation, application performance, support digital ways of working and digital transformation efforts, support rapid deployment and pop-up locations.

Pain Relievers

Reduce business risk (security/downtime), reduce business costs, improved speed of service for customers, get connectivity to sites faster

Proposition Suggestion

"Your teams are using new digital ways of working to provide a personal and unique experience to your customers. They use multiple devices, working on mobile or tablet devices and spending less time sat at fixed workstations. Staff are working remotely and business data has moved to cloud-based SaaS applications. There is more dependence on reliable Internet access than ever before. Has your network evolved to keep up?"



Service Overview: Executive Summary

Customer Challenges

Businesses are consistently looking for ways to decrease costs across the IT estate. At the same time, security, compliance, application performance and availability are top of mind on the business risk register.

Businesses are looking to deliver digital transformation initiatives and improve productivity and communication between teams and enable flexible working. These changes all impact where people work, where data is stored and the overall user experience.

Wi-Fi and Internet access are now mission-critical pieces of infrastructure, where it once was a convenience.

The business needs a modern network infrastructure which becomes the secure, flexible foundation to power the next stage of growth.



Service Overview: Executive Summary

Secure SD-WAN Service

Our Secure SD-WAN service has been designed to ensure that your business connectivity is always available and prioritises the application performance. It ensures that the right applications have the right priority on the network, ensuring a great experience for internal and guest users. Whether they're connected at the desktop or working on WIFI using tablet or mobile devices, our SD-WAN service keeps everybody secure and productive. SD-WAN adapts over time as needs change.

Our service is built on Gartner Magic Quadrant leading technology from Fortinet, combined with the partners' experience and expertise of delivering Wide Area Networks. SD-WAN helps tackle three main challenges with current WAN solutions.



Service Overview: Managed SD-WAN Service

SECURITY

Traditional Wide Area Networks are built on MPLS and are typically designed to allow every office to talk to every other office for maximum communication flow. Internet Access is usually centralised through a single set of security devices and there is only one secure way in and out of the network. This approach has great benefits but also increases the risk of spreading dangerous malware and viruses throughout the organisation. A machine infected with a virus in one office can soon be replicated across the entire organisation and the security devices can be powerless to stop it.



SD-WAN is different. Every office is fully equipped with a Next Generation Firewall (NGFW). This means that every location has full security screening for any data going into or out from that location. Whether that's out to the Internet or internal to the organisation, security is applied to every activity which takes place. This reduces your business risk of data breaches.



Service Overview: Managed SD-WAN Service

APPLICATION PERFORMANCE

Traditional Wide Area Networks are manually optimised for traffic flow by classifying business applications into a couple of categories e.g. 'Voice', 'Video' and 'Internet'. Policies are applied to these traffic types which determine how much priority one should get over the other in the event that the network is busy.

The challenge is that, as more applications have moved to the Cloud, more and more traffic just looks like "Internet Browsing" to these traditional systems. They struggle to differentiate mission critical access to services like Office 365 and Salesforce as these are all just "Internet Applications".



SD-WAN is different. We can detect over 3,000 applications and dynamically optimise the network to ensure your team are getting the very best experience. We have a full Cloud Application database which is continually updated to help us detect mission critical applications running in the Cloud and apply the appropriate experience for your team. This technology ensures everyone in your team is empowered to be fully productive.



Service Overview: Managed SD-WAN Service

INSIGHT

Traditional Wide Area Networks provide limited information when it comes to applications and gaining deep insight and building analytics is challenging. Typically this is achieved by exporting data to a 3rd party system for reporting.

The challenge here is that customers grow and change all the time. Their needs from a network develop as the business evolves and new applications are deployed. Without real-time insight into network performance, it can be difficult to assess the consumption by application. In addition, identifying unapproved applications is not possible without additional systems being deployed.



SD-WAN is different. The traffic patterns for all locations are reported centrally into a single dashboard. At a glance we can identify the network usage at every location and then dig down to see which applications are using how much of the bandwidth. We can control monitor the growth of applications over time, identify anomalies and immediately identify and block unapproved applications.

We can monitor the devices for compliance to our baseline security policy and ensure every location adheres to the standards which we have set.



Service Overview: Key Features & Benefits

Feature	Benefit
Security	Next Generation Firewall at every location protects all users from internal and external threats
Application Intelligence	Over 3000 apps can be detected and prioritised on the network automatically according to your needs
4G/5G Rapid Deployment	4G and 5G connectivity enables you to get new locations up and running whilst the fixed line connectivity is being installed. Perfect for pop-up retail outlets.
Network Optimisation	Use those "Failover" circuits. Business data can be sent across primary and secondary connections maximising your investment in the current site connectivity. In the event of a line failure, our application intelligence will ensure key applications have priority.
Centralised Management	A single set of security policies and device health standards is managed in one location for all devices. Reduces the risks of downtime and security breaches
Analytics and Reporting	Regular monthly reports are published so that you can see how your network is supporting your business goals. This can help you plan for new applications, technology deployments or simply right-sizing the connectivity for your next location.
Optimise your SaaS Apps	Internet traffic for SaaS applications can be used directly from each location. Each location has a Next Generation Security Firewall (NGFW), we can optimise their experience for SaaS apps by connecting the site directly to the Internet. Reduce contention on the WAN without compromising security.
Managed Service Flexibility	SD-WAN is available as a fully managed and monitored service 24x7x365 or with co-management enabling you to make changes when you need.



#WeAreExclusive

In partnership with
FORTINET®

Go to Market Data Sheet



SD-WAN Data Sheet

Our Managed SD-WAN Service ensures that your business network keeps everybody safe and productive regardless of where they are. It adapts to your business changes and continually prioritises business data so that everybody has an amazing experience.

Security

Every office is fully equipped with a Next Generation Firewall (NGFW). This means that every location has full security screening for any data going into or out from that location. Whether that's out to the Internet or internal to the organisation, security is applied to every activity which takes place. This reduces your risk of data breaches.

Centralised Management

A single set of security policies and device compliance standards is managed in one location for all devices. This standardisation means every device is kept up to date, the configuration is backed up and has an identical security policy. Reduces the risks of downtime and security breaches.

Flexibility

We can detect over 3,000 applications and dynamically optimise the network all day every day to ensure that your team are getting the very best experience. This technology ensures everyone in your team is empowered to be fully productive throughout their working day.

Optimise your SaaS apps

Internet traffic for SaaS applications can be used directly from each location rather than sending all Internet traffic through once central pair of security devices. Each location has a Next Generation Security Firewall (NGFW) so we can optimise their experience for SaaS applications by connecting the site directly to the Internet. Reduce contention on the WAN without compromising security.

Analytics and Reporting

Regular monthly reports are published so that you can see how your network is supporting your team's productivity. This can help you plan for new applications, technology deployments or simply right-sizing the connectivity for your next location.



Business Benefits

Security

Next Generation Firewalls at every location protects all users from internal and external threats. Prevent the spread of malware across your internal organisation network. Endpoint protection brings advanced security to desktop and mobile devices.

Application Intelligence

Over 3000 applications can be detected and prioritised on the network automatically according to your needs.

Centralised Management

A single set of security policies and device health standards is managed in one location for all devices. Reduces the risks of downtime and breaches

Network Optimisation

Use those "Failover" circuits. Business data can be sent across primary and secondary connections maximising your investment in the current connectivity.

4G/5G Rapid Deployment

Supports 4G and 5G connectivity enabling you to get your new location up and running straight away whilst the fixed line connectivity is being installed.

Application Intelligence

Dynamic Traffic Prioritisation

Detect and prioritise over 3,000 applications in real-time across the entire network. Ensure the network is optimised for amazing application experiences for everyone.

Route SaaS Apps directly to the Internet

Now that every location has a Next Generation Firewall, we can safely connect to the Internet and route SaaS traffic directly instead of bringing everything back to a central location.

Standardised Configuration

Our centralised management standardises the application performance targets right across the network all from a single pane of glass.

Network Security

Enhanced Security

Security needs to be as close to your users as possible. By adding SD-WAN appliances to every location, the Next Generation Firewall capabilities will protect your teams from internal and external threats.

Endpoint Protection

Brings security right to your user so they are protected, wherever they are working. Protects each computer and mobile device from virus and malware attacks while enabling secure web browsing.

Insights and Analytics

Identify risks, security threats and shadow IT applications within your organisation. Take immediate action to secure your business data.



#WeAreExclusive

In partnership with
FORTINET®

Go to Market Battlecard



SD-WAN Battlecard

What is it?

Secure SD-WAN is a fully managed service from [PARTNER]. We are using Fortinet Next Generation Firewalls on-site in place of the traditional router. This provides a router, a security appliance and the intelligence to detect over 3,000 different business applications. We can then apply a single security and application acceleration policy across the whole organisation. Every location has faster access to their business apps and is more secure than ever before.

Elevator Pitch

Your teams are using new digital ways of working to provide a personal and unique experience to your customers. They use multiple devices, working on mobile or tablet devices and spending less time sat at fixed workstations. Staff are working remotely and business data has moved to cloud-based SaaS applications. There is more dependence on reliable Internet access than ever before. Has your network evolved to keep up?

LISTEN OUT FOR CUSTOMERS WHO:

- Are growing rapidly due to success, mergers or acquisitions
- Are in the hospitality and retail sectors where controlling Internet access performance is critical
- Are moving more workloads to the cloud and need to guarantee performance and security
- Are rolling out new VoIP or Unified Communications Solutions and want to guarantee performance
- Are concerned about unauthorised applications taking up bandwidth or causing security risks

Buyer Engagement

It's best to get buy-in for SD-WAN from business decision makers to start rather than technical managers or procurement teams. SD-WAN supports business change initiatives such as digital transformation and removing security/compliance issues from business risk registers.

THE TECHNICAL BUYER

The key points to emphasise are all around how we make life easier for the tech team. Reducing the risk of data breach by securing each location. Optimising network bandwidth to reduce "slow" applications. Identify unapproved applications and block them quickly. Get new sites up and running quickly with 4G/5G solutions. They benefit from high levels of resilience network availability.

THE BUSINESS DECISION MAKER

It's all about controlling costs and reducing risk. We have fixed price bundles. The solutions minimises network downtime and improves application performance for all internal and external customers. We provide performance on demand, keep all their apps working quickly and provide a secure flexible foundation for the business to grow.



SD-WAN Battlecard

Traditional Competitive Vendors

The standard range of Next Generation Firewall (NGFW) vendors all play here as well as some modern “born in the cloud” vendors. It’s key to position Fortinet as a leader not just in WAN Edge but also NGFW and Secure Remote Access. Typical competition would be Cisco (Viptella), Meraki and Silverpeak.

Long-standing providers of security appliances such as Cisco and Meraki are still offering siloed solutions; a dedicated firewall appliance which then needs a number of additional solutions to bring capabilities such as IDS/IPS, Anti-Malware or Web Filtering. **Only Fortinet offers a complete offering.**



© Gartner 2020 Magic Quadrant for WAN Edge

Non-Traditional Competitive Vendors

Secure Access, Secure Edge (SASE) providers have predominantly been moving away from hardware-based solutions. This new set of providers offer services using cloud-hosted platforms like Zscaler and Cloudflare. The most realistic competitor here is Zscaler. They are the leader in Secure Web Gateways hosted in the public cloud and have a very comprehensive set of features to rival our offering with Fortinet. The key things to know are; A client would need to take Zscaler’s most expensive package to get all the required features; MSP’s report application performance issues as every piece of data is sent to the Cloud for inspection; Zscaler works well in an entirely remote workforce but is not a good branch office solution.

Summary

A number of these “born in the cloud” offerings provide a single point of service which is included in the overall portfolio we offer in our Fortinet solution. This should be the primary pushback in any competitive discussions. These solutions offer part of the answer and then leave the customer with a disparate set of tools to manage in order to achieve the overall security required.

SD-WAN CAN REPLACE THESE TECHNOLOGIES

Application Accelerators | Intrusion Detection and Prevention Systems | VPN Concentrators | Web Content Filtering Solutions



SD-WAN Battlecard

Good to Know: Meraki messaging suggests customers don't need an MSP

One of the common vendors in this space is Meraki. Their messaging to Enterprise customers encourages a self-service approach to SD-WAN i.e. Take Meraki routers, add simple Direct Internet Access (DIA) connects and remove the Managed Service Provider and MPLS from the equation. In this model, they would suggest that SD-WAN is cheaper. There are drawbacks to this model such as;

Lack of expertise in Managed WAN

As an MSP, you have years of experience managing IT Solution, vendors and suppliers. Customers who self-serve are unlike to have this scale or breadth of experience.

Meraki provides an incomplete solution

In order to provide a simplified single dashboard, compromises have been made around the security and level of control available. The features are not as comprehensive when compared to the Fortinet solution. Meraki requires additional Cisco software products to be able to provide the same level of application control and security. All of this is included in the Fortinet solution.



2020 LEADER
by Gartner for WAN Edge
2019 RECOMMENDED
by NSS Labs for SD-WAN



2020 LEADER
by Gartner for Firewalls
2019 RECOMMENDED
by NSS Labs for NGFW



SD-WAN Battlecard

Conversation Starters

What concerns, risks or challenges do you perceive with your current connectivity solutions?

Is it matching your business goals? Is it reliable? Do you have a good service partner?

What is the impact of an outage on your network?

Loss of productivity, loss of earnings, loss of business reputation, loss of status?

Do your applications perform well wherever your team are based?

Is there a marked difference when working remotely, over WIFI or at certain site locations?

Do you use online Collaboration solutions such as Microsoft Teams or Cisco Webex?

How well does it perform for you, are you able to use the HD Video calling without issues?

Are you able to control which applications take priority on your network?

Do some apps just take over unexpectedly and saturate the network? Can you identify unapproved applications and see what impact they are having?

Keywords

Reduce business risks, improve speed, improve network availability, slow performance, home working, mergers and acquisitions, network security, application performance, shadow IT

Co-Sell Opportunities

- ✓ LAN and WIFI
- ✓ Connectivity
- ✓ Professional Services
- ✓ Cloud or Hosting Solutions
- ✓ Backup and DR Services



#WeAreExclusive

In partnership with
FORTINET®

Go to Market Customer Pitch Deck

Our Offices Are No Longer Where We Do Business

With business apps now in the cloud and prevalent high-speed Internet access, remote working is on the rise.

Our teams can work flexibly around family commitments. Reducing stress, avoid time lost time in commuting and overall helping to support mental wellbeing.

UK Businesses are downsizing office space and implementing desk-sharing policies to reduce overheads.

61%

of UK companies had a cyberattack in 2019



The way we work has changed

Every day our teams are using multiple devices to work with their colleagues and customers. We spend less time sitting at fixed locations on desktop devices, the office is no longer the single place of business.

- We use Cloud based SaaS apps and collaborate with HD Video calls, instant messaging and file sharing.
- COVID has enforced home working, but it is here to stay in one form or another

81%

of workers expect to work from home at least one day a week post lockdown

of employers will expand or introduce working from home on a regular basis

70%



Our Business Data Isn't Where It Used To Be

The trend of moving data and applications off-premise and into the cloud continues. Whether that's public cloud from AWS, Google or Microsoft.

Businesses are continuing to place their data off-site which is changing what they need from their WAN solution.



How do we control security and end-to-end performance?

Security is the Priority

Digital transformation is key to modern business success, but we cannot overlook the foundations. Firstly business data needs to be secured, and accessible to our teams wherever they are working.

In a recent survey, Gartner identified that 72% of businesses confirmed that security is the number one concern when it comes to their network.

Data breaches can cause significant brand damage and lose the trust of our customers.

That's why we've put security at the heart of our SD WAN solution



Virus and Malware Impact

Over half of UK businesses have fallen victim to Cyberattacks or security breaches in the last 12 months.

It's not just large enterprises who are being targeted;

68%

of small UK
businesses

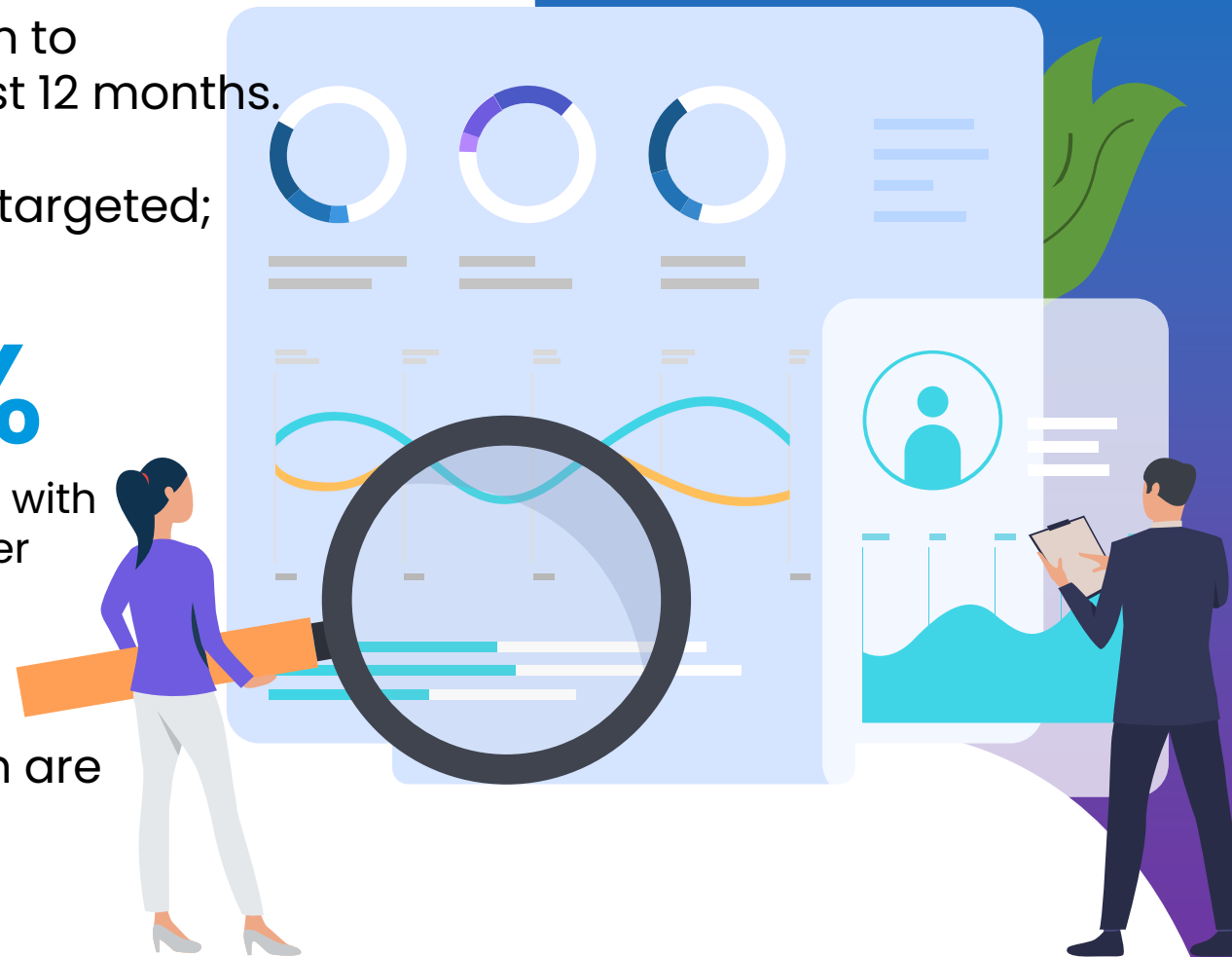
75%

of large UK
businesses

57%

of charities with
income over
£5m

In addition the reputational brand and trust damage can have long term impacts which are difficult to put a financial number on.



Has Your Network Evolved?



SD-WAN from Fortinet

Your business needs a secure, flexible network foundation that can adapt as your business needs change over time. SD-WAN provide more control over applications and security than traditional network deployments.

- **Security**
Protect from Internal and External threats
- **Application Performance**
Accelerate your mission critical apps and block unauthorised applications
- **Insight**
Deep analytics help you see how the network is supporting your business growth



Security

Protect from Internal and External threats with advanced security and intelligence.

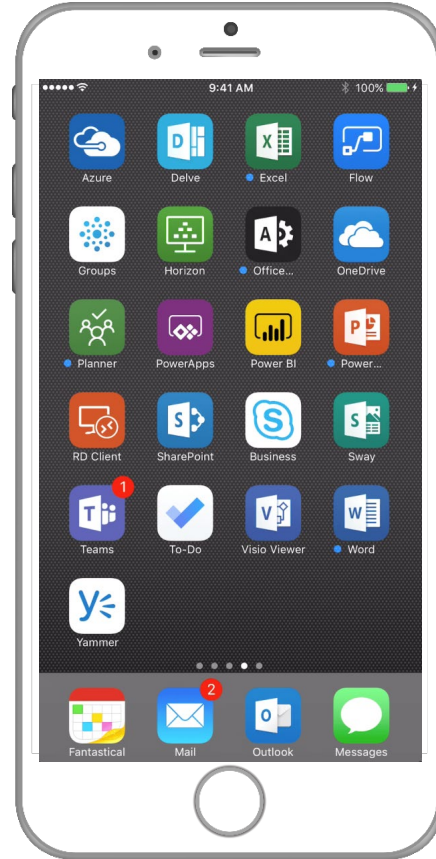
With SD-WAN, every location is equipped with a Next Generation Firewall. Now we can protect against virus and malware threats from inside the organisation as well as outside. We can stop the spread of malicious programs throughout the business.

The application detection engine can also identify unauthorised applications on the network and block them.

All security policies are managed centrally from a single dashboard so it's easy to manage and report on compliance.



Application Performance



SD-WAN can automatically identify and prioritise over 3000 business applications providing an optimised experience for everyone.

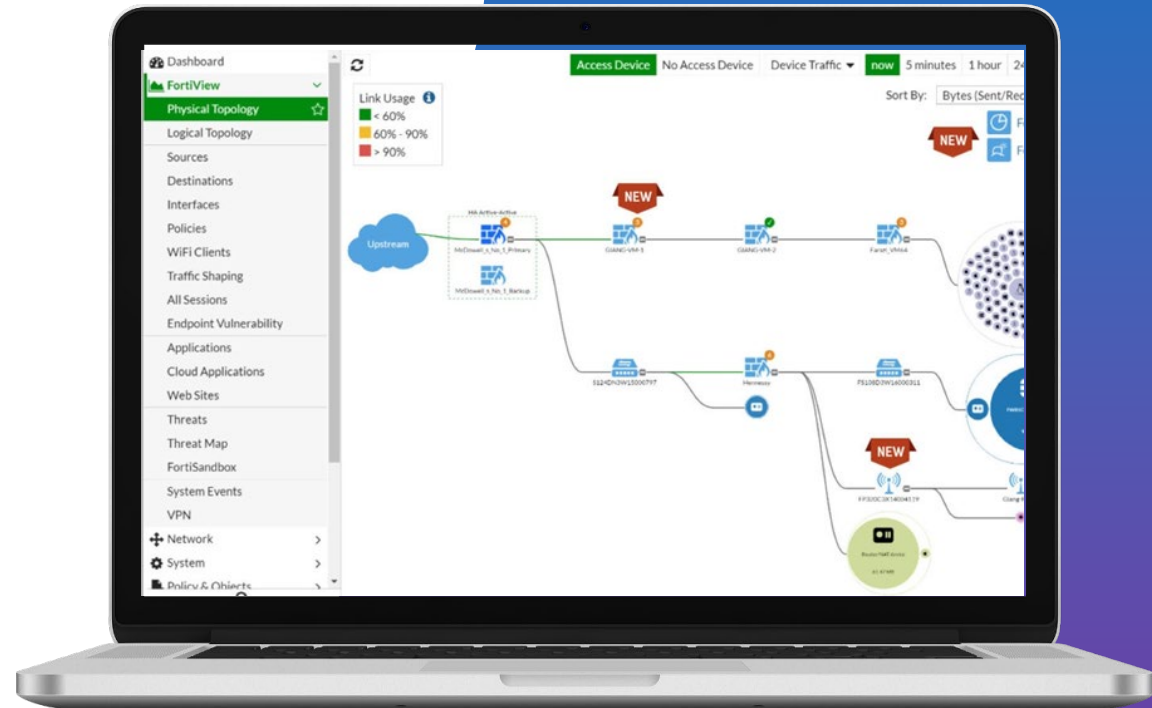
The network adapts to your goals ensuring that the applications provide the best experience every time. You set the priority that's important to your business.

SD-WAN can also mitigate security risks by identifying unapproved software applications running on the network and blocking their access.

Insights and Analytics

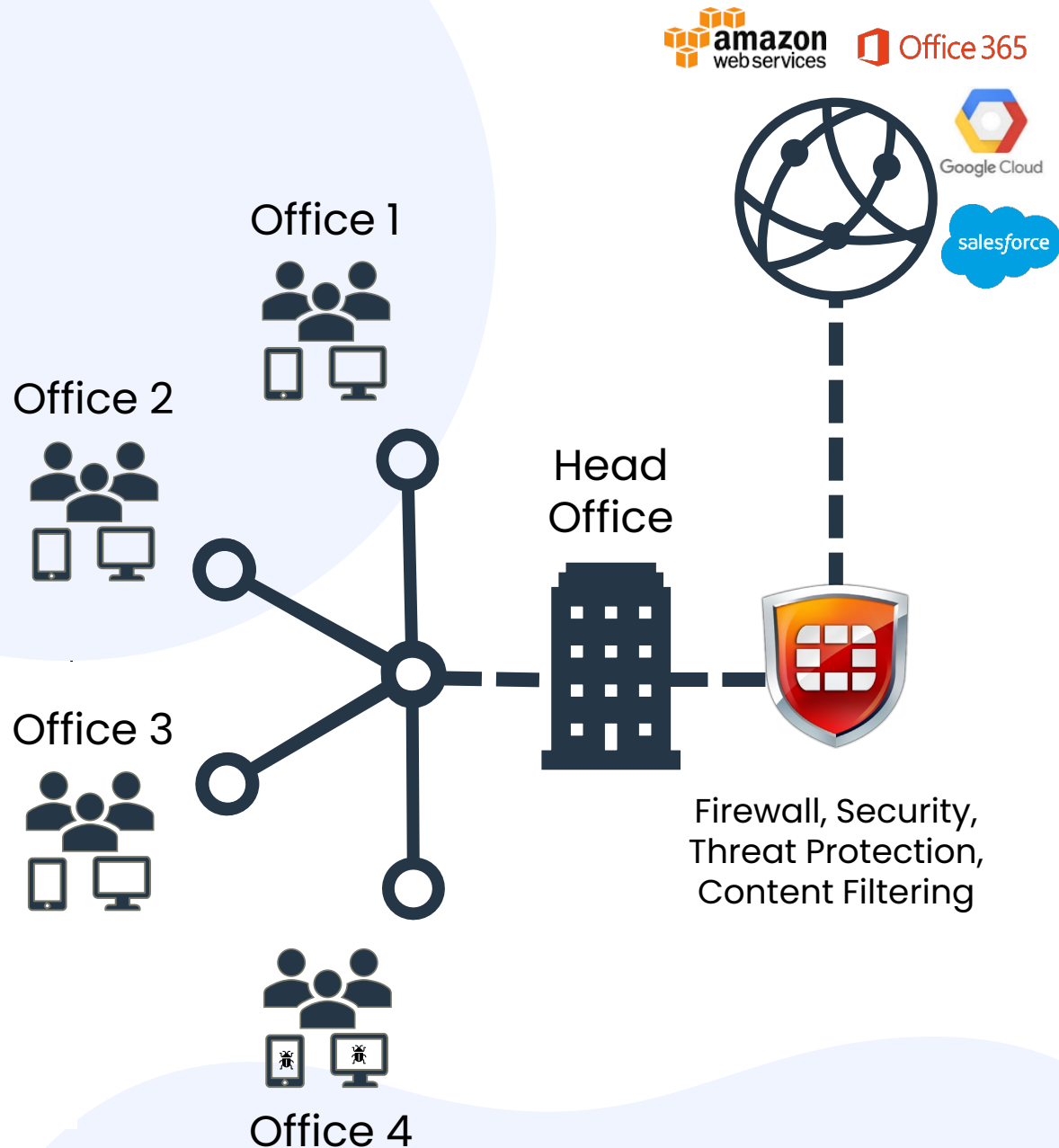
Gain full insight into your business applications and track the changing needs of your organisation. Analyse metrics to ensure that teams get the performance they need, when they need it.

Identify risks, security threats and Shadow IT applications



30% of business technology spend is Shadow IT

It is not controlled, secured or monitored by the IT team



Traditional MPLS Networks

A typical MPLS network has two key features

- Each site can communicate freely with every other site
- Internet access is centralised through one single site at the head office location

However as businesses have evolved, more and more of our teams are using Internet based SaaS apps. This means that tunnelling all the traffic through a single head office location can cause congestion on the network.

Additionally, as security threats have evolved, phishing attacks are responsible for over 80% of intrusions in UK organisations. In an MPLS network, there is little to stop this spreading across all locations. Security and filters are only applied to traffic between the Head Office and the Internet.

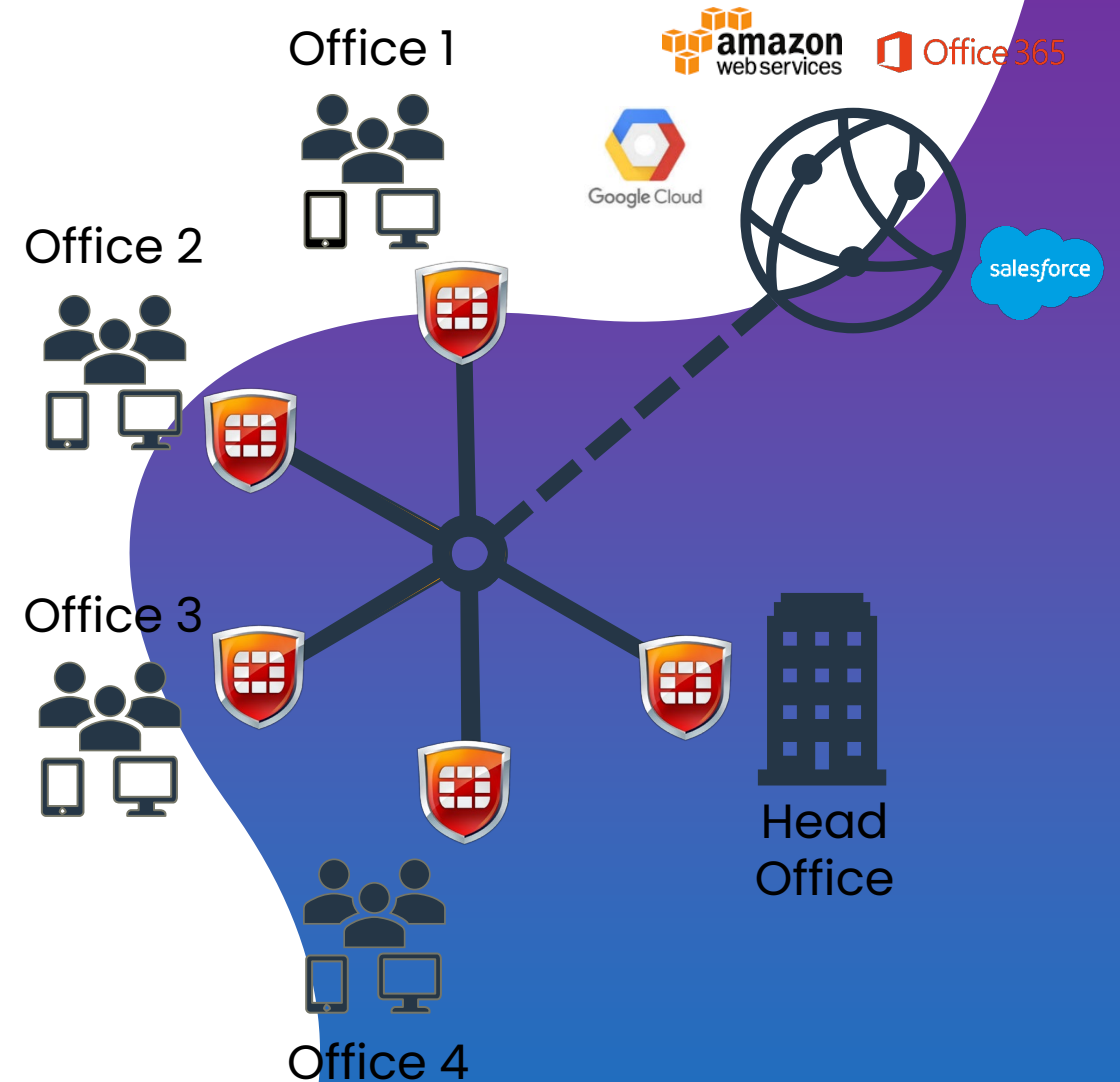
SD-WAN is Different

With SD-WAN, every location has a fully capable Next Generation Firewall (NGFW) on-site. Providing Advanced Firewall Services such as;

- Internal and External Threat Protection
- Web Content Filtering
- Application Acceleration
- Malware detection and blocking

Now we can directly connect these sites to the Internet as well as the Head Office and automatically prioritise, and secure every application experience.

In this design, should a phishing attack occur it would automatically be contained to one single site. The specific device would be quickly be identified for action to be taken.



Creating your SD-Branch

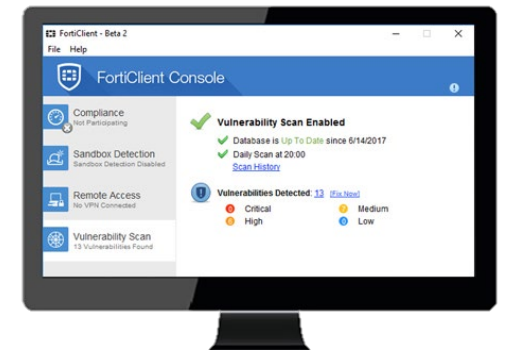
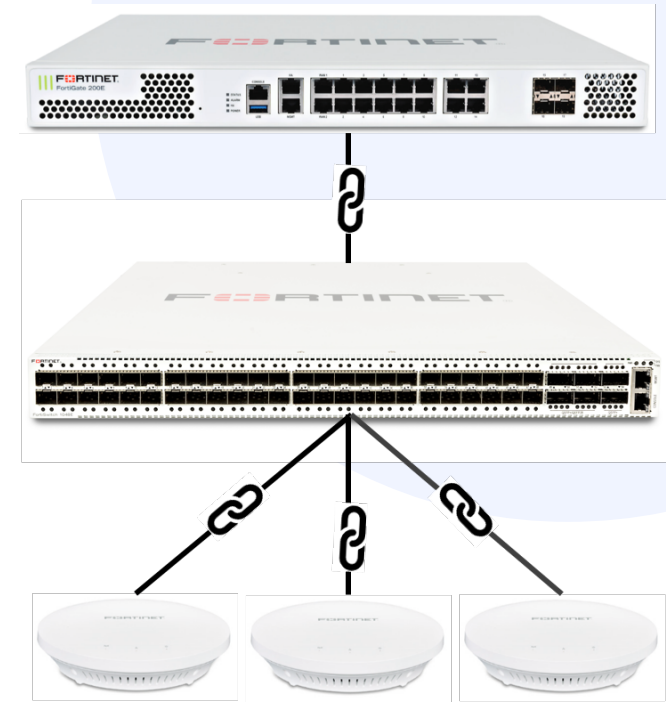
Security and Acceleration Everywhere

Our Secure SD-WAN Solution doesn't stop at the edge.

With high-speed LAN switching and Wireless Access Points, we can bring the same level of insight, security and application experience wherever you are working inside the building.

Forticlient client protects each computer and mobile device from virus and malware attacks while enabling secure web browsing.

Everything is still managed and reported centrally so you have a single pane of glass to understand what's happening at all times.



Fortinet: A Secure Foundation for SD-WAN

Security and Performance are two key features of our SD-WAN solution
 Fortinet are independently recognised for their capability in both areas

2020 LEADER
 by Gartner for WAN Edge
2019 RECOMMENDED
 by NSS Labs for SD-WAN



© Gartner 2020 Magic Quadrant for WAN Edge

APPLICATION PERFORMANCE

2020 LEADER
 by Gartner for Firewalls
2019 RECOMMENDED
 by NSS Labs for NGFW



© Gartner 2020 Magic Quadrant for Network Firewalls

SECURITY

Ready to go SDWAN Blueprints

	Branch Office	Small Office	Medium Office	Large Office
Size	<p>Our pre-configured bundles contain everything you need. Just choose the size to match your locations.</p> <p>1 – 25 People Up to 80Mbps</p>	<p>10 – 50 Up to 250Mbps</p>	<p>50 – 150 People Up to 500Mbps</p>	<p>150 – 500 People Up to 1Gbps</p>
Capability	<p>Every location is equipped with the same intelligent security and application performance features.</p> <p>Fortigate NGFW with DSL or FTTC technology</p>	<p>Fortigate NGFW with fixed fibre technology</p>	<p>Fortigate NGFW with fixed fibre technology</p>	<p>Fortigate NGFW with fixed fibre technology</p>
Optional	<p>Each location can be enhanced with optional upgrades for greater resilience or integration with your on-site devices.</p> <p>Add resilient, secondary connectivity to each site</p> <p>Add 4G Backup, Wireless Access Points, LAN Switching</p>			



Executive Summary

We aggregated key findings from our Secure SD-WAN assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report as well for actionable steps your organization can take to optimize your network for Direct Internet Access, protect your organization from external/branch office threats, and ultimately save money.

Applications



Application usage should have a strong influence on your network architecture. Understanding which types of applications are used and specifically business application performance can improve user experience and productivity.

Security

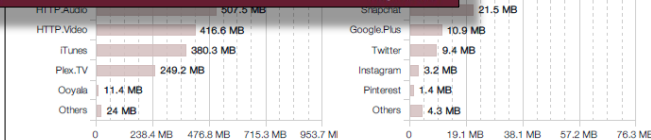


Maintaining a full security stack at the WAN edge is critical in any SD-WAN deployment where public Internet circuits are leveraged. Note that any threats observed within this report have effectively bypassed your existing network security gateway, so they should be considered active and may lead to increased risk (such as a data breach).

Utilization



In addition to individual applications, understanding overall utilization can help with capacity planning, circuit selection, and streamlining network traffic over time. This awareness can also help reduce operational costs associated with backhauling traffic over more expensive WAN links (such as MPLS).



SD-WAN Readiness Assessment

One of the best ways to see if SD-WAN will benefit your business is with our readiness assessment.

The assessment will validate your network's current security, analyse current traffic flows assess user productivity and overall network performance.

Our team deploy a device into your network for 5-7 days and then produce a comprehensive report covering;

- Which applications consume the most bandwidth
- Which high risk applications are running on the network
- If any vulnerable applications are in use
- Which applications are in use by which teams

At the end, you'll have a good understanding about your current network and how SD-WAN could help.

Roadmap from SD-WAN Assessment to Deployment

Commence Rollout

We run our SD-WAN readiness assessment at your location.

Assessment

SD-WAN hardware is deployed on-site

- Baseline Security
- Baseline App policies

Monitor for 7 days

Week 1

Review application performance and security logs

Optimise the configuration for each location

Monitor for 7 days

Week 2

Final review of performance and security logs

Final adjustments as needed

Monitor for 7 days

Week 3

Fully optimised and secured SD-WAN configuration

Report on gains achieved in security and application performance

Week 4

Proof of Concept Phases



#WeAreExclusive

Marketing Guidance



30, 60 and 90 day marketing plan

It's important to create a multi-channel structure campaign across social media to drive prospects (existing clients and net-new) into the sales funnel for SD-WAN.

Here we have created a recommended 30, 60 and 90 day initial marketing plan to get you on-track. The overall potential Sales funnel is as follows:

Broad distribution to drive people to a webinar

- Social Media content
- Email mailing list

Webinar (max 30 clients at a time)

- Overview of service offering
- Drive interested parties to a workshop

Workshop (can be 1:1 or max 10 clients in a specific vertical)

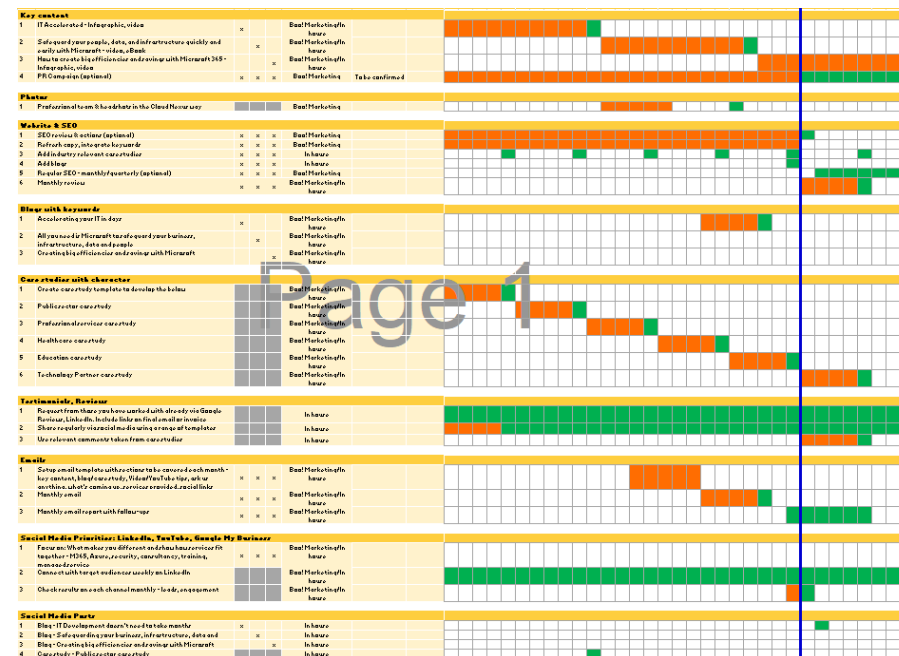
- Broad dive into areas where SD-WAN could help their business

CTAP Assessment

- Provide tangible outputs which show exactly how SD-WAN could help their business



An editable Excel version of this document is in your Accelerator Pack





#WeAreExclusive

Value Add Services

From Exclusive Networks



Our Services 1st Approach



Assess IT

Credit and Risk

Size Scope Stage

Rapid response pre-sales team for small and medium business opportunities

Mobile team of **30** experienced pre-sales engineers



Host IT

Public Cloud and hosting

Shift to managed consumption overcoming resource and complexity challenges with predictable monthly billing.

Secure. Simple.



Consume IT

Finance and Leasing

Subscribe with X-OD

Shifting CapEx to OpEx.

Instant revenue & commissions for the channel

Payment over time for End-user



Deploy IT.

Enable IT.

Install and Testing

Successfully delivered projects **1-200 days**

Remote / onsite configuration

Global and local

Authorised training centre



Support IT.

Manage IT.

Technical and Managed services driving value consumption

Increase end customer satisfaction

Security-as-a-Service