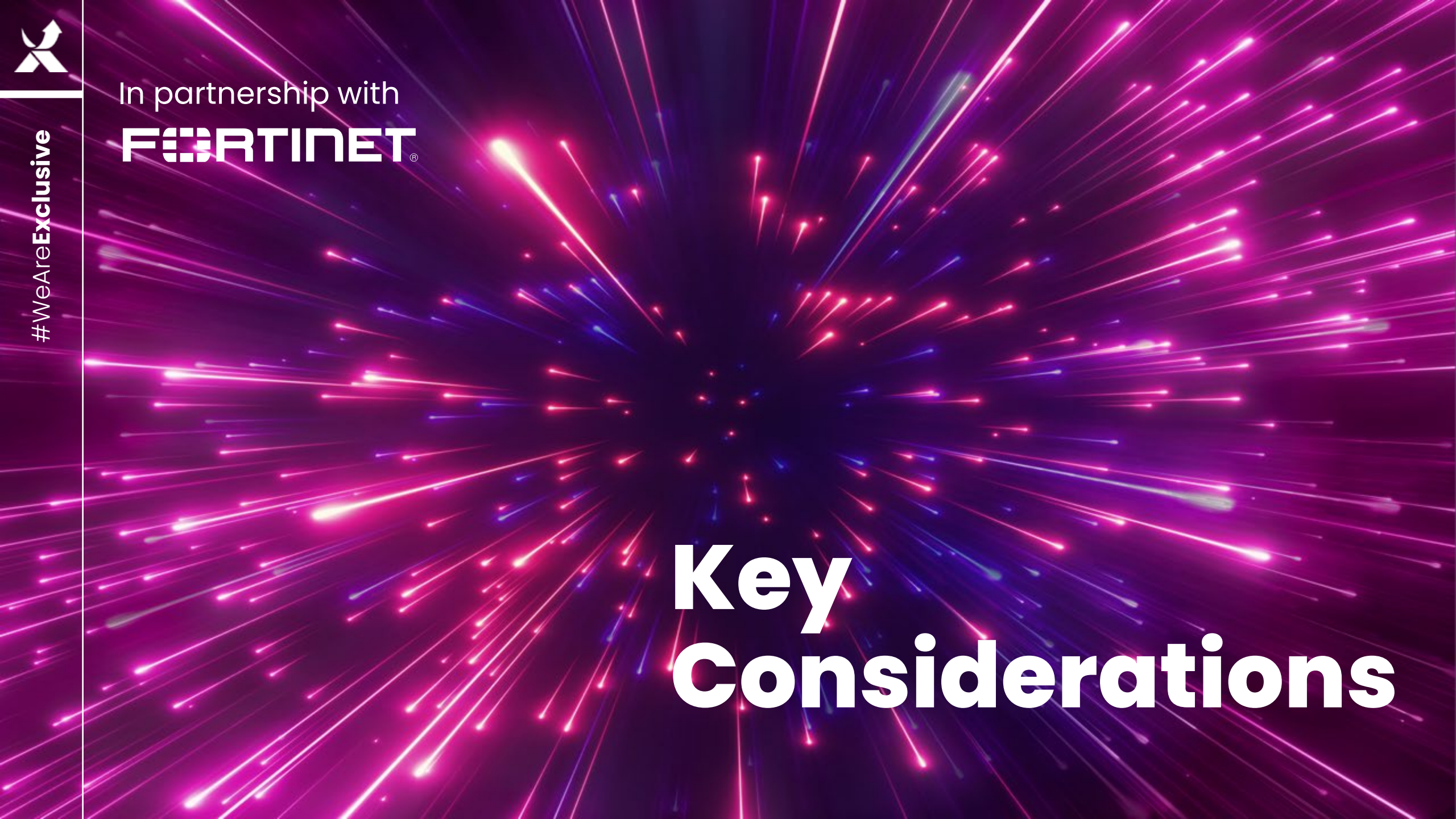
In partnership with
FORTINET
#WeAreExclusive
Key
Considerations

#WeAreExclusive

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.

#WeAreExclusive

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

#WeAreExclusive

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 to 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

#WeAreExclusive

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

#WeAreExclusive

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.

#WeAreExclusive

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.

#WeAreExclusive

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

#WeAreExclusive

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

ATERA

Autotask®

ConnectWise®

Kaseya®

servicenow

solarwinds msp

#WeAreExclusive

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