TITANIUM

BY FULCRUM IT PARTNERS

EVERYTHING YOU NEED TO KNOW ABOUT MIGRATING FROM MPLS TO SD-WAN

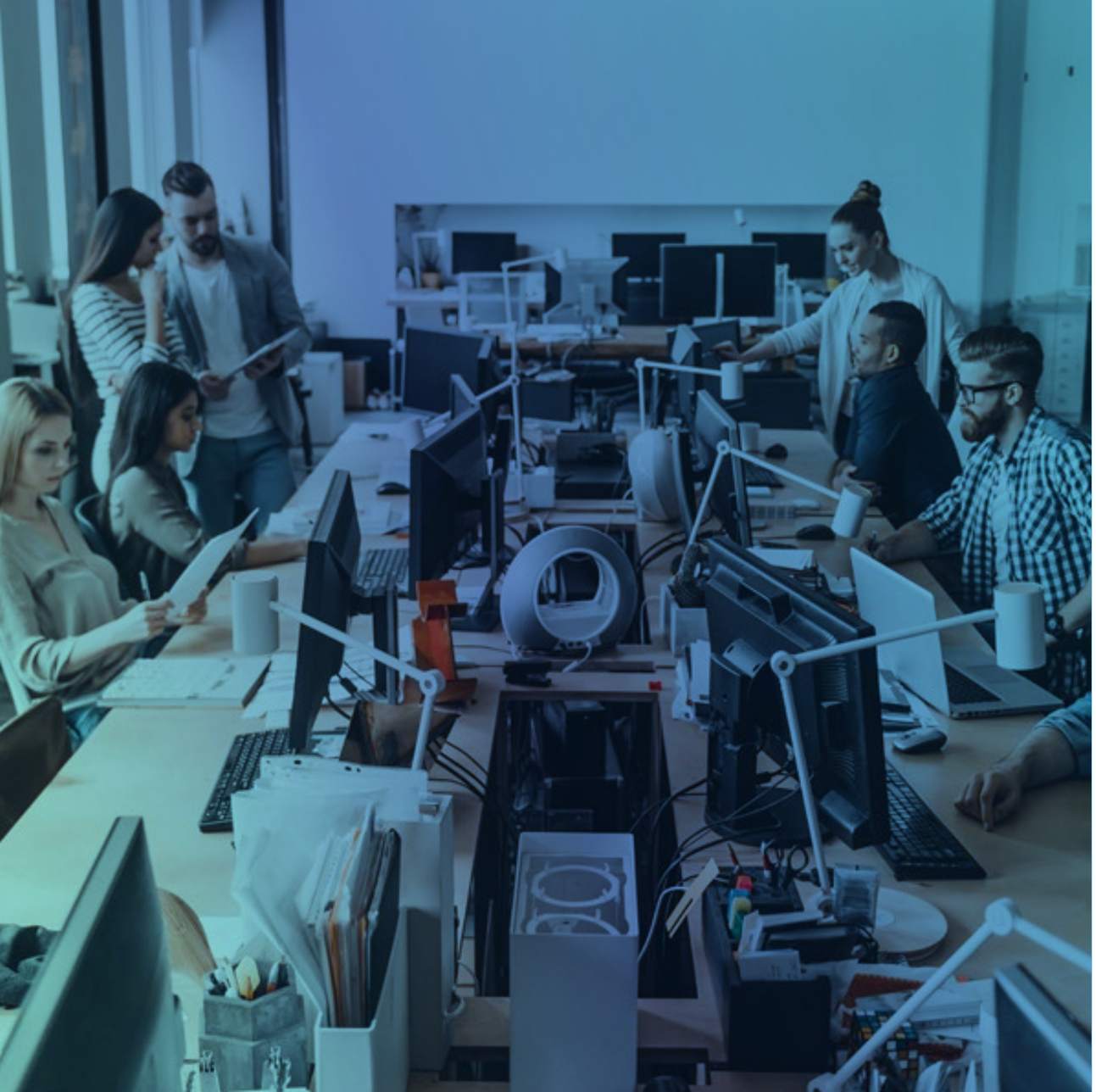


Table of contents

Executive summary

Enterprise networks have undergone a transformation in recent years. Demand for cloud services and the transition to remote and hybrid work has put significant pressure on legacy networks, driving the adoption of new technologies like SD-WAN.

While traditional networks using technology such as MPLS are not completely redundant, businesses that want the agility, flexibility and scalability the cloud and remote working strategies offer, do need to ensure their networks are optimised for the new modern workplace.

Problems with latency and poor performance are barriers to getting the full benefits of cloud services and a distributed workforce, which is why IT business leaders need solutions that work for traditional and new working patterns.

In this guide we explore these challenges and how you can design and deploy a secure network that reduces complexity and costs while improving performance and security.

Understand the jargon!

Throughout this guide we use various acronyms. Here is a quick glossary of networking terminology.

LAN

A LAN, Local Area Network, comprises all the components - cables, access points, switches, routers etc. - needed for devices to exchange data securely in one physical location. In a business environment, such as an office, a LAN ensures employees and guest users can access your corporate network when working at that location.

WAN

When an organisation has multiple LAN environments, such as in different offices, a WAN connects these smaller networks across longer distances. WAN, Wide Area Network, refers to a group of networks distributed across a large geographic area - different cities or countries - which are connected to each other so they can exchange data. Typically these networks are run in a private environment, your organisation's, to allow secure operations across multiple sites including business premises and remote hubs.

MPLS

If you're reading this guide it's probably because you're already using MPLS technology and are exploring updating or replacing it. MPLS stands for Multiprotocol Label Switching. It routes data packets (for example when you send an email, use VoIP or video conferencing) from one internet router to its destination using labels. These labels contain information about the data packet's priority level and forwarding decisions - a predetermined path that routes traffic using the shortest path over private wide area networks.

SD-WAN

Software-Defined Wide Area Networks (SD-WAN) are next generation WANs that enable end-to-end enterprise connectivity to corporate applications, cloud services and workloads regardless of location. As the name suggests, SD-WAN makes the network control and management processes available as software so they can be configured and deployed easily. It is a highly flexible and scalable solution that connects remote networks across large geographic distances.

It should be noted that SD-WAN doesn't necessarily replace MPLS. SD-WAN networks can manage multiple types of connections, including MPLS, and route traffic over the best path in real time. It connects your sites (offices and remote workers) to your cloud environments using multiple connectivity services such as Azure Virtual WAN, AWS Transit Gateway, MPLS, internet and even 4G/5G.

Secure SD-WAN

Secure SD-WAN integrates an organisation's network infrastructure and security architecture, enabling networks to transform at scale without compromising security. This approach, pioneered by cybersecurity companies like Fortinet, combines next-generation firewalls with SD-WAN networking capabilities to provide consistent security enforcement across flexible perimeters. It also eliminates MPLS-required traffic backhaul to deliver an improved user experience without compromising security.

SASE

Secure Access Service Edge (SASE), pronounced 'sassy', is an enterprise networking and security concept first defined by Gartner. SASE packages up different network security functions, such as SD-WAN, SWG, CASB, ZTNA and FWaaS, into a unified, cloud-native service.

SSE

A component of a SASE solution, SSE stands for Security Service Edge and can also be deployed independently. SSE is the convergence of SWG, CASB, and ZTNA network security functions into a single cloud service.

SWG

Secure Web Gateway (SWG) protects end users from threats such as phishing and malware from the internet.

CASB

Cloud Access Security Broker (CASB) are security policy enforcement points that can be on-premises or cloud-based, which interjet when a cloud-based resource is accessed that is governed by a specific policy or policies. These include, but are not limited to, authentication, single sign-on, authorization, credential mapping, device profiling and encryption policies.

ZTNA

Zero Trust Network Access (ZTNA) is a solution that hides an application or set of applications from discovery, public visibility, reducing the surface area for attack. To access the application, end users are verified based on identity, context and policy adherence criteria.

FWaaS

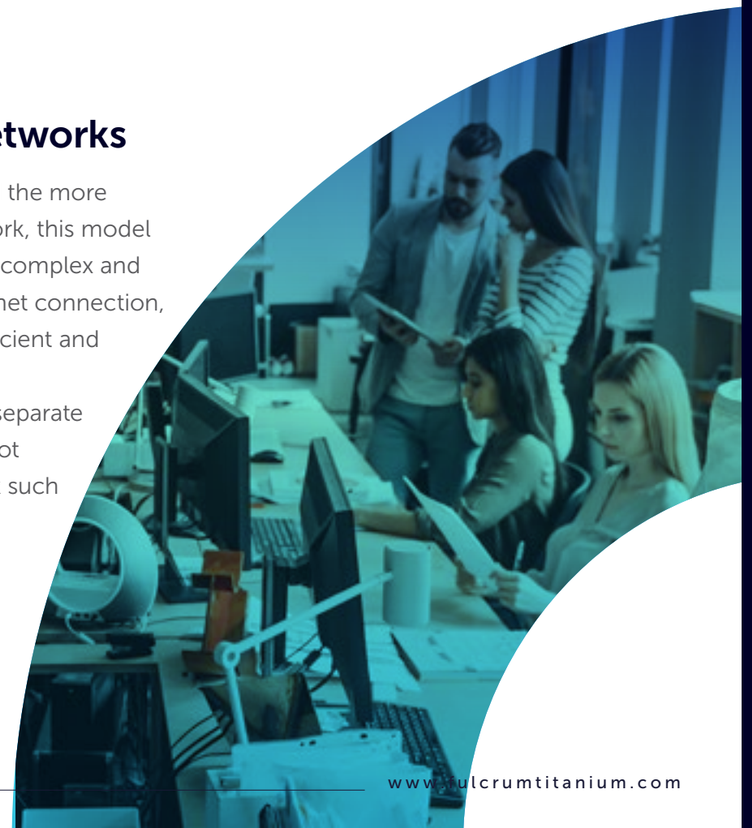
Firewall as a Service (FWaaS) combines next-generation firewall security with a unified threat management (UTM) platform to protect from advanced threats. FWaaS is a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities including web filtering, advanced threat protection (ATP), an intrusion prevention system (IPS) and more.

Why migrate to SD-WAN?

A traditional enterprise WAN utilising MPLS involves installing physical MPLS circuits at multiplesites so that data packets can be transported between them. For example, between a branch office and a corporate data centre based at HQ. This approach is secure and effective, ensuring data is moved quickly along predetermined paths and is protected within a virtual private network (VPN).

The benefits of MPLS networks

Before the advent of cloud services, and the more recent increase in remote and hybrid work, this model worked well. While legacy MPLS can be complex and expensive compared to a standard internet connection, when used as originally designed it's efficient and provides a good end-user experience.
As it's a virtual private network it is also separate from the public internet and therefore not vulnerable to some types of cyberattack such as denial of service attacks.



MPLS and the cloud

But once you start migrating workloads, apps and data to the cloud, MPLS becomes more of a barrier to productivity than an asset. That's because with MPLS all traffic from the cloud needs to go through a central hub, corporate HQ, before being sent on to a branch office or end-user. It's a hub-and-spoke connection model. This creates a pinch point which is also exasperated by the bandwidth required by many cloud services, such as video and mobile apps.

Backhauling traffic from a remote site (both business premises and remote workers' home offices) via the data centre at HQ, wastes bandwidth, increases latency and slows down network and application performance.

For many businesses it is more effective to send traffic directly to the cloud and remove the MPLS pinch point altogether. If your organisation has migrated fully to the cloud a legacy MPLS network is likely to be expensive to maintain, and does not provide you with the flexibility and scalability your cloud services require.

New technologies for today's network architectures

This is where SD-WAN steps in. SD-WAN supports multiple connection types, such as broadband, 4G/5G LTE and also MPLS. It uses rules and policies to select the best path to send traffic, instead of the predetermined paths MPLS uses. For example, SD-WAN technology identifies data packets by application, user, source and destination and then selects a WAN link based on network conditions, traffic characteristics and your quality of service (QoS) requirements. It applies policies across all WAN devices so data is sent by the most efficient and secure route depending on its attributes. This is known as dynamic path selection.

This centralised approach also increases network security as it can apply internal security policies across the entire network. This has clear benefits when utilising cloud applications that require secure remote access such as Microsoft 365, Google Workspace and Amazon Web Services (AWS). Security for cloud apps can be integrated into your connectivity fabric, with mission-critical data and traffic protected and segmented from other parts of the enterprise network.

Hybrid approach

Businesses that have on-premise data centres and legacy apps may still have a MPLS network requirement. If you need to transport data from a regional office to corporate HQ, or between offices, an existing MPLS network is a secure and effective way to do this.

In this scenario a hybrid approach is an option and, as explored earlier, SD-WAN solutions route network traffic in the most efficient way possible to meet your QoS requirements, which could be via a MPLS connection.

SD-WAN summary of benefits

Whether you continue to use your MPLS network for some traffic, SD-WAN can support your legacy workloads as well as new cloud services. Here are the key advantages of migrating to SD-WAN:

1: Improves performance

SD-WAN is configured to prioritise business-critical traffic and real-time services and route them by the optimal path. This reduces latency issues, and packet loss, and improves productivity for the business and end-users.

2: Boost security

SD-WAN allows you to apply corporate security policies across the entire network, on-premise and in the cloud. Best-in-class solutions, secure SD-WAN, also integrate with next generation firewalls, IPS, URL filtering, malware protection, and cloud security solutions to enhance protection.

3: Reduces complexity

Networks have become increasingly complex, especially with digital transformation and remote working initiatives. SD-WAN simplifies the WAN infrastructure and manages traffic through a centralised controller.

4: Helps you get the benefits of the cloud

Enabling direct cloud access from a branch office or remote site, eliminates backhauling traffic so cloud applications perform at their best. This also improves network performance across other areas of the network - as traffic to the cloud is no longer routed to HQ first.

5: Reduces costs

SD-WAN solutions select the best route to transport data, leveraging low-cost local internet access where appropriate and direct cloud access. MPLS networks can be expensive because they do not allow you to scale bandwidth up and down, instead you pay for worst-case contingencies so overall you pay for more than you need. SD-WAN pricing models vary, such as pay-as-you-go, flex up/down licensing and managed services, so you can choose the best option for your business.

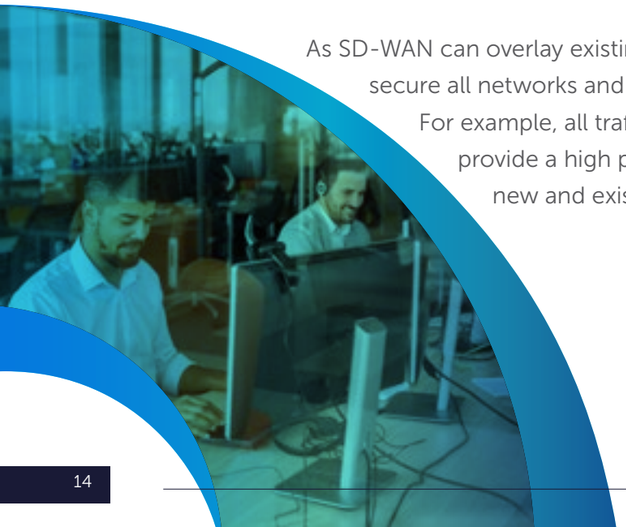
Use cases for SD-WAN

If your business is using cloud services and has multiple sites, SD-WAN will give you an advantage. This includes businesses with remote users as work from home initiatives has effectively turned many companies into multi-location organisations.
Below we explore how SD-WAN can help businesses across these different scenarios.

Multi-site organisations

Organisations with multiple business premises often have a complex IT infrastructure that creates many headaches for the IT team. This is especially true when sites have been added through mergers and acquisitions, which all need to be securely connected but may be using diverse networks and technology.

Inconsistent technologies deployed across individual sites create vulnerabilities and a lack of visibility of cybersecurity threats, potentially increasing the attack surface if networks are not connected securely.



As SD-WAN can overlay existing connection types, it can be deployed quickly to secure all networks and integrate them with corporate security solutions. For example, all traffic can be routed through a next-gen firewall to provide a high performing security perimeter encompassing all new and existing sites.

IVC Evidensia case study

For a real life example of how SD-WAN supports growing businesses, read our case study with veterinary group IVC Evidensia. Click here.

IVC EVIDENSIA

Remote and hybrid workforce

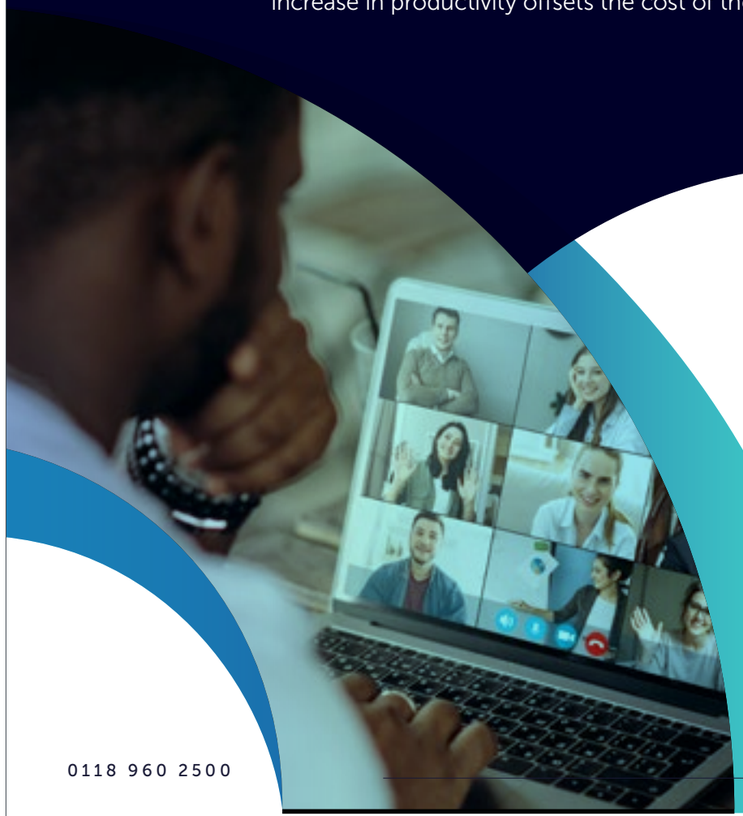
When remote workers are reliant on their home broadband connection or VPNs they often have an unequal experience compared to their colleagues working in an office due to poor network performance and bandwidth contentions. They may also pose a security risk if accessing business-critical applications via an unsecure connection.

SD-WAN uses your organisation's policies to determine the best pathway based on the characteristics of both the data packet and its source and destination. This includes security policies so the more critical the data packet, and more vulnerable it is, the more secure the pathway selected.

In a home working environment SD-WAN enables some traffic to go to the corporate HQ; some to go directly to cloud services (Microsoft 365, AWS etc.) under the company's rules and parameters; and other traffic is routed externally - such as traffic to social media sites. This ensures critical data and applications are protected while freeing up the company's bandwidth and infrastructure from less critical and sensitive traffic.

Should you roll out SD-WAN for remote workers?

Not every employee working from home needs SD-WAN. If end-users just need to access cloud applications like Microsoft 365, their access is governed by your security policies and identity and access controls, and SD-WAN is probably not needed. However, if they need to access larger applications in the cloud or on-premise, or if the increase in productivity offsets the cost of the SD-WAN, this option is worth exploring.



How to overcome migration challenges

Before you embark on a migration from MPLS to SD-WAN it is helpful to understand what factors might stand in your way to a successful transition, and how to overcome them.

In our experience of helping organisations migrate to SD-WAN, these are the most common challenges you may face:

1: Internal capacity and experience

According to Gartner a true SD-WAN solution supports zero-touch provisioning (ZTP) which in theory means deployment is straightforward. When provisioning branches or home users, ZTP allows your IT team to remotely provision a router anywhere in the WAN.

However, you still need the expertise and time to design the network solution, select and install the SD-WAN products and set up SD-WAN network management and monitoring.

As with any IT project, best practice is to conduct an internal skills and resource assessment and address any shortfalls with training, hiring or engaging external support.

2: Selecting the wrong product

The WAN is mission-critical and therefore the selection of a SD-WAN product cannot be taken lightly.

Before you select a product you must have a clear picture of what it needs to do, and how it will integrate into your existing IT environment.

Key points to consider include:

- Integration with legacy routing protocols such as BGP and OSPF
- The ability to talk to legacy non-SD-WAN sites and work across MPLS networks, as well as the SD-WAN fabric
- The ability to scale the solution as new non-SD-WAN sites are added during the transition, and later if new sites are acquired
- Interoperability with security solutions
- A consumption model that works for your business.

3: No clear business case

When selecting a SD-WAN product it must also be aligned with your business case for transitioning to the technology. As explored earlier in this guide there are many reasons organisations migrate from MPLS to SD-WAN, and advantages when you do.

Be clear why you're embarking on this transition and what your expectations are before you choose a product. Some products work better with a legacy infrastructure than others, but perhaps do not deliver the SD-WAN innovation you may want. Other products may be more focused on SD-WAN and offer poorer integration with legacy protocols. If reducing costs is a driver for the migration then consumption models will help determine the right product.

With a clear business case for migrating to SD-WAN you can better evaluate different vendors and solutions.

4: Lack of planning

As explored in the next section of this guide, planning is a vital step to a successful migration. To minimise disruption you will need to:

- Understand how the SD-WAN solution connects to your data centre, cloud and security stack
- Create a standardised template for your branch architecture
- Factor in any network upgrades that might be required, such as new circuits, routers or IPs, and when this work will be complete
- Identify how your applications will utilise the SD-WAN
- Plan how legacy sites will interoperate until they become SD-WAN sites.

It is also vital that your project team knows exactly what their responsibilities are and who will do what. At this stage you may also want to revisit your internal capacity and expertise. Bringing in external support to help deploy the solution or provide a managed SD-WAN service, may be the best option for your team, instead of the DIY approach.

5 Steps to a successful mpls to SD-WAN migration

Whether you are planning to replace your MPLS network completely with SD-WAN or operate a hybrid network, we recommend following these steps to ensure a successful migration.

Network audit and review

Start with your current network and conduct an audit and review across all sites. This should include:

- **Devices**: what devices are connecting to your network including BYOD
- **Cybersecurity vulnerabilities:** a network survey will help you identify any vulnerabilities such as outdated security patches
- **Bandwidth demand:** review the current usage and distribution of your bandwidth
- **Network infrastructure:** audit any problems with your network. infrastructure
- **Data security:** review data and file security and current controls and policies
- **Network upgrades:** identify any poor performing hardware.

Network design

SD-WAN network design should take into account the existing network infrastructure and what can be kept, what needs to be upgraded and what connections should be replaced. SD-WAN can overlay your existing network, but existing routers and gateways must be able to integrate with the SD-WAN solution.
A key aspect of SD-WAN design is how it integrates with the cloud and how it manages policy enforcement, encryption, external traffic routing and application performance.
At this stage you will decide on the right SD-WAN product and services for your organisation.

Migration roadmap

The next step is to develop a roadmap which will chart the steps that need to be taken technically and practically to transition from your current network to SD-WAN. This will include controls and process maps, key tasks, KPIs and deliverables, milestones and deadlines.

Depending on the size of your network, migrating from MPLS to SD-WAN is generally not something that can be done overnight, or even a long weekend. For many organisations your legacy network will be connected to the SD-WAN for some time as you move each site to SD-WAN.

A controlled step-by-step approach is also advantageous as it is not uncommon to uncover hidden issues during the migration project. These issues can then be resolved before migrating the next site to SD-WAN.

SD-WAN migration

Now the magic happens! The technology is installed and configured, tested and deployed. With detailed planning this should progress according to your migration roadmap and result in a successful transition to SD-WAN.

Optimise, monitor and manage

After your new technology and services go live, you now enter a period of optimising performance before transitioning to BAU. At this stage there will be further opportunities for optimisation and improvements to fit the evolving needs of your business. SD-WAN's dynamic pathway selection is designed to accelerate data traffic, but it can only do this if it's given the right information. Ongoing optimisation will help you make the technology work harder for your business, and get a better return on your investment.

Our approach

Fulcrum Titanium provides a managed SD-WAN solution that ensures our customers not only get the benefits of secure SD-WAN, we also monitor and manage the technology for you - optimising the performance of your critical applications.

We practice what we preach, following the migration steps outlined in this guide and then supplying a high-performance, secure and affordable service.
Our SD-WAN managed service features:

- Managed installation with engineers on site
- Zero touch provisioning
- Routing of applications based on configured policy
- Complete visibility of network conditions and security landscape
- Intuitive user interfaces
- Dynamic propagation of changes
- Centrally defined security policy
- 24/7 service desk with 4h break-fix on parts

Powered by Fortinet

Fulcrum Titanium has partnered with Fortinet, one of the most trusted names in network security and a Leader in the Gartner®2021 Magic Quadrant™ for WAN Edge Infrastructure.
Fortinet Secure SD-WAN delivers the following key business outcomes:

Improved User Experience: An application-driven approach provides broad application steering with accurate identification, advanced WAN remediation, and accelerated cloud on-ramp for optimised network and application performance

Accelerated Convergence: The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) to secure all applications, users, and data anywhere
Efficient Operations: Simplify operations with centralised orchestration and enhanced analytics for SD- WAN, security, and SD-Branch at scale

Natively Integrated Security: A built-in next-generation firewall (NGFW) combines SD-WAN and security capabilities in a unified solution to preserve the security and availability of the network.

To find out more, book a discovery call with our network security team.

CLICK TO BOOK A DISCOVERY CALL

FORTINET

Next steps

Do you have any questions? If you want to learn more about migrating to SD-WAN or would like to explore further whether it's right for your organisation, speak to us.

Book a free 30 minute, no obligation discovery call with one of our network consultants to discuss your objectives, ask any questions and take the next step.

CLICK TO BOOK A DISCOVERY CALL

About Fulcrum Titanium

Fulcrum Titanium specialises in integrating state-of-the-art networking and cyber secrity technologies to offer businesses comprehensive, straightforward solutions, which are proactively supported and enable organisations to operate with ease.

Fulcrum Titanium is well-practised in supporting organisations of all sizes, and from all sectors, at every stage of their digital journey. By providing the very best technology advice, products and services, we help our customers to achieve digital transformations which increase their employees' engagement, enhance their customers' experiences, generate greater productivity and take their businesses to a whole new level.

Contact us

Need to learn more about how our solutions can help drive your business forward? Contact our team today!

Email Fulcrum Titanium
enquiries@fulcrumtitanium.com

Call Fulcrum Titanium
+44(0)118 960 2500

Find out more
www.fulcrumtitanium.com

TITANIUM

BY FULCRUM IT PARTNERS