



#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

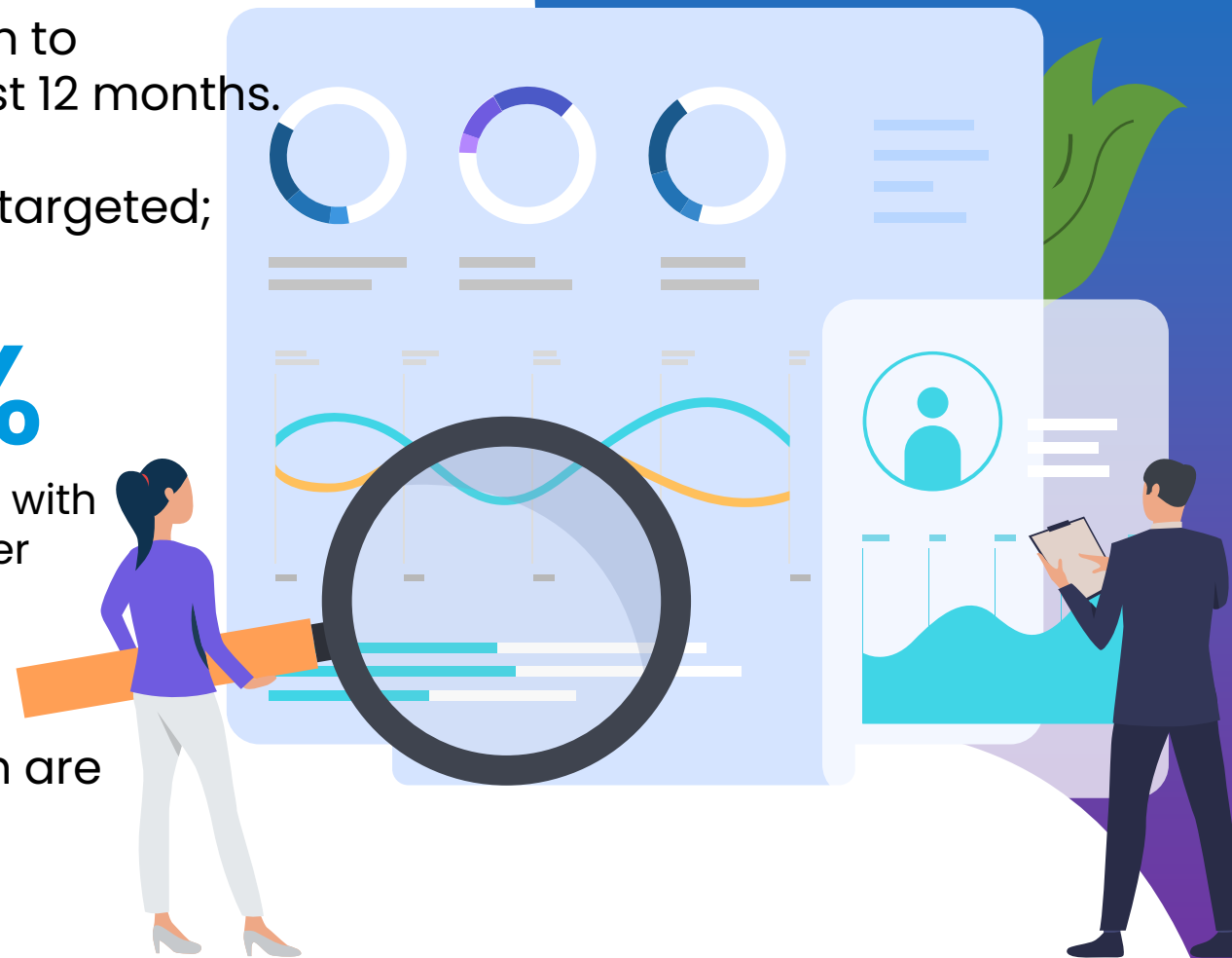
75%

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.

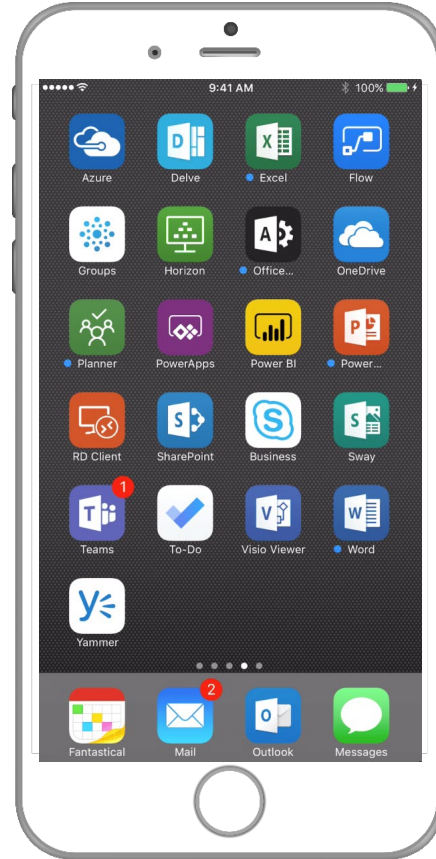
With SD-WAN, every location is equipped with a Next Generation Firewall. Now we can protect against virus and malware threats from inside the organisation as well as outside. We can stop the spread of malicious programs throughout the business.

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.

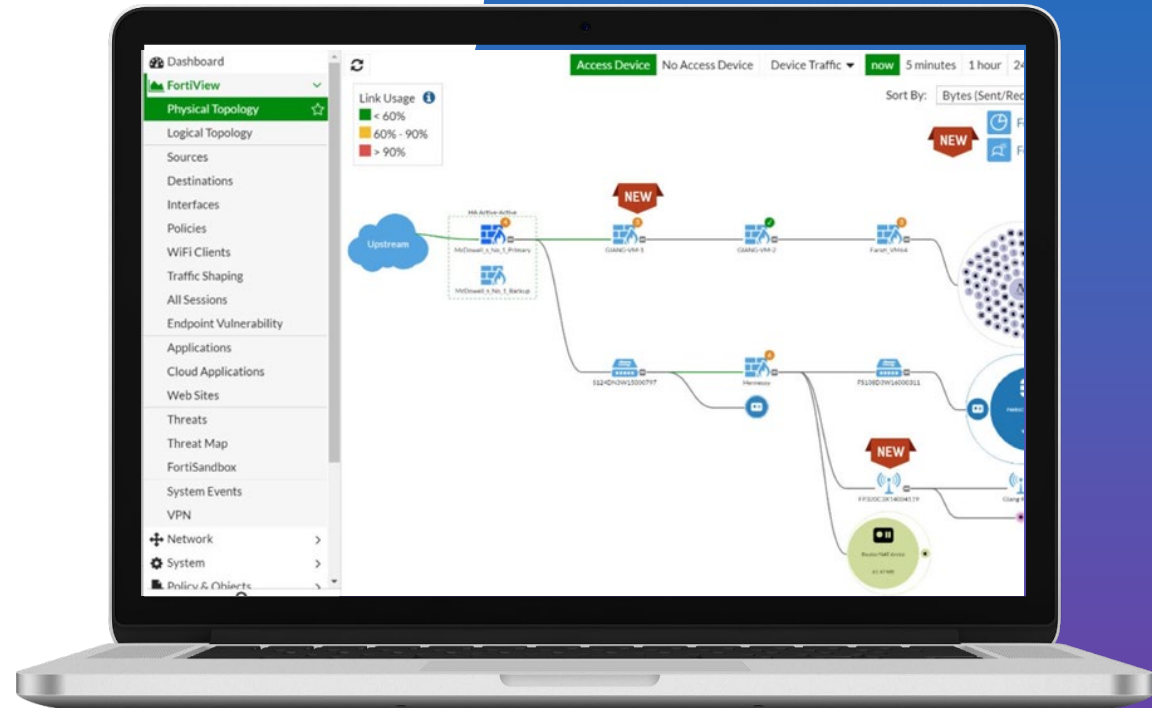
The network adapts to your goals ensuring that the applications provide the best experience every time. You set the priority that's important to your business.

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

Insights and Analytics

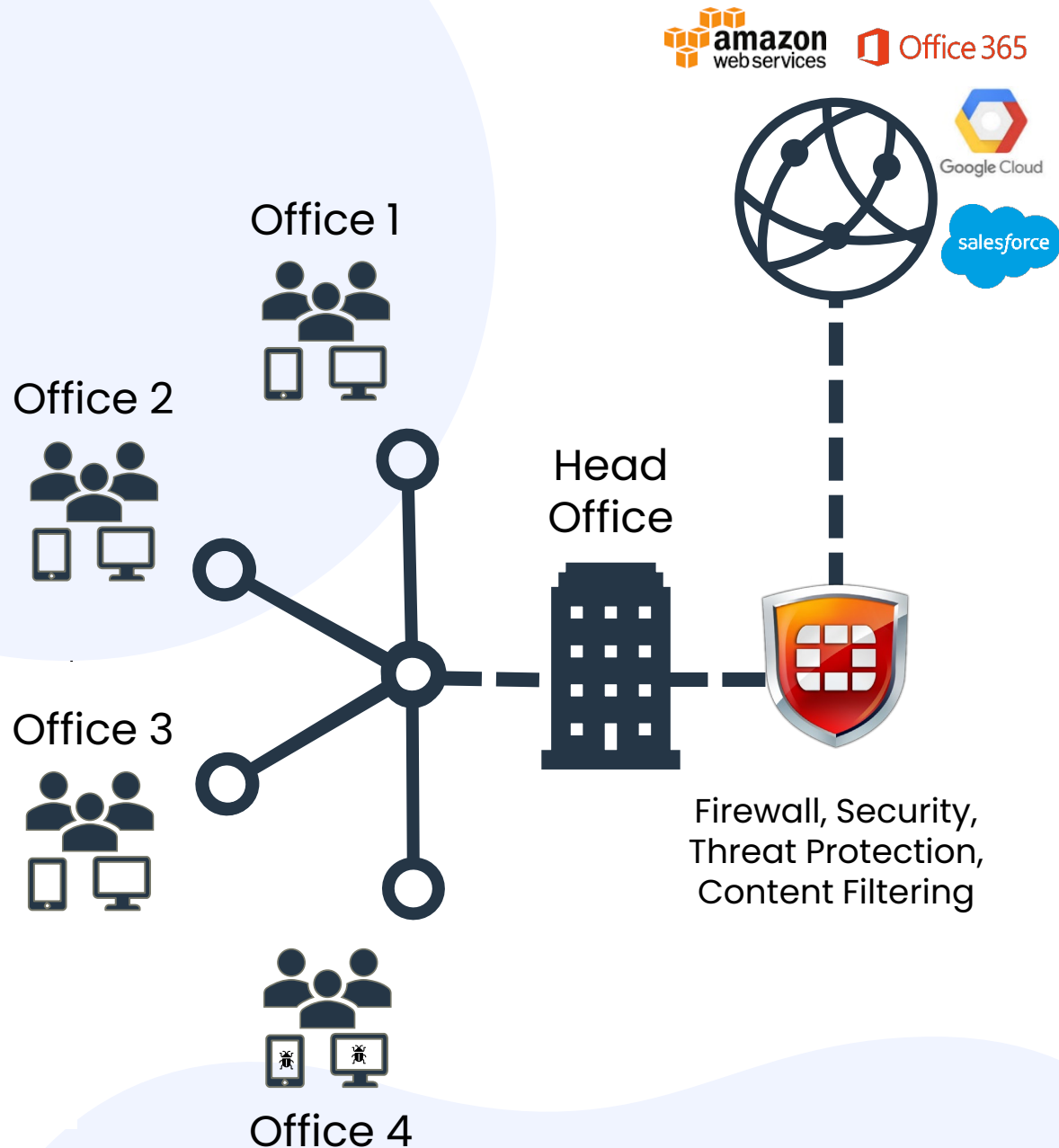
Gain full insight into your business applications and track the changing needs of your organisation. Analyse metrics to ensure that teams get the performance they need, when they need it.

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.

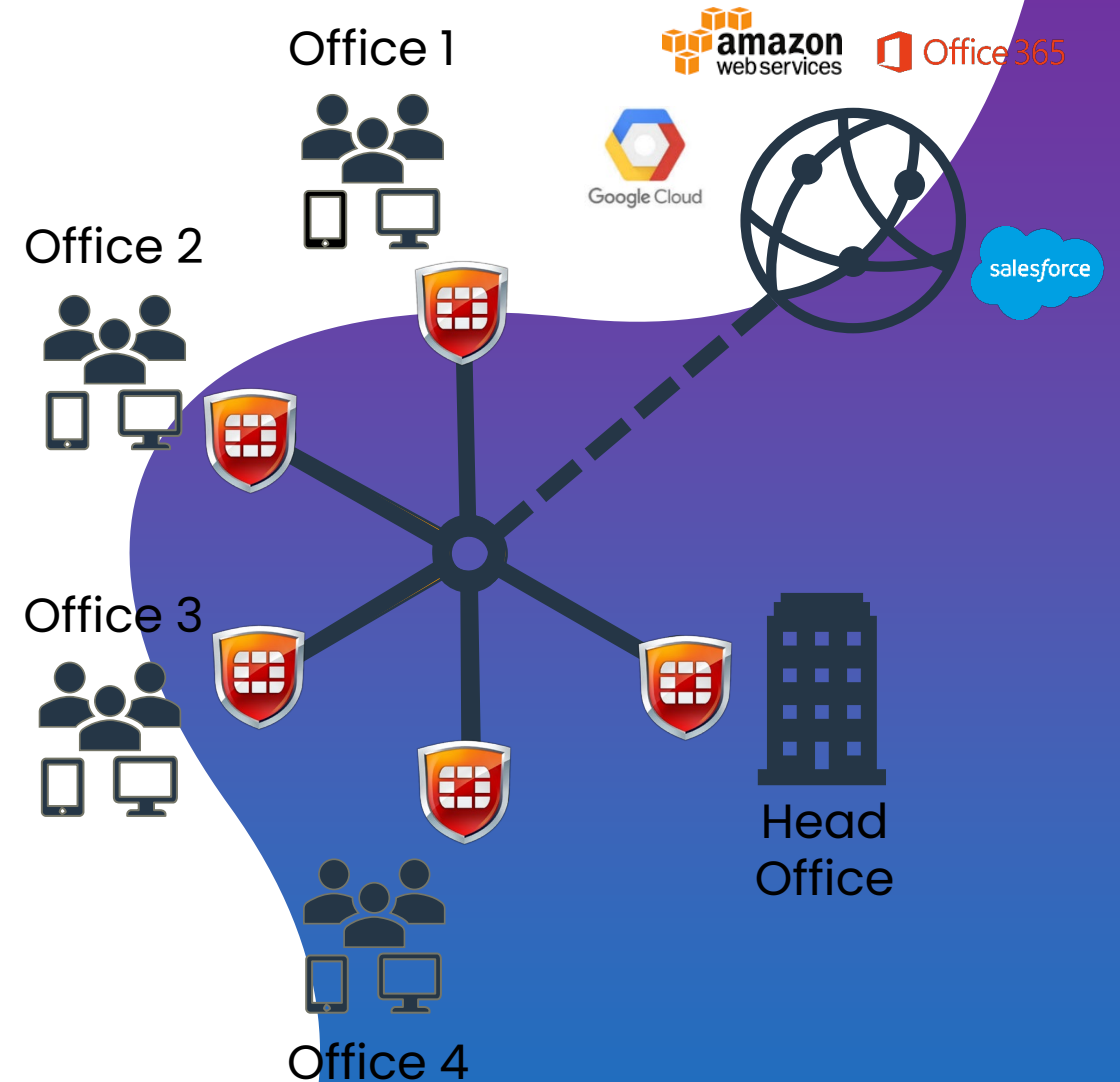
SD-WAN is Different

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

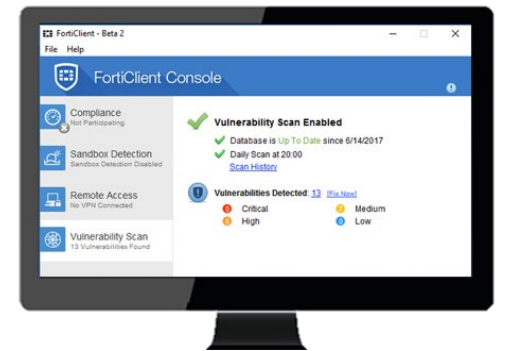
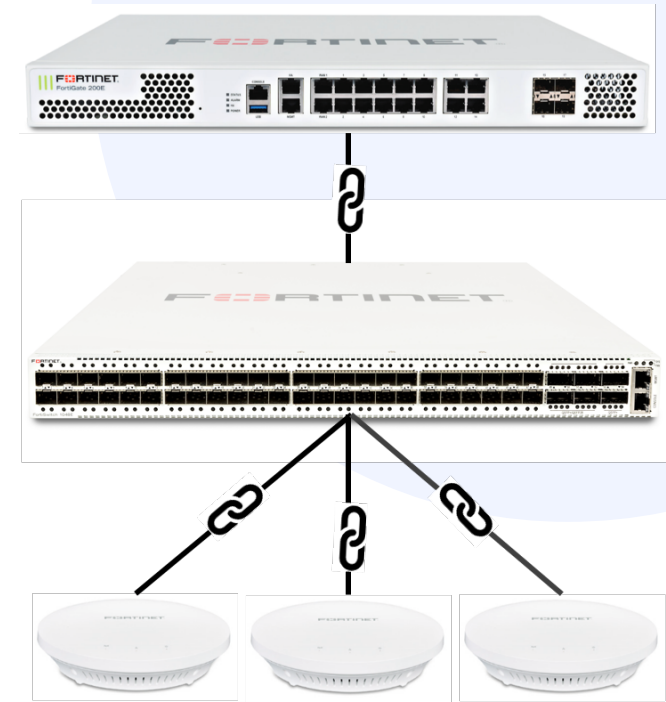
Security and Acceleration Everywhere

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

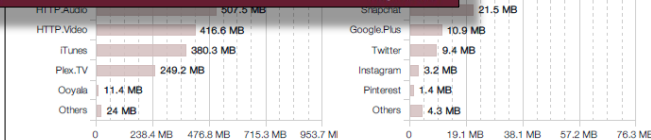


Maintaining a full security stack at the WAN edge is critical in any SD-WAN deployment where public Internet circuits are leveraged. Note that any threats observed within this report have effectively bypassed your existing network security gateway, so they should be considered active and may lead to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