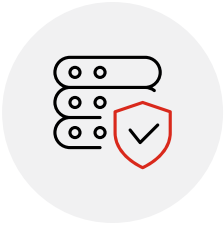
Engineered for Secure SD-WAN

Why organisations are choosing security-driven networking

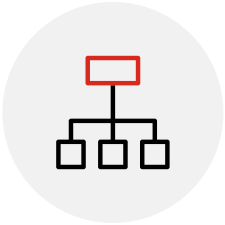
FORTINET®

Introduction

The remote working model is here to stay. It will operate alongside traditional headquarters and branch business models. By treating remote workers effectively as a branch, organisations can provision them faster, protect the business network more effectively, and save costs. Regardless of whether organisations are managing traditional branches or remote workers, it's essential to design networks with security in mind from the beginning. There are four key considerations to this:



1 **Securing the edge:** how users access their data is important, so securing the edge is critical. It's important to understand where digital assets are, how users interact with applications and data, and how to do this with security in mind.



2 **Simplifying the network:** network architects need to be able to simplify network design without sacrificing scale to make it easier to manage networks effectively even as they grow.

3 **Securing the cloud:** as services migrate to the cloud, more network edges are created, and security is a key concern.

4 **Reducing costs:** it is possible to bring in a highly reliable and robust security solution that is cost effective while bringing risk down to a more acceptable level.

Key challenges facing IT teams

Businesses have experienced a costly few months as they have provisioned more work-from-home users and, in many cases, re-tooled their business to cope with the disruption caused by COVID-19. Now that the initial flurry of activity has died down, organisations must review their networking and infrastructure arrangements, particularly in light of security concerns.

Many organisations find themselves racking up technical debt as a result of having to move fast. These organisations are choosing solutions that work now but are unlikely to continue providing significant value into the future. Reworking these limited, short-term solutions will cost time, money, and, potentially, opportunities into the future, creating a technical debt that companies will eventually have to pay.

These concerns were starting to emerge even before COVID-19 hit; businesses have had to accelerate their planned digital transformation and, in some cases, pivot to unplanned solutions to meet the immediate challenge. Companies are best served choosing the right solution from the start rather than using stop-gap approaches. This usually involves scaling using cloud solutions.

As organisations have been working fast to secure and enable the network, many are finding that their resources are stretched thin. Often, a single security team manages the entire distributed environment. Therefore, it's essential to have security solutions that are quick and easy to deploy and manage, and can reliably protect the organisation against known and unknown threats.

Increased reliance on the cloud to enable remote working and branches alike, means organisations need increased visibility into the environment. Managing everything in a single pane of glass is the gold standard for organisations looking to present a strong security posture while fully enabling remote working and branch structures.

IT faces increasing complexity and teams need to minimise this complexity, maximise the application experience and, where possible, reduce costs. SD-WAN and SD-Branch have emerged as the ideal solutions to these challenges as long as the chosen solution has security built in from the start.

IT teams have identified five key challenges that need to be addressed to secure the network and deliver strong user experiences:

1. Protecting the network edge.
2. Protecting endpoints and monitoring devices.
3. Securing and protecting access.
4. Zero-touch provisioning.
5. Improving the user experience.

This whitepaper explores these challenges and offers insights to address them using Secure SD-WAN and Secure SD-Branch technologies.

Secure SD-WAN and Secure SD-Branch

Secure SD-WAN dramatically simplifies traditional WAN complexity, and provides better cloud application performance and secure connectivity to the cloud. SD-WAN leverages a software-driven approach to choose the right path for the traffic coming to the WAN edge so even bandwidth-heavy applications deliver a strong user experience. However, security is missing from most SD-WAN solutions, creating significant risk for organisations, especially as the branch network edge expands.

Security is missing from most SD-WAN solutions, creating significant risk for organisations, especially as the branch network edge expands.

IT decision-makers must review business priorities and protect essential business assets. SD-WAN alone is no longer enough due to increased risk complexity, which is broadening the attack surface for cybercriminals. It's essential to protect the branch because new edges created by branch access to the cloud need to be secured. Digital transformation requires access to key applications at the edge, not through data centres that can cause latency. However, managing security at the branch requires resources that most enterprises don't have or can't spare, especially as they try to manage costs in an uncertain environment. This is why organisations must choose not just SD-WAN solutions but Secure SD-WAN solutions. Secure SD-WAN doesn't just manage traffic; it analyses it for threats and then remediates those threats as appropriate.

Secure SD-Branch integrates WAN and LAN platforms, reducing the number of devices required and extending Secure SD-WAN features into the network. It adds secure switches, wireless APs, access control, and LTE support, which helps consolidate devices and reduce management overhead. Regardless of branch location, or even if it's an individual, Secure SD-Branch makes it secure and manageable. It lets administrators discover and protect all endpoints when they seek network access, including unsecured IoT devices, and detect anomalies.

Low total cost of ownership

As Secure SD-WAN and Secure SD-Branch solutions can be seamlessly incorporated into the overarching corporate security framework, and one device can replace multiple point solutions, it offers a lower total cost of ownership.

Managing through a single pane of glass

The proliferation of point solutions, devices, and network edges makes managing security incredibly complex. Secure SD-WAN and Secure SD-Branch address this complexity by providing highly intuitive visualisations that can be accessed anywhere in the world to help teams monitor both the physical and logical network topologies at a high level, then drill down when needed to investigate any issues. Instead of managing a plethora of systems, teams can gain full visibility through one single pane of glass.

This functionality lets IT teams:

- update and disseminate corporate WAN policies to all locations or reconfigure individual devices
- set up IPsec VPNs with one click
- see both WAN and security functions in one view
- consolidate network operations centre (NOC) functions with security operations centres (SOC)
- reduce complexity and increase the efficiency of secure IT operations.

Here's how Secure SD-WAN and Secure SD-Branch can address the five key challenges faced by IT teams:

1 Protecting the network edge

Secure SD-WAN and SD-Branch converge security and network access, and manage all access layer, WAN, and security elements through a single pane of glass.

In the past, branches connected to the internet via the corporate network located at headquarters, and security was managed and controlled centrally. Now, branches are connecting directly to the internet, creating a new edge with new risks that need to be addressed. SD-WAN lets businesses manage this increasing complexity but doesn't address the security concerns directly. Secure SD-WAN is essential to deliver both visibility and security. It both manages traffic and analyses it for threats.

Securing the dynamic edge requires:

- zero trust and visibility to identify and secure users and devices on and off the network
- hybrid cloud convergence with a single security context across all infrastructure footprints
- dynamic cloud security to secure and control cloud infrastructure and applications
- artificial intelligence (AI)-driven security operations to automatically prevent, detect, and respond to cyberthreats.

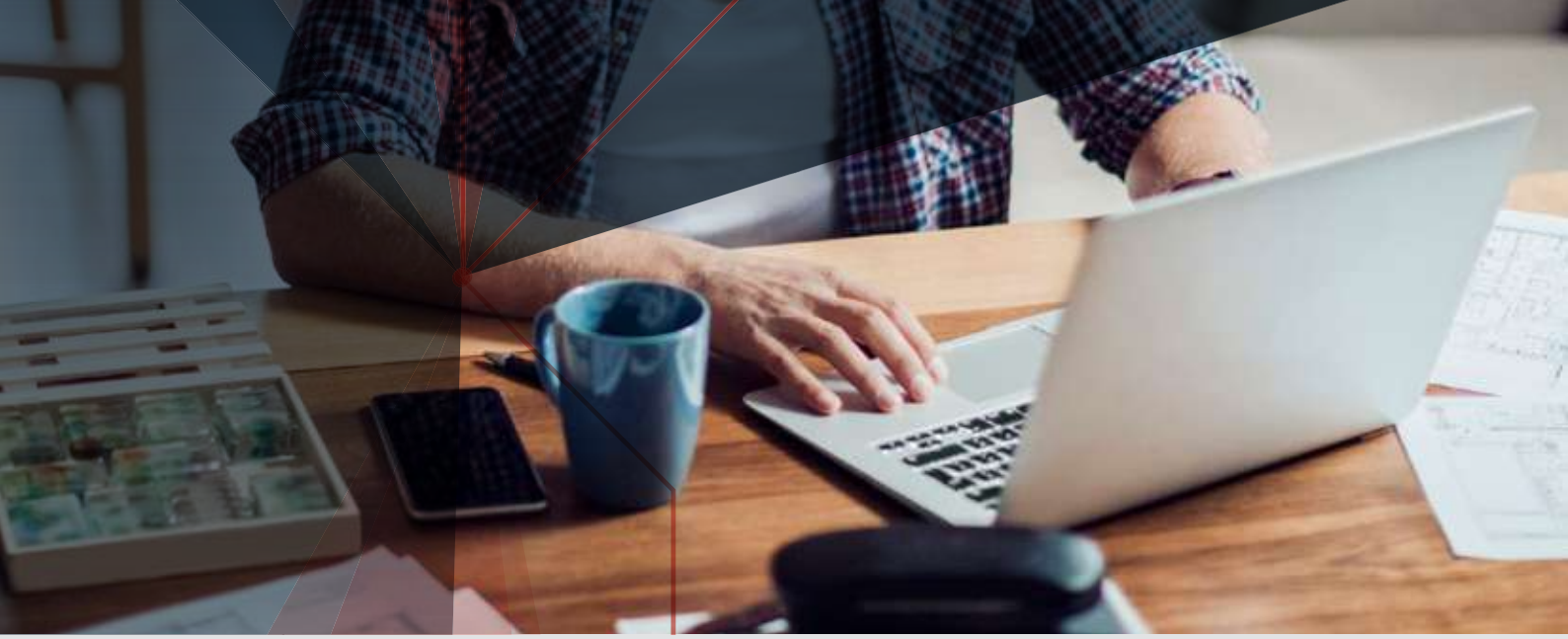
2 Protecting endpoints and monitoring devices

As new edges form, it's essential to protect endpoint devices regardless of whether they sit at a headquarters, branch office, or home office. Organisations can reduce the innate complexity in this mission by consolidating numerous devices and vendors down to one device that includes SD-WAN and security.

IoT devices and other endpoints entering the branch network introduce new vulnerabilities for attackers to exploit. Secure SD-WAN and SD-Branch technologies automatically discover, classify, and secure new devices as they enter the network. This increases visibility and anomaly detection without the need for additional equipment to be installed at every site.

Secure SD-WAN and SD-Branch technologies automatically discover, classify, and secure new devices as they enter the network.

It's also possible to monitor devices and gather information that can be used to determine whether device activity is suspicious based on benchmarks. Anomalous behaviour can be flagged and addressed faster, leading to fewer successful cyberattacks.



3 Securing and protecting access

With more users sitting outside the corporate firewall, managing access is an essential element in the overall security posture. Remote workers may not be using company-owned devices but these personal devices need access to the network so the employee can do their job. This creates a security risk because personal devices are rarely secured to the same level as corporate-owned devices. Therefore, simple Wi-Fi access management, even password-protected, isn't really enough to maintain strong security.

A secure access solution lets the organisation seamlessly and securely onboard user devices and provides captive portal services for guest access. With security and network management unified through a single pane of glass, any security measure can be applied to any user or device regardless of how it is connected: by wire; wirelessly; or by VPN.

4 Zero-touch provisioning

DevOps and zero-touch provisioning (ZTP) are crucial for organisations to move fast and effectively. ZTP offers quick and easy deployment and management, while local web traffic filtering and access to corporate applications through a VPN reduce bandwidth requirements.

ZTP is valuable because it's not secure to send fully configured devices to branches, and it's not feasible to send IT team members to every branch. Using ZTP, an unconfigured device arrives at the branch. When plugged in, it automatically connects to the deployment service in the cloud, is authenticated, and connected to the central system. This means security teams can reduce the amount of time they spend deploying, managing, and orchestrating policies across all security devices and extend this capability across branch locations without requiring additional IT staff on site.

5 Improving the user experience

With organisations increasingly depending on cloud-based systems and Software-as-a-Service (SaaS) for business tasks, users in the branch network and remote workers need to be able to access these applications with the same level of performance that's enjoyed by their colleagues in head office. This requires a solution that can identify applications, control the path they take, and secure access.

Users must be able to access the apps they need, when they need them. Bandwidth management and application controls are crucial for prioritising critical apps while blocking or throttling others. SD-WAN does this seamlessly but, if security isn't built in, it can actually create security vulnerabilities. Secure SD-WAN closes these gaps and provides secure access to mission-critical applications with peace of mind.

Fortinet SD-WAN and SD-Branch are leading the way

Unlike many SD-WAN applications, where security is added as an afterthought, Fortinet delivers Secure SD-WAN as an integrated feature of its next-generation firewall. This means security is built in from the ground up, rather than being bolted on afterwards. This approach delivers more reliable and responsive security while simultaneously delivering all the experience, performance, and cost-efficiency benefits of SD-WAN.

Security is an essential component of SD-WAN because SD-WAN bypasses the centralised protection that would be provided by backhauling traffic through the data centre. Additionally, most SD-WAN solutions can't inspect the encrypted traffic that makes up most network traffic today. This is a target area for cybercriminals, making built-in security a must-have for SD-WAN solutions.

Fortinet's Secure SD-WAN solution provides both networking and security for branch networks in a single, consolidated solution, minimising complexity and maximising security. This lets organisations enforce security consistently and manage it through a single pane of glass. Fortinet's Secure SD-WAN solution is the only SD-WAN offering with a next-generation firewall and centralised management, as well as SSL inspection for application identification accuracy.

Fortinet has achieved significant industry recognition for its Secure SD-WAN solutions. For example, Fortinet was placed highest in ability to execute in the challengers quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure.[1] NSS Labs independently evaluated eight SD-WAN products and found Fortinet to have the highest value and the lowest total cost of ownership.[2] Fortinet was also named the 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure for its Secure SD-WAN solutions. This distinction is based on feedback and ratings from end-user professionals who have experience purchasing, implementing, or using Fortinet Secure SD-WAN.[3]

Fortinet's Secure SD-WAN customers tend to achieve five unique benefits:

Cost reductions of up to 40 per cent while simplifying the network

Improved user experience by five times for business-critical applications

Reduced WAN complexity by simplifying workflow for both security and SD-WAN

Time savings of more than 90 per cent with automation

Lower MPLS costs.

Using the SD-WAN ROI calculator [**www.fortinet.com/products/sd-wan#secure-sdwan-roi-calculator**], it's possible to see just how much organisations can save with Fortinet Secure SD-WAN.

1 https://www.globenewswire.com/news-release/2019/12/04/1956335/0/en/Fortinet-Placed-Highest-in-Ability-to-Execute-in-the-Challengers-Quadrant-of-the-2019-Gartner-Magic-Quadrant-for-WAN-Edge-Infrastructure.html
2 https://searchnetworking.techtarget.com/news/252465526/Fortinet-TCO-low-Silver-Peak-high-in-NSS-Labs-SD-WAN-report
3 https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2020/fortinet-recognized-as-2020-gartner-peer-insights-customers-choice-for-wan-edge-nfrastructure

Next steps

SD-WAN is the future of networking. Choosing a highly secure, robust, and reliable SD-WAN solution is crucial to avoid unnecessary technical debt and gain faster access to the benefits offered by SD-WAN.

To find out if SD-WAN is right for your business, Fortinet can conduct a Secure SD-WAN assessment report. This report will help you understand the limitations of your current network as well as the potential benefits you could gain from implementing a Secure SD-WAN solution.

For more information on the assessment, visit
https://www.fortinet.com/offers/secure-sd-wan-assessment