



EBOOK

INCREASING AGILITY, PERFORMANCE & SECURITY WITH SD-BRANCH

A NAK connecting the dots guide



EXEC SUMMARY

The Internet of Things (IoT), cloud and SaaS applications, bring-your-own-device (BYOD) and guest Wi-Fi are all exponentially adding complexity to the branch IT infrastructure, whether that be in a retail outlet, a restaurant, a café, or a regional office. IT teams are under significant pressure to deliver the best possible experience at every location, while at the same time rise to the challenge of moving at speed and maintaining and securing a now very complex environment.

Whereas the IT needs of the remote location have changed significantly over recent years, the fundamental architectural topology has not, and this is creating unacceptable security risk, unmanageable IT workloads and an inability to move at the pace required by the business.

We believe it is time for distributed organisations to re-imagine their branch infrastructure. To converge security and networking, to embrace the software-defined era and create a modern, digital infrastructure that is secure, reliable, and agile.

SD-Branch is the concept of redefining the network edge in the branch and providing that single pane of glass onto your branch infrastructure. It enables you to connect your end-to-end network, optimise branch connectivity, perform zero-touch provisioning, and provide your centralised teams with greater visibility and control of your distributed environment.

Over the coming pages we provide you with NAK's perspective on SD-Branch and the value it delivers.

SECURING BRANCH INFRASTRUCTURE

The branch is no longer a contained environment where a handful of owned devices are authenticated by your network and all traffic is routed via and secured in your centralised infrastructure. Today, your branch network must support IoT devices, a multitude of handheld wireless devices, employee devices and a guest Wi-Fi service. What is more, you are unlikely, or should not be, backhauling all traffic to your centre as much of it is destined for the cloud or internet.

This means that you have an exponentially greater attack surface area and this needs to be secured. You need to protect this redefined network edge and protect everything that is directly or indirectly connecting to your branch network.

A Fortinet SD-Branch solution provides you with that first step towards taking a SASE approach to securing the network edge and creating a Zero-Trust network. It enables you to place a next-generation firewall at each location that not only protects your network-edge to internet or WAN connections, but to extend across every part of your branch network and secure every device connecting to this network.

While it is estimated that **25%** of cyber-attacks are targeting IoT, less than **10%** of IT security budgets are spent on securing these devices.

Source: RetailTouchpoints



OPTIMISING BRANCH CONNECTIVITY

Over recent years we have seen a major advance in WAN technology and a significant take-up of SD-WAN solutions. This is enabling distributed organisations to optimise the cost of their connectivity while at the same time deliver a far better end-user experience.

In simple terms SD-WAN places intelligence within the branch that analyses every network request and determines the best possible route for this traffic. Access to cloud or SaaS based applications is routed directly over lower-cost direct internet connections, while access to centralised systems continue to be routed over point-to-point managed WAN connections.

With Fortinet SD-Branch, you gain the ability to not only secure the branch network, but to introduce SD-WAN intelligence at those locations where it will deliver the greatest benefit. The FortiGate solution is not only a next-generation firewall but provides you that software-defined network gateway delivering a leading SD-WAN solution. This allows you to optimise connectivity at each site and then gain the multitude of benefits of SD-WAN including greater resilience, cost/performance, and end-user experience.

It is estimated that over half of organisations have implemented some form of SD-WAN and 90% of organisations have plans to adopt or extend SD-WAN deployments.

Source: IDG Research

AGILITY THROUGH ZERO-TOUCH PROVISIONING

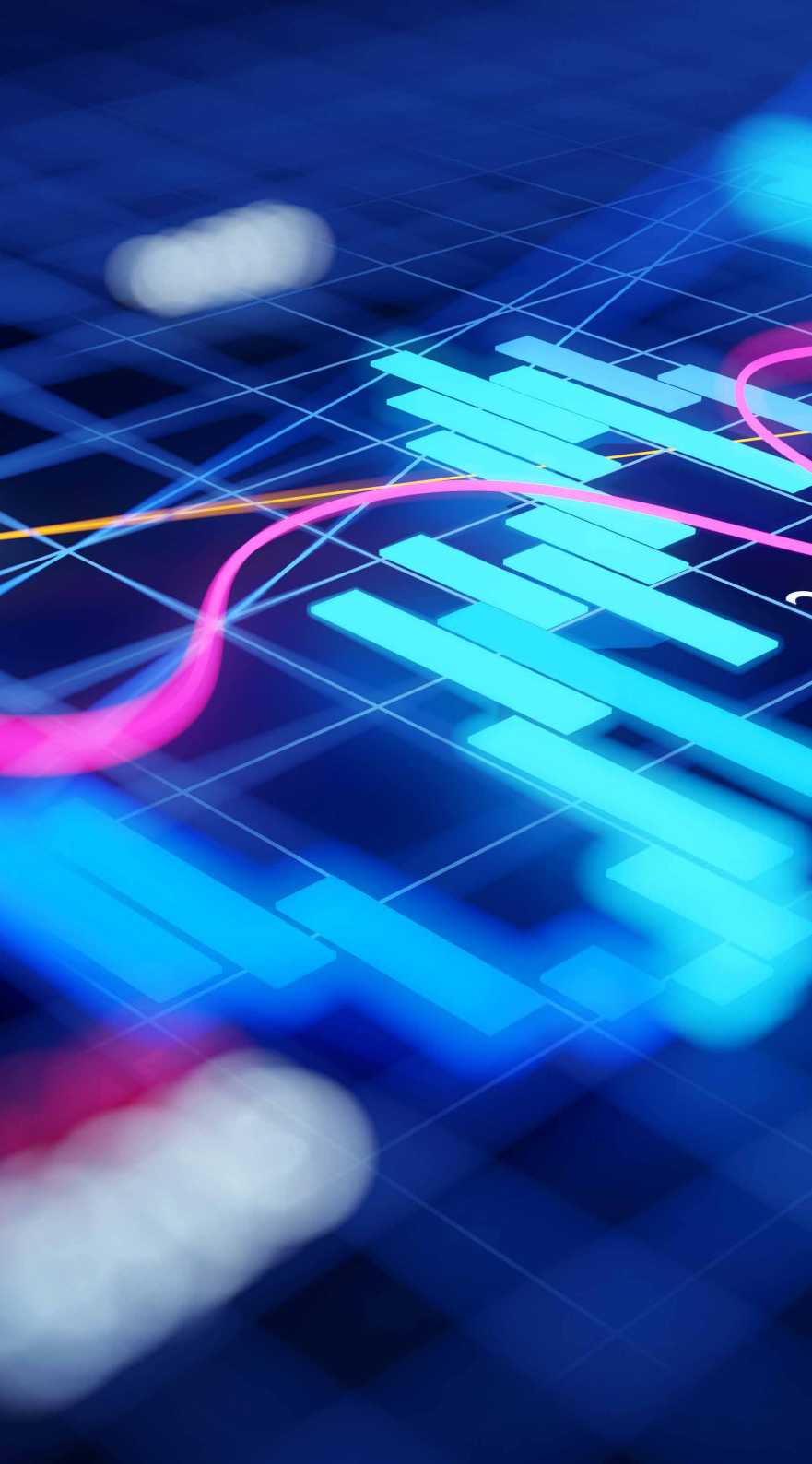
In many sectors such as retail and hospitality, agility is key in managing a branch network. IT teams are expected to be able to provision new locations at speed, to scale or move locations and even support temporary 'pop-up' locations. In order to do this what is required is the ability to simplify branch infrastructure and for this to be provisioned with little or zero-touch onsite provisioning.

Cloud managed infrastructure is changing the game for IT teams managing distributed networks. This is where their adoption of a software-defined network enables the control and configuration to be extracted from the physical hardware and a managed layer hosted in the cloud. This allows an appliance to be simply plugged in and if it has internet access, it can effectively call home and download its configuration.

With Fortinet SD-Branch you gain a zero-touch provisioning solution. A security and networking solution that is cloud-managed with your centralised teams having full control over your branch infrastructure regardless of their location. They gain full visibility, control, and management. Configuration becomes standardised across your entire branch network and a centrally defined security policy consistently applied across your end-to-end environment.

“Almost half of IT teams believe they spend too much time managing the network.”

Source: Sirkin Research



GREATER VISIBILITY & PERFORMANCE

The branch network is often made up of different technologies layered on top of each other, WAN, LAN, wireless and multiple security solutions. This makes it virtually impossible to gain a holistic view of the infrastructure and how this is operating.

With SD-Branch this all changes as you are able to deploy a single solution that encompasses all of the components. Not only do IT teams gain the ability to manage and optimise the infrastructure remotely, but also to monitor performance and gain detailed visibility. This means that issues can be detected quickly and leveraging AI powered ML resolved immediately. It also means that the network and security elements are working together to prevent cyber threats with anomalies in network activity being immediately flagged to prevent breaches.

SD-Branch also provides your IT team with far greater control of your distributed network. As a software-defined infrastructure you gain the ability to define policies centrally and to have these automatically applied across the end-to-end network. This creates consistency that is always easier to manage, and it also ensures that every location and every component is continually optimised.

Over two-thirds, **67 percent** of organisations say that network blind spots are one of the biggest challenges they face when trying to protect their data.

Source: Vanson Bourne Survey

THE VALUE DELIVERED WITH SD-BRANCH



Increase Agility

By simplifying deployment and utilising a software defined infrastructure, you significantly increase the speed at which you can respond to business need.



Improve Visibility

By unifying every part of your branch infrastructure, you'll gain unprecedented visibility across your end-to-end network.



Improve Experience

By leveraging AI powered ML to continually monitor and optimise your branch network and ensure the best possible experience is always delivered.



Reduce Risk

By putting in place market leading security at every branch and ensuring that your security policies are consistently applied in each and every location.



Reduce Management Overhead

By providing you with a cloud-managed infrastructure with zero-touch provisioning, reducing the time your team spends managing the network.



Reduce Cost

By embracing SD-WAN to optimise connectivity and delivering a far better cost/performance, with resilience and without provider lock-in.



HOW CAN NAK HELP

NAK are not just a Fortinet Partner, we have extensive experience of providing secure managed network to distributed organisations. We are helping our customers to take incremental steps towards a SASE based architecture that combines networking and security and embraces the SDN era. We can help you to review your current branch-based technology in terms of business needs, performance and security, and assist you in building a future roadmap to take you to where you want to be.

Let's Start With A Chat

We are more than happy to connect you with one of our technical specialists. By talking to them you can quickly gain an understanding of what is possible, and the approach being taken by similar organisations.

Let Us Take A Deeper Look

We also offer a more detailed look at your current environment. As a Fortinet Partner we participate in their Cyber Threat Assessment Program (CTAP) which enables us to provide a detailed assessment of your branch environment both in terms of network traffic and SD-WAN readiness, and current level of threat detection and prevention. We would be more than happy to understand where you have concerns and perform the appropriate assessment.

To take either of these next steps, simply contact the team on:

Call: 0300 456 0471

Email: enquiries@nak.co.uk

Web: nak.co.uk