



SD-Branch Customer Success Stories

Real-World
Benefits of
the Fortinet
SD-Branch
Solution



Table of Contents

Executive Summary	3
Introduction	4
Why Fortinet SD-Branch?	6
SD-Branch Architecture	8
7 Customer Success Stories	9
Conclusion	17



Executive Summary

Software-defined branch (SD-Branch) is a solution for distributed organizations that builds on software-defined WAN (SD-WAN) to improve application performance. Adding Ethernet and Wi-Fi from the same vendor enables unified networking at a branch location.

Taking it a step further, Fortinet SD-Branch converges networking and security products to deliver all the networking and security functionality a branch requires in one integrated solution. It includes SD-WAN, next-generation firewall (NGFW), Ethernet switching, Wi-Fi access points (APs), and 5G/LTE gateways. All of these components use a single operating system and are managed with one user interface.

This ebook covers the details of branch network challenges and how Fortinet SD-Branch solves them. It also offers examples with customer success stories. These Fortinet case studies come from organizations across industries, including retail, healthcare, finance, and energy.



Introduction

SD-Branch is a site model (especially for remote sites) in which most network and security equipment is managed within a single pane of glass. SD-Branch technology usually includes SD-WAN, network security (firewalling), Ethernet switching, Wi-Fi APs, and 5G/LTE gateways for redundant WAN links. SD-Branch allows IT professionals to aggregate the control and management of branch networks, allowing largely distributed branch deployments to have a single point of management.

Why is SD-Branch needed?

As digital acceleration has required branch networks to do more, IT administrators often struggle to attain control and visibility over these networks. As business-critical IoT use at branches has increased and applications have shifted to a multitude of clouds, it has become even more difficult to ensure network security and reliability.



SD-Branch helps solve these challenges with the following:

High performance

User experience and device performance are often key drivers for the shift to SD-WAN from older MPLS technology. By including SD-WAN as part of an SD-Branch deployment, IT teams can leverage features like application awareness, accurate traffic identification (even if encrypted), multi-path intelligence, network segmentation, and WAN resiliency. This guarantees that all user and device applications receive optimal performance, regardless of what systems they need to communicate with.

Visibility

Many SD-Branch deployments feature a large number of remote sites with little to no on-site IT presence. Disparate networking equipment can limit IT visibility into what devices are connecting to the network

and how to ensure that they are placed in proper security contexts. SD-Branch solutions allow for improved visibility, as all on-site equipment is part of a single solution.

Easy management

SD-Branch simplifies management by consolidating the number of management interfaces that IT teams need to use to manage a branch. This reduction in management overhead allows IT to focus on strategic initiatives rather than day-to-day network management.

What organizations need SD-Branch?

SD-Branch is suitable for any distributed organization moving to SD-WAN to improve application performance and simplify management across security and networking. The more sites in the network and the smaller the IT team, the more value SD-Branch will bring.

“With Fortinet, I was able to go from a team of five people just managing all this different infrastructure, to one person and a help desk.”

– Minh Le, Chief Information Officer, Checkers Drive-In Restaurants





Why Fortinet SD-Branch?

The components of our industry-leading SD-Branch solution, SD-WAN, network firewall, and wired and wireless LAN equipment all receive top marks from analysts. The Fortinet SD-Branch solution is part of the Fortinet Security Fabric platform, centered on our industry-leading firewall and the operating system that runs on it, FortiOS. This enables security and networking products to converge and work together to provide the most secure and reliable branch network possible.

Fortinet LAN equipment is managed by the FortiGate Network Firewall, allowing for a single source of truth for the branch. FortiGate also includes comprehensive SD-WAN capabilities to automatically find the shortest path to corporate applications, enabled by intelligent steering and dynamic routing capabilities native to FortiOS.

Fortinet provides a full “branch-in-a-box” solution with rapid deployment capabilities that are simple and effective to manage while offering reliable security.



Advantages

The key advantages of Fortinet SD-Branch are:

- **Full visibility into branch operations** (both networking and security)
- **Ease of management** with a single pane of glass to configure, deploy, and manage security, SD-WAN, WLAN, LAN, and WAN backhaul
- **Automated onboarding and protection of IoT devices** with built-in NAC and virtual patching capabilities
- **Low total cost of ownership** through reduced licensing and decreased management overhead

With these advantages, organizations using the Fortinet SD-Branch solution achieve better business outcomes.

Differentiators

Fortinet SD-Branch is unique in providing:

- **Security to the edge:** Simplified networking and security policy management with a single point of control improve operational efficiency and branch security.

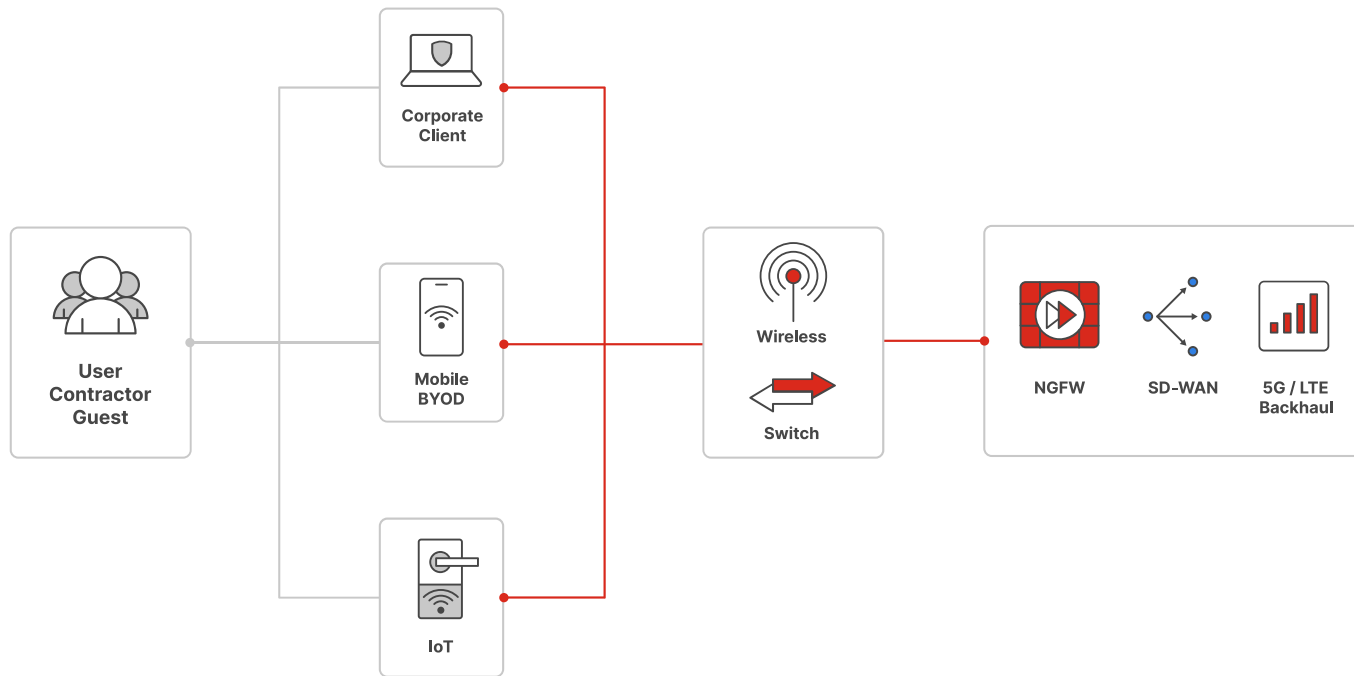
- **Improved device visibility and control:** Built-in features for branch IoT allow for the secure onboarding of headless devices onto the network via NAC rules built into the tool.
- **Management ease:** All network components (LAN, WLAN, WAN) are integrated with the Fortinet Security Fabric, allowing a single configuration file to contain all networking and security settings.

No matter the deployment size, the Fortinet SD-Branch solution will fit an organization's unique needs. Our solution is flexible, offering firewalls, switches, and APs in a variety of sizes and form factors. Wherever an organization is on its digital acceleration journey at its branch, Fortinet will consolidate security and networking to reduce complexity, increase security effectiveness, provide consistent policy orchestration and enforcement, and ensure a reliable user experience across all applications.



SD-Branch Architecture

The Fortinet SD-Branch solution offers protection and convergence from the LAN to the WAN.



7 Customer Success Stories

Fortinet SD-Branch is the industry's most secure convergence of networking and security. It offers SD-WAN, firewall, wired Ethernet, Wi-Fi access points, and 5G/LTE gateways, all within our unified Security Fabric platform. The following testimonials detail how Fortinet's unique approach offers organizations a simple and secure path to SD-Branch

1

Family-Owned Supplier of High-Quality Hire Equipment Improves Customer Experience with Fortinet SD-Branch



Customer Overview

Operating for over 70 years across Australia and New Zealand, with 1,500 employees and three data centers globally, Kennards Hire needed to stay ahead of the curve with technology and security. The company prides itself on customer service, and technology is key to turning that into a competitive advantage. To improve efficiency and reduce internet connectivity costs for more than 180 branches, Kennards Hire deployed Fortinet SD-Branch.

Challenges

- Needs to empower employees to increase efficiency
- Requires a cost-effective solution
- Must support flexible communication between all 180 branches

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiExtender
- FortiManager
- FortiAnalyzer

Business Outcomes

- Improved network performance and reliability
- Enabled rapid rollout: 20 minutes to bring a branch's networking and security online
- Deployment of SD-Branch to 180 branches in eight weeks
- Reduced staff resources required to manage security and networking
- Saved the business hundreds of thousands of dollars per year

[Read the case study](#)



2

Pharmacy Chain Builds a Secure Network and Expands Its Retail Services with Fortinet LAN Edge and Secure SD-WAN



Customer Overview

Several years ago, a large Brazilian retail pharmacy chain had ambitious plans for growth by launching new stores and implementing digital innovation for employees and customers. However, its aging network would not support such demand, so Pague Menos searched for a new solution to converge networking and cybersecurity.

Challenges

- Desire for new solutions to support the company's growth plans
- Requirements for secure and reliable solutions that support business-critical applications
- Need to improve the reliability of connections between store locations and corporate offices

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiAP
- FortiADC
- FortiManager
- FortiAnalyzer

Business Outcomes

- High availability of network infrastructure to support about 1,600 stores
- 60 new digital services available to customers in real time
- Complete network visibility and easy management in a single pane
- Secure connection that ensures reliability and data confidentiality

[Read the case study](#)



3

Skilled-Nursing Company Taps Fortinet Secure SD-Branch for Converged Networking and Security



Customer Overview

Diversicare operates 61 skilled nursing centers across the United States. Its critical task is to ensure that core systems are highly reliable and patient information remains secure. However, its network and security infrastructure involved too many vendors and was too complex to manage.

Challenges

- Complex landscapes and multi-vendor system strain small IT team
- Problematic technical debt from previous solutions
- Hard to comply with HIPAA regulations
- Need simplified management

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiNAC
- FortiManager
- FortiAnalyzer

Business Outcomes

- Improved security for patient information and other vital data
- Strengthened compliance with federal regulations regarding patient care and data security
- 40% reduction each week in staff time spent managing network and security infrastructure
- Improved ability of IT staff to fill in for one another when needed
- Streamlined corporate expansion through the easier rollout of standard technologies to new skilled-nursing centers

[Read the case study](#)



4

Spanish Renewable Energy Company Sets New Industry Benchmark for Secure IT/OT Convergence in the Cloud



Customer Overview

Capital Energy has a role in the entire renewable energy generation value chain of Spain and Portugal. To support its digital transformation, the company required a partner that could help manage the complexity of its converged IT/OT environment, increase cybersecurity, and support the company's Google Cloud footprint.

Challenges

- Complying with new energy regulations mandated by the EU
- Achieving digital transformation to support goals for sustainable growth
- Finding a solution capable of managing complex IT and OT environments
- Enabling secure access to third-party contractors

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiManager
- FortiAnalyzer
- FortiSIEM

Business Outcomes

- Increased access security through a cloud-based access hub for third-party contractors
- Enhanced OT data acquisition security through secure SD-WAN architecture
- Increased visibility and simplified administration with the Fortinet Security Fabric platform

[Read the case study](#)



5

Fortinet Helps Checkers Drive-In Restaurant Chain Improve Management and Visibility and Keep Its Traffic Flowing



Customer Overview

Checkers Drive-In Restaurants, Inc. is a quick-service restaurant chain with 265 corporate-owned locations and another 600 franchise locations across 38 states. Before working with Fortinet, the Checkers' CIO said the company's infrastructure was "a mess."

Challenges

- Improving standardization and reliability
- Employing more innovative solutions
- Replacing an IT environment where nothing was managed
- Achieving high availability

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP

Business Outcomes

- Saved Checkers millions of dollars in personnel costs over a two-to-three-year period
- Provides high availability and centralized management at scale, with full control over security
- Protects hundreds of locations with outstanding threat intelligence
- Enables Checkers to meet its goal of opening 100 restaurants per year

[Read the case study](#)



6

African Bank Adopts Zero-Trust Access Strategy with New Integrated SD-WAN Security Architecture



Customer Overview

With a strong focus on clients, integrity, and professionalism, one medium-sized African bank offers an extensive range of private and corporate financial services driven by teamwork and customer focus.

Challenges

- Financial institutions in Africa are a popular target for cybercriminals
- Desperate need to reevaluate its IT security defenses
- Legacy system was complicated and costly to manage

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiAP
- FortiSwitch
- FortiClient
- FortiNAC
- FortiManager
- FortiAnalyzer
- FortiWeb

Business Outcomes

- Increased resistance to attack with more granular zero-trust access control
- Reduced administration time and the cost of site visits through central visibility and control
- Increased application performance and protection through greater traffic segmentation
- Gained the ability to properly assess security posture, easing the task of Payment Card Industry Data Security Standard compliance
- Reduced WAN costs by 50% through the replacement of MPLS links

[Read the case study](#)



7

Fortinet Saves Waste Management Inc. \$100 Million Over Five Years**Customer Overview**

Houston, Texas's Waste Management, Inc. is North America's largest waste management and environmental services company, providing services that range from collection and disposal to recycling and renewable energy generation. Its more than 42,000 employees support nearly 21 million residential, industrial, municipal, and commercial customers.

Challenges

- To easily deploy a solution that has the speed and security required
- To upgrade slow network connectivity to handle modern applications
- To cut costs on existing MPLS and the provider's annual billings of \$35–\$40 million
- To prepare for the future of networking and cybersecurity

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiManager

Business Outcomes

- Upgraded 1,200 sites within six months
- Engineers quickly brought up to speed
- Fortinet delivered better ROI
- Reduced IT's annual budget by roughly \$20 million

[Read the case study](#)

Conclusion

The right SD-Branch solution lets IT administrators gain control and visibility over branch networks. Fortinet SD-Branch delivers on the key needs for IT groups struggling to manage branch networks at scale. Wherever your organization is on its digital acceleration journey, by consolidating networking and security products and managing both in a single pane of glass, you can reduce complexity, provide consistent policy orchestration and enforcement, and ensure a reliable user experience across today's expanding networks with Fortinet. For more information, visit our [SD-Branch webpage](#).





www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 14, 2024 3:28 PM / 2865037-0-0-EN