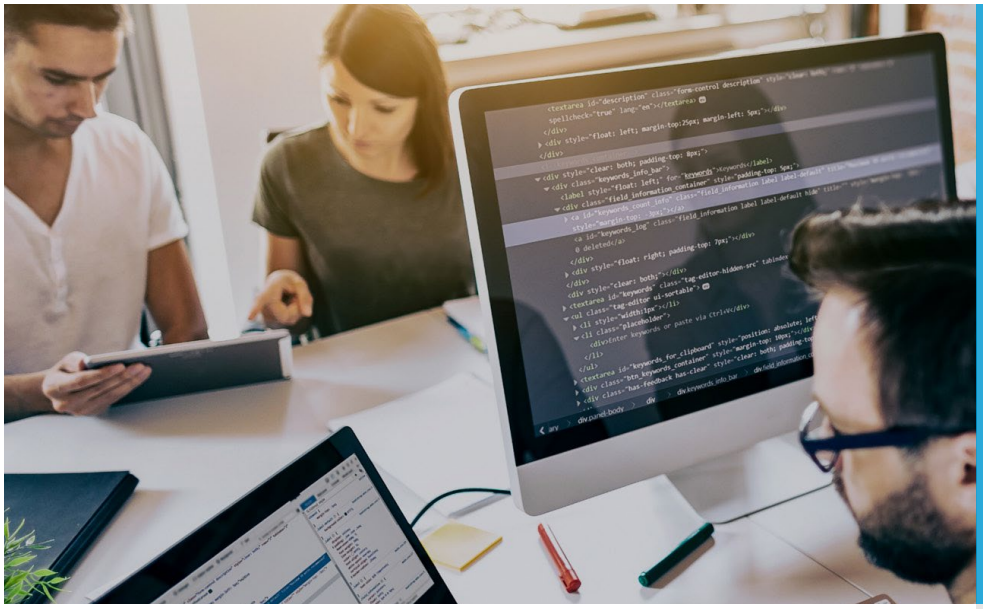
AT&T Cybersecurity

AT&T Business

AT&T SASE Branch with Fortinet



Take your collaboration needs to the clouds and back with the **#1 managed SD-WAN provider*** in North America.

Built-in security at the WAN edge with industry-leading performance.

Connecting and protecting every user, device, and network edge

If your business existed just five years ago, it probably looked very different from today, at least in terms of connectivity. Today you need flexibility to operate in many locations, connect remote employees, and meet your customers' desires for high quality experiences on demand. Cloud-based applications and tools can give you that flexibility. But is your network keeping up?

Many businesses are switching from legacy wide-area networks (WANs) to software-defined WANs (SD-WANs). SD-WAN offers faster connectivity and cost savings. It also means better performance for software-as-a-service (SaaS) applications, digital voice, and video services. In fact, 60% of enterprises will implement SD-WAN by 2024 to meet increasing needs for SaaS applications and cloud services. Fewer than 20% of companies used SD-WAN in 2019.[1]

Potential benefits

- Boosts application performance
- Improves network resiliency
- Supplements MPLS
- Reduces security risk
- Reduces the number of devices deployed and hosted within the data center
- Keeps users connected to the applications they need most, even when network traffic is high
- Provides visibility and security to your network
- Boosts IT efficiency with deployment, policy design, 24x7 monitoring, maintenance, and troubleshooting by AT&T Security Network

* Frost Radar™: North American Managed SD-WAN Services Market, 2021

[1] "Forecast Analysis: Enterprise Networking Connectivity Growth Trends, Worldwide," Gartner, September 20, 2019

Traditional WANs are often set up with a "hub-and-spoke" design that routes traffic through a data center for filtering and security checks. This increases latency and slows performance. These legacy WANs struggle as more devices and users connect to them. Often, traditional WANs can't meet the performance demands of cloud-based tools like voice over IP (VoIP) and videoconferencing. Your customers have high expectations and more devices, so it's more important than ever to maintain a stable, fast, and secure connection.

Connecting your branch offices directly to the internet can improve performance while reducing costs. Moving to a more distributed cloud connectivity model means you can use widely available, low-cost options for connectivity such as broadband, 4G/LTE, and 5G. Using SD-WAN you can also manage data flow, improve network resiliency, and prioritize bandwidth for business-critical applications. And you'll be better able to meet higher demand from remote workers.

SD-WAN for today's threat landscape

The move to SD-WAN brings some challenges along with connectivity, performance, and financial gains.

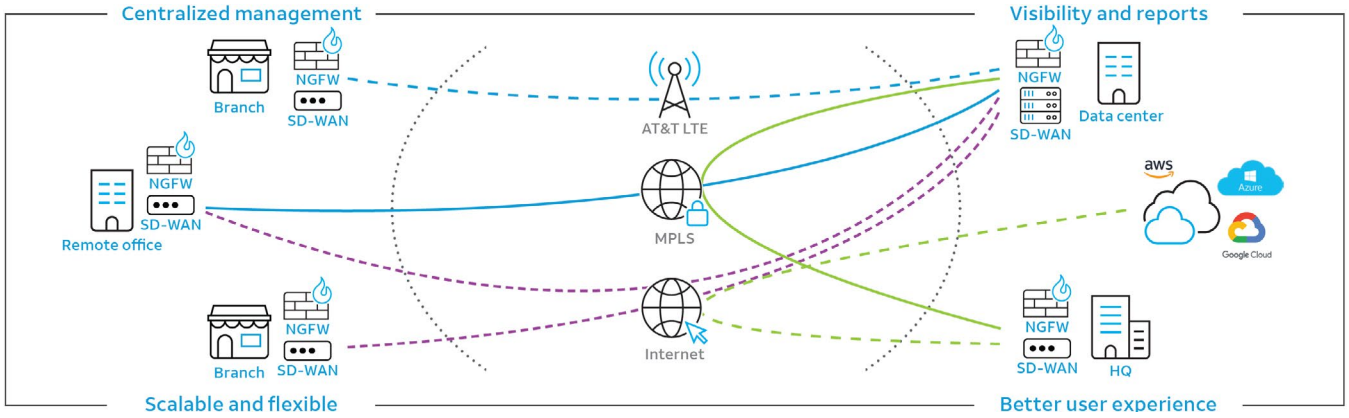
- **Complexity:** SD-WAN architectures can be difficult to troubleshoot and manage across all branches. This adds to the burden on limited IT staff and often creates unknown gaps for threats to exploit.
- **Security:** Connecting directly to the Internet adds new risks compared to routing traffic through a data center. In effective SD-WAN networks, security is built into the entire infrastructure. Direct internet connections are more secure and high volumes of traffic can be inspected without inhibiting network performance.
- **Encrypted traffic inspection:** Most SD-WAN solutions can't inspect network traffic that uses secure sockets layer (SSL)/ transport layer security (TLS) encryption, which makes up over 90% of network traffic across Google today.[2] This potentially leaves them at risk from cyber-criminals hiding malware in networks to steal data. You can accept the risk or buy more appliances to inspect encrypted traffic at the edge of the network.

[2] Source: Based on data provided by Google in their latest Transparency Report https://transparencyreport.google.com/https/overview?hl=en

Enter secure networking — AT&T SASE Branch with Fortinet

AT&T Business has traditionally supported advanced networking features like dynamic routing, IPv4/v6, and multicast support. Now, our next-generation firewalls (NGFWs) with Fortinet provide both networking and security for branch networks in one solution.

With an integrated NGFW and SD-WAN solution, you can improve both WAN efficiency and security. Using AT&T SASE Branch with Fortinet you can enforce policies consistently across your branch locations. Plus, IT and business leaders can mitigate risks from digital transformation.



Key SD-WAN capabilities included with AT&T SASE Branch with Fortinet

Application awareness and automated path intelligence

With traditional WAN, it can be hard to maintain the quality of user experience per application. Traditional WAN infrastructure relies on packet routing. Packet routing limits application visibility and, in turn, the ability to set granular controls.

AT&T SASE Branch with Fortinet uses “first-packet identification” to identify applications from the leading packet of data traffic. This broad application awareness helps analysts at the AT&T Security Network Operations Center (SNOC) understand which applications are being used across the enterprise. Then, they work with you to make informed decisions about SD-WAN policies. The solution references an application control database of over 5,000 applications, a number that grows as threats and the digital network evolve.

Application awareness opens the doors to automated path intelligence. You can set priorities for routing across the network based on the specific application and user. The solution uses the application's SLA and selects the best WAN link/connection for the situation. AT&T Business next-generation firewalls with Fortinet enable one of the fastest application steering methods in the industry and unrivaled application identification performance. Related features include:

- **WAN path remediation,** which uses forward error correction (FEC) to overcome adverse WAN conditions like poor or noisy links. This makes the transmission of data more reliable and improves user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic. This enables the receiving end to recover from packet loss and other errors that occur when the data is sent. It also improves the quality of real-time applications.
- **Better network resiliency,** to accommodate more devices, cloud application use, and remote workers. Your business can thrive in a changing digital landscape.
- **Tunnel bandwidth aggregation,** which provides per-packet load balancing and delivery. The firewall does this by combining two overlay tunnels to maximize network capacity if an application requires more bandwidth.
- **Automatic failover capabilities,** which change to the best available link when the primary WAN path degrades. This automation is built into the NGFWs. It improves the end user's experience and productivity.

NGFW security and compliance

AT&T SASE Branch with Fortinet delivers enterprise-class security and branch networking capabilities in one solution. Critical security features include:

- **SSL/TLS inspection and threat protection** for visibility and prevention against malware. You won't need separate encryption inspection appliances.
- **Web filtering service** to enforce internet security and reduce complexity.
- **Complete threat protection** anti-virus, and intrusion prevention system (IPS)
- **Highly scalable overlay VPN tunnels** with high throughput to encrypt traffic and keep it confidential
- **Granular SLA analytics,** including application transactions for quick remediation.

AT&T SASE Branch with Fortinet also offers the Branch-in-a-Box option to supercharge your network and productivity. This package includes:

- Fortinet **switches** to help extend network and security controls to the LAN. With these switches, you can have more LAN connections and granular controls for each LAN segment.
- Fortinet powered **access points** give you more visibility and control of wireless network traffic by enforcing the same policies as the wired network.
- Fortinet **extenders** provide an LTE-based backup WAN connection. They can also serve as a primary connection to kiosks, retail pop-up stores, small branch offices, point of sale systems, and other locations.

Highly secure SD-WAN enabled tracking and reporting

Make the most of the latest digital technologies – without opening the door to new security risks.

helps you comply with privacy laws, security standards, and industry regulations. AT&T Threat Management helps you monitor real-time threats, assess risk, and mitigate potential hazards to your security. The AT&T team also monitors firewall policies and automates compliance audits.

With AT&T SASE Branch with Fortinet, you have more visibility into network and application performance (both real-time and historical statistics). Dedicated experts at the AT&T SNOC use rich SD-WAN analytics to help you fine-tune your business and security policies to improve user experiences.

Scalable and flexible SD-WAN solution

AT&T SASE Branch with Fortinet is designed to support complex branch deployments with advanced routing and cloud on-ramp capabilities. Thousands of businesses like yours use Fortinet solutions to reduce their need for point products like legacy routers and improve business application experiences.

Fully managed or co-managed options

Get the benefits of a fully managed experience with the agility of self-service. Make quick policy changes through a portal as needed or let the cybersecurity experts at AT&T Business handle operations and implementation.

Why AT&T and Fortinet?

AT&T secure networking solutions help you make the most of the latest digital technologies—without opening the door to new security risks. AT&T SASE Branch with Fortinet delivers enhanced SD-WAN features with proven security capabilities.

Together, we'll help you solve the challenges that stand in the way of innovation. We'll deliver the integrated connectivity and protection you need to thrive in a competitive marketplace.

Secure networking with low latency

Automated monitoring and management

Proactive, AI-informed threat protection

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. With experience across all industries, we understand your business demands and deliver the right insights, guidance, and solutions for you.

Contact your AT&T account manager or submit a request to learn more about how AT&T SASE Branch with Fortinet can make your network more secure and improve performance.