# AT&T SASE Branch with Fortinet

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

## Potential benefits

- Boosts application performance via instant identification and intelligent routing
- Improves network resiliency with WAN path remediation and auto-failover capabilities
- Enables organizations to supplement MPLS with a variety of network circuits including broadband and LTE
- Helps reduce risk with network segmentation, AI-driven threat detection and prevention, and policy enforcement
- Reduces the number of devices deployed and hosted within the data center
- Minimizes the IT burden with deployment, policy design, 24x7 monitoring, maintenance, and troubleshooting provided by AT&T Security Network

## Managing risk in a multi-cloud world

With the rise of cloud-based applications and tools to support new business initiatives, organizations with multiple branch locations are switching from legacy wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures. SD-WAN offers faster connectivity, cost savings, and performance for software-as-a-service (SaaS) applications as well as digital voice and video services. In fact, by 2024, 60% of enterprises will have implemented SD-WAN, compared with less than 20% in 2019, to support increasing needs for SaaS applications and cloud services.[1]

Traditional WANs are often deployed with a "hub-and-spoke" architecture, which funnels traffic through a central data center for filtering and security checks — increasing latency and slowing down performance. This is especially problematic for cloud-based tools like voice over IP (VoIP) and videoconferencing, which need to deliver high-quality performance for demanding users.

In response, many organizations are starting to connect their branch offices directly to the internet to improve performance. By moving to a more distributed cloud connectivity model, they can use widely available, low-cost options for connectivity, such as broadband, 4G/LTE, and 5G — and then manage the data flows with SD-WAN. In addition to the performance gains and potential cost savings, SD-WAN allows organizations to improve network resiliency and prioritize bandwidth for business-critical applications.

## SD-WAN for today's threat landscape

Organizations that move to SD-WAN have to balance the connectivity, performance, and financial gains with some potential challenges:

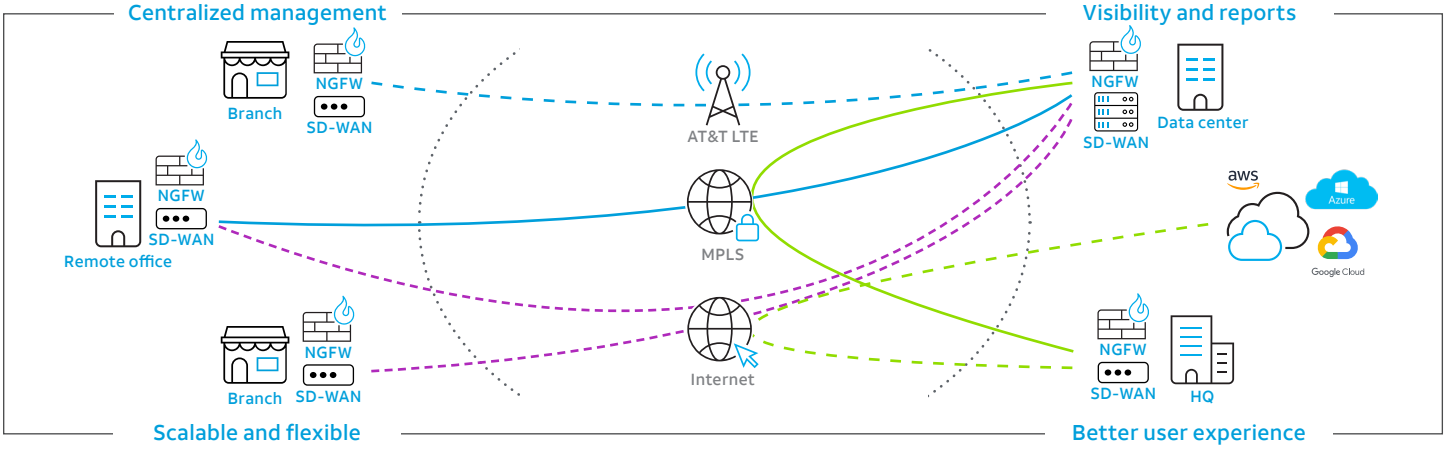
- **Complexity:** SD-WAN architectures can be difficult to troubleshoot and manage across all branches. This adds to the burden on limited IT staff and often creates defensive gaps for threats to exploit.
- **Security:** Without the centralized protection provided by backhauling traffic through the data center, organizations can be exposed to internet-based risks. Effective SD-WAN implementation requires additional security within the enterprise infrastructure to secure direct internet connections and inspect high volumes of traffic without inhibiting network performance.
- **Encrypted traffic inspection:** Most SD-WAN solutions lack the ability to inspect secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic, which comprises 72% of network traffic today.[2] Specifically, as cybercriminals are hiding malware to infiltrate networks and using it to exfiltrate data, organizations either put themselves at risk or must purchase additional appliances to inspect encrypted traffic at the edge of the network.

**Most SD-WAN solutions lack the ability to inspect secure sockets layer (SSL)/ transport layer security (TLS) encrypted traffic, which comprises 72% of network traffic today.[2]**

## Enter security-driven networking — AT&T SASE Branch with Fortinet

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

With an integrated NGFW and SD-WAN solution, enterprises can improve both WAN efficiency and security. AT&T SASE Branch with Fortinet delivers robust protection for a distributed workforce, enabling consistent policy enforcement across branch locations. Plus, IT and business leaders can mitigate the risks associated with digital transformation.



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

*Application awareness and automated path intelligence*

With traditional WAN, enterprises have a hard time maintaining the quality of user experience per application. This is because traditional WAN infrastructure relies on packet routing, which limits application visibility and thus, the ability to apply granular controls.

AT&T SASE Branch with Fortinet uses "first-packet identification" to intelligently 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, enabling them to work with businesses to make well-informed decisions regarding SD-WAN policies. The solution references an application control database of over 5,000 applications, a number that continues to grow as both the threat landscape and digital network evolve.

Being application-aware opens the doors to automated path intelligence — prioritizing routing across network bandwidth based on the specific application and user. Offering a per-application-level SLA, this solution selects the best WAN link/connection for the situation. AT&T next-generation firewalls with Fortinet enable the fastest application steering in the industry and unrivaled application identification performance. Related features include:

- **WAN path remediation,** which utilizes forward error correction (FEC) to overcome adverse WAN conditions such as poor or noisy links. This enhances data reliability and delivers a better user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission. This improves the quality of real-time applications.
- **Tunnel bandwidth aggregation,** which provides per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity if an application requires greater bandwidth.
- **Automatic failover capabilities,** which change to the best available link when the primary WAN path degrades. This automation is built into the NGFWs, reducing complexity for end-users while improving their experience and productivity.

*NGFW security and compliance*

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

- **SSL/TLS inspection and threat protection** to provide visibility and prevention against malware that obviates the need for separate encryption inspection appliances
- **Web filtering service** to enforce internet security and reduce complexity, minimizing the need for a separate secure web gateway device
- **Complete threat protection** including sandboxing, anti-malware, and intrusion prevention system (IPS)
- **Highly scalable overlay VPN tunnels** with high throughput for ensuring that traffic is always encrypted and stays confidential
- **Granular SLA analytics,** including application transactions for quick remediation

Highly secure SD-WAN-enabled tracking and reporting helps with adherence to privacy laws, security standards, and industry regulations. AT&T analysts help monitor real-time threat activity for your organization, facilitate risk assessments, detect potential issues, and mitigate problems. They also monitor firewall policies and help automate compliance audits.

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

*Scalable and flexible SD-WAN solution*

AT&T SASE Branch with Fortinet is designed for supporting complex branch deployments with advanced routing and cloud on-ramp capabilities. In fact, thousands of customers already use Fortinet solutions to reduce their use of point products such as legacy routers, while improving business application experiences.

## Why AT&T and Fortinet?

Built by business, for business, AT&T secure networking solutions enable today's distributed organizations to make the most of the latest digital technologies — without opening the door to new security risks. AT&T SASE Branch with Fortinet integrates enhanced SD-WAN features with proven security capabilities.

Together, AT&T and Fortinet help organizations solve the challenges that stand in the way of high-quality user experiences. We're experts in delivering the integrated connectivity and protection organizations need to survive and thrive in the competitive marketplace.

**Security-driven networking with low latency**

**Automated monitoring and management**

**Proactive, AI-informed threat protection**

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

### References


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

[2] John Maddison, *"Encrypted Traffic Reaches A New Threshold,"* Network Computing, November 28, 2018.


**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.