AT&T Business

Your network in the 5G era

Agility redefined, volume 2: Building the network that matches —and evolves with—your business needs

Introduction

The network.

It's evolved—and is evolving—to something new. Once it was just a way to connect endpoints, but now it can be much more. Mesh it with new technologies, and it can be configured in new ways quickly. That's agility.

What the optimal network looks like differs from one organization to another. Today, all the possibilities and capabilities can morph so fast it can be dizzying.

It comes down to this. The network must transform at the pace of your business. It must be adaptable. Nimble. Scalable.

That's agility redefined.

"Just as consumers now expect their technologies, apps, and devices to work virtually seamlessly to give them a personalized experience, businesses should now expect the same from their networks," says Sue Galvanek, Vice President of Enterprise Networking and Edge Solutions at AT&T Business.

> **"Just as consumers now expect their technologies, apps, and devices to work virtually seamlessly to give them a personalized experience, businesses should now expect the same from their networks."**
>
> —Sue Galvanek, Vice President of Enterprise Networking and Edge Solutions at AT&T Business

The arrival of 5G, of course, has caused excitement—and questions. How does 5G affect a network transformation strategy? Many businesses, unsure of what move to make next, also ask—

- How should our current infrastructure evolve?
- What technologies and solutions should we invest in that can optimize—and customize—our capabilities across the entire network ecosystem?
- How do we account for the security of our evolving network?

In this paper we will look at (1) challenges facing businesses, (2) how the core network powers your business from edge to edge, (3) what the arrival of 5G means for your network, and (4) how cybersecurity fits into the picture.

Section 1:

Your network at the crossroads—challenges facing businesses

Keeping up with change and converging multiple technologies

The pace of technological advance seems to be at light speed. Businesses of all sizes—and their IT teams—scramble to keep pace. Consider:

- An enterprise now must move efficiently across multiple clouds and cloud platforms for processing, networking, colocation, and content delivery
- Tides of data continue rising—businesses look to big data, artificial intelligence (AI), and automation to optimize the cost and scale of the experiences they want to create
- On top of all that, businesses must also manage devices, apps, and a variety of voice and collaboration tools so their teams can connect across geography, platforms, and devices
- In addition, IT teams must assess the best way to integrate such things as software-defined networking (SD-WAN) and edge compute into their networks
- And…emerging 5G technology is projected to change the game for businesses and consumers over the next decade

All of these separate networks, solutions, and connections can create potential gaps. They often lack interoperability—or at most have spotty compatibility. These can be challenges that stand in the way of a network with a robust, agile ecosystem.

"Your network is at a crossroads," says Roopa Honnachari, Industry Director - Business Communication Services, ICT, Frost & Sullivan. "Technology is advancing at light speed. You have options and combinations never before available. You've got to sort through the complexity to get it right—to put your organization on the right trajectory."

More bandwidth, please

Businesses are insatiable for bandwidth. At corporate branch offices, large email attachments, file sharing platforms, web conferencing, and social media consume bandwidth. In order to serve these needs, corporate data centers commonly require from gigabits to terabits per second.

Additionally, businesses rely on more video to interact with employees, partners, and customers. All that video data needs more bandwidth and requires a higher class of service (CoS) to maintain voice quality and prevent choppy images or frozen frames. Many are turning to fiber, which delivers high-speed bandwidth and scalability to support these critical applications to business.

Cloud configurations

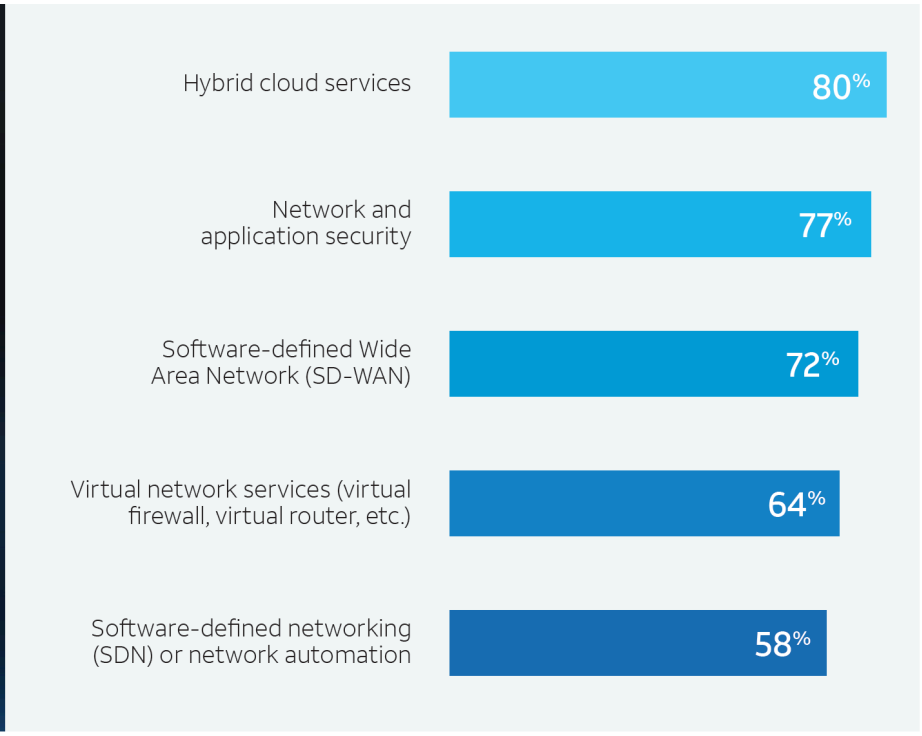
Another complexity is that organizations are deploying multiple clouds and moving their processing to cloud platforms.

Organizations can struggle creating an integrated network that brings together their data centers, public clouds, and private clouds in a hybrid environment that optimizes cost and performance.

> **"Your network is at a crossroads. You've got to sort through the complexity to get it right to put your organization on the right trajectory."**
>
> — Roopa Honnachari, Industry Director – Business Communication Services, ICT, Frost & Sullivan

Top 5 tech trends businesses are prioritizing

5G remains such a new technology, businesses are currently prioritizing other technologies—a trend that will likely shift as 5G use cases evolve.



Source: 2019 Frost & Sullivan SD-WAN Survey

Investment constraints

Budget pressures drive many to seek cost-effective approaches to network connectivity.

For example, the growing availability of high-speed broadband connectivity has lowered the costs for many network services. Some lower priced connectivity options, however, may also deliver less optimal quality-guarantees when it comes to latency, throughput, and repair time.

When it comes to SD-WAN, some see it as a lower cost network alternative for their connectivity without understanding that SD-WAN is not connectivity. SD-WAN is a management layer that can take advantage of multiple connectivity options to deliver improved levels of service, performance, and value.

The challenge here is that with so many technology options it's hard to figure out what will provide the best solution for your business. It's tempting to assume all of the technologies perform about the same and then only use cost as the primary driver for the network. It's better to ask, "What unique combination of solutions will meet the distinctive needs of my business locations and help deliver highly reliable, consistent performance?"

In this regard, many businesses are trying to build without blueprints, perhaps investing in something that works for one business situation, but is not ideally suited for another.

Section 2:

How the core network powers your business

Why is the core network important?

Networks, connectivity, services, and solutions are powered by a provider's core network. The performance and reach of the core have a direct impact on a business's network.

Think of the core network as a central nervous system. It's essential to every function in the body. Now think of core networking solutions, services, and products as various organs—eyes, heart, lungs, liver. These are like Ethernet, VPN, internet, security, virtualization, and others. And like organs, if they aren't connected to a strong, robust nervous system, they can't do the jobs they are designed to do.

Core networking technologies

A business can discover new levels of productivity and efficiencies with digital platforms that allow increased levels of agility. Powerful digital tools and capabilities allow businesses to command and control their networks in response to changing needs. For example, businesses can make changes on their own using digital control, including requesting service at a new location, upgrading speeds, prioritizing traffic, changing routing, and much more. Following are core networking technologies to consider.

MPLS

MPLS technology enables customers to have fully meshed, any-site-to-any-site, private IP network connectivity. In other words, it's like organizations having their own private, high-performance internet-like experience.

MPLS networks have several defining characteristics. They offer high-speed bandwidth options. They also can provide enhanced Class of Service (CoS) routing—which provides customizable quality and speed when transmitting data.

MPLS also offers any-to-any routing for efficient connections to virtually any site—avoiding the latency (hair-pinning from a head-end site) associated with legacy hub-and-spoke WAN architectures. MPLS can be particularly useful for data center replication or for large sites that need extra-high-capacity connections, because MPLS VPNs can scale from megabits to gigabits per second.

These performance standards support designs for mission-critical and time-sensitive applications.

End-to-end network-based security is built into this technology. MPLS operates on a private network, which avoids exposure to public internet risks associated with Distributed Denial of Service (DDoS) attacks and unauthorized network access. This is especially important for companies with regulatory compliance mandates, like healthcare companies.

IPsec

Internet Protocol Security (IPsec) allows users to connect their private infrastructure (WAN/LAN) through the public internet while helping protect against cyber threats. It creates a virtual, encrypted connection between points on the public internet. IPsec monitors outgoing and incoming traffic, encrypting and authenticating data packets, so users can isolate their networks while sending and receiving traffic over the internet.

IPsec VPN supports both software-based and customer-premises equipment (CPE). It functions on the network layer, running in the background so users don't have to configure or interact with it. It also allows administrators to monitor all traffic that passes over the organization's network.

IPsec VPN, MPLS VPN, or both?

Both IPsec VPN and MPLS VPN provide highly secure network connectivity as a key feature, but they achieve it in different ways. An MPLS VPN is private, but shared, network where an IPsec VPN will be created over an internet connection. While each type of VPN can be its own standalone network for a customer, they can also be combined into a hybrid VPN that is enhanced by the strengths of both.

1. An MPLS VPN offers protection by transporting data over a private network, thus avoiding use of the public internet. Each customer's traffic is segmented from other customers using an industry-standard customer identification tagging technology known as label switching. The customer may choose to encrypt its traffic (or not) when transmitted over the MPLS VPN. Encrypting the data in an MPLS VPN environment provides an additional layer of security, but that may come at the expense of latency (CoS). For instance, if video is not encrypted correctly, the network management system may not be able to identify the data as video and assign it a higher priority.
2. An IPsec VPN uses the internet as the underlying network, including dedicated internet access, wired broadband internet, or cellular internet, including 5G. The privacy and security needed for a customer's VPN is created by encrypting data during transit from its originating location to its destination. The encryption may be created with hardware or software solutions, depending upon the needs of the customer. The range of hardware solutions includes simple, low-cost VPN appliances to robust, feature-rich devices that support advanced performance-based routing. IPsec VPNs are also advantageous with LTE / 5G for locations that are temporary, like a pop-up store, semi-mobile location like a food truck, or in hard-to-reach places like an ATM machine.
3. Hybrid VPNs come with a wide variety of configuration options to meet virtually any customer need. It might be combining MPLS and broadband internet at the same location to take advantage of advanced performance routing. Or, using MPLS for data center connectivity with IPsec VPNs for branch locations. Or it could be one of the myriad combinations in between. With this versatility, hybrid VPNs could be an integral part of most any network need.

Site typing

Instead of taking a one-solution-fits-all approach to a network, site typing allows a business to look at their specific network needs, site by site. Then, the organization builds the network around each site's ideal needs: bandwidth, privacy, security, level of performance, site availability, budget, integration with current network infrastructure, and the ability to be future-ready.

Site typing is key to the performance of applications and user experience. A business can customize the right type of connectivity to deliver the performance, scalability, and reliability required to support specific sites in the network.

Hybrid networks

Hybrid networks combine multiple technologies in a network infrastructure.

For example, businesses can deploy MPLS VPN at larger or mission-critical sites and IPsec VPN at smaller or less critical sites, and link them together. Or, they might choose to deploy both MPLS and IPsec at the same site—with the MPLS VPN carrying essential or latency-sensitive traffic such as video and the IPsec VPN carrying latency-tolerant traffic such as email.

For example, a business with MPLS VPN connection at a site may choose to augment bandwidth at that site with a broadband internet connection with IPsec security.

Using a combination of these approaches can improve outcomes for a business.

Wi-Fi and internet offload

Another hybrid configuration combines MPLS VPN and public Wi-Fi. Public Wi-Fi has become standard in many industries. Consumers expect this convenience at retail locations, restaurants, and hotels. It also provides data which can be analyzed and aggregated to provide businesses with an understanding of consumer behavior through data analytics.

Internet offload occurs when you remove traffic destined for the internet from transmission using private MPLS VPN. For example, you can keep all your business-critical apps and sensitive transmissions protected on the MPLS VPN, while offloading non-essential traffic and consumer browsing to the public internet. This can save bandwidth expenses and enhances MPLS VPN performance without sacrificing security for sensitive data.

Enhancing VPN functionality and versatility

Software-based solutions can reshape how organizations provision and manage their WANs. For example, with generic (or universal) equipment, an on-demand platform can offer connectivity like a cloud-provisioned solution. Also, through VPNs, you can create a private virtual network connection between the customer's network and the cloud or cloud service provider. This allows a business to utilize APIs in a fully orchestrated manner and connect with cloud service providers in a matter of minutes—all in a highly secure way.

Here, network functions act like apps and are used as needed. With this model, companies can still choose from the network function vendors they prefer, deploy exactly the functions they want, and buy the connectivity they need all through a single provider. This is all easily managed through a centralized self-service portal with robust visibility, management, and control.

These solutions provide the enterprise more ways to construct their WANs to make them more agile, more flexible, and better able to meet the current and future needs of the business at lower cost and with greater resilience.

Multi-function CPE

Multi-function devices integrate numerous commonly used functions onto a single platform, such as firewalls, routers, WAN optimization, visibility applications, and SD-WAN. Businesses configure and manage these devices through cloud-based software control via a web-based portal.

SD-WAN solutions

Software-Defined WAN (SD-WAN) is a network management, link, routing, and application-performance technology that has been adopted by many companies. Many more are anticipating making it part of their network.

First, let's dispel some myths.

Myth #1: SD-WAN provides connectivity. You can simply replace your current network connectivity with SD-WAN.

Fact: This is not the case. SD-WAN is not connectivity, but it manages the connectivity which it uses.

Myth #2: SD-WAN, MPLS VPN, and other new network technologies are incompatible.

Fact: Most of these network technologies are complementary.

As an edge overlay solution, SD-WAN will have performance characteristics for your core network.

An organization can deploy, configure, and manage SD-WAN easily through an administrative portal. Businesses that want to focus their IT resources on other priorities opt for managed SD-WAN.

There's an even split when it comes to DIY vs. managed SD-WAN. According to a recent Frost & Sullivan survey, 54% of IT decision makers indicated they prefer a fully managed SD-WAN service, with 46% preferring to manage their SD-WAN themselves.

Source: 2019 Frost & Sullivan SD-WAN Survey

SD-WAN use case: Large financial technology firm

About the company

This financial technology (Fintech) firm serves more than 150 community banks and credit unions and is one of the largest core banking solutions providers in the U.S.

Challenges and needs

As the firm upgraded to a private cloud environment, IT executives recognized a need for a more configurable network with automatic failover and other advanced features that would better enable its clients to use technology advances.

Solutions

The company relied on professional networking services consultants to help plan, transform, and optimize their network. The firm already had MPLS networking, wireless, carrier-grade internet, and broadband connectivity. In going with an SD-WAN solution, they created a hybrid configuration that offered tremendous flexibility and enhanced their ability to make needed changes at the speed of today's business.

SD-WAN gave them (1) intelligent dynamic routing, (2) optimized cloud connectivity, and (3) visibility into applications and performance. The Fintech also installed a versatile, universal device that enables a variety of virtual network functions (VNFs). They would no longer have to rely on traditional, single-purpose hardware for each type of function they wanted for their WAN.

Results

Installing the SD-WAN solution complements their existing MPLS architecture, has resulted in a 75% reduction in downtime for the company's networks, and has provided an 80% reduction in help desk calls following WAN outages.

They've had tremendous feedback from their clients on the success of the platform—greater visibility, enhanced uptime, and the ability to centralize management of devices.

In addition, they enjoy faster, more stable updates. The SD-WAN solution also gives them a simple, predictable OpEx model for hardware, enhanced security using micro-segmentation, a centralized firewall, a growing suite of add-on security features, and a standardized configuration across the institution.

Section 3:

5G is here! (So, now what for the network?)

Wireline, core networking, 4G, and 5G will coexist for the foreseeable future.

We are not looking at either-or scenarios for network architecture. Instead, we look at "and." The arrival of 5G will not trigger the instant extinction of current networking technologies and solutions. Instead, current and new tech will evolve together.

5G will definitely make for some exciting, powerful new use cases. However, you will still need elements of your underlying architecture to support and take care of other use cases where 5G doesn't make sense.

What is 5G?

5G is the next generation of wireless communications technology. In essence, 5G will put the network edge closer to users and devices. It uses mid-band frequencies and millimeter wave (mmWave) to help accomplish this.

5G offers significantly larger spectrum allocations and enables exponentially increased data rates. It has a reduced range compared to today's 4G frequencies—but the antennae needed for 5G are much smaller. This will allow for a dense network of small cells, enhancing the current user experience.

User Experience = Speed + Latency + Reliability

5G offers monumental leaps in capacity (bandwidth), speed (data transit), proximity to the edge (lowering latency and boosting compute power), and traffic management (such as network slicing, where operators open dedicated virtual networks over a common network infrastructure to provide functionality specific to the service or customer).

Integrate 5G into the network strategy

5G and network solutions can interconnect the digital landscape to help optimize processes and deliver outcomes. Here's how they work better together.

- *5G and core networking solutions complement each other to accomplish a variety of business goals.*

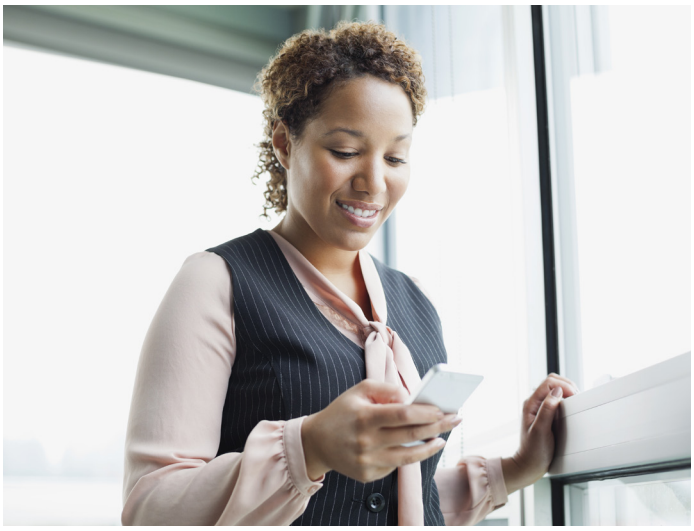
Applications that rely on committed speed and need virtually unlimited use are best suited for a wireline solution. Other applications may need the flexibility of mobile 5G. Together, 5G technology with the core network can create a rich ecosystem to more seamlessly integrate services, solutions, and products.

- *Implementing 5G with existing core networking solutions allows your infrastructure to evolve—so you can enjoy enhanced performance today and be future-flexible as network tech transforms. Also, by meshing 5G and core networking solutions, you avoid the cost of losing core solutions and potentially diminishing business-essential functions.*

There's more than the price tag to worry about when removing a core network infrastructure. There's also the cost of possibly losing the Class of Service, SLAs, and emergency failover that network solutions provide. This could harm operations, customer experience, and more.

- *Intertwining 5G with the core network can help achieve competitive advantage and network flexibility.*

5G will eventually open tremendous opportunities for new use cases that improve user experiences while enhancing productivity and efficiency. It will also provide more flexibility in designing the core network. A business can work together with the right provider to build solutions based on the site-typed requirements of the organization.



Section 4:

Wrapping the network and solutions in security

Everything we've discussed to this point has focused on building a network and solution portfolio that meets the specific needs of a business. But how do you help to defend the network, with all of its threat planes and entry points?

You wrap it in multiple layers of cybersecurity. In other words, you have to—

- Assess your cyber strategy and risk levels
- Be able to counter identity theft and fraud
- Protect the endpoint devices on your network
- Prepare for a breach through threat detection and response
- Choose and implement network security solutions that are compatible with your network and other cybersecurity technologies

It can be a steep challenge to figure out cybersecurity options and assess the best choices for a complex network.

Many businesses turn to cybersecurity providers that deliver automated security processes and managed services to help reduce the complexity.

Organizations with greater cybersecurity maturity may tend to outperform their revenue goals—more so than those with lower-rated security

In March 2020, AT&T Cybersecurity, in association with the Enterprise Strategy Group (ESG), completed a research survey of 500 cybersecurity and IT professionals who are directly involved with their organization's cybersecurity strategies, controls, and operations.

The goal of the research was to validate if, and to what degree, organizations more in alignment with best practices prescribed by the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) can operate more secure environments and better enable their businesses.

91% of surveyed businesses rated as being leaders in cybersecurity maturity exceeded their revenue goals for the company's latest fiscal year (57% exceeded by 7%+, 34% exceeded by 2% - 6%).

What are the characteristics of a cybersecurity leader? Aligning security strategies with critical business assets, consolidating and addressing security event data, constant training, process improvement, continuing investment, and aligning practices prescribed by the NIST CSF.

Source report:

The relationship between security maturity and business enablement: Exploring the relationship between cybersecurity and positive business and security outcomes. April 2020.

Section 5:

AT&T Business Solutions

AT&T Business delivers capabilities that integrate virtually seamlessly, from the core of your network all the way to the far reaches and edges of your digital technologies—from connectivity to the cloud to endpoints in a tech ecosystem wrapped in security.

"Putting intelligence in the customer edge means moving compute to the customer location," explains Rupesh Chokshi, AT&T Assistant Vice President of Edge Solutions. "That allows for local processing of data on site, providing privacy for companies that need it, and application- level controls."

AT&T operates an incredibly strong, high-performing core network, and has a full breadth of robust and comprehensive solutions in our portfolio that can help accommodate businesses of all sizes across virtually all industries.

These products can be combined together to do most anything your site-typed network needs. And it doesn't have to be done all at once. We can help your business evolve over time. You may hear others tout their capabilities, but you probably won't hear them talking about how they can tie it all together.

AT&T VPN

AT&T VPN allows you to connect your locations and users more securely. For offices, business partners, cloud providers, remote and mobile workers. You can also get faster response times with better application performance by adding VPN to your cloud service provider platform with AT&T NetBond® for Cloud. AT&T NetBond for Cloud can provide up to 50% lower latency for applications (Frost & Sullivan 2018 United States MPLS VPN Services Market Leadership Award).

Internet services

AT&T Dedicated Internet provides ultra-reliable, dedicated internet for critical business needs, with identical upload/download speeds up to 1Tbps. Also, our high-speed internet services offer fast and highly secure internet solutions with speeds up to 1Gbps. Available options include symmetric or asymmetric connections, dynamic or static IP, internet backup, single contract, consolidated invoicing for multiple sites, and more.

Virtualization

AT&T FlexWare™ is a multifunction device that is based on the concept of Network Function Virtualization. Network functions such as routing, firewall, SD-WAN, WAN acceleration, and more are deployed as Virtual Network Functions (VNFs) on the AT&T FlexWare device. These virtual network functions can be configured and managed via a cloud-based orchestrator. More importantly, AT&T provides these virtualized functions from a variety of vendors, making it not just a multi-function device but also a multi-vendor platform so you can choose and deploy functions that best meet your needs.

> **"Putting intelligence in the customer edge means moving compute to the customer location."**
>
> — Rupesh Chokshi, AT&T Assistant Vice President of Edge Solutions

AT&T SD-WAN

AT&T Business is the first provider in the industry to announce both a network-based SD-WAN solution AND an over-the-top solution. A typical SD-WAN solution is deployed in the over-the-top manner where an SD-WAN device is deployed at every customer site and IPsec tunnels are established over the network transport links among sites.

With our network-based solution, customers have the flexibility to deploy MPLS-only sites, IPsec-only sites, and SD-WAN sites—all part of a single, cohesive hybrid VPN. This design enables existing customers with MPLS or IPsec VPNs to easily evolve to SD-WAN without undergoing a complete network re-design.

AT&T Business is also integrating SD-WAN solutions with the AT&T FlexWare platform. SD-WAN functionality can be deployed as a VNF on an AT&T FlexWare device and service chained with other VNFs such as routing and a firewall.

We also offer a managed SD-WAN solution for organizations that want to focus their IT resources on other priorities. We install and manage the SD-WAN for you. "AT&T's managed SD-WAN offer combines edge solutions and core network services, hence creating a tightly integrated overlay and underlay solution," says Roopa Honnachari, Industry Director – Business Communication Services, ICT, Frost & Sullivan.

The most common SD-WAN configuration is one dedicated, business-class MPLS VPN or Dedicated Internet Access link and one broadband link. We have also seen that AT&T SD-WAN, AT&T transport, AT&T security, and AT&T voice services are often integrated by our clients. Coupled with our industry-leading network connectivity options—MPLS, dedicated and broadband internet, wireless, and AT&T Wireless Broadband (a fixed cellular option that can be bundled with SD-WAN)—and our cybersecurity portfolio that can wrap the network in high security—AT&T Business can create a custom-fit, high-performance network design for you.

Networking solutions, 5G, and you

Our 5G and our core wireline networking products are complementary, offering a more seamless experience between fixed and mobile applications. We can help you with—

- **Strategy.** 5G will be deployed gradually, and will exist alongside and in tandem with LTE, 4G, and other existing wireline technologies. Maximize your business potential so your end-to-end network is adaptive, and to make the pivot to 5G where and when it makes sense.
- **Integration path.** Transformation can be complex and disruptive to businesses. It is important to have a trusted partner that will guide you through 5G and network integration. Work with your existing infrastructures to further enhance what you already use.
- **Cost considerations.** The investment in infrastructure for companies looking to integrate 5G requires serious consideration in areas of the business where it makes economic sense. Let us help you with your next-generation network planning for long-term business agility.
- **Networking solutions.** Your business needs the flexibility to determine which connectivity solutions meet your needs. AT&T Business looks at each site requirement for the right solution that fits into your overall network strategy. Our product portfolio of advanced network, data, internet, 5G, and application services can help solve your business challenges.

AT&T Business Center

Manage your wireline services online with AT&T Business Center. With Business Center you can access near-real-time ordering, monitor and manage your network with bandwidth utilization alerts, personalize your dashboard, and manage your U.S. and global networks 24/7. Our easy-to-access dashboard is designed to simplify the self-service experience and help you manage, run, and grow your business with agility.

AT&T Cybersecurity

AT&T Cybersecurity helps to wrap your network in security. No matter what stage of your cybersecurity maturity you're in, we can help you enhance your defense-and-response capabilities.

For example, if you're wondering where to start, we help you assess your current IT readiness and cyber risk. From there, we work with you to build a roadmap for you to bolster your defense.

That roadmap can include stronger security for your endpoints—all the devices (company-owned, BYOD, and IoT) that connect to your network. Each endpoint expands your threat surface, so it's vital to wrap them in security.

From the endpoints, we look inward to the network infrastructure. Just as we site type for network architecture, we site type for security. We offer internet security for SD-WAN, mobility, and cloud, firewalls (cloud-based and premises-based), DDoS defense, and enhanced network scanning based on government cybersecurity indicators.

Finally, the roadmap will cover threat detection and response—finding the attacks on your network and helping you respond against them before they impact your business. We provide continuous security monitoring, alarm validation and incident investigation, and security orchestration and incident response automation, all in one solution.

Marrying the ideas of customizing your network to fit your needs with customizing your cybersecurity to fit your network means an enhanced, high-performing, well-defended network that supports your business outcomes in virtually every facet.

Conclusion

Businesses expect a network that can respond to their dynamic needs. They need the visibility and control to help simplify management of what are often thousands of endpoints.

"There are an estimated 32 million businesses in the U.S.," says Sue Galvanek, Vice President of Enterprise Networking and Edge Solutions at AT&T Business. "That's potentially 32 million different network configurations. If you are one of those businesses, you want the one network build that's a spot-on fit for your specific needs. AT&T Business has the breadth and depth of networking solutions to make that happen."

That's agility—redefined.

> **"There are an estimated 32 million businesses in the U.S. — that's potentially 32 million different network configurations."**
>
> —Sue Galvanek, Vice President of Enterprise Networking and Edge Solutions at AT&T Business

For more information contact your AT&T representative.