Support business continuity with highly secure remote workforce solutions

Adapting to global conditions and establishing a remote workforce is critical to keeping your business running. But you also need to be sure it doesn't compromise your cybersecurity. AT&T Cybersecurity can help you affordably navigate the complexity and threats you face every day—with an eye toward the future.

The arrival of the pandemic in early 2020 has challenged businesses in numerous ways. Among these is cybersecurity. Whether organizations are ramping up the scope of an existing remote workforce or scrambling to enable newly remote teams quickly, the pressure is on.

AT&T Cybersecurity is uniquely positioned to help you establish a highly secure, remote workforce that can safely operate now and scale up or down in response to changing business requirements.

Preserving employee productivity and security

Technology teams in organizations have been tasked with the duty of keeping legions of remote workers connected and productive. The scale of changes has put tremendous stress on IT systems and teams as everyone does their best to balance connectivity, collaboration, and cybersecurity.

The reality is that most organizations have had to make sudden and unplanned changes in the way workers connect to the corporate network, and how they access corporate data and applications in the data center and cloud. This kind of rapid transformation can introduce new cyber risks and vulnerabilities. What's more, attackers are taking advantage of shifts toward remote work—and the uncertainty from global conditions—to launch ever more targeted cyber-attack campaigns.

Features and benefits

- Provide highly secure access to applications for remote users
- Help shield users from the latency issues
- Unburden VPN connections
- Provide highly secure access and data from any device
- Protect and manage BYOD devices
- Maintain security awareness for remote employees

What does post-pandemic remote work look like? The following solutions are designed to address specific challenges organizations are facing and ways to help them protect their users, networks and data.

Highly secure access from nearly any device

The increasingly diverse population of today's suddenly remote workforce has been pushing more users to connect to corporate resources from a variety of devices, both personally and corporate-owned. AT&T Global Security Gateway and AT&T Enterprise Application Access provide highly secure access to the applications and data that employees need to complete their work, whether it resides in the data center or in the cloud. With these solutions administrators can grant access to specific applications, based on role or by user, reducing risk associated with traditional VPNs that provide access to an entire network segment.

Highly secure internet browsing

Today's modern workforce needs comprehensive protection when they connect to the internet, wherever they are conducting business. AT&T Global Security Gateway and AT&T Enterprise Traffic Protector protects users against web-based threats including trojans, ransomware, and phishing attacks, even when they are off the corporate network. Administrators can also enforce acceptable use policies, customized by department or user to provide that the websites that employees visit are safe and appropriate for the workplace.

Fortify access and data on virtually any device

With any type of remote workforce, users connect to corporate resources from all manner of devices, both personally and corporate-owned. AT&T Unified Endpoint Security solutions give you a platform with the flexibility to protect and manage virtually any kind of employee device, no matter who owns it or where it's being used.

AT&T Cybersecurity can also help streamline deployment with support to fast-track device onboarding, deployment, configuration, and enrollment on corporate-owned and "bring your own device" (BYOD) devices. We provide 24x7 helpdesk support and offer additional services through remote administration, helping alleviate the burden on critical IT security staff that the current environment may be causing.

Expand security awareness beyond the office

As workers transition from offices to their homes, practicing good cybersecurity hygiene becomes even more critical. You need to help your staff maintain heightened security awareness and readiness at all times. AT&T Cybersecurity can help reinforce security policies and best practices through our tailored security awareness solutions. We provide continuous and timely threat intelligence with the AT&T Alien Labs™ team and help security employees stay up on the latest threat trends to shape defenses that will backstop these security awareness efforts.

Assess cloud security readiness and risk

As you move to the cloud, consider getting a second look at planned security controls and potential configuration issues or vulnerabilities. There may be new threats and bad actors that could put remote employees and your whole business at risk. AT&T Cybersecurity consulting services can act as a trusted advisor to help set the strategy, design, and security readiness of your cloud security architecture during this transformation.

Monitor public cloud environments

It can be very difficult to provide that the public cloud environments supporting your remote workforce are free from threats. AT&T Threat Detection and Response services can continuously monitor public cloud IaaS and SaaS environments alongside on-premises network and endpoint monitoring to help you and your staff stay highly secure.

Five pillars of strong, adaptable, multilayered cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

Pillar 1: Cyber strategy and risk assessment Use our consulting and planning services to address the essentials of security.	
Strategy roadmap and planning	Delivers expert resources, knowledge, and methodology to build a unified security program.
Enterprise security assessment services	Help prepare your organization against persistent cyberattacks by identifying gaps in your environment.
Risk-based cyber posture assessment	Get a quick assessment and make plans to address gaps.
Security compliance	Can help you adhere to regulatory requirements and meet strategic business objectives.
Vulnerability scanning	Can rapidly scan systems and applications to identify potential exposure or vulnerabilities.
Penetration testing	See how your security holds up to real-world scenarios while working towards compliance.
Cybersecurity IQ training	Measure and improve your org's cybersecurity awareness.
Pillar 2: Identity and fraud detection Help reduce fraud in real-time when end customers use their mobile devices to conduct critical online transactions.	
AT&T Authentication and Verification Services (AAVS)	AAVS APIs provide enterprises with consented access to AT&T mobile subscriber data to help them verify the identity of their end customers and detect and reduce fraud.

Pillar 3: Endpoint security We are your trusted source with strategic and innovative suppliers so you can have the visibility and control of your data.	
VMware Workspace ONE(R)	Deliver a digital workspace that empowers the workforce to bring the technology of their choice — devices and apps — at the pace and cost the business needs, all with high security.
IBM MaaS360 from AT&T	Provide a high level of end-to-end mobile security across devices, apps, content and users.
MobileIron	Manage and monitor endpoints, apps, and content while keeping data highly secure.
Lookout mobile endpoint security	Leverage an endpoint app on employee devices with real-time visibility into mobile risk via a cloud-based admin console.
Pillar 4: Network security AT&T provides what your business needs to connect and help protect your users, data, and applications residing on-premises, remotely, or in the cloud.	
Global Security Gateway	Provide highly secure remote access and protection against web-based threats across users, whether working from the office, from home, or other locations.
Next generation firewall	Help protect on-network users, data, and devices against a wide-range of malware and unauthorized access.
Distributed denial-of-service security	Preserve the availability of your web servers and applications with 24x7 monitoring of network traffic by AT&T Security Operation Center and mitigation of DDoS attacks. Self-monitoring options available.

Pillar 5: Threat detection and response Enhance your ability to detect and respond to cybersecurity threats.	
Managed threat detection and response	24x7 security monitoring from AT&T Cybersecurity
USM Anywhere™	Threat detection, incident response, and compliance assistance in a single platform.
Incident response and forensics	Helps you develop a plan to respond to attacks and mitigate the impact of incidents quickly.
USM Anywhere for MSSP's	Create a managed security service offering with USM Anywhere.

To learn more about AT&T Cybersecurity solutions, visit www.cybersecurity.att.com or have us contact you.

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. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.