AT&T Business | **paloalto®** NETWORKS

Accelerate your journey to the cloud and protect your mobile workforce

with remote workforce solutions from AT&T, powered by Palo Alto Networks

Potential benefits

- Gain centralized visibility across on-site and remote users

- Provide highly secure access to applications hosted in the data center or cloud

- Enable safer internet browsing for remote users, whether on or off network

- Enforce corporate acceptable use policies to reduce usage of time-wasting websites

- Quickly scale to accommodate new users

- Reduce burden on in-house technology teams with AT&T-provided deployment, security policy design, 24x7 monitoring, maintenance, and troubleshooting

Technology should help, not hinder

Remote workers, no matter where they are, must have simple and effective connections to the applications and data they need for work. To meet these requirements, organizations face the challenge of balancing user experience with security. As users connect from both managed and unmanaged devices, standalone virtual private networks (VPNs) introduce uninspected traffic into your servers. Backhauling user traffic to physical firewalls for policy and security enforcement is costly to scale, causes higher latency, and results in a poor user experience. Meanwhile, with applications and data spread out over public and private clouds, piecemeal security solutions are difficult to configure, and provide inconsistent security policy enforcement. Businesses need a solution that can offer comprehensive security, scale on demand, and enable access regardless of where or how users connect.

Remote work has been gaining in popularity over the past several years but the COVID-19 pandemic greatly increased the number of users working from offsite locations. Since then, many organizations have determined that "work from home" will become their new normal, so they will need remote access and security solutions that will support these initiatives long-term. Remote workforce solutions from AT&T, powered by Palo Alto Networks, provide highly secure access to resources hosted in the data center, the internet, or private and public clouds.

AT&T Business | paloalto NETWORKS

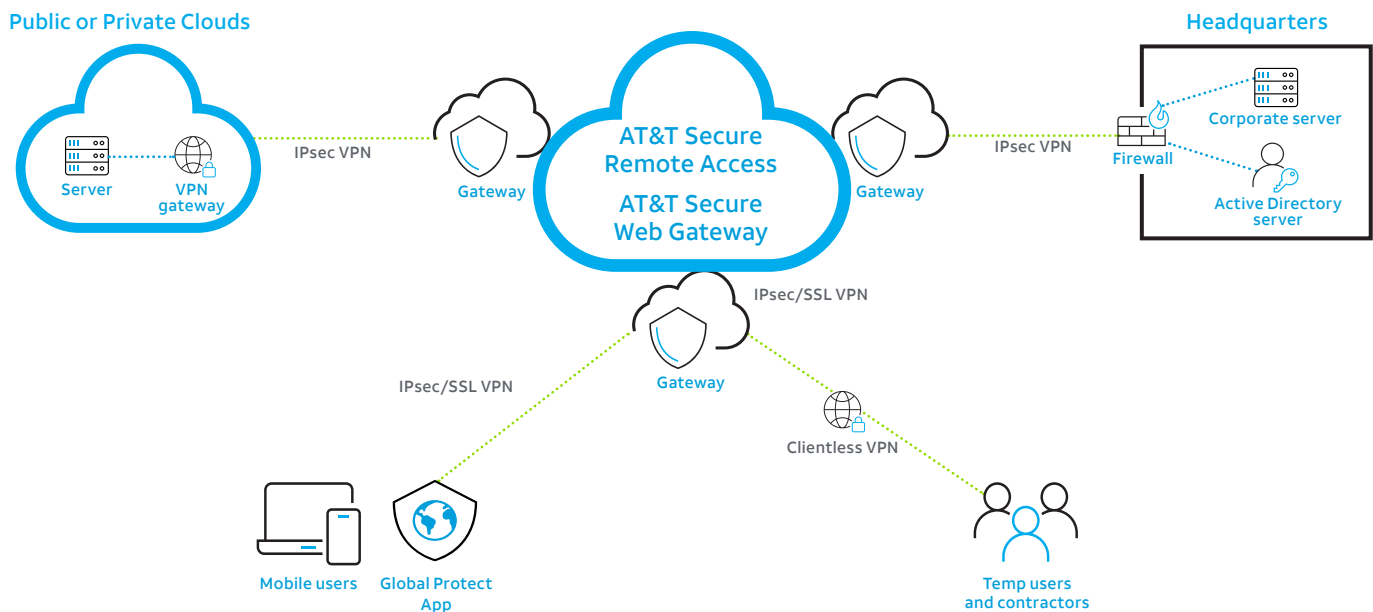## Help eliminate complexity with a suite of security capabilities

Remote workforce solutions from AT&T, powered by Palo Alto Networks, use a cloud-based infrastructure to deliver a suite of security and networking services for remote users. Organizations benefit from a single pane of glass that sets up the connectivity and cybersecurity employees and contractors need, including:

- **VPN options** to protect data in transit: IPsec, SSL/IPsec, and clientless VPN

- **Firewall as a service (FWaaS)** to help prevent threats from impacting workers

- **Zero Trust network access (ZTNA)**, offering controlled, role-based access to only the resources workers need

- **Secure web gateway (SWG)**, using static analysis and machine learning to block employee access to known malicious or time-wasting sites

- **ML-powered threat prevention** to block exploits, malware, command-and-control traffic, and even zero-day threats

- **Domain name system (DNS) security**, featuring analytics and machine learning, to protect against threats in DNS traffic

If a business already uses AT&T next-generation firewalls, powered by Palo Alto Networks, to protect their headquarters or servers, they can extend the same security policies to remote users with AT&T Secure Remote Access and AT&T Secure Web Gateway, powered by Palo Alto Networks. Employees and contractors can access the same applications and protection against threats in the same way as they had in the office.

Remote workforce solutions from AT&T, powered by Palo Alto Networks

Public or Private Clouds

Server — VPN gateway

IPsec VPN — Gateway

AT&T Secure Remote Access

AT&T Secure Web Gateway

Gateway — IPsec VPN — Firewall

Headquarters

Corporate server

Active Directory server

IPsec/SSL VPN

Gateway

IPsec/SSL VPN

Clientless VPN

Mobile users — Global Protect App

Temp users and contractors

AT&T Business | **paloalto**® NETWORKS

Deploy and scale quickly and reliably

Just because work left the office doesn't mean business stops. Budget constraints combined with unpredictable demand can add up to poor performance or workers unable to securely connect to resources. With more than 100 gateways in 76 countries, remote workforce solutions from AT&T, powered by Palo Alto Networks, scale on demand to fit business needs, providing consistent connectivity and security for data and applications on-premises or in the cloud. Quality of service (QoS) capabilities enable you to prioritize bandwidth for optimal performance of critical applications.

As a cloud-delivered service, the deployment of this solution is timely, requires no on-site appliances, and quickly scales to accommodate new users or locations.

AT&T SASE with Palo Alto Networks

AT&T Secure Remote Access
- Provides highly secure access to only the applications required to complete job duties
- Optimizes network performance by shortening logical paths to reach cloud-hosted resources
- Helps improve user experience by offering consistent access and protection

AT&T Secure Web Gateway
- Enables safer internet browsing by blocking access to known malicious websites
- Helps enforce acceptable use policies by reducing usage of time-wasting sites
- Inspects encrypted SSL traffic in the cloud, helping preserve network performance

Why choose an AT&T managed solution?

AT&T brings many benefits to organizations by focusing on their specific security requirements, which may vary depending on the size, type of industry, and plans for future development.

Combining a managed security service with a comprehensive cloud-delivered security solution is one way to achieve the highest level of protection, simplify operations, and lower the total cost of ownership.

Managed security services for AT&T Secure Remote Access and AT&T Secure Web Gateway, powered by Palo Alto Networks, include:

Deployment strategy and execution
- **Rapid deployment** completed by certified engineers who collaborate with businesses on solution architecture and security policy design
- **Testing and troubleshooting** of traffic forwarding and security controls to validate that the service is operating in alignment to business/network requirements

AT&T managed or co-management models
- **Co-management** provides the flexibility to process changes to security policies, access controls, and firewall rules through self-service portal, or to request changes be processed by the AT&T Cloud Operations Team*
- **Ongoing contact** between the AT&T Cloud Operations Team and technology providers to upgrade and maintain the solution
- **Support** for future service delivery needs, including feature turn-ups or security architecture updates
- **24x7 monitoring** and help desk support

Co-management includes six MSS supported change requests per month

Comprehensive visibility
- **Dashboards** that provide a consolidated view of each unique environment
- **Detailed drilldowns** by location, user, and device
- **Automated and on-demand reporting**
- **Ability to share sys log data** with AT&T USM Anywhere and integration with AlienApps for unified visibility of events

AT&T Business | **paloalto** NETWORKS

Together, AT&T and Palo Alto Networks help protect organizations of all sizes while allowing for more streamlined connectivity and productivity in today's distributed work environment. We provide best-in-class security and protect against threats to reduce risk of data breaches and enhance user experience. By adopting this type of modern, flexible, cloud-based approach to network and data security, organizations are also helping position themselves for whatever comes next.

To learn more about how AT&T and Palo Alto Networks help businesses secure their infrastructure and data in a single solution, visit us online: *AT&T Secure Web Gateway* and *AT&T Secure Remote Access*

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.

About Palo Alto Networks

Organizations everywhere are undergoing a profound digital transformation, fundamentally reshaping the ways they operate, innovate, and connect with the people they serve. As the global leader in cybersecurity, Palo Alto Networks continually delivers innovation to enable and secure this digital transformation — even as the pace of change is accelerating. The most innovative companies in the world are choosing Palo Alto Networks. We are a cybersecurity partner to 95 of the Fortune 100 and secure over 73,000 customers in 150 countries around the globe. They rely on us to protect their most valuable data and assets. We are committed to providing them the visibility, trusted intelligence, automation, and flexibility that helps them advance. Our comprehensive portfolio delivers best-of-breed capabilities to secure the network, cloud, and ever expanding edge in a way that is integrated, automated, and simple. Every day, we innovate to create cybersecurity solutions that ensure our customers are secure today for a better tomorrow.