AT&T Business | paloalto® NETWORKS

A modern architecture to enable and protect the remote workforce

Work from anywhere is everywhere

While the concept of remote work isn't new, COVID-19 certainly accelerated the pace of change. **Digital transformation initiatives were expedited. Consumers and businesses demanded more digital interactions to replace those commonly occurring face to face. Nearly overnight, businesses around the world created work-from-home infrastructure and policies to ensure the health and safety of their employees, their families, and communities.**

The desire to move applications and services closer to the customer has inspired enterprises to rapidly invest in more software-as-a-service (SaaS) solutions, as well as other public cloud services. With business agility and flexibility being key drivers of competitive advantage going forward, the trend toward remote work is likely to continue.

In a McKinsey & Company survey of business executives[1], 93% indicated an increase in remote work or collaboration in the months following the start of the pandemic. Of those reporting an increase, 54% believe changes in remote work will remain for the long term. Of the 34% who reported an increase in migration of assets to the cloud, 54% believed those increases will similarly persist.

Indicated an increase in remote work or collaboration in the months following the start of the pandemic **93%**

Business executives who report an increase in remote work or collaboration believe the increase will remain for the long term **54%**

Those who reported an increase in migration of assets to the cloud believed those increases will similarly persist **54%**

New and more efficient ways of doing business have emerged, opportunities to enhance the customer experience have been identified, and businesses have uncovered new means of competitive advantage. But all of it comes at a price. As more organizations rapidly adopt cloud strategies and services, corporate networks are increasingly decentralized, and their legacy approaches to networking and security are tested in ways they weren't designed to withstand.

For remote work, legacy infrastructure isn't up to the task

In what would have taken months to accomplish pre-pandemic, enterprises around the world transitioned to remote work in a matter of days. On the surface, this is an impressive feat, especially for large, matrixed organizations with tens of thousands of employees. But a deeper evaluation reveals challenges as IT teams attempted to deliver a reliable, secure, and productive remote work experience while relying on legacy remote access technologies.

In its traditional role, virtual private network (VPN) acts a gateway for remote users to access the resources hosted at the data center. This is well and good, assuming everything the user needs is located on premises. But as organizations adopt cloud strategies at a faster rate and hybrid environments come into play, critical applications and data have become spread across on-site and cloud environments. Legacy VPN, designed to support small numbers of concurrent users connect to onsite servers, is ill-equipped to manage massive numbers of remote workers in disparate locations, particularly when accessing cloud-based applications.

Legacy network connectivity products, like VPN, come with some operational and security constraints. While VPN does encrypt and protect data in transit between the data center and the user through a private tunnel, it typically provides access to an entire network segment. This can put sensitive data at greater risk than is necessary and increase the potential for malware to spread laterally throughout the network.

But to fully internalize the limitations of legacy VPN to remote work at scale, consider its hub and spoke architecture. In this architecture, users are sitting at the end of spokes of various lengths, depending on their distance from the hub or data center. The greater the distance between the user and the hub, the more latency will be produced, but VPN is nonetheless the optimal solution because the goal is only to reach the hub.

When critical user applications reside in the cloud, performance and latency issues are more pronounced because of the virtual distance between the user and the cloud. In this case, traffic headed to the application must first travel to the VPN gateway. From there, the traffic is directed to the internet and on to the application. The application's response then travels back to the VPN gateway and then to the user.

This process termed *backhauling*, and the abysmal user experience it creates, disincentivizes employees to stay connected through VPN. Frustrated by less than stellar performance and delays that impact productivity, users will frequently disconnect from VPN when access to the data center is no longer necessary. Opting out of VPN in favor of a direct connection to the internet or cloud-based application effectively bypasses security controls, such as firewalls hosted at the data center, putting endpoints and data at risk.

Attempts to overcome limits of legacy connectivity solutions introduce new challenges

It's common practice for administrators and security professionals to attempt to compensate for the limitations of legacy remote connectivity solutions with compromises that may have unintended security consequences. Perhaps the most common of these is the user-initiated tunnel, which allows users to tunnel into the data center or hub as needed. The issue here, as discussed previously, is that users disconnect once their work with a necessary application is complete. Without being connected to the network, users access the internet directly and traffic is no longer inspected.

A split-tunnel VPN introduces a different version of the same problem, routing traffic destined for the data center through a VPN tunnel, with all other traffic sent directly to the internet. This helps resolve the latency issue for internet bound traffic but again, like the user-initiated tunnel, internet, and cloud traffic is not inspected at all, making the user's device and the network vulnerable to cyberattack while drastically impairing visibility and control.

Many organizations attempt to supplement VPN tunneling with web proxies for times that users are disconnected from the network. Websites can be blocked as needed and web traffic monitored. However, web proxies are not capable of doing a full inspection of network traffic and the inspection that it does perform will vary greatly from what is conducted at the data center.

These limitations outline the reasons most organizations consider augmenting VPN with a unified and cloud-delivered solution for the modern remote workforce. A mobile workforce needs high-performance access to the data center, the internet, and public, private, and hybrid clouds. A solution designed to support these users at scale should provide highly secure, productivity-inducing access to these applications, wherever users are located.

Cloud-delivered remote workforce solutions pave the way forward

To effectively support the massive shift toward remote work, organizations need to enable access to mission-critical applications and data, wherever they reside (data center or cloud), do so in a way that is easily scalable, and ensure all of it is secure. To further reduce opportunity for data misuse or loss, user access should follow the principle of least privilege, which is to say that employees should only have access to the applications and data they need to perform their duties – no more, no less. Enabling access by application, role, or user is key.

Striking the right balance between a consistent, high-value user experience and robust security can be a challenge. A bad user experience can negatively impact productivity, as staff struggle to access the applications and data they need or give up trying. Likewise, breakdowns in security can leave organizations open to operational disruption, incur significant costs related to non-functioning systems or data loss, and damage organizational reputation and trust. A unified approach to security is critical, one that follows each user as they go about their day and doesn't rely on a connection to the data center or hub.

A true cloud-delivered remote workforce solution takes a unified approach to remote access, a productivity-enabling user experience, and security. It will provide session protection, regardless of whether the user is on or off the corporate network. It uses machine learning (ML) to prevent threats from occurring and provides full traffic inspection, optimizing for security while offering greater visibility into what's happening on the network. And it implements data protection policies that prevent unauthorized access or misuse of sensitive data.

A true remote workforce solution built for the demands of mobile and highly distributed teams must offer a unified, singular approach to user experience, visibility and control, and security.

Make a unified approach to secure remote access a priority

While the benefits of cloud migration are plentiful, especially for enterprises focused on increased flexibility, agility, and proximity to the customer, many will likely continue to operate in a hybrid environment, where applications and data are split between onsite servers and the cloud. Finding a partner who can assist the organization through every phase of digital transformation is essential to enterprise success.

A true remote workforce solution built for the demands of mobile and highly distributed teams must offer a unified, singular approach to user experience, visibility and control, and security. It must interoperate with existing onsite solutions and applications, be flexible and scalable as more people return to the office or transition to remote work, and it must provide visibility across users wherever they're located, with the ability to apply unified security policies to all users.

Driving a high-value remote work user experience and maintaining centralized, single-pane-of-glass network visibility and control are keys to a successful deployment. But it's critical that a cloud-delivered solution protect all application traffic and deliver more security coverage than legacy point solutions combined to ensure a complete, enterprise-quality end user experience.

When evaluating a remote workforce solution against key metrics of scalability, user experience, visibility and control, and security, business and IT leaders should prioritize approaches to security that support rather than impede other defined metrics for success. The following technologies and approaches should be considered in addition to common VPN options or securing data in flight, like IPsec, SSL/IPsec, and clientless VPN.

Zero Trust Network Access (ZTNA)

Designed to employ the concept of least privilege, ZTNA technologies enable IT teams to assign user access only to those applications and data necessary for the individual user to do his or her job. ZTNA helps prevent lateral attack, where a user's credentials or device may become compromised and then used by the attacker to move laterally to other services.

ZTNA also enables controls to prevent vulnerable or non-updated devices from connecting to the network. This is preferable over VPN, in which the same access is granted to users regardless of whether their particular device is up to date on patches or otherwise exposed from a security standpoint. ZTNA's default position is to deny access, delivering it only after the user is authenticated and then enabling access through a secure and encrypted tunnel, to the services the user has been explicitly granted.

Likewise, robust ZTNA technologies should also perform traffic inspection for malware, data loss, and malicious behavior to ensure threats are not introduced even after the user authenticates. The protection offered by ZTNA is critical to enhancing the remote user experience. The reduction in traffic backhauled to the data center results in lower latency when connecting to cloud-hosted applications. On the administrative side, the reduction in data center appliances and operational overhead helps lower capital expenses.

Secure Web Gateway (SWG)

As the remote workforce continues to grow, businesses need a scalable solution for protecting users from web-based threats when they aren't connected to the corporate network through VPN. Rather than connect directly to a website or cloud-based application or service, user traffic first passes through an SWG, which then will apply functions like URL filtering to enforce acceptable use policies (i.e., block websites known to host malware, inappropriate content, or content deemed "time-wasting") and malicious content inspection, among other security controls. An SWG also enables complete visibility of the entire network to IT, regardless of where the user is located.

A secondary but important benefit of SWG is its decryption of SSL traffic in the cloud. While encrypted traffic is good for user privacy, it can introduce challenges to network security as attackers use encryption to shield malware from being discovered. Legacy-based security perimeters can similarly inspect SSL traffic, but the task is heavily processor-intensive. IT administrators, seeing the bottleneck in performance and user productivity, often disable the function to improve user experience. Unburdened by the same restrictions, SWG inspects traffic without negatively affecting network performance.

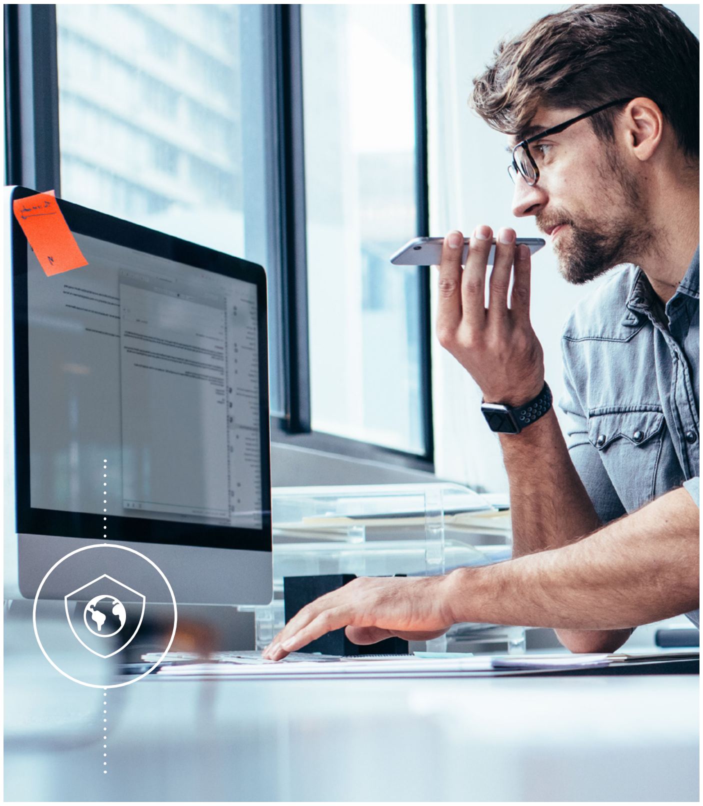
Firewall as a Service (FWaaS)

As more organizations have adopted cloud strategies, added more company and employee-owned devices to their networks, and begun using SaaS offerings, the notion of defined network perimeter protected by traditional firewall has slowly disappeared. Beyond the capabilities of a traditional firewall that provides stateful inspection of incoming and outgoing traffic, a next-generation firewall (NGFW) is application aware, actively helps prevent network intrusion, and leverages threat intelligence to enhance protection.

FWaaS takes the concept of NGFW a step further, delivering its capabilities as a cloud-based service. FWaaS provides visibility and control down to the application level, distinguishing between dangerous and safe applications, and even allows features within an application to be turned on or off (e.g., the chat function within a social media application). A strong remote workforce solution should enable FWaaS protection equivalent to those of a NGFW by aggregating traffic from multiple sources (e.g., on-premises servers, branch offices, mobile users and cloud infrastructure) into the cloud and applying security policies consistently across all locations and users.

DNS Security

Around since the early 2000s, DNS tunneling is a common form of attack used to access corporate networks, remotely control malware to disrupt command and control systems, and steal valuable data. In this approach, an attacker purchases a domain name, configures its domain name servers to his own DNS server, and once a DNS request is made by anyone inside the network, a two-way data transfer channel is established. DNS security uses a combination of machine learning (ML) and global threat intelligence to identify malicious domains in real time and prevent security threats before they occur.



Remote workforce solutions from AT&T, powered by Palo Alto Networks, deliver a unified approach to remote access and security for a more compelling user experience

Relying on cloud-based infrastructure, remote workforce solutions from AT&T, powered by Palo Alto Networks, deliver a comprehensive suite of combined networking and security services, including VPN, firewall as a service (FWaaS), zero trust network access (ZTNA), secure web gateway (SWG), and domain name system (DNS) security. They are offered as a fully managed or co-managed solution including deployment, security policy design, 24/7 monitoring and help desk support, as well as approved security patches and upgrades.

AT&T SASE with Palo Alto Networks

AT&T Secure Remote Access

- Provides secure, user-specific access to network applications and data, limiting exposure of resources the user doesn't need.
- Optimizes network performance by shortening the logical paths to cloud-hosted applications and data.
- Offers secure, consistent access that strikes the right balance between a productive and valuable user experience and network protection.

AT&T Secure Web Gateway

- Blocks access to identified malicious websites.
- Helps enforce acceptable use policies designed to reduce usage of productivity-draining web properties.
- Inspects encrypted SSL traffic in the cloud to preserve network performance.

Conclusion

From accelerated digital transformation initiatives to completely rethinking the way (or where) the modern workforce perform their jobs, the COVID-19 pandemic has dramatically influenced the way enterprises and organizations go about providing users with secure access to the applications and data they need. The massive, near overnight shift to highly distributed remote work, with many workers looking to stay that way, user-based access to applications and resources is more important than ever.

Consolidating networking and network security infrastructure to align with today's digital business approach is critical. Together, AT&T and Palo Alto Networks keep organizations of all sizes secure while allowing for more streamlined connectivity and productivity in today's distributed work environment. Our modern, flexible, cloud-based approach delivers a superior user experience along with best-in-class security to help businesses stay agile, flexible, and well-positioned for success.

References

[1] "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," McKinsey Global Survey, October 5, 2020

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*

© 2021 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.