Enable and protect your remote workforce

Global organizations are sharpening their strategies that enable their employees to work from virtually any location at any time. But working in different types of remote settings brings with it the potential for significant cybersecurity threats that must be anticipated, defended against, and quickly remediated.

This paper discusses the cybersecurity challenges associated with an increasingly remote and virtual workforce, and how remote security solutions should be imagined and architected.

Working outside the traditional office setting has accelerated during the past decade. Organizations have stepped up their network transformation efforts to align with such trends as telecommuting, working while traveling, and the rapid adoption of web-based applications. But now, these "work outside the office" trends have moved into hyperdrive.

Organizations are under intensified pressure to develop new, efficient, more flexible, and safer ways for employees to work away from traditional office settings. In fact, the attraction of working outside a traditional business office is so strong, that many employees say they would be willing to take a pay cut in order to have that option.[1]

But with the growing trend toward remote work comes a looming challenge: Organizations are struggling to offer their employees, customers, and trading partners highly secure remote access to vital applications and essential data.

Along with remote access challenges, another major problem is becoming increasingly clear: Malware, phishing, social engineering, and ransomware are all well-known threats. However, new campaigns are more targeted and include attacks on many types of devices.

Additionally, most devices, whether corporate-issued or personally owned, are being used off network, which often means a loss of visibility and control, and subsequently an increased risk for breach. When corporate assets, networks applications, and cloud services are being accessed by under-secured or unmanaged endpoints, the cybersecurity threat vector created by the work-from-home phenomenon broadens.

From this point forward, business and technical executives alike need to assume that cybersecurity challenges will continue to proliferate, as organizations and workers become comfortable with the notion of working remotely for some or even all of their work hours.

The trend toward remote work that began in earnest during a time when ample network bandwidth, inexpensive endpoint computing devices, and highly functional remote access tools became commonplace is likely to accelerate. It is also probable that cybersecurity threats that target applications, devices, and networks will surge in remote access settings. Without new strategies and tools, organizations are likely to fall victim to a higher number of cybersecurity breaches, which could take longer to detect and be costlier and more complex to recover from.

Organizations are under intensified pressure to develop new, efficient, more flexible, and safer ways for employees to work away from traditional office settings.

1 "Latest Work-At-Home/Telecommuting/Mobile Work/Remote Work Statistics," Global Workplace Analytics, March 2020.

Acknowledge and understand cybersecurity risks for remote workers

Over the years, IT organizations have put in place tools to help employees and other members of the virtual enterprise work remotely. The number of people working remotely has steadily increased, as has the total amount of work produced outside the traditional office setting. Now, more employees than ever are working remotely, and any given organization's virtual private network (VPN)—which was never intended to support so many simultaneous users—is straining under the surging demand. Research indicates that in March 2020 alone, VPN usage in the U.S. escalated by a whopping 150%.[2]

Another consideration is that the VPN was deployed with the expectation that employees and other remote users would likely be using corporate-issued devices and software, all with the proper and most recent security settings and privileges. Clearly, that no longer is the case, nor is it likely to be so in the future. Additionally, Security Operations Center (SOC) staff is overwhelmed, trying to triage substantially more alerts each day with an often-overworked staff and a tight budget. One report indicated that a typical enterprise SOC has to sort through at least 10,000 alerts each day.[3]

The pressure SOC analysts—and their cybersecurity tools—are under is caused by the rapid expansion in the number and complexity of threats to remote users. These include everything from mobile malware and email-based phishing to ransomware, identity theft, and machine-learning-based hacking algorithms.

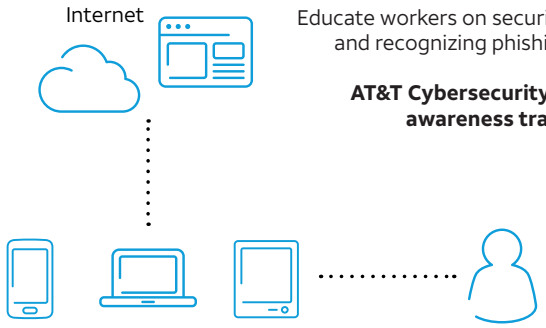
Then, add in a stark reality: Many, many end users fail to practice good cybersecurity "hygiene" on everything from passwords to social engineering, particularly without the watchful gaze of on-site IT and security professionals to help and "encourage" those remote workers.

Secure remote access challenges

With far more employees attempting to utilize applications, data, and services over a VPN using a public internet connection, organizations are coming to a realization of the mounting challenges and problems in providing highly secure access.

VPNs are clearly straining under the weight of additional users sending more rich media and unstructured data over the network. This creates massive performance bottlenecks and expanding security threats with more (often unsecured) endpoint devices demanding instantaneous access to do their jobs.

There are many reasons why overloaded VPNs may be compromised, but sometimes the solution can be as simple as increasing the capacity of the VPN concentrator or adding more or higher-bandwidth network circuits. However, one drawback to traditional VPNs is that they usually provide access to an entire network segment, which increases security risk. Network segmentation helps mitigate these risks, but most legacy VPNs often lack segmentation functionality, thus exposing wider swaths of physical and virtual networks to increased vulnerabilities during remote access sessions. For these reasons, some businesses are considering alternative cloud-based remote access solutions to provide more granular control and scalability.



Educate workers on security best practices and recognizing phishing attempts.

AT&T Cybersecurity employee awareness training

Help protect and manage laptops and mobile devices, including 24x7 support from AT&T.

AT&T Endpoint Security

2 "US VPN Use Could Soar 150% as COVID-19 Spreads," Infosecurity Magazine, March 2020.

3 "How Many Daily Cybersecurity Alerts Does the SOC Really Receive?" Bricata.com, October 2019.

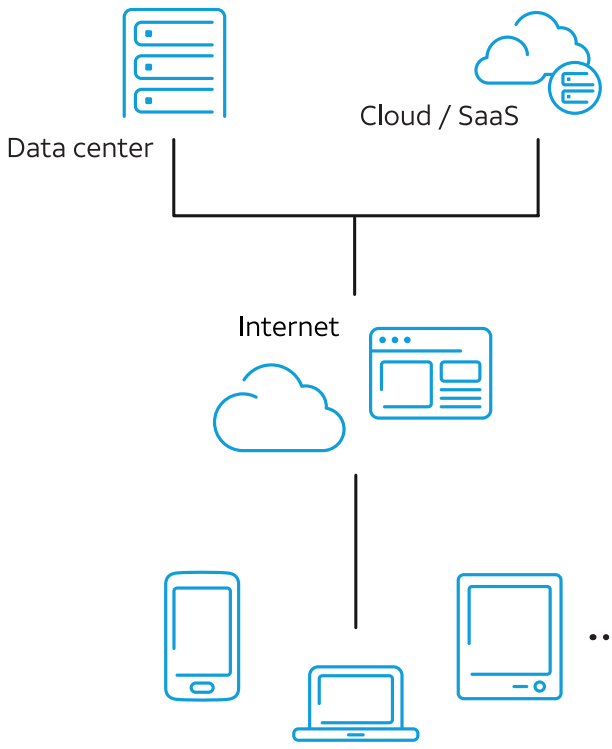
Help the new remote workforce withstand cybersecurity risks

Against this backdrop of increased cyber-risk in a new era of remote access and new work arrangements, organizations have to come up with new policies, processes, and technical solutions to support this new breed of mobile-centric workforce.

In order to provide highly secure, frictionless remote access, organizations have to rethink their tactics at all points in the IT ecosystem—data centers, departmental systems, edge computing, and cloud gateways.

Overcoming the numerous new and intensified threat vectors requires organizations to think and act upon the following security issues:

- Identity management
- Permissions and privileges
- Policy management
- Bring-your-own policies for devices, applications, and cloud services
- Cybersecurity training to help users practice smart security when working remotely and accessing applications and data, while also educating them on how to avoid the traps bad actors will set for them in order to gain access



Provide highly secure remote access directly to applications in the data center or the cloud as a supplement or alternative to VPN-based solutions.

AT&T Global Security Gateway
AT&T Enterprise Application Access

Help protect remote workers' internet browsing from web-based threats and zero-day attacks.

AT&T Global Security Gateway
AT&T Enterprise Traffic Protector

What to look for in remote security solutions

In order to deliver and scale highly secure access for employees, contractors, and partners that access data, applications, and services remotely, organizations need to take a comprehensive view of security. Specifically, it's important to invest in solutions that are designed to integrate with each other from the start, rather than acting as another point product that is "bolted on" after the fact.

Here are some key technologies and capabilities your organization should consider to buttress your efforts to support a remote workforce:

Remote application acccess. Using a cloud-based highly secure remote access solution provides access to individual applications that can be granted by role or by user.

Get help with remote application access

Secure web gateway. As important and utilitarian as the internet has become, it is also fraught with risk. Secure internet gateways efficiently and automatically filter and inspect outbound user traffic to build a barrier against accessing malicious sites or content that would run afoul of corporate policies.

Get help with secure web gateway

Endpoint security. No matter what type of endpoint remote workers may be using—desktops, notebooks, tablets or smartphones, point-of-sale systems or internet of things devices—organizations need full visibility into what is happening with applications and data being accessed remotely. Remote-access security tools must deliver the visibility and control for proper access credentials and policy management, regardless of format or location of the endpoint device.

Get help with endpoint security

Unified Endpoint Management (UEM). As remote users utilize a wider array of endpoint devices that include mobile devices and laptops dependent upon their locations or preferences, organizations need UEM tools that provide that endpoints are managed in the same way and with the same security protections and protocols, regardless of device.

Get help with unified endpoint management

Mobile Threat Defense (MTD). In today's always connected world, businesses need a solution that helps protect against key threat vectors of device, network, and application and social engineering such as phishing attacks. MTD combined with UEM allows businesses to take immediate action on devices that experience any of the threats while keeping company data highly secured.

Get help with mobile threat defense

Security assessment and training. Consulting services for vulnerability identification and evaluation can be essential in helping organizations plan and assess their existing and planned security architectures and operations. User training is also an important step to help correct and eradicate poor user cyber hygiene, which remains one of the most prevalent entry points for remote access security threats. This is particularly important as workforces shift to locations such as homes and public spaces served by open WiFi networks.

Get help with security assessment

Get help with training

Conclusion

Working remotely is fast becoming the "new normal" for employees and their organizations. The flexibility for employees and organizations is far too compelling for enterprises to go back to a headquarters-based model.

Providing for secure remote access for onsite and virtual workforces is essential for organizations, especially with remote workers often using under-protected or even unsecured endpoints and network connections. That means that organizations need to make smart, strategic decisions on the tools and services they use to bolster cybersecurity readiness.

Regardless of industry, geography, or number of employees, organizations must look for remote access tools that unify their visibility and protection. It is also crucial that organizations look at these and other cybersecurity tools holistically, rather than as individual point products, in order to help prevent security remote access gaps and to promote efficient deployment and management.

This content was commissioned by AT&T and produced by TechTarget Inc.