Remote Work Is Here to Stay

MK Palmore, VP and Field CSO for Palo Alto Networks, discusses the threat landscape created by remote work and strategies for securing remote access now and in the future.

What types of adversarial activities warrant closer attention in government enterprises?

The threat landscape is extensive, and adversaries continue to be fairly successful in their attacks. Financially motivated criminals are responsible for the vast majority of intrusions; however, insider threats warrant extra focus because the number of successful insider attempts is increasing. The last thing you want is someone walking out with the keys to the kingdom and you not knowing it. In addition, credentials are a prime target of malicious activity. With proper credentials an adversary can gain access to an environment, evaluate the data there and then successfully exfiltrate valuable information.

How has remote work impacted cybersecurity?

Government employees went from operating with business-approved devices from business-approved locations through business-provided pipes to mostly remote access. That introduced a whole new set of problems in terms of securely accessing the business information they need on a day-to-day basis. In addition, the number of attack vectors grew exponentially. Most organizations adopted secure remote access solutions so their users could connect safely and to maintain operability. Now that organizations realize they can be productive remotely, I think they'll maintain some portion of their secure remote access capability even when they return to more "normal" operations. With secure remote access, there's no limit to how they might be able to respond with agility to future challenges.

What overall strategy allows organizations to secure users, data, applications and other resources regardless of their location?

The secure access service edge (SASE) model lets organizations apply security no matter where their users, applications or services are located. It dictates that enterprise users need access to a variety of business resources and information. To maintain business operability and meet their missions, enterprises must figure out how to do that securely. Secure remote access — which includes secure connectivity, identity access management, access control, continuous validation of secure connectivity throughout an interaction and more — will be the mark of a functioning cybersecurity apparatus moving forward. The other component is being able to scale cybersecurity talent and resources to accommodate growth.

What challenges go along with using cloud-based security services?

We find the people responsible for configurations make the same mistakes in cloud environments that they make in on-premises environments. The cloud doesn't alleviate network defense of security; it makes it more difficult. With the shared security model, organizations must understand the responsibilities of the cloud provider and their own responsibilities to protect enterprise data. Understanding and managing those gaps requires government security teams to get even more involved in terms of identifying security tools that might be helpful. And then, even though cloud providers offer cloud-native tools to help with these things, enterprises often need help with getting tools that are easily accessible, scalable and solve their business problems.

How can AI and machine learning help level the playing field against adversaries?

Given the tools available to adversaries, the frequency of automated attacks and the increasing complexity of our environments, there's no way to keep pace with the adversarial environment if AI and machine learning aren't baked into your appliances. With AI and ML, baseline data collection and rudimentary activities — for example, moving from one application to the next in order to gather information — can get done automatically; so by the time the data is teed up in front of a human, all of that time-intensive work has been boiled down to a decision that needs to be made: Do I need to investigate this further, escalate it or dismiss it?

What has the pandemic taught us about cybersecurity?

It's taught us that cybersecurity must be a component of existing technology investments and a baked-in additive to the technology advances that we hope to adopt in the future. Without security, those technology advances will always represent a potential vulnerability that adversaries will try to exploit. The pandemic also highlighted our reliance on digital information both for business reasons and as consumers. Folks absolutely must figure out a way to access that information securely as they plan their roadmaps for digital transformation.


Securely Connect and Scale Remote Workforces
With Prisma™ Access
paloalto NETWORKS
PRISMA
paloaltonetworks.com/remote-security