POINT OF VIEW

Use ZTNA to Protect Today's Hybrid Workforce

How IT Security Teams Can Succeed in the Work-From-Anywhere Era

Executive Summary

After shifting to remote work due to COVID-19 restrictions, a significant number of employees want to continue doing their jobs with work-from-anywhere (WFA) flexibility. This poses a challenge to employers: how to best accommodate the desire to work remotely, whether full- or part-time.

Unfortunately, many organizations don't or can't give employees this flexibility due to an inability to provide consistent, high-quality security. The main problem is security teams are using different security solutions for employees in the office versus what they use for remote users.

There is an easy solution available. Just use the same zero-trust network access (ZTNA) service to protect employees no matter where they are located, on- or off-site.

Using multiple products is not only inefficient, but also less secure and more difficult for both IT staff and the users they support.

Less Security, Higher Expense, and Hard to Use

To manage security for multiple locations and networks, many IT teams use multiple products that have their own unique consoles or dashboards that are not all integrated, and deal with separate IT policies in multiple places. When juggling more than one product, the odds of misconfiguration and errors greatly increase, and troubleshooting becomes much more difficult.

Increased costs can be another downside of using multiple products. Almost invariably, it's more expensive to license two products and their associated services versus purchasing only one.

From the employee viewpoint, having multiple products makes accessing applications different from when they're in the office versus when they are away from it. This can result in confusion and frustration, particularly if one of the products is more difficult to use like an old, slow virtual private network (VPN).

Shift From VPNs to ZTNA

The best solution is to use the same security for everyone, no matter where they may be located and what resources they need to access. Most will agree that to improve security for remote access, organizations should shift from using VPNs to ZTNA because ZTNA provides more verification and authentication of users and devices than a VPN. ZTNA also automates the encrypted tunnels and provides granular application access, which improves both security and the user experience.

Although people have been talking about zero-trust security solutions for more than a decade, vendors don't necessarily use the terminology the same way. Part of the confusion stems from the fact that ZTNA is often only associated with cloud-application access. But most organizations don't have all their applications in the cloud.

"Seventy-four percent of respondents whose companies had been breached admitted those incidents involved access to a privileged account."[1]

Consistent Policies and Controls

Workers need access to cloud applications, but they may also need access to applications located at a data center or branch location. ZTNA should be used no matter where the applications or the users are located. Everything should be secured with consistent policies and controls across operating environments, including across multiple clouds.

The reason ZTNA is often considered a "cloud-only" solution is because many cloud-only vendors are optimized for situations where users are remote and applications are in the cloud. Cloud-based ZTNA has issues when users are in the office and accessing an on-premises hosted or data center (DC)-hosted application. Hybrid ZTNA solutions can be deployed on-premises or in the cloud and optimized for wherever users or applications are located. If ZTNA is going to be everywhere, it can't be a cloud-only solution.

To achieve ZTNA across the network infrastructure for users located anywhere, one solution is needed that has flexible deployment options and can offer consistent security policies. An integrated next-generation firewall (NGFW) with built-in ZTNA that is available for the organization, in the cloud, or even as-a-service, can control all access for everyone.

One key advantage of using firewall-based ZTNA is that the traffic will flow through a complete security stack. Updated threat information ensures intrusion prevention and signature matching to identify known threats and attacks.

Conclusion

Supporting employees working from multiple locations has placed more pressure on networking and security teams. They don't need to add more complexity by using multiple products that do the same thing. To improve both security and the user experience, ZTNA is replacing prior technologies such as VPN for remote access. But it shouldn't be limited only to remote users.

It's better for security teams and users if ZTNA works the same way everywhere, both on-premises and off. Instead of a piecemeal approach, it's more secure and inherently easier to implement ZTNA everywhere by starting with an NGFW solution that integrates with a cybersecurity mesh platform architecture. This holistic approach delivers unified visibility, automated control, and coordinated protection.

[1] Andrew Martins, "Poor Access Management Leads to Majority of IT Hacks, Study Finds," Business News Daily, June 29, 2022.

August 18, 2022 11:27 PM
1711760-0-0-EN