Cyolo

The ‘Last Mile’ of Application Security:
Extending Your Zero Trust Network Access (ZTNA)

Many companies today allow a hybrid approach to work, with people balancing time in the office and working from home or elsewhere. Driven by digital transformation and accelerated by the COVID-19 pandemic, this new mode of working introduced added challenges for security professionals. While the lasting power of this new hybrid work approach is yet to be seen, the problems uncovered have the capacity to affect and advance the security posture of many companies well into the future.

> *Nearly every computer system in existence relies on the idea of inherent trust, or that users are who they claim to be.*

Now that users have left the building, the riskiest threat vector is the identity perimeter. When everyone worked from the office, it was easy enough to extend trust to users who were on the corporate network with acceptable corporate credentials. This castle-and-moat model worked for many organizations for many years. Then, when the need to remotely access corporate resources began to appear, the Virtual Private Network (VPN) was born.

VPNs follow the same logic of trusting users based on the validity of their username and password to place them onto that same corporate network, as though they were physically present in the office. From a security perspective, what this means is that a compromised VPN user could knowingly or unknowingly bring in a malicious ‘tag-a-long,’ who could then move laterally within the network. All it takes to compromise a VPN is to phish a password from an employee and log in. After the bad actor gains access, they can quickly find out what network they are on and then scan for exploitable vulnerabilities before executing their weaponized malware files.

IDENTITY-TO-APPLICATION

- Zero trust
- Secure access
- Secure connectivity

Zero Trust Network Access (ZTNA) was designed to replace or augment VPNs as a tool for accessing both on-site and cloud services, while simultaneously enforcing advanced security policies on remote workers. But ZTNA solutions still face the challenges of validating users based on their identity and limiting their access to only the applications they need to complete their work.

Furthermore, many ZTNA tools work in a legacy world, where inherent vendor trust still exists. To securely route traffic to the needed application, ZTNA providers typically decrypt the traffic. After route determination, they re-encrypt the traffic and send it along its way. **This approach has three main problems:**

Each decryption/re-encryption is bandwidth-intensive and slows down the entire journey.

By hosting decryption keys, the ZTNA cloud router violates the zero-trust model. Any breach of the provider could have negative security implications for their customers.

ZTNA was designed for remote workers who access cloud applications. Most ZTNA providers struggle to support on-site users or hosted applications.

Access and connectivity control advance ZTNA and strengthen security by taking users directly to the applications they need to do their job, instead of supplying access to the entire network segment. Beyond actually adhering to zero-trust principles, this direct identity-to-application approach enables a stronger security posture, with greater user adoption. With a software-based approach, many organizations can decrease the number of physical firewalls and VPN head-ends and realize significant savings when reducing the number of end user VPN licenses.

Cyolo has abolished the need for vendor trust by creating the world's first true zero-trust, secure access and connectivity solution. Now, organizations can safely connect people to work, without compromising security or access controls.