4 Remote Access Reasons to Adopt Unified ZTNA

Secure, remote-access solutions provide users with the minimum required access to application and infrastructure, leveraging identity and context as decision criteria for access.

However, approaching this with point solutions is proving to be limiting (they either don't scale or address security requirements of modern hybrid networks) and typically are not integrated with a wider microsegmentation and access initiative. New approaches to remote access, if pursued as part of a zero-trust initiative, can be integrated as part of a unified zero-trust platform to ensure seamless functionality, enforce process-level controls, and utilize policies based on risk, usage, and other end-user factors.

As organizations start adopting a zero-trust approach to security, applications and user access cannot be looked at in silos and can benefit from a platform which addresses the zero trust access controls based on the context of applications and users throughout the network. Benefits of an integrated, unified solution include:

- Leveraging 3rd party feeds that the platform offers, including threat intelligence, vulnerability data, and others, that can enhance the security context for remote users;
- Network visualization and mapping capabilities offered by the platform can be leveraged by the remote access solution for easier management and policy enforcement;
- Platforms typically provide additional layers of context to the access data, such as, if the user is remote or local, location, as well as other active directory and security attributes, enabling the platform to make real-time decisions to grant in-time access.

Key Scenarios Leveraging Remote Access Native to a Zero Trust Platform

Scenario #1: Seamless On-Prem/Off-Prem Access to Dynamic Workloads

Challenge Current non-integrated point solutions make it challenging to manage and enforce access policies while users transition between on-prem and off-prem, without impacting user experience and ease of use/administration.

Solution For a secure, remote-access solution, integrating seamlessly into a unified zero-trust platform for dynamic workload segmentation capabilities enables remote access with automated policy enforcement and granular access control to dynamic workloads, such as S3 buckets, Kubernetes clusters, containerized applications and services, Lambda functions, and more. With this kind of platform integration, access policies are enforced automatically and seamlessly whether users are on-prem or off-prem, and don't usually require any reconfigurations or reinforcements.

Scenario #2: Application-specific End User Access

Challenge Enterprises need to provide secure access to specific applications that employees need to do their jobs. Traditional VPNs provide network-centric-only access and are ill-suited to this need, thereby exposing larger attack surfaces to the malicious actors.

Solution A remote-access solution, integrate into a unified platform, provides user identity- and device security posture-based granular and secure direct access to applications, even on the same network segments. This granular access control is enforced irrespective of the user being on-prem or off-prem. In this platform approach, applications are not exposed to the internet,

reducing the attack surface and lowering risk. An integrated solution normalizes the user experience on and off the corporate network and can be a low-latency, low-complexity, higher-security solution that simplifies deployment and improves the user experience for both end users and IT admins.

Scenario #3: Role- and Identity-based Cloud Services Access

Challenge Today's hybrid organizations need to provide secure role- and identity-based remote access for employees, contractors, and administrators to enterprise applications and application/workload segments with services and infrastructures distributed across public clouds, VPCs, campuses, and data centers. Applications and workload segments can span multi-cloud or hybrid cloud infrastructure environments. Using traditional VPNs and siloed ZTNA point solutions is cumbersome and expensive.

Solution A platform-integrated solution enables role- and identity-based secure access to distributed applications, cloud services, and workload segments across any public cloud, hybrid cloud, or data center with zero-complexity deployment and operations. This approach is usually software-based, seamless across environments, and makes it easier to define and manage policies at scale across clouds. When integrated with workload-to-workload segmentation, users can achieve maximum security of applications and services being accessed by internal and external users.

Scenario #4: Strategic Third-party Access

Challenge Enterprises need to provide third-party contractors, vendors, and partners with secure access to applications in their cloud or data centers, without adding these users to enterprise AD/SSO and without requiring a VPN or DMZ.

Solution When the remote access solution is integrated into the zero-trust platform, it can more easily integrate with multiple identity providers for authentication, eliminating the need to add external users to active directory servers or set up VPNs or a DMZ for access. Enabling third-party access requires no VPN setup and no changes to network or firewall configurations, while facilitating seamless operations across fragmented networks due to multiple campuses or M&A activities.

Conclusion

To ensure a smooth experience and apply risk-, usage-, and user-based policies, organizations must consider incorporating remote access into their zero-trust initiative as part of an integrated, unified platform. This approach will provide the most comprehensive protection while allowing greater control over processes and users.