Menlo Security

BRIEF

Enable Seamless Access to Private Applications for Remote Users without Compromising Security

Menlo Zero Trust Private Access (ZTPA) Leverages an Isolation Core™ to Grant Safe Access to Specific Private Applications without VPN Clients or Agents

Benefits:

- Provides a true zero trust approach for internal web applications
- Reduces IT complexity and overhead
- Enables secure application access without endpoint agents
- Shields applications from untrusted users and endpoints

The new normal has spread users, devices, applications, and data away from a centralized data center and out to hundreds or thousands of distributed locations, including remote offices, factory floors, worksites, dining room tables, and coffee shops across the globe. The move to the cloud has mitigated many of the challenges associated with expanding accessibility, but legacy internal web applications present a different challenge. How can organizations provide distributed users with the unhindered access to internal web apps they are used to in the data center without severely expanding the surface area for attackers to target?

VPNs Fall Short

Virtual private networks (VPNs) have traditionally been used to provide secure connections between remote users and mission-critical applications. However, an explosion of remote workers resulting from digital and cloud transformation—as well as work-from-home mandates caused by the Covid-19 global pandemic—has overwhelmed VPNs, creating major bottlenecks that have devastated application performance and user productivity. Organizations have gotten around this problem by using split tunneling or exposing Internet traffic altogether, neither of which is a good option.

Even when deployed properly, VPNs are also extremely vulnerable to hackers. VPNs run over the public Internet, effectively exposing traffic to enterprising threat actors who use phishing, drive-by, and zero-day attacks to steal credentials and gain access to users' devices. Once compromised, these authenticated devices allow threat actors to move laterally across the network, infecting other systems and devices along the way. From a management standpoint, VPNs are difficult to configure and require restrictive policies that are complex and error-prone. As appliances, VPNs are hard to scale elastically as users become incrementally more distributed and mobile. In most cases, VPNs also require hardened laptops and endpoint agents, further increasing IT complexity.

Applications are the entry point to a network. Once the attacker enters via the application, they have access to the internal network.

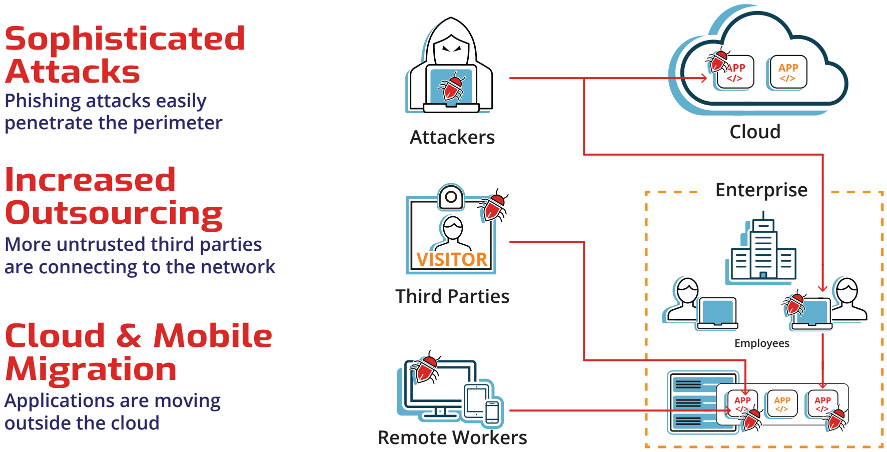

Fig 1: Applications are the new entry point into the network. Once the attacker comes into the network, they have access to the VLAN and they can move sideways.

A Zero Trust Approach to Application Access

A new approach to network security is needed to overcome the critical flaws of VPNs and the common exploits of attackers. This new approach must be rooted in zero trust, the notion that a user is not trusted unless their identity is extensively verified. This can be done effectively and efficiently through cloud-delivered security services.

Menlo Zero Trust Private Access (ZTPA) provides fast, seamless access to any internal application without relying on legacy VPN services that allow open access to internal resources. It does this by using an isolation layer to remove applications and services from direct visibility on the public Internet. Rather than accessing the original application, Menlo ZTPA leverages our Isolation Core™ to create a mirror image of the application on the endpoint device via the cloud. This approach effectively grants access to a specific application rather than the underlying network by using an air gap, thereby eliminating a threat actor’s ability to directly interact with the application. Furthermore, Menlo’s Isolation Core™ shields the application from parameter tampering, web scraping, API abuse, and a host of other problems not addressed by other zero trust network access (ZTNA) solutions.

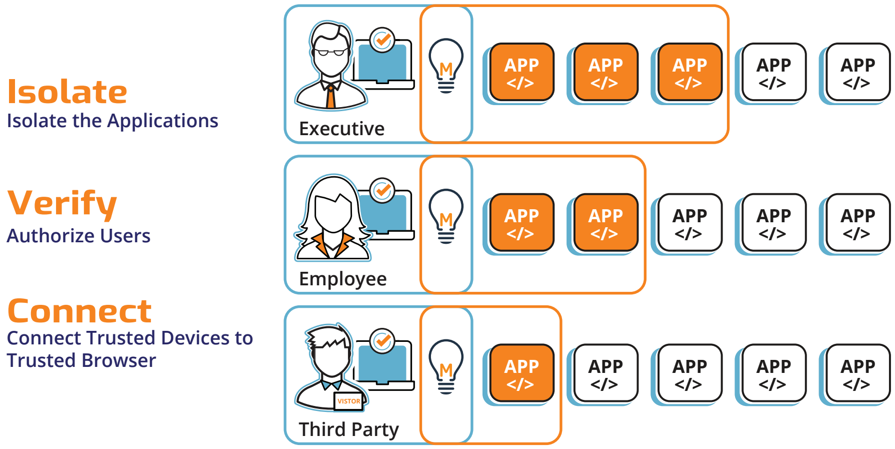

Fig 2: Menlo Zero Trust Private Access (ZTPA), zero attack surface

Allows organizations to grant application-level access to highly distributed users without exposing internal networks to untrusted entities.

Reduce Surface Area without Limiting Authorized Access

Menlo ZTPA allows organizations to grant application-level access to highly distributed users without exposing internal networks to untrusted entities. Menlo ZTPA improves the flexibility, agility, and scalability of application access—enabling digital businesses to thrive without exposing internal web applications directly to the Internet, and thus reducing the surface area and the risk of attack. Menlo's unique agentless approach coupled with its Isolation Core™ reduces IT complexity while continuing to provide seamless and secure access to private applications.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 695-0695
ask@menlosecurity.com