WHITE PAPER

Apporto Zero Trust Virtual Desktop

Desktops Designed with Zero Trust as a core architectural principle to meet the modern security challenges in a remote work environment.

Remote Work is the New Normal

Companies are searching for the best ways to enable anytime, anywhere access to their staff. Owl Labs reports that 52% of global employees currently work remotely once a week. At the same time, Cybersecurity Ventures expects global cybercrime costs to grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015. Witness the recent surge of ransomware attacks on large industrial companies (e.g., Colonial Pipeline). Furthermore, education is the number one industry affected by security incidents, according to Baker Law.

This is the environment in which IT departments are struggling to provide remote access. IT departments must provide secure, consistent access while meeting the performance and productivity demands of a diverse user base. How can this be done without compromising IT security or user experience? In this white paper, we will examine how Apporto helps IT achieve a zero trust architecture that meets the needs of a hybrid workforce.

Challenges of Remote Access

VPN technologies have been at the core of enabling remote access for the last thirty years. However, the surge in remote work due to the pandemic and the increased focus and sophistication of threat actors on VPNs has resulted in a growing challenge: The attack surface, previously confined to only the corporate network, now includes a variety of devices - managed or unmanaged which must also be protected, with data stored everywhere and in large swaths of the internet. See Fig.1

Apporto

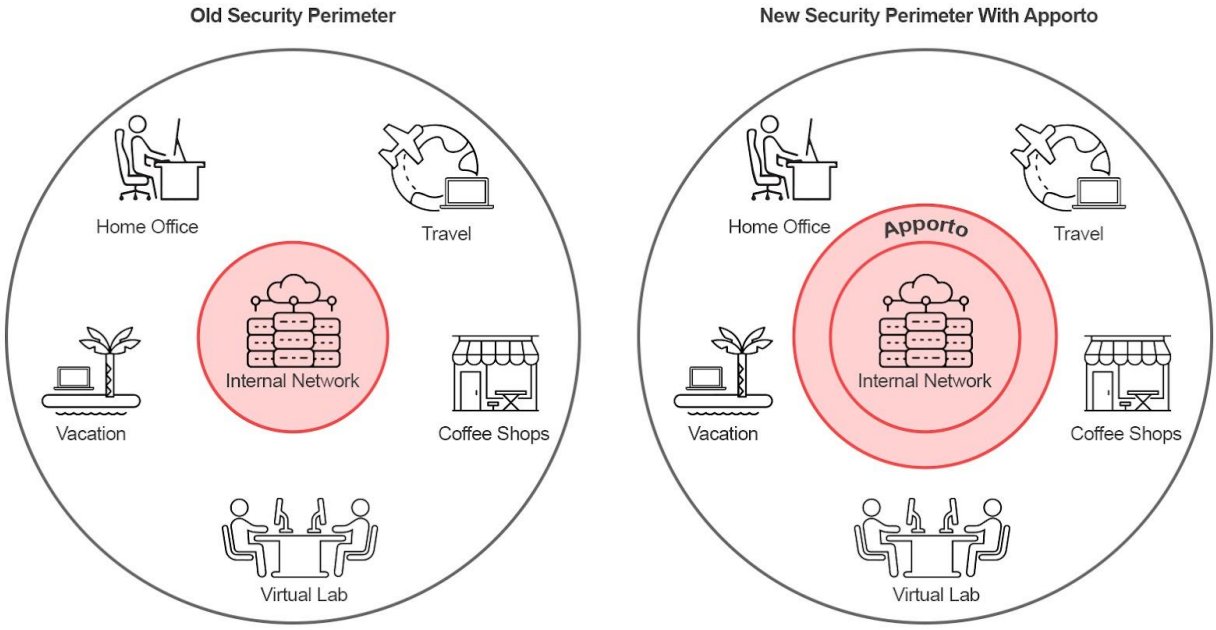


Fig. 1

The 2021 VPN Risk Report summarized its findings by stating that 93% of companies are leveraging VPN services, yet 94% are aware that cybercriminals are targeting VPNs to gain access to network resources. Further, 67% of enterprises are considering a remote access alternative to a traditional VPN.

The zero trust journey can be a very long one. It took Google, a very agile company, six years to move to a zero trust architecture. One of the first steps of zero trust is identifying the most critical assets (data, services) and the most vulnerable systems (typically endpoint devices). The Apporto cloud desktops specifically address this use case.

A More Secure Cloud PC: Always in the Browser

Whereas many legacy Desktop as a Service (DaaS) and Virtual Desktop Infrastructure (VDI) companies can deliver virtual desktops in a browser, this capability is often an afterthought to their design and is not recommended for many important use cases (videoconferencing, graphical applications, etc.). Furthermore, end-users often need access to local resources, e.g., cameras, printers, folders. To make those resources available most legacy DaaS and VDI companies strongly recommend that users install and use a client, keep that client up to date, and they then recommend that IT Admins secure the endpoint with a VPN and enterprise-managed security policies. In other words, a cloud desktop that uses a client expands the attack surface to the endpoint and the IT team is back to managing and maintaining the endpoint's security

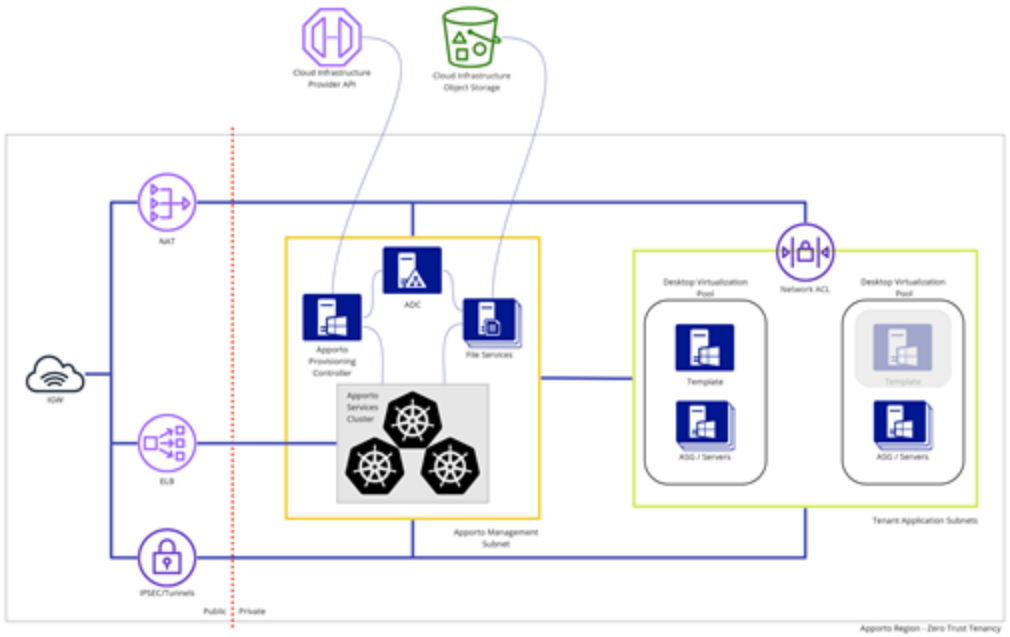
Apporto, on the other hand, is always delivered in the browser and does not rely on the endpoint to be secured. Unlike VPN access which grants the remote worker's laptop access to the physical network and therefore can be an attack entry point that must be secured using ACLs, the Apporto Cloud Desktop only allows the remote worker to interact with the delivered desktop via HTML events and messages which provide a very limited attack surface. Essentially, the most critical aspect for securing an Apporto Desktop is utilizing strong user identity assurance that can be added to any SSO solution.

Least Privilege Access

A fundamental tenet of zero trust is that users should be provided the least amount of privileges/resources needed for their tasks.

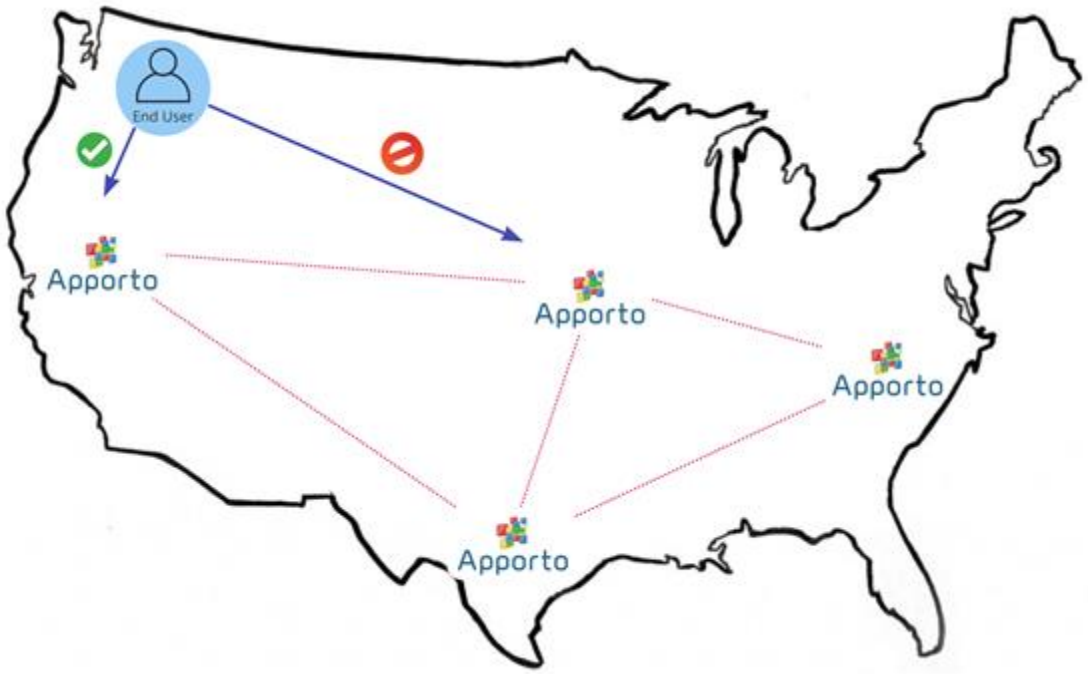
Apporto achieves this with a three-pronged technology approach:

1. On the Cloud Desktop, a user can only see the Applications they are authorized to launch.
2. From the Cloud Desktop, a user can only access the Services and Networks they are Authorized to use.
3. Ingress to the Cloud Desktop, users and services can only reach the Cloud Desktop if authorized.



Each Cloud Desktop secures Application launching through industry-recognized technologies. Apporto provides a simple management console to the IT Admin to allow them to leverage their skills in Security Group management to simply and efficiently control application access. Apporto's management console enables administrators to publish or hide applications or shared folders based on the users' role/group affiliation. For instance, a user who is a member of the Engineering team who does not need or have access to SAP would not see the SAP client on his desktop. Similarly a user who does not need access to specific data would not even see the shared folder.

Apporto secures the network. Egress from the Cloud Desktop is managed by the same Apporto management console. Per-user network rules are easy to define and maintain, regardless of the Cloud Desktop configuration. Network Ingress is also secured. Apporto Tenants can link Cloud Desktops with existing corporate networks securely and efficiently. Nothing enters; nothing leaves unless it is explicitly allowed.



Another historical problem with legacy VDI/DaaS solutions has been poor user experience. This is often the result of high network latency or improperly configured applications. Poor user experience is frustrating to users and leads many to use the managed cloud desktop for one set of applications and their unmanaged physical desktop for applications such as video conferencing or chat.

This defeats the purpose of the managed cloud desktop since it's often inevitable that end-users will store some of the data on their physical desktop, e.g., uploading or downloading a file from a Teams chat. Apporto addresses high network latency by utilizing a unique geo-optimizing technology. This means that Apporto can assure that an end-user is always connected to the closest data center to ensure minimal network latency. Apporto's network of data centers ensures that no user is ever further than 50ms from their cloud desktop. Research has shown that at a latency less than 50ms, most people cannot distinguish between a local vs. remote experience. In addition to our regional infrastructure, Apporto has implemented several additional technologies that enable the bridging of edge video and audio devices into the cloud desktop through the browser. These features allow users to remain on the cloud desktop for all their use cases - even for highly demanding applications such as video conferencing.

Apporto Cloud Desktop: Security, Manageability, and Performance

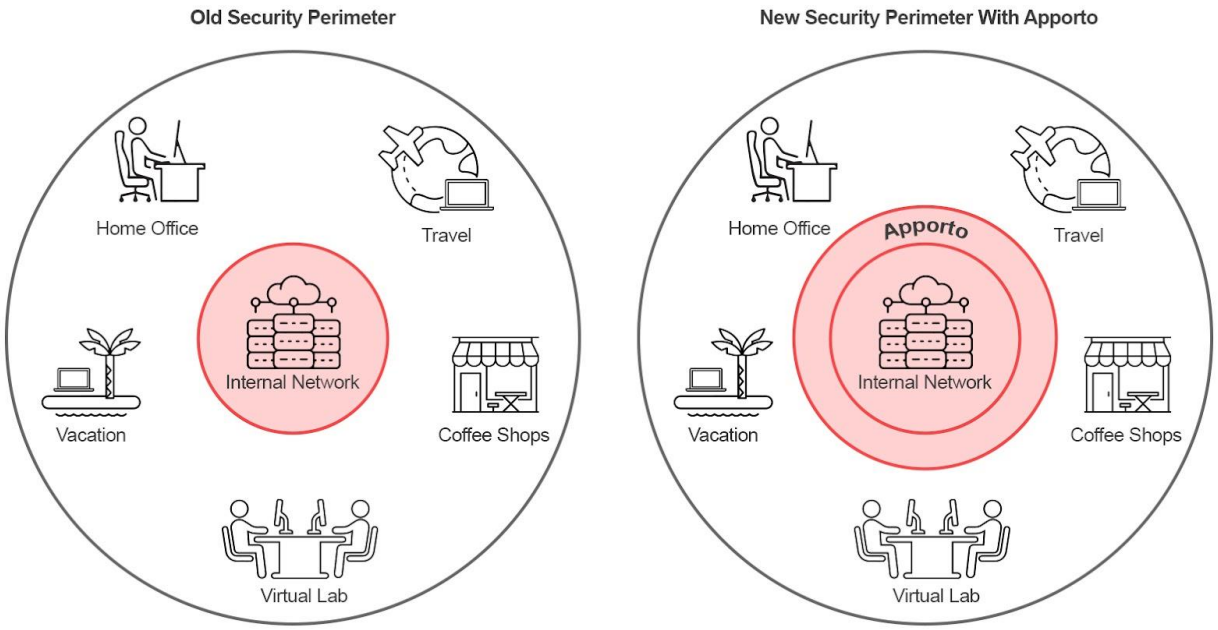


Fig. 2

A Cloud Desktop reduces the attack surface significantly by allowing all data to be kept inside a secured perimeter. No data need to be shared onto an unmanaged device nor need to exit the organization on an unmanaged network. IT Admins have control of data ingress and egress and can audit activity. See Fig 2

Keeping resources in the Cloud allows scaling and right-sizing usage with just a few clicks. IT Admins no longer have to worry about shipping new laptops and resources. Onboarding becomes as simple as distributing credentials.

Network Segmentation

In the past, network architects targeted their security at the perimeter. Individuals within the perimeter were assumed to be trustworthy, and, therefore, not a threat. A zero trust architecture calls this assumption into question. Insiders can be sources of breaches. Furthermore, when a bad actor penetrates the perimeter, they move laterally until they locate sensitive data.

Zero trust assumes that the system will be breached and designs security as if there is no perimeter. Hence, zero trust's motto - "never trust, always verify" - starting with the network

To prevent lateral movement, the network segmentation feature enables administrators to prevent unauthorized users from gaining access to assets they should not have access to.

Network administrators can control the flow of traffic between virtual desktops and IP addresses or URLs based on permissions setup in Apporto.

For instance, virtual desktop users in finance are specifically granted access to network resources such as the ERP. Others, such as marketing for example, are prevented from accessing the ERP - whether the ERP is an internal resource or an external service.

Screen Watermarking

A common concern is that rogue employees or bad actors may use a camera to take a picture or video recording of sensitive information. To deter this, the screen watermarking feature displays a static watermark over the user's screen. The layer is semi-transparent and allows the end user to still see and work with his/her content.

The screen watermark contains the end-users' metadata, typically the user's name or email address. Therefore, any internally leaked information can be tracked and traced back to the user who leaked the information.

Conclusion

Apporto has leveraged decades of experience to create a modern, secure cloud desktop service. We minimize the attack surface by using a client-less virtual desktop; We embrace the principle of least privilege for apps and data and visibility/control of all data ingress/egress. We partner with admins by providing them with a simple control panel that makes the support of a remote workforce easy and worry-free.

Ready to Learn More?

We'd love to learn more about your specific secure desktop needs. Contact Apporto today to start the conversation, ask questions, or see a demo.