CAMEYO

WHITE PAPER

Securing Remote & Hybrid Work with Zero Trust

Your Checklist for Zero Trust Security Solutions

Securing digital resources is a constantly moving target that organizations struggle to meet. There are arguably more threats to your data than ever before, especially with the shift to a remote & hybrid workforce. Organizations have also shifted to digital tools and connectivity solutions that extend the boundaries and blur the lines of on-premises vs. external.

A traditional security stance is no longer adequate for protecting business-critical data. As a result, one framework for safeguarding valuable business systems and securing critical data access – the Zero Trust security model – has become incredibly relevant. So, what is the Zero Trust security model, and why is it critically important today? How has the shift to a distributed workforce brought this into focus?

Zero Trust - The Modern Security Model

If you think back over the past few decades of traditional infrastructure and security design, most corporate networks treated anything external to the corporate network as untrusted and anything inside the corporate network as a trusted source. The traditional corporate firewall has been the “end all be all” of the security for the entire internal network for years now.

It is supposed to keep the bad guys out and protect the internal, trusted network. However, as new threats such as ransomware and others make their way past firewall technologies and into the

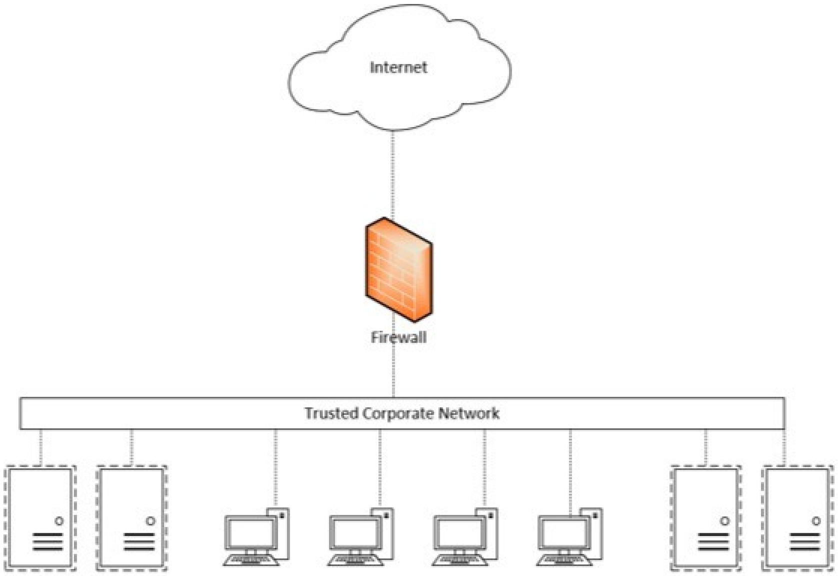
In This Paper

internal network with new types of attacks, this traditional security model is no longer sufficient. How are threats getting past the perimeter?

No matter how good a perimeter firewall is, it cannot stop today's internal threats. There are too many types of malicious code vectors, zero-day attacks, and other threats to prevent them all. Also, attackers use crafty ways of infecting internal workstations with malware and other malicious code through phishing scams, drive-by website attacks, etc.

Once cybercriminals infect an internal client, the threats now come from inside the perimeter network. After the attacker is on the inside of a traditional network perimeter, the safeguards and security boundaries no longer apply. They can generally move laterally across the inside network, exfiltrating and leaking data and compromising other internal systems with little resistance. The new types of attack vectors used by attackers today are increasingly making the traditional "protect the perimeter approach" obsolete.

Below is a very simplistic overview of a traditional network design. Workstations and servers are all found on the internal trusted corporate network. On the other side of the firewall is the Wide Area Network (WAN) connection to the Internet. In traditional network design, this is the untrusted network. All workstations and servers on the trusted corporate network can communicate without any restrictions or limitations to both the types of traffic and the internal source.



Traditional network design trusts all traffic on the internal corporate network.

> "No matter how good a perimeter firewall is, it cannot stop today's internal threats."

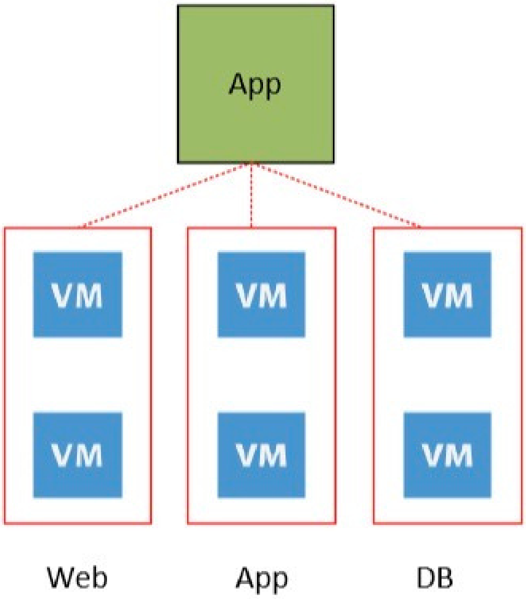
With the threats mentioned above becoming widespread, organizations are undergoing a paradigm shift in how they approach security both externally and internally. No longer is it safe to view internal resources as trusted and secure for allowing access to business-critical data and services. The Zero Trust security model is not associated with a specific technology or architecture. Instead, it is a holistic security approach that centers on the belief that all internal and external resources should not be trusted, and that they should all be automatically validated regardless of the requesting entity's location. There is no longer a trusted internal network with the Zero Trust security model where all nodes trust one another by default.

"No longer is it safe to view internal resources as trusted and secure for allowing access to business-critical data and services."

How Zero Trust Has Evolved

In the early days of Zero Trust, it was all about micro-segmentation. With micro-segmentation, nodes can only "see" and communicate with nodes they are allowed to communicate with, even if these reside on the same internal network. Early Zero Trust models were made possible by software-defined networking solutions that allowed creating micro security boundaries between nodes.

Below is an example of traditional micro-segmentation in establishing Zero Trust policies for network communications. Virtual machines are only allowed to communicate with specific VMs. In the conventional 3-tier application, which includes web, app, and DB tiers, only the VMs in each respective tier and logical workflow can communicate.



Zero Trust architecture including micro-segmentation.

With the threats mentioned above becoming widespread, organizations are undergoing a paradigm shift in how they approach security both externally and internally. No longer is it safe to view internal resources as trusted and secure for allowing access to business-critical data and services. The Zero Trust security model is not associated with a specific technology or architecture. Instead, it is a holistic security approach that centers on the belief that all internal and external resources should not be trusted, and that they should all be automatically validated regardless of the requesting entity's location. There is no longer a trusted internal network with the Zero Trust security model where all nodes trust one another by default.

The Zero Trust security model generally works hand-in-hand with other security best practices, such as the least privilege access model. Users and systems only have access to those resources and types of network communication required, no more or no less. To successfully establish a Zero Trust security model, organizations must implement solutions that can confirm the entity's identity requesting resources and then validate that the entity has the authorization to access the resource.

Why Zero Trust is Now Crucial

Most businesses have had to shift to a remote & hybrid work model, so the vital question essentially becomes – where is the network perimeter?

Today's hybrid architecture and network topologies blur the lines between on-premises and external resources. Meanwhile, security firm Kaspersky reports that from 2019 to 2020 there was a 767% increase in ransomware, while Check Point 2021 Cyber Attack Trends mid-year report shows another 93% increase from those elevated numbers in the first six months of 2021. And research from Palo Alto Networks shows that Remote Desktop Protocol (RDP) has been the primary attack vector in 50% of all ransomware attacks since 2018.

The issue is that legacy remote access technologies like RDP and Citrix were born in an era of implicit trust – users are either all the way in, or all the way out. These technologies require organizations to either open up ports in their firewall to give people access or to put everything behind a VPN, with both scenarios introducing significant security risks.

> "Kaspersky reports a 767% increase in ransomware (2019-2020), while Check Point shows another 93% increase in 2021."

Securing Remote & Hybrid Work

The Zero Trust access model is not limited to on-premises resources accessed by on-premises or external hosts. Organizations must provide proper security for resources accessed by legitimate remote end-user clients. When the global pandemic began, many businesses may have shifted to remote workers using traditional remote access technologies such as VPN to access files and applications. VPN has many security concerns inherent with the classic "perimeter" network model used for decades. With a traditional VPN, it is generally assumed that remote VPN clients are trusted.

However, if malware-compromised remote clients connect to the corporate network via VPN, the malware is now directly connected to your corporate network. Other remote access solutions such as Remote Desktop Session Hosts exposed to the Internet are generally under a constant barrage of brute force login attacks from the outside. By default, RDS technologies assume all connections from external sources are allowed for connectivity purposes.

These types of traditional remote access technologies assume trust as part of their basic architecture. When organizations need Zero Trust access to business-critical applications, Virtual App Delivery (VAD) solutions like Cameyo allows businesses to provide secure access based on validated identity.

Cameyo's Zero Trust Security Model

Cameyo's Virtual App Delivery (VAD) platform is built with a native Zero Trust architecture which includes industry-first innovations like our Port Shield, Cloud Tunneling, and NoVPN technologies - all designed to proactively protect against ransomware and brute force attacks.

Port Shield

Cameyo Port Shield is the first built-in security technology of its kind that automatically closes RDP and HTTP ports to the entire world, and then dynamically opens and closes them specifically to authenticated users, building a dynamic IP white-list. Port Shield safeguards against the dramatic rise in exploit, brute force, and ransomware attacks aimed at remote & hybrid workers by reducing the attack surface, including within Cameyo's own components. Port Shield provides yet another layer of security for organizations that need to ensure their people have access to all of the business-critical apps they need to be productive while securing both remote & hybrid workers and the corporate network at the same time.

NoVPN

Cameyo NoVPN empowers organizations to give all of their remote workers secure access to internally-hosted web apps without requiring a VPN. This enables organizations to give remote workers secure access to Windows desktop and Intranet web apps from behind the corporate firewall without the cost and user-experience compromise of VPNs so that people can access business-critical applications from anywhere in the world just as productively as if they were in the office.

Cameyo NoVPN simply gives remote & hybrid workers access to a browser behind the firewall, so they can easily access their company's internally-hosted web apps via Chrome or any HTML5 browser, but with the added security of accessing those from behind the corporate firewall. NoVPN utilizes Cameyo's Self-Hosted service, which can be installed in minutes on any Windows Server 2016 or 2019 without extra components or prerequisites and without opening Firewall ports. Once installed, the IT admin simply generates a NoVPN URL from their new server's page in Cameyo's cloud portal. Remote workers can then access the company's web from this URL (or set a shortcut on their desktop), just as they would if they were within the corporate network. The result is a seamless user experience without connectivity or network performance issues which are common to VPNs.

Secure Cloud Tunneling

Cameyo's Secure Cloud Tunneling expands upon its native Zero Trust security architecture and continues Cameyo's tradition of providing the most secure access to business-critical applications on any device while reducing the attack surface for any organization with remote & hybrid workers.

Secure Cloud Tunneling provides access to on-premise applications without opening firewall ports, by turning RDP into an outbound network protocol. It bridges the gap between the competing needs of today's IT and security teams. IT teams need to move quickly to enable remote & hybrid productivity in a rapidly changing workplace, but security teams need to be more methodical to ensure heightened security for a remote & hybrid workforce that is increasingly under attack. Secure Cloud Tunneling provides the best of both worlds, giving IT teams the ability to be nimble without requiring security teams to make any compromises for remote technologies.

Layered Revert

Cameyo's Layered Revert provides users with temporary user profiles which are wiped out at the end of each session. Combined with Cameyo's Session Sync profile virtualization technology, it preserves user's data while flushing the rest of his Windows profile, preventing any threats or persistent exploits.

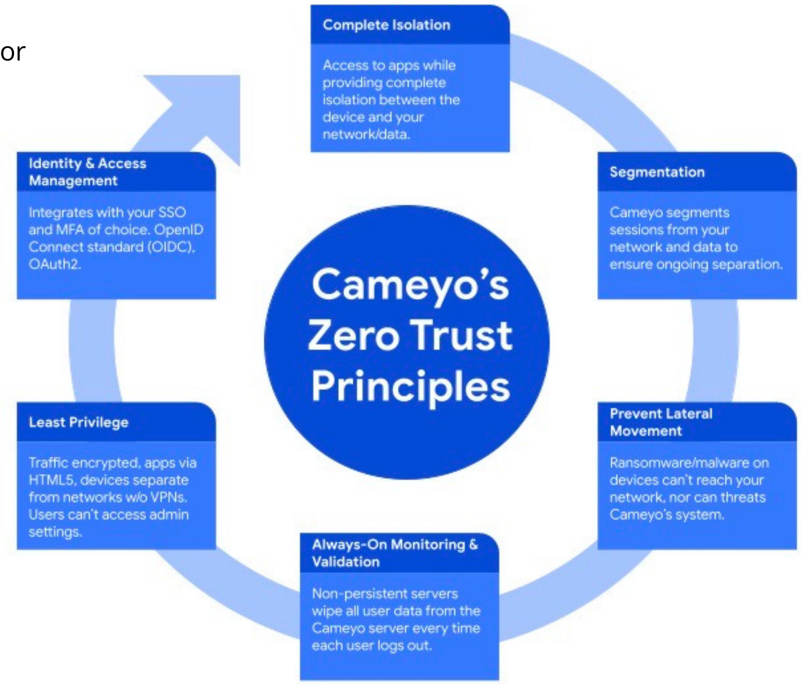
One Step Beyond

Cameyo not only shields its servers and users against compromised users and devices, it also distrusts its own components. Cameyo's engine manages sessions from the user's context with low system permissions. Nothing within the user's session can reach the server's core. Hence, even if Cameyo itself was vulnerable, it couldn't affect the server's security. As described above, at the end of each session, all traces are entirely removed as if the user never did anything on the server. Additionally, Cameyo safeguards the server against Cameyo's own components and libraries. As an example, Cameyo's HTTPS server is blocked to everyone except specific user IPs using Port Shield, and executed on a separate server through Cloud Tunneling. None of the recent malware, ransomware and vulnerabilities were relevant to Cameyo's users thanks to this multi-layered approach. To date, no Cameyo customers were infected or compromised.

Your Checklist for Zero Trust Evaluation

As you evaluate Zero Trust security solutions, below are six key criteria you can use as a checklist, followed by a description of how Cameyo's platform addresses each criteria:

- ***Device Access Control*** – Cameyo never trusts any device (even managed devices) because those devices can be compromised. Cameyo gives users secure access to the apps they need to be productive while providing complete isolation between devices and their organization's network/data.
- ***Segmentation*** – Even once users are in a session, Cameyo segments that session from other users on the same server and from customers' networks and data, ensuring ongoing separation. Device-browser separation further isolates the user's device from the remote server. With Cloud Tunneling and Port Shield, Cameyo eliminates the need of using VPNs, which are themselves a breach of the segmentation security rule.
- ***Prevention of Lateral Movement*** – Even in the case where a device has ransomware or malware, that malware cannot reach the customer organization's network/data, nor can malware on their systems reach the Cameyo system.
- ***Always-On Monitoring & Validation*** – Cameyo utilizes non-persistent servers, so all customer user data is wiped from the Cameyo server every time the user logs out.
- ***Least Privilege*** – With Cameyo all traffic is encrypted and apps are delivered from a secure HTML5 browser, separating the user's device from the corporate network and eliminating the need for VPNs. Cameyo also utilizes Windows limited user privileges, Terminal Services security, and temporary user profiles, ensuring users are unable to access admin privileges, settings, and files. Additionally, Cameyo's modules are themselves executed with the least privilege principle, safeguarding against any potential vulnerabilities within Cameyo's own components.
- ***Identity & Access Management*** – Cameyo integrates with the customer's Single Sign-On (SSO) provider of choice, and the Multi-Factor Authentication (MFA) they have set up with their SSO applies to Cameyo. HTML5 traffic is encrypted.


Complete Isolation
Access to apps while providing complete isolation between the device and your network/data.
Segmentation
Cameyo segments sessions from your network and data to ensure ongoing separation.
Prevent Lateral Movement
Ransomware/malware on devices can't reach your network, nor can threats Cameyo's system.
Always-On Monitoring & Validation
Non-persistent servers wipe all user data from the Cameyo server every time each user logs out.
Least Privilege
Traffic encrypted, apps via HTML5, devices separate from networks w/o VPNs. Users can't access admin settings.
Identity & Access Management
Integrates with your SSO and MFA of choice. OpenID Connect standard (OIDC), OAuth2.
Cameyo's Zero Trust Principles

ISO 27001 Certification

In addition to Cameyo's continued commitment to delivering the most secure access to applications from any device, the company's ISO 27001 certification also highlights the company's commitment to information security. This certification was achieved after an extensive third-party audit and evaluation of Cameyo's systems, processes, and platform confirmed that Cameyo meets the highest standards when it comes to establishing, implementing, maintaining, and improving its information security at all levels. Maintaining ISO 27001 certification requires an ongoing audit cycle that will ensure Cameyo's ISMS continues to meet the highest standards.

Conclusion

Security is one of the core pillars on which organizations build their digital assets. As threats and new threat vectors have evolved, new security best practices help ensure data is secure from modern threats. The traditional perimeter security approach is no longer effective against modern malware and other threats.

A Zero Trust model assumes there is no trust between any node, even if it exists on the trusted corporate network. Businesses must extend the Zero Trust model to secure remote employees distributed across many different geographic locations.

Let Cameyo Help

Here at Cameyo, our team has decades of experience in IT security, and our founder & CTO has 12 security patents. In addition to building the Cameyo platform with one of the industry's most robust Zero Trust architectures, our experienced team is here to help you every step of the way. Schedule a demo below to discuss with one of our experts today.

Book Your Demo