As organizations increasingly move to cloud services, have more work locations, adopt Bring-Your-Own-Device policies, and deploy Internet of Things (IoT) devices into their networks, their traditional way to protect a network perimeter must change. The castle-and-moat model of hardening network perimeters to prevent a compromise can no longer effectively provide security in a world of increasingly advanced and sophisticated threats. The Zero Trust model of security arose to address these threats. Zero Trust is a design approach to architecting an information technology environment that reduces an organization’s risk exposure in a world where it must factor user, device, transport/session, application, and data security independently and collectively.

Implementing a fully executed Zero Trust architecture is likely beyond the reach of most organizations today. However, by starting with individual capabilities that operate in complementary layers within the Zero Trust model, organizations will realize many benefits from an architecture built on conditional access control.

Most organizations will start Zero Trust with a focus on users and devices. Attivo Networks adds another layer of access control that focuses on applications, data, and access for post-authentication protection.

WHAT IS A ZERO TRUST ARCHITECTURE?

A Zero Trust architecture treats all users as potential threats and prevents access to data and resources until it can appropriately authenticate and authorize user access. A Zero Trust architecture gives users only the bare minimum access they need to perform their job. If a device gets compromised, Zero Trust contains the damage. The concept of Zero Trust has been around for more than a decade, but the technology to support it is only now moving into the mainstream. A Zero Trust architecture leans heavily on multiple components and capabilities of identity management, asset management, application authentication, network segmentation, and threat intelligence. Architecting for Zero Trust should enhance cybersecurity without sacrificing the user experience.
A practical Zero Trust implementation looks at five elements:

**Device Trust:** Organizations must identify and inventory each company-controlled device and have a solution that monitors, manages, and controls them. They can use unified endpoint management (UEM) solutions to check if mobile, desktop, and IoT devices comply with security policies and requirements, blocking those that do not. They can also rely on Endpoint Detection and Response (EDR) solutions to detect possible malicious endpoint activities.

**User Trust:** Organizations must move beyond simple password authentication schemes and use more secure user authentication methods. They can implement Identity and Access Management (IAM) solutions with adaptive access mechanisms such as password-less authentication (e.g., biometrics, certificates), multi-factor authentication (MFA), conditional-access policies, and dynamic risk scoring.

**Transport/Session Trust:** Organizations can implement the principle of least-privilege access with micro-segmentation, transport encryption, and session protection. They can limit application access to specific resources on a per-app basis, reducing the chance of a rogue application accessing data it shouldn’t.

**Application Trust:** Organizations must enable their workforce to securely and seamlessly access any application they need to do their job, including traditional Windows applications, from any device. As they modernize their user authentication mechanisms, they can allow users to use single sign-on (SSO) solutions to access applications for improved security and user experience. They can also isolate traditional applications that do not adhere to Zero Trust by using a virtual desktop or application environment to bridge the traditional architecture and the Zero Trust architecture.

**Data Trust:** Organizations must protect against data breaches, leaks, and unauthorized data modification. Data loss prevention (DLP) solutions and Cloud Access Security Brokers prevent unwanted exfiltration or destruction of sensitive data. The organization can also enhance data classification and integrity to increase trust along the chain.

Once an organization has established trust across all five pillars, they can make informed decisions to grant or deny access and continually re-verify. If the trust level changes, organizations must be able to act immediately. Besides, by establishing trust across the five pillars, they gain visibility and can gather analytics across the digital workspace environment to build automation and orchestration, increasing efficiencies without losing security.
TRADITIONAL ZERO TRUST DEPLOYMENT MODELS

Most organizations that choose to implement Zero Trust start with User Trust and Device Trust since they already have Identity Access Management (IAM) and Endpoint Detection and Response (EDR) solutions that address these two areas. Getting IAM and EDR solutions to the level of Zero Trust does not usually require entirely revamping them.

The below diagram illustrates a typical deployment model where users authenticate to a remote VPN. VPNs can validate users with Active Directory (AD) to grant and provide access to the corporate network and use SAML SSO for secure access to CDN applications.

However, while getting to this stage is an excellent start to Zero Trust, organizations must continually authenticate and apply authorizations to grant access to network resources. An attacker can still compromise user endpoints, evade detection, infiltrate a network, and access the environment. Attackers can also steal a user’s identity and perform domain reconnaissance to discover permissions associated with various users, groups, and such in Active Directory or access any system, application inside the network.

Once the user authenticates, attackers can perform network reconnaissance to detect and fingerprint services and applications running in the network, find application versions, identify Common Vulnerabilities and Exposures (CVEs) associated with the application, and exploit known and zero-day vulnerabilities. While network-based security solutions alert on reconnaissance activity, attackers can avoid detection by performing slow and stealthy reconnaissance.
IMPLEMENTING ELEMENTS OF A ZERO TRUST ARCHITECTURE WITH THE ATTIVO THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend® platform provides solutions to address shortcomings seen in Active Directory protection and network enumeration and discovery to strengthen the organization’s Zero trust model.

With Active Directory, Zero Trust is challenging to implement because every system must talk to the primary AD domain controller to access and function on the network. If attackers compromise an endpoint, they have full access to discover permissions in AD. Attackers can use various tools and methods to escalate privileges and gain domain dominance.

The following lists a few well-known Active Directory discovery activities attackers use to gain domain dominance:

1. Domain Controller Discovery
2. Local Administrator Account discovery and exploitation
3. SMB Net session enumeration to discover privileged users
4. Kerberos Silver Ticket Attack
5. Kerberoasting Attack
6. Permission Group Discovery
7. Elevate domain credentials to perform
   a. Golden Ticket Attack
   b. DC Sync Attack
   c. DC Shadow Attack

Once the attackers gain domain dominance, they can deploy malware, ransomware, and other tools across the network or steal and exfiltrate data.

The Attivo Networks ThreatDefend® platform offers additional controlled access management functions to allow applications access to data and resources once the domain authorizes them. It does so without interfering with daily operations. The ThreatDefend platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate
incident response. The platform’s components include the BOTsink deception server, the Endpoint Detection Net (EDN) Suite, and ADSecure for Active Directory protection. These components work together to deny, detect, and derail discovery, lateral movement, privilege escalation, and data gathering activities that attackers could get away with if they compromise a validated user account on an authorized device.

Consider Data Trust as it relates to validated users. Once the network has authorized a user and validated access, it allows the user to access all the data on the local system and within AD. The EDN suite can hide and deny access to local files, folders, network or cloud shares, removable storage devices, and privileged accounts unless the user accessing these objects has specific permissions to access them, not just general permissions to access all the data on the device. Additionally, the ADSecure solution can conceal and restrict access to sensitive AD objects, allowing only authorized applications to gain access and returning decoy objects to unauthorized applications. ADSecure permits domain administrators and other authorized groups to query AD actively, but not accounts operating with merely User-level permissions.

Within the realm of Application Trust, ADSecure can limit access to only trusted or validated applications for specific data forms within the user context. Not only does the user issuing the query have to be authorized, but so does the application invoking it. For example, the solution can allow the standard Windows User Manager snap-in to access user and group permissions, but not other applications like the command line or PowerShell interfaces.

Another function within the ThreatDefend platform that can implement Application Trust is the Deflect function for network reconnaissance when attackers attempt to find open ports and services. Attackers can use authorized applications to connect to open ports and services. Should an attacker attempt to probe for open ports or services to compromise, the Deflect function redirects the activity to a decoy with a corresponding port and service to engage the attacker.

The ThreatDefend platform provides these capabilities in a flexible and easily deployable manner, working with partners to integrate and automate functions for faster incident response, often with technologies that already exist on the network. In particular, research using the MITRE ATT&CK® Do-It-Yourself APT 29 and APT 3 evaluations show that the ThreatDefend platform can enhance EDR detection performance by an average of 42%. Furthermore, the ThreatDefend platform adds detections in the middle of the ATT&CK matrix, where EDR focuses on earlier tactics, and solutions like DLP focus on the latter, thus providing more effective coverage of tactics and techniques across the entire matrix.
Organizations can start by deploying the ADSecure solution on endpoints. Next, they can continue by adding the rest of the EDN suite and BOTsink servers to protect and achieve Zero Trust capabilities. Whether they decide to use a physical, virtual, or cloud-based appliance, they can deploy anywhere the enterprise network is, on-premises, in the cloud, and remote sites.

CONCLUSION

Implementing a Zero Trust architecture takes time and a careful assessment of security controls, access requirements, and processes. Because it involves rearchitecting or changing many aspects of the environment, organizations should approach Zero Trust as a multi-pronged and phased effort. When incorporating the ThreatDefend platform into a company's Zero Trust program, they will gain distinct and complementary capabilities, unlike what other identity access management controls can provide. Organizations, both large and small and with matured and maturing programs, can all realize immediate benefits from including Attivo Networks solutions into their programs. More information about the ThreatDefend platform is available at attivonetworks.com.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.