CORVUS ZTNA Implementation Considerations

Consider the following points before selecting and implementing a Zero Trust technology solution for your organization. This checklist can be used to guide conversations with potential ZTNA vendors. Learn more about ZTNA in this article.

1. Consider Architectural Elements - Does the solution easily integrate with your current IT environment?

- [ ] Determine whether Zero Trust will apply to on-premise resources, cloud resources, and applications or end users.
- [ ] Consider the kinds of credentials that will be used in the Zero Trust architecture.
- [ ] Determine the access management technologies that will be used.
- [ ] Consider common assets such as physical servers, virtual servers, cloud workloads, end—user laptops, and mobile devices.
- [ ] Determine whether agents from third—party tools are compatible with the workload types involved.

2. Evaluate the Core Pillars of Zero Trust - Has your organization defined how Zero Trust will be implemented and enforced?

- [ ] Ensure the ZTNA solution interfaces with identity stores in real time to enforce user access on predefined policies.
- [ ] Evaluate the microsegmentation needs and compatibility with your workloads.
- [ ] Evaluate decision criteria for the ZTNA solution including device location, device validation, user validation, user access, and behaviors.

3. Considerations in Tools and Services - Does the solution align with core key Zero Trust Principles?

- [ ] Is the product a complete VPN replacement?
- [ ] Does the product have cloud access broker capabilities?
- [ ] Does the product require an agent to be installed on a device?
- [ ] Does the product integrate with Endpoint Detection and Response (EDR) solutions?
- [ ] Does the product offer a microsegmentation engine (usually agent—based) to enforce limited access to users?
- [ ] Does the product include identity store integration, network and application discovery, and policy assignment?
- [ ] Does the ZTNA vendor offer support to troubleshoot issues?
- [ ] Validate ZTNA vendor security practices to ensure they are appropriately safeguarding credentials and access to your environment by following Third-Party Risk Management (TPRM) best practices.

4. Implementation of Zero Trust - How will your organization enforce strict access mechanisms at the user, device and application level?

- [ ] Define the least level of access required for users and groups.
- [ ] Define requirements over device posture that can connect to resources.
- [ ] Design the Zero Trust architecture based on how data moves across the network and how users access information.
- [ ] Group and categorize services and systems for access and authorization requirements.
- [ ] Enforce a least privileged access model once identities are challenged, confirmed, and validated (through integration with directory services).
- [ ] Assure ongoing monitoring is in place to continuously detect and track traffic in the environment.