

COMPONENT	 CRAWL	 WALK	 RUN
Identity & Access Management (IAM)	Organizations implement basic, central identity management capabilities such as: role-based access control (RBAC); strong privileged access management capabilities; and ensure that shared services such are mature.	Organizations implement fine grain identity capabilities such as: attribute-based access (ABAC) model ... Additionally, applications need to be integrated into or (through existing federation) into MFA.	Organizations have strong identity leveraging the risk components of Zero Trust...The Attribute Based Access Control (ABAC) model is used to define access policies across the enterprise...This allows for granular, yet flexible access control policies.
Network & Infrastructure	Organizations can segment and define their network infrastructure using large perimeter and employ macro-segmentation.	Organizations can segment their network infrastructure by configuring ingress and egress micro-perimeters and include some internal micro-segmentation. Granular policies can be defined at the perimeter.	Organizations have internal micro-segmentation based around all application flows and application traffic is encrypted end-to-end.
Endpoint Device & Mobility	Organizations should have central management of all end user and central devices.	Organizations can establish the identity of devices on the network, disallowing unknown devices from connecting...Technologies are put in place to perform device posture assessments when connecting to the network from any location.	Organizations allow or disallow devices to connect to enterprise resources based upon policy.... Device posture assessments are performed continuously during the lifetime of a device connected to the network.
Application Security	Organizations control access to applications using local authorization. On-premises applications are accessed through the physical network or VPN.	Centralized authentication and authorization technologies are employed to control access to applications. SSO technology is configured for the workforce to access on-premises applications.	Access to applications is authorized based on real-time risk analysis and authentication and authorization happens continuously throughout the connection...Use Breach and Attack Simulation Tools (BAS) to identify how attackers would laterally move within a network.
Data Security	Organization uses static controls for restricting access to data. Organization partially encrypts data at rest and leverages least privilege to control access to data.	Organization encrypts all data at rest and leverages least privilege to control access to data. Device risk and other attributes are also considered when making access decisions to data.	Organizations encrypt all data at rest and in-motion... Access to data is controlled using dynamic and contextual risk-based decision and only allows just-in-time and just-enough access.
Visibility & Analytics	Organizations send all logs to a centralized system.	Organizations send most of their logs to a centralized SIEM.	Organizations collect logs across all ZTA components to a central SIEM and integrate analysis across multiple sensor types to create automated alerts.
Automation & Orchestration	Organizations determine hosting location and access of the application during provisioning.	Applications inform the infrastructure and network components of a changing state.	Applications adapt to ongoing environmental changes for security and performance optimization.