appgate

ZERO TRUST MATURITY MODEL ROADMAP

WWW.APPGATE.COM

ZERO TRUST MATURITY MODEL ROADMAP

Zero Trust is a journey, not a destination. It is a mindset or a philosophy, not a technology that you can buy. The end goal of the journey is to mature your security program from implicit trust to adaptive, agile Zero Trust built on least privilege access.

The benefits are paramount … the business can innovate and grow while simultaneously improving security and lowering risk. A Zero Trust maturity model can help you identify and prioritize the indicators and fundamental drivers to achieve your Zero Trust goals. Follow the maturity tracks to understand each stage and the steps you can take to advance your security strategy.

About this guide:

The Zero Trust journey impacts five key areas described below, which align closely with definitions created by the Cybersecurity and Infrastructure Security Agency (CISA). Maturity reflects advancing from one phase to the next across the pillars.

- **Identities:** Users or entities (subjects) authenticated by an identity provider and uniquely defined by a set of attributes.
- **Devices:** Hardware that connects to a network, including internet of things (IoT) devices, mobile phones, laptops, servers and others.
- **Networks/Environments:** Any open communications medium used to transport packets, data, messages, etc., including enterprise internal networks, wireless networks, public/private cloud networks, and the Internet.
- **Applications/Workloads:** The entire application stack, whether operated in the cloud or on-premises, from the app layer through hypervisor or self-contained components of processing.
- **Data:** Information transmitted on devices, in applications and networks that must be secured, categorized, classified and encrypted at rest and in transit.
- **Overlay pillars:** There are three overlay pillars: visibility & analytics, automation & orchestration, and policy

TERMINOLOGY LEGEND:

ZT = ZERO TRUST
PDP = POLICY DECISION POINT
PEP = POLICY ENFORCEMENT POINT

ZERO TRUST MATURITY MODEL

appgate

STAGE - 0

IMPLICIT TRUST

Trust is too broad with a lack of verification. People make mistakes and attackers count on implicit trust to achieve their objectives without detection.

- Policies are static
- Access is overly broad
- Identity, security, and network tools are siloed
- Technical debt with user and business friction

STAGE - 1

BASIC ZERO TRUST

Minimal Zero Trust principles are operational. Start small, addressing a clear pain point to immediately improve security, lower risk and deliver business value.

- Policies are identity-aware
- Access is more fine-grained, but not precise
- Limited identity and security integration
- Improved user experience with less business friction

STAGE - 2

CONTEXTUAL ZERO TRUST

Access is granted based on a multi-dimensional view of identity, device and context. This lowers risk and accelerates security and operational maturity.

- Policies are identity-driven and context-aware
- Access is granular, least privilege
- Security and infrastructure are well integrated
- The business is more agile

STAGE - 3

ADAPTIVE ZERO TRUST

Security adapts to circumstance, risk, enterprise needs and processes. It represents the pinnacle of security and agility in a digitally transformed world.

- Policies are driven by business processes
- Access is dynamic and adapts to attributes and risk
- Integrated tools and systems provide a feedback loop
- Agile, digitally transformed business

IDENTITIES

ZERO TRUST MATURITY MODEL

	STAGE 0		STAGE 1		STAGE 2		STAGE 3
	IMPLICIT TRUST		**BASIC ZERO TRUST**		**CONTEXTUAL ZERO TRUST**		**ADAPTIVE ZERO TRUST**
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1:**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Identity Providers	Multiple, siloed IdPs for different user populations. Disparate and misaligned identity attributes and groups.	*Federate or retire IdPs, or establish a meta-directory. Connect ZT system to multiple IdPs and normalize attributes and groups, for consistent policies.*	IdPs are loosely connected and partially aligned. Gaps covered through manual processes or scripts. ZT system provides uniform user experience and access policies.	*Centralize on a single primary IdP and associated processes. Eliminate siloed IdPs – decommission or freeze (read-only), and disentangle them from existing tools & processes.*	Centralized IdP with one set of identity lifecycle processes. ZT policies rely on IdP attributes and groups for accurate, dynamic, and very effective access control.	*Extend IdP and ZT policy connections to the broader set of business processes and systems. Update systems with attributes meaningful to policies.*	Single, centralized IdP with automated connections to governance, lifecycle, and business processes. Any exceptions are deliberate, documented, and well-understood.
Authentication	Mostly siloed application authentication. Some limited use of Single Sign-On (SSO).	*Require SSO for new and "easy" applications. Deploy ZT with centralized authentication across multiple IdPs.*	SSO used for selected apps. ZT as a unifying authentication layer, tied into SSO system.	Expand SSO to more applications, adopting modern authentication methods (SAML, OIDC). Enable ZT system to trigger step-up authentication if user or device exhibit higher risk factors.	SSO in place for most COTS apps, and some in-house built apps.	*Enable internal app dev teams to use SSO toolkit or framework.*	Widespread SSO for home-built apps. Non-SSO apps (e.g. mainframes) accepted only when secured by ZT access, with contextual MFA enforced.
MFA	Little or no MFA in place, and used inconsistently.	*IdP enforces MFA at authentication time. Establish preferred MFA factors and sound onboarding & recovery processes.*	MFA in place for high sensitivity apps and users. MFA enforced at authentication time only. Multiple MFA factors supported for user choice & better sec	*Deploy ZT PEPs logically or physically inline of traffic flow, with access to identity and workload context.*	MFA triggered at access time, based on policy, workload/user sensitivity, and context.	*Enable ZT system with enhanced set of user, device, workload, and system attributes. Extend ZT policy model to include these attributes.*	MFA triggered during session by system events, user and device context, as well as workload and system attributes, drawn from multiple sources.

appgate

DEVICES

ZERO TRUST MATURITY MODEL

	STAGE 0		STAGE 1		STAGE 2		STAGE 3
	IMPLICIT TRUST		**BASIC ZERO TRUST**		**CONTEXTUAL ZERO TRUST**		**ADAPTIVE ZERO TRUST**
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1:**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Classification and Compliance	Limited visibility into device compliance. Little posture checking, control, and management.	*Implement basic compliance for managed devices like OS version, AV/EDR installed, local firewall enabled, device patched for any access.*	Devices controlled via one-time, indirect methods, such as limited local permissions, remote management and company issuance.	*Implement contextual evaluation on all devices for access (especially to critical resources) like geo location, time of day, network source. Validate against compliance requirements.*	Devices validated at time of access based on security and compliance posture and network attributes. Log compliance status and changes.	*Factor all available information about a device and source network at time of connection, as well as throughout the life of the connection for continuous trust evaluation.*	Access based on detailed device config and compliance posture as well as external information about the source network, device risk, and threat level. Process and data integration between ZT and compliance systems.
Workload & Data Access	Access to workload/data does not depend on visibility into the device that is being used to access the data.	*Deploy simple pre-access checks for high risk, privileged, and sensitive workload/data access such as: OS version checks, firewall on/off, etc.*	Access to workload/data considers basic device posture at time of first access.	*Include device attributes such as geo-location, time of day, patch levels, AV/EDR presence, process hash checks, network type/location, impossible travel, etc.*	Access to workload/data considers continuous deep device posture compliance and context before access	*Build triggered device risk events from UEBA, EDR, NAV, vulnerability mgmt. system, etc.*	Access to workload/data considers real-time risk analytics about devices, users, and networks. Request-to-connect and approval workflows as needed.

appgate

NETWORKS AND ENVIRONMENTS

ZERO TRUST MATURITY MODEL

	STAGE 0 IMPLICIT TRUST		STAGE 1 BASIC ZERO TRUST		STAGE 2 CONTEXTUAL ZERO TRUST		STAGE 3 ADAPTIVE ZERO TRUST
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Data Center networks	Too-open networks, very little control, monitoring or management capabilities. Complex firewall rulesets.	*Deploy basic ZT policies for highest-risk users or most-sensitive resources.*	Server or service-specific access rules, based on hostname or IP address and port.	*Enhance policies to use server metadata or CMDB to control access. Enable dynamic detection of changes*	Access between servers and applications now follows least privilege approach, with small pockets of implicit trust.	*Use ZT mechanism to dynamically evaluate both inbound access, as well as intra-service access within and between network segments.*	Minimal pockets of implicit trust between server components. All inbound and intra-service access based on attributes from workloads and enterprise systems. All new services deployed accessed only via ZT policies.
Cloud Networks	Default settings for networks, wide open rules, and some connections to enterprise LANs. Some cloud services exposed to internet.	*Eliminate WAN connections between enterprise and cloud network. Deploy PEPs at cloud network entry points. Remove internet-exposed services.*	Individual server/service-based inbound rules, with nothing exposed unnecessarily.	*Isolate groups of workloads from one another via basic network segmentation through dedicated and separate VPCs. Configure security group to only permit inbound access via ZT PEP.*	Access to all cloud resources is controlled by ZT policies, which use workload metadata to determine access. Implicit trust between servers and applications is now limited to tightly coupled elements.	*Dynamically evaluate both inbound access and intra-service access within and between network segments, leveraging metadata, external rule repositories and real-time risk and posture evaluation.*	All inbound and intra-service access based on dynamic and contextual policy.
Enterprise Office (User) Network	Flat, open networks, with internet access and too-broad access to network services. Large attack surface. Coarse-grained network ACLs, if any.	*Deploy ZT with basic device posture checks. Hide the most sensitive assets from unauthorized users. Begin replacement of VPN, with unified remote and on-prem access for some users and some workloads.*	Visitor traffic segregated from users. Reduced VPN user population. Some users have ZT access for both remote and on-prem.	*Individual server/service-based inbound rules. Continue migrating remote VPN users and reduce NAC reliance for on-prem users with ZT access.*	Majority of people use ZT access for both on-prem and remote users. Shrinking minority still on VPN.	*Combine user and device identity with built-in and external posture checking for complete picture of trustworthiness, for all network connected devices.*	Café-style network: internal network treated as if users were connecting from a coffee shop, with zero implicit trust or privilege. All VPNs decommissioned, and reduced or eliminated NAC.
Third Party Access	VPN access with too-broad network permissions, putting organization at risk. Wide open, risky site-to-site connections in place. Many undocumented access rules.	*Shift highest-risk third-party users to ZT access. Begin to simplify in-place ruleset and require MFA.*	Users on ZT access with MFA. Limit network access controls to reduce attack surface while retaining productivity.	*Terminate use of VPN for third-party access. Leverage vendor/partner's identity provider for authentication. Agree on device posture checks.*	Integration of third party's enterprise identity provider. Fine-grained access policies. Device posture checks enforced. Enable clientless ZT access for some scenarios.	*Terminate long-lived site-to-site connections, replacing with ZT connections. Enable business teams to more easily cooperate.*	Reliable and robust third-party access enables business innovation, including server-to-server integrations.
Internet Access	No outbound filtering, insight or monitoring.	*Deploy DNS traffic capture and filtering for on-prem users. Deploy SWG and CASB for web and SaaS filtering and visibility.*	Outbound DNS capture and filtering based on static categories. Traffic metadata monitoring with manual analysis and response. Basic web filtering and SaaS controls.	*Capture and filter DNS traffic for remote and on-prem users. Tie web and SaaS access to role, and enforce source IP constraints.*	Web access filtered based on site category, plus identity and role. Web filtering and SaaS access enforced on devices	*Enable ZT system to consume DNS, threat intel, and traffic analysis as input into dynamic risk score.*	Fine-grained outbound access control based on source of request, real-time feeds, threat analysis, frequency of visit. Web access dynamically feeds back into user and device risk score.

appgate

APPLICATIONS / WORKLOADS

ZERO TRUST MATURITY MODEL

	STAGE 0		STAGE 1		STAGE 2		STAGE 3
	IMPLICIT TRUST		**BASIC ZERO TRUST**		**CONTEXTUAL ZERO TRUST**		**ADAPTIVE ZERO TRUST**
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1:**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Application / Workload Identification	Static workload identification by hostname and IP address.	*Deploy tools to detect app access, and roll into ZT policies. Create processes for new application deployment, tying into ZT system and policies.*	Tools identify already-deployed applications. Manual or semi-automated workflows for newly deployed applications. Some integration with CMDB and cloud APIs.	*Application deployment tools and processes use scripts or create ZT metadata, for automated detection of workloads across environments.*	New workloads detected automatically via scripts or metadata. Alignment of ZT policies and CMDB data and processes.	*New application tools and processes automatically apply metadata and API calls to make visible to ZT system.*	Workload lifecycle tightly integrated into ZT system via APIs.
Application Authentication	Local application authentication. Few or no identity attributes.	*Externalize application authentication to enterprise identity provider.*	App users use centralized authentication, and some identity attributes.	*Configure or deploy toolkits for application SSO, including MFA*	SSO and static MFA. Access uses dynamic contextual attributes for the identity/device.	*ZT system aware of application sensitivity and identity context.*	Dynamically applied MFA. Continuous, contextual reauthentication based on app activity and user risk.
Application Access and Authorization	Some apps are directly exposed to the internet, some accessible to all internal users or via VPN.	*Deploy ZT access which hides applications from internet, and from unauthorized users.*	Sensitive apps are protected by a ZT PEP. Most apps still permit overly broad access by any user on the network.	*Require ZT access control for all new applications, and incrementally onboard existing applications based on sensitivity or value.*	All apps are only accessible by authorized users via a ZT PEP.	*Tie access policies to business processes, enable application access to ZT context.*	Some apps perform just-in-time role provisioning, or access driven by workflows. ZT context is consumed by most applications.

appgate

DATA

ZERO TRUST MATURITY MODEL

	STAGE 0		STAGE 1		STAGE 2		STAGE 3
	IMPLICIT TRUST		**BASIC ZERO TRUST**		**CONTEXTUAL ZERO TRUST**		**ADAPTIVE ZERO TRUST**
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1:**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Encryption and Obfuscation	At rest: Data largely unencrypted. In motion: Some unencrypted network protocols. No data obfuscation.	*Implement disk encryption on servers and cloud resources, enforce full-disk encryption via device posture checks. All network traffic routed via encrypted tunnels. Deploy tokenization for highest-risk data.*	At rest: Full disk encryption. In motion: Mostly encrypted network protocols. Some global tokenization or masking.	*Applications encrypt most sensitive data fields. Dynamic data tokenization or masking based on user roles & attributes.*	At rest: Some application data encrypted. In motion: Data fields encrypted in addition to network. Role or attribute based tokenization or masking.	*Deploy application data encryption more broadly. DLP uses ZT context to dynamically control access and data tokenization or masking.*	Data encryption in use by most applications. Dynamic and contextual tokenization or masking.
Inventory & Classification	Little or no inventory or tagging.	*Deploy manual, tool-augmented data classification systems across highest-value repositories and people.*	Manual and inconsistent tagging. Coarse-grained data inventory (directory, app, or database level).	*Deploy enhanced tools or plugins which enforce tagging, with some automated classification abilities.*	Regular and enforced manual tagging, augmented with some automated/ML tagging.Medium-grained tagging (file, column).	*Deploy tools for automated data analysis and tagging, with ML. Build classification into processes and app development systems.*	Robust, reliable, and enforced tagging, continuous automated analysis and tagging via ML. Fine-grained tagging (row or item level).
Access Control	All-or-nothing access to data, at file or database level. Enforcement via application roles.	*Deploy ZT PEP to control access at URL or application level.*	ZT PEP examines data tags, controls access to entire URL, application, file system, or database.	*Enhance ZT system and policies to apply to finer-grained data elements. Enable application to consume ZT context for accessing identity.*	ZT PEP controls access to documents and database elements. Application has some awareness of ZT context.	*Configure access policies to include user and device risk, mapped to data sensitivity. Enable app and DLP to consume ZT context.*	Risk-based dynamic controls (authentication, segregation of duties, process controls). Detect and respond to attempts to access blocked data. Just-in-time app role provisioning. DLP awareness of ZT Context.

appgate

OVERLAY PILLARS

ZERO TRUST MATURITY MODEL

	STAGE 0		STAGE 1		STAGE 2		STAGE 3
	IMPLICIT TRUST		**BASIC ZERO TRUST**		**CONTEXTUAL ZERO TRUST**		**ADAPTIVE ZERO TRUST**
Maturity Track	**Stage 0:**	*Transition to Stage 1*	**Stage 1:**	*Transition to Stage 2*	**Stage 2:**	*Transition to Stage 3*	**Stage 3:**
Policy and Process	Siloed on-prem and remote access policies. Network access policies disconnected from identity.	*Deploy ZT system for both remote and on-prem access, for an initial set of users.* *Define policies with basic, static identity attributes.*	Unified on-prem and remote access for some users and some resources. Identity-aware access policies.	*Roll out ZT system to additional groups of users, onboarding most systems and applications. Extend policies to control server-to-server access. Enhance access policies to use contextual and dynamic identity attributes, and resource metadata.*	Unified on-prem and remote access for most users and most resources. Dynamic and contextual access policies, based on attributes and metadata.	*Enforce ZT access policies for all new users and apps, via onboarding processes and tools. Connect access policies to business processes (e.g. ITSM, HR). Automate policies via DevOps and CI/CD, and apply policies to IoT/OT Devices and Containers.*	ZT network access everywhere - unified on-prem and remote access for all users and all resources. Access driven by business processes and policies "as code".
Visibility & Analytics	Manual and incomplete system and device inventory. Limited identity context in logs.	*Deploy CMDB and integration or federation tools. Connect ZT system logs into enterprise SIEM.*	Mostly reliable system and device inventory. Identity-enriched logs for some users.	*Apply tools and processes to eliminate CMDB gaps. Enforce accuracy via default-deny policies.* *Broaden ZT logs to cover most users, connect to NOC and SOC systems.*	Highly reliable and automated CMDB and SIEM logs. Enriched logs enable non-repudiation, quicker detection and response to anomalous activity.	*CMDB attributes and device posture checks enforced by access policies. Deploy advanced analysis tools, systems, and visualizations for SOC and NOC.*	Integrated access control with device and vulnerability mgmt. Advanced analysis and ML for proactive, highly-effective, and responsive security operations on risk, incidents or aberrations.
Automation & Orchestration	Manual integration of security events and data across silos. Misaligned and incomplete data result in lack of integrity and poor effectiveness.	*Begin automating integrations via tools and scripting.* *Break down barriers between IT, security operations, network, monitoring, and lifecycle systems.*	Begin automation of some integration flows. Better alignment and elimination of process and integration silos, improved security effectiveness.	*Deploy a centralized orchestration system, and begin replacing manual or scripted steps across the environment.* *Deploy and follow standardized compliance guidelines, processes, and measurements.*	Orchestrated flows across most security and IT components. Well-aligned security, IT, and compliance processes.	*Orchestration required for all new IT and security components, improving system reliability, visibility, and velocity.* *Standardize on metrics and measurements*	Bi-directional integration and orchestration framework used by broader IT and security ecosystem, including cloud-based providers. Metrics available to optimize and improve processes and outcomes.

appgate

Appgate SDP is REAL
Zero Trust Access

Purpose-built on Zero Trust principles, Appgate SDP strengthens and simplifies access controls for global organizations and agencies. Its agile software-defined perimeter architecture delivers the industry's most comprehensive Zero Trust Network Access solution. Learn more at **appgate.com/ztna.**

appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at **appgate.com.**

ZERO TRUST MATURITY MODEL ROADMAP