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

© 2022 Appgate
ZERO TRUST MATURITY MODEL

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
# Zero Trust Maturity Model

## Maturity Track

| Stage 0: Multiple, siloed IdPs for different user populations. Disparate and misaligned identity attributes and groups. |
| Stage 1: IdPs are loosely connected and partially aligned. Gaps covered through manual processes or scripts. ZT system provides uniform user experience and access policies. |
| Stage 2: 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. |
| Stage 3: Single, centralized IdP with automated connections to governance, lifecycle, and business processes. Any exceptions are deliberate, documented, and well-understood. |

## Transition to Stage 1
- Federate or retire IdPs, or establish a meta-directory.
- Connect ZT system to multiple IdPs and normalize attributes and groups, for consistent policies.
- Require SSO for new and “easy” applications. Deploy ZT with centralized authentication across multiple IdPs.
- Centralize on a single primary IdP and associated processes. Eliminate siloed IdPs’ de-commission 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.
- Single, centralized IdP with automated connections to governance, lifecycle, and business processes. Any exceptions are deliberate, documented, and well-understood.

## Transition to Stage 2
- 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.
- Enable internal app dev teams to use SSO toolkit or framework.
- Enable ZT system with enhanced set of user, device, workload, and system attributes. Extend ZT policy model to include these attributes.

## Transition to Stage 3
- 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.
- Extend ZT policy model to include these attributes.

## Identity Providers
- Mostly siloed application authentication. Some limited use of Single Sign-On (SSO).
- SSO used for selected apps. ZT as a unifying authentication layer, tied into SSO system.
- SSO in place for most COTS apps, and some in-house built apps.
- Widespread SSO for home-built apps. Non-SSO apps (e.g., mainframes) accepted only when secured by ZT access, with contextual MFA enforced.

## Transition to Stage 2
- 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
- MFA triggered at access time, based on policy, workload/user sensitivity, and context.

## Transition to Stage 3
- Little or no MFA in place, and used inconsistently.
- IdP enforces MFA at authentication time. Establish preferred MFA factors and sound onboarding & recovery processes.
- Deploy ZT PEPs logically or physically inline of traffic flow, with access to identity and workload context.
- Enable ZT system with enhanced set of user, device, workload, and system attributes. Extend ZT policy model to include these attributes.

## MFA

* © 2022 Appgate*
### Stage 0: Limited Visibility

- **Classification and Compliance**: Limited visibility into device compliance. Little posture checking, control, and management.
- **Workload & Data Access**: Access to workload/data does not depend on visibility into the device that is being used to access the data.

### Stage 1: Basic Zero Trust

- **Transition to Stage 1**: Implement basic compliance for managed devices like OS version, AV/EDR installed, local firewall enabled, device patched for any access.
- **Stage 1**: Devices controlled via one-time, indirect methods, such as limited local permissions, remote management and company issuance.

### Stage 2: Contextual Zero Trust

- **Transition to Stage 2**: Implement contextual evaluation on all devices for access (especially to critical resources) like geo location, time of day, network source. Validate against compliance requirements.
- **Stage 2**: Devices validated at time of access based on security and compliance posture and network attributes. Log compliance status and changes.

### Stage 3: Adaptive Zero Trust

- **Transition to Stage 3**: Implement contextual evaluation on all devices for access (especially to critical resources) like geo location, time of day, network source. Validate against compliance requirements.
- **Stage 3**: 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.

---

**DEVICES**

**ZERO TRUST MATURITY MODEL**

**Maturity Track**

<table>
<thead>
<tr>
<th>Stage 0:</th>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implicit Trust</strong></td>
<td><strong>Basic Zero Trust</strong></td>
<td><strong>Contextual Zero Trust</strong></td>
<td><strong>Adaptive Zero Trust</strong></td>
</tr>
<tr>
<td>Transition to Stage 1</td>
<td>Transition to Stage 2</td>
<td>Transition to Stage 3</td>
<td></td>
</tr>
</tbody>
</table>

**Classification and Compliance**

- Stage 0: Limited visibility into device compliance. Little posture checking, control, and management.
- Stage 1: Devices controlled via one-time, indirect methods, such as limited local permissions, remote management and company issuance.
- Stage 2: Devices validated at time of access based on security and compliance posture and network attributes. Log compliance status and changes.
- Stage 3: 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**

- Stage 0: Access to workload/data does not depend on visibility into the device that is being used to access the data.
- Stage 1: Access to workload/data considers basic device posture at time of first access.
- Stage 2: Access to workload/data considers continuous deep device posture compliance and context before access.
- Stage 3: Access to workload/data considers real-time risk analytics about devices, users, and networks. Request-to-connect and approval workflows as needed.
<table>
<thead>
<tr>
<th>Maturity Track</th>
<th>IMPPLICIT TRUST</th>
<th>BASIC ZERO TRUST</th>
<th>CONTEXTUAL ZERO TRUST</th>
<th>ADAPTIVE ZERO TRUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center networks</td>
<td>Too-open networks, very little control, monitoring or management capabilities. Complex firewall rulesets.</td>
<td>Deploy basic ZT policies for highest-risk users or most-sensitive resources.</td>
<td>Enhance policies to use server metadata or CMBD to control access. Enable dynamic detection of changes.</td>
<td>Use ZT mechanism to dynamically evaluate both inbound access and extra-service access within and between network segments.</td>
</tr>
<tr>
<td>Cloud Networks</td>
<td>Default settings for networks, wide-open rules, and some connections to enterprise LANs. Some cloud services exposed to internet.</td>
<td>Eliminate WAN connections between enterprise and cloud network. Deploy PEPs at cloud network entry points. Remove internet-exposed services.</td>
<td>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.</td>
<td>Dynamically evaluate both inbound access and extra-service access within and between network segments, leveraging metadata, external rule repositories and real-time risk and posture evaluation.</td>
</tr>
<tr>
<td>Enterprise Office (User) Network</td>
<td>Flat, open networks, with internet access and too-broad access to network services. Large attack surface. Course-grained network ACLs. Tiny.</td>
<td>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.</td>
<td>Visitor traffic segregated from users. Reduced VPN user population. Some users have ZT access for both remote and on-prem.</td>
<td>Combine user and device identity with built-in and external posture checking for complete picture of trustworthiness, for all network connected devices.</td>
</tr>
<tr>
<td>Third Party Access</td>
<td>VPN access with too-broad network permissions, putting organization at risk. Wide-open, risky site-to-site connections in place. Many undocumented access rules.</td>
<td>Shift higher-risk third-party users to ZT access. Begin to simplify in place ruleset and require MFA.</td>
<td>Users on ZT access with MFA. Limit network access controls to reduce attack surface while retaining productivity.</td>
<td>Terminate long lived site-to-site connections, replacing with ZT connections. Enable business teams to more easily cooperate.</td>
</tr>
</tbody>
</table>

**Stage 0: Implicit Trust**

- **Transition to Stage 1**: Deploy basic ZT policies for highest-risk users or most-sensitive resources.

**Stage 1: Basic Zero Trust**

- **Stage 1**: Server or service-specific access rules, based on hostname or IP address and port.

**Stage 2: Contextual Zero Trust**

- **Stage 2**: Access between servers and applications now follows least privilege approach, with small pockets of implicit trust.

**Stage 3: Adaptive Zero Trust**

- **Stage 3**: 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 access only via ZT policies.
<table>
<thead>
<tr>
<th>Maturity Track</th>
<th>Stage 0: Implicit Trust</th>
<th>Stage 1: Basic Zero Trust</th>
<th>Stage 2: Contextual Zero Trust</th>
<th>Stage 3: Adaptive Zero Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application / Workload Identification</td>
<td>Static workload identification by hostname and IP address.</td>
<td>Deploy tools to detect app access, and roll into ZT policies. Create processes for new application deployment, tying into ZT system and policies.</td>
<td>Application deployment tools and processes use scripts or create ZT metadata, for automated detection of workloads across environments.</td>
<td>New workloads detected automatically via scripts or metadata. Alignment of ZT policies and CMDB data and processes.</td>
</tr>
<tr>
<td>Application Authentication</td>
<td>Local application authentication. Few or no identity attributes.</td>
<td>Externalize application authentication to enterprise identity provider. App users use centralized authentication, and some identity attributes.</td>
<td>Configure or deploy toolkits for application SSO, including MFA. SSO and static MFA. Access uses dynamic contextual attributes for the identity/device.</td>
<td>ZT system aware of application sensitivity and identity context. Dynamic applied MFA. Continuous, contextual reauthentication based on app activity and user risk.</td>
</tr>
<tr>
<td>Application Access and Authorization</td>
<td>Some apps are directly exposed to the internet, some accessible to all internal users or via VPN.</td>
<td>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.</td>
<td>Require ZT access control for all new applications, and incrementally onboard existing applications based on sensitivity or value.</td>
<td>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.</td>
</tr>
<tr>
<td>Maturity Track</td>
<td>Stage 0: IMPLICIT TRUST</td>
<td>Stage 1: BASIC ZERO TRUST</td>
<td>Stage 2: CONTEXTUAL ZERO TRUST</td>
<td>Stage 3: ADAPTIVE ZERO TRUST</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Encryption and Obfuscation</strong></td>
<td>At rest: Data largely unencrypted. In motion: Some unencrypted network protocols. No data obfuscation.</td>
<td>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.</td>
<td>Applications encrypt most sensitive data fields. Dynamic data tokenization or masking based on user roles &amp; attributes.</td>
<td>Deploy application data encryption more broadly. DUP uses ZT context to dynamically control access and data tokenization or masking.</td>
</tr>
<tr>
<td><strong>Inventory &amp; Classification</strong></td>
<td>Little or no inventory or tagging.</td>
<td>Deploy manual, tool-augmented data classification systems across highest-value repositories and people.</td>
<td>Deploy enhanced tools or plugins which enforce tagging, with some automated classification abilities.</td>
<td>Deploy tools for automated data analysis and tagging, with ML. Build classification into processes and app development systems.</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>All-or-nothing access to data, at file or database level. Enforcement via application roles.</td>
<td>Deploy ZT PEP to control access at URL or application level.</td>
<td>ZT PEP examines data tags, controls access to entire URL, application, file system, or database.</td>
<td>Configure access policies to include user and device risk, mapped to data sensitivity. Enable app and DUP to consume ZT context.</td>
</tr>
</tbody>
</table>

**DATA ZERO TRUST MATURITY MODEL**
<table>
<thead>
<tr>
<th>Maturity Track</th>
<th>Stage 0:</th>
<th>Stage 1:</th>
<th>Stage 2:</th>
<th>Stage 3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and Process</td>
<td>Siloed on-prem and remote access policies. Network access policies disconnected from identity.</td>
<td>Deploy ZT system for both remote and on-prem access, for an initial set of users. Define policies with basic, static identity attributes.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**OVERLAY PILLARS**

**IMPLICIT TRUST**
- Siloed on-prem and remote access policies.
- Network access policies disconnected from identity.

**BASIC ZERO TRUST**
- Deploy ZT system for both remote and on-prem access, for an initial set of users.
- Define policies with basic, static identity attributes.

**CONTEXTUAL ZERO TRUST**
- 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.

**ADAPTIVE ZERO TRUST**
- 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.

---

**Maturity Track Stage 0:** Transition to Stage 1

**Stage 0:**
- Siloed on-prem and remote access policies.
- Network access policies disconnected from identity.

**Stage 1:**
- Deploy ZT system for both remote and on-prem access, for an initial set of users.
- Define policies with basic, static identity attributes.

**Stage 2:**
- 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.

**Stage 3:**
- 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.

---

© 2022 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](http://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](http://appgate.com).

**ZERO TRUST MATURITY MODEL**

© 2022 Appgate