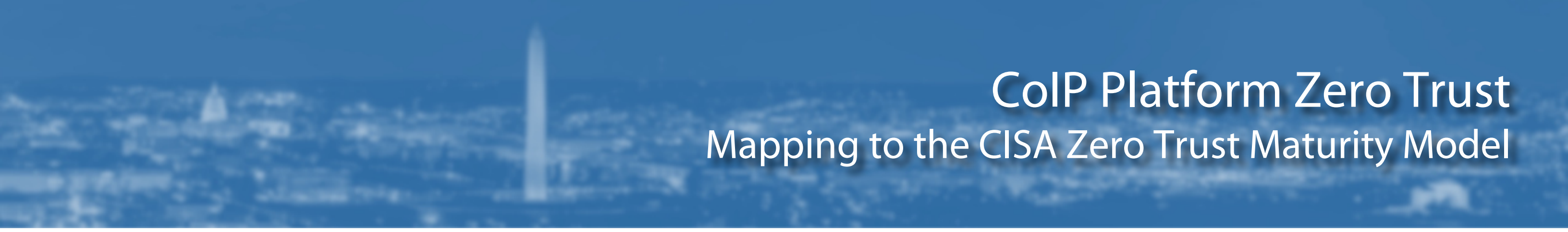
CoIP® Platform Zero Trust

Mapping to the CISA Zero Trust Maturity Model

zentera™



CoIP Platform Zero Trust

Mapping to the CISA Zero Trust Maturity Model

About CoIP Platform

Zentera's CoIP Platform provides a comprehensive suite of tools to help organizations rapidly transition to a Zero Trust security model. Onboarding a resource to CoIP Platform allows an administrator to define and enforce security controls limiting access to the resource to authenticated and authorized users, devices, and applications. It monitors network activity to expose implicit trust relationships and provides the necessary tools to convert them to explicit policies for security enforcement.

CoIP Platform is uniquely positioned as a security overlay to the existing networks. This allows resources to be onboarded and brought into a Zero Trust posture without modifying the resource's network infrastructure. The overlay approach enables Zero Trust controls to be quickly deployed to secure resources in bare metal, hyperconverged infrastructure, cloud, and even OT environments.

About this Document

This document helps map the security controls and capabilities of CoIP Platform version 8.1 to the CISA Zero Trust Maturity Model version 1.0 (June 2021).

Please note that at the time of writing, the Zero Trust Maturity Model is a Pre-decisional Draft; as the model continues to evolve this document will be updated to reflect the latest version.

Related Documents

For more information on CoIP Platform's architecture, please refer to *CoIP Platform Zero Trust Architecture – Implementing NIST SP 800-207 with a Zero Trust Overlay*

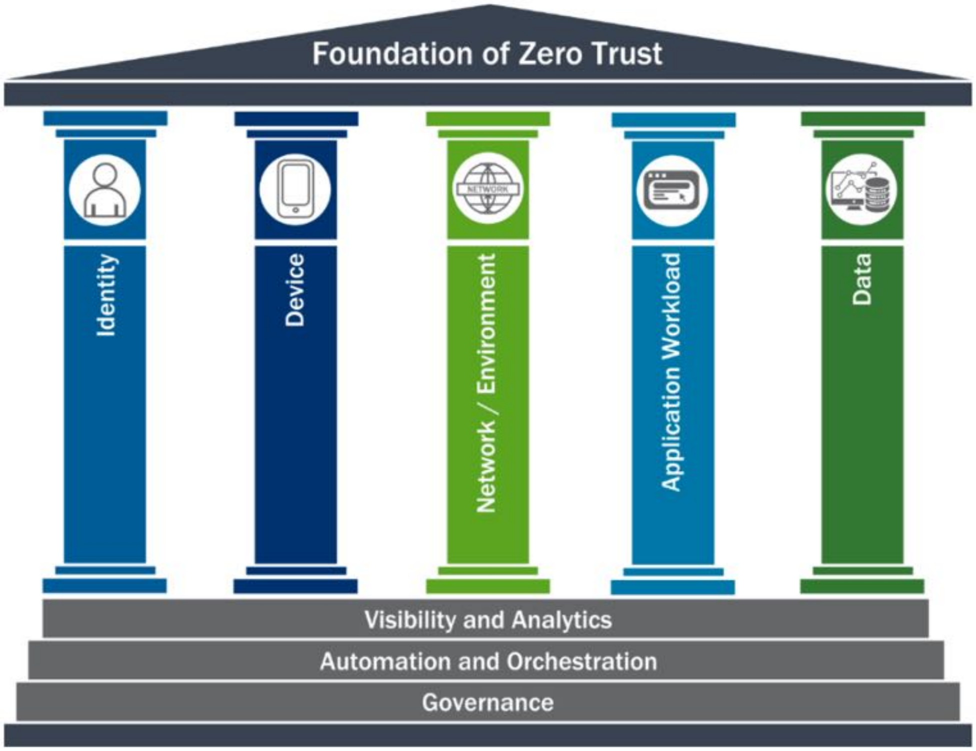
Other detailed technical and operational documentation can be found on our support site, support.zentera.net (registration required).

The CISA Zero Trust Maturity Model

In the wake of Executive Order 14028, various agencies have published guidance to help agencies accurately communicate the concept of Zero Trust: what it is, what the goals are, and how to achieve it. For its part, the Department of Homeland Security through CISA was directed to develop guiding security principles for Zero Trust adoption. The Zero Trust Maturity Model is the result of this effort.

The Zero Trust Maturity Model provides guidance for each of five distinct pillars – Identity, Device, Network, Application, and Data. Each pillar is intended to stand alone, so an agency can decouple efforts to modernize one pillar from another. In practice, however, it is important to consider the overall direction of modernization to ensure that improvements made to one pillar can interoperate with each other to properly support the Zero Trust initiative.

The pillar concept, along with several foundational pieces (Visibility and Analytics, Automation and Orchestration, and Governance) are depicted in the graphic below.



Source: CISA Zero Trust Maturity Model (Pre-decisional Draft), v1.0, June 2021

About CoIP Platform

CoIP Platform is a patented Zero Trust security solution which overlays existing networks. This enables existing applications to be ”retrofitted” for Zero Trust, avoiding intensive infrastructure re-engineering, which can impact application performance and usability.

CoIP Platform does not require adoption of a 3rd party SaaS, and is available for on-premises and air-gapped deployments.

Zero Trust Implementation Challenges Solved by CoIP Platform

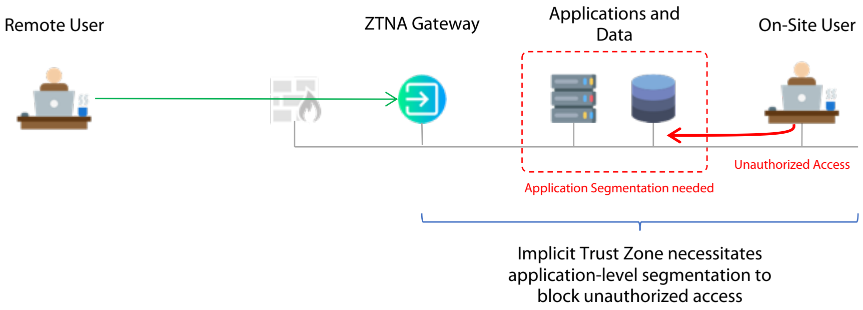
If there’s one thing made clear by the Zero Trust Maturity Model, its that the desired protection scope is *comprehensive*, and many of the considerations are inter-related. This can make it difficult and costly to achieve optimal levels of security using traditional application, network, and security practices.

For example, OMB M-22-09 mandates that “Federal applications cannot rely on network perimeter protections to guard against unauthorized access. Users should log into applications, rather than networks…” The statement is simple, but using traditional tools, implementing the intent can trigger a cascade of potential changes:

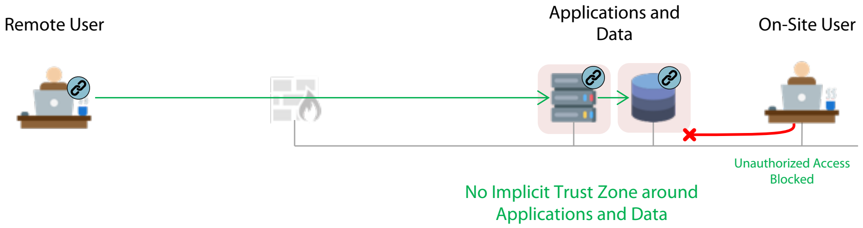
- Rearchitecting or redeploying the application to ensure it uses the enterprise-managed identity and MFA
- Upgrading network switches and routers to support network segmentation of this application server (SDN, etc).
- Migrating the application server and data dependencies to this new network segment
- Implementing privileged access management controls to ensure that only authorized users can log in
- Complex network configuration to ensure that ITSM and SIEM tools can continue to access each segmented application server
- Mitigating the impact of these changes on other applications in the same datacenter pending Zero Trust implementation

Implementing these changes requires significant time and effort for system architecture, build, and integration. Agencies using traditional methods may find it difficult to achieve compliance by EO 14028’s FY 2024/E deadline.

Also, note that simply implementing a ZTNA gateway for end-user and IT administrator access does *not* reduce the complexity and scale of the problem. The application must still be segmented to prevent unauthorized access at the network level. Typical ZTNA gateways drop traffic from authenticated users onto the LAN, potentially mixing authenticated traffic with unauthenticated traffic. Care must be exercised not to allow this to create a new implicit trust zone.


Remote User
ZTNA Gateway
Applications and Data
On-Site User
Unauthorized Access
Application Segmentation needed
Implicit Trust Zone necessitates application-level segmentation to block unauthorized access

Zentera's CoIP Platform is different. Deploying as a Zero Trust overlay fabric, security enforcement points are distributed to application servers, OT, and IoT devices. Agencies can continue to use their existing network and application infrastructure, but simply add a layer of software-defined segmentation to eliminate implicit trust zones and attribute-based access control to restrict access to authenticated and authorized users and servers.

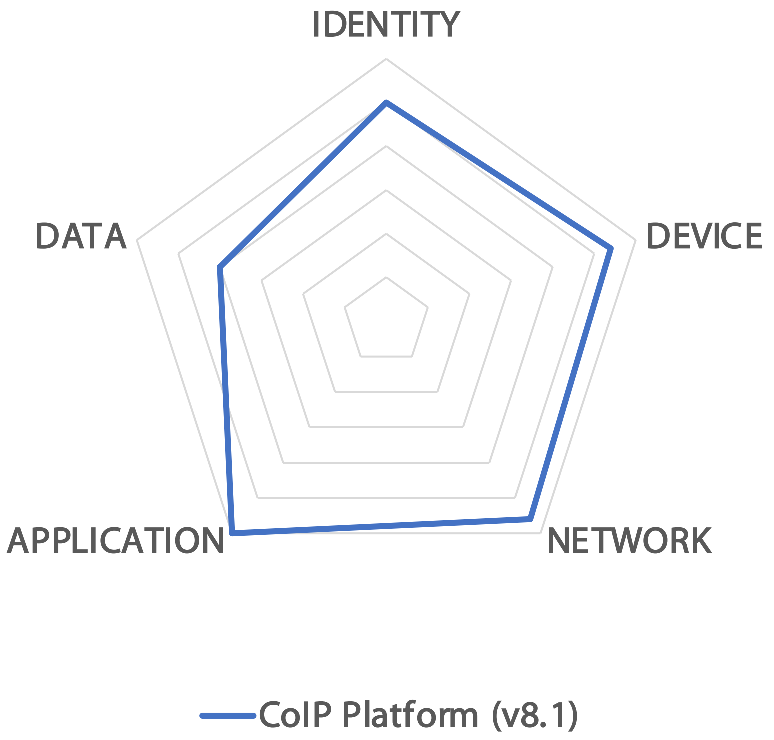

Remote User
Applications and Data
On-Site User
Unauthorized Access Blocked
No Implicit Trust Zone around Applications and Data

The overlay approach to Zero Trust avoids painful rip-and-replace, saving agencies a significant amount of time and effort and reducing the risk to implement Zero Trust controls on schedule and on budget.

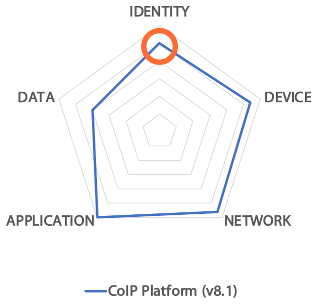
CoIP Platform Mapping to the Zero Trust Maturity Model

The mapping between CoIP Platform and the CISA Zero Trust Maturity Model is demonstrated below and explained in the subsequent sections. Note that full achievement of these maturity levels may be dependent on the maturity of agency operational processes.

As illustrated in the diagram, Zero Trust protections can be added to allow existing applications to approach a full CISA "Optimal" state with no or minimal deployment changes.



Identity

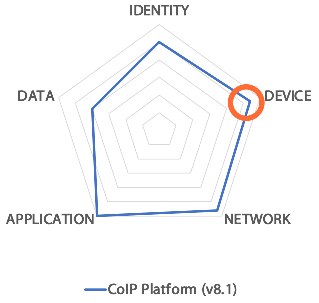


CoIP Platform fully leverages the agency's existing Identity Providers through SAML 2.0, OpenID Connect, OAuth 2.0, and LDAP connectors. This enables existing identity information to inform access policy decisions, and allows for multi-factor authentication, including PIV cards or other hardware tokens as needed.

CoIP Platform contributes toward achieving an Optimal maturity level by validating identity for each new network session, and then continuously validating identity for the duration of the session. Sessions with revoked credentials or changed access levels will be terminated.

CoIP Platform gathers identity and session analytics, which can be provided to 3rd party analytics/UEBA for ML-based automation. CoIP Platform provides the necessary API hooks for external tooling to automatically trigger policy changes, terminate sessions, and even quarantine endpoints as may be necessary.

Device

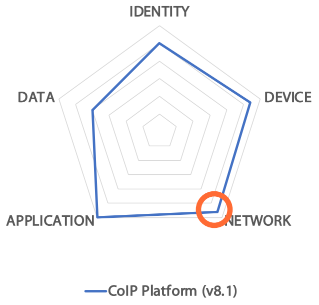


CoIP Platform gathers information about the client devices involved in a network transaction to validate the device against agency use policies. Device data includes unique hardware and software identifiers, network interface information, geolocation, and cryptographic identity, which are sufficient to uniquely identify devices.

Device identity is not limited to user devices; device identity information is also gathered for cloud servers, on-prem datacenter and bare metal servers, containers, and OT/IoT devices that may be protected with Zero Trust.

CoIP Platform is not intended to replace traditional endpoint protection, such as EDR or anti-virus software. Zentera will release support for access policy determination based on EDR security posture analysis in Q1 2023.

Network



Zentera's approach enables an Optimal maturity level for Network to be achieved in less than one day.

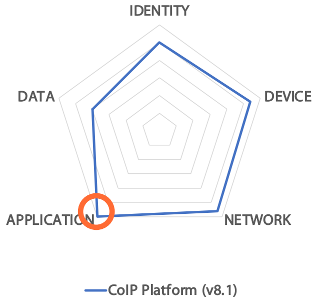
CoIP Platform implements Application Chambers, which are the fully-distributed micro-perimeter concept of the Zero Trust Maturity Model. Application Chambers may be applied to any type of asset – server-based, container, or OT/IoT. The Application Chamber fully controls ingress and egress to cloak a protected asset, and makes it simple to apply rules enforcing the use of trusted, encrypted DNS resolvers, as is mandated by OMB M-22-09.

CoIP Platform also enables ZTNA, least-privilege access direct to chambered assets, eliminating any implicit trust zones.

CoIP Platform implements an overlay Application Network, which allows administrators to create isolated networks on top of disconnected IP networks without a VPN. For example, all surveillance cameras in all sites could be isolated from their local networks, able to connect only to authorized network video recorders, thereby eliminating the potential for unauthorized access.

Finally, CoIP Platform enables legacy LAN traffic to be transparently encrypted in TLS 1.3 tunnels. CoIP Platform does not require changing application routing to transit a 3rd party SaaS.

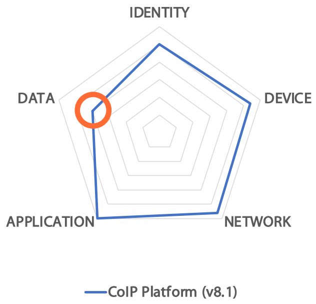
Application



In CoIP Platform, *every* network transaction can be authenticated and authorized. This is not limited to user sessions - it includes server-to-server data sessions, DNS lookups, NFS activity and more. Each access must be authorized by policy, and each policy may be associated with specific application processes.

CoIP Platform does not use deep packet inspection, which is expensive and can degrade network performance; instead, applications are identified with cryptographic identity. CoIP Platform offers full visibility over the entire process context that leads to the creation of a socket and transmission/reception of packet traffic, including the user, command line and options, and the full process tree. These process "trust factors" enable targeted, application aware policies.

Data



CoIP Platform provides controls to help agencies manage data security with access policies that enforce least-privilege data controls. Segmentation controls help to localize data, while policies limit access to safe methods, limiting the potential risk to data.

CoIP Platform also provides data access segmentation tools that can automatically mount or unmount network stores to make them available for users during the duration of their access session.

CoIP Platform does not natively enforce data at rest security, and may be used in conjunction with 3rd party data security tools or architectures that enforce and require data encryption at rest.

Visibility, Automation, and Governance

CoIP Platform implements distributed security enforcement across all onboarded devices. Telemetry for each of the five pillars is continuously gathered and made available through logs; these can be exported using RFC5424 syslog format to SIEM tools for alerting and offline analysis in BI tools.

CoIP Platform's configuration may be fully automated using APIs; agencies may use Zentera's SDKs as a reference for building their own tooling. This enables policies to be generated, updated, and continuously verified, so that any potential deviation is rapidly detected and flagged for remediation.

CoIP Platform security policies enable end-to-end controls. Regardless of the configuration of the underlying networks, a policy that specifies that a given user can access a server using RDP with copy/paste controls enabled will be applied regardless of whether that user is remote or on-premises. Eliminating location dependencies on policy application is a huge benefit for governance, giving agencies concrete ways to demonstrate Zero Trust maturity, and ultimately, compliance with Executive Order 14028.

About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

More Resources

On the web:
www.zentera.net

Email:
sales@zentera.net

Phone:
+1 (408) 436-4811

zentera™