Zero trust

What is zero trust?

Contrary to popular belief, zero trust is not a product or a service. It's a strategic approach behind an architectural model that, put simply, focuses on:

- Encrypting all data at rest and in transit.
- **End user identity, which must be authenticated with multiple factors (MFA)**.
- Every **device** and user must be authenticated **continuously when attempting to access organizational data**.

A true zero trust environment requires this focus across five different pillars:

- Identity
- Device
- Network
- Application workload
- Data

Why begin the zero trust journey?

- The advancement of cyber threats and the rate of attacks are accelerating. Small, medium, and Fortune 500, as well as state and local governments, healthcare, retail, finance, manufacturing, technology, agriculture—you name it, it's vulnerable.
- Current controls, no matter how effective today, will soon be ineffective.
- Federal regulatory requirements; Executive Order 14028 requires agencies to create a zero trust implementation plan, and M-22-09 requires the implementation of the plan by the end of 2024.
- The shift away from the network perimeter has resulted in networks losing their edge. This new architectural design with no edge requires new solutions and strategies to protect from threat actors.

*edge—singular noun. If something has an edge, they have an advantage that makes them stronger or more likely to be successful than another thing.

Proper implementation of zero trust makes it significantly more difficult for threat actors to move around inside their targeted environments, reducing the risk of data acquisition and exfiltration or ransomware attacks.

Where are you now?

The Cybersecurity and Infrastructure Security Agency (CISA) zero trust Maturity Model can be used as a reference to understand where you are now and what the optimal state is. Every organization's path to zero trust is different, and knowing where to begin by assessing the current state, risks, priorities, and timelines, requires cross-organizational groundwork.

	Identity	Device	Network/ Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA). • Limited risk assessment.	• Limited visibility into compliance. • Simple inventory.	• Large macro-segmentation. • Minimal internal or external traffic encryption.	• Access based on local authorization. • Minimal integration with workflow. • Some cloud accessibility.	• Not well inventoried. • Static control. • Unencrypted.
	Visibility and Analytics Automation and Orchestration Governance				
Advanced	• MFA. • Some identity federation with cloud and on-premises systems.	• Compliance enforcement employed. • Data access depends on device posture on first access.	• Defined by ingress/egress micro-perimeters. • Basic analytics.	• Access based on centralized authentication. • Basic integration into application workflow.	• Least privilege controls. • Data stored in cloud or remote environments are encrypted at rest.
	Visibility and Analytics Automation and Orchestration Governance				
Optimal	• Continuous validation. • Real time machine learning analysis.	• Constant device security monitor and validation. • Data access depends on real-time risk analytics.	• Fully distributed ingress/egress micro-perimeters. • Machine learning-based threat protection. • All traffic is encrypted.	• Access is authorized continuously. • Strong integration into application workflow.	• Dynamic support. • All data is encrypted.
	Visibility and Analytics Automation and Orchestration Governance				

How can CBTS help?

CBTS' enterprise cloud architecture and security services combine to deliver solutions with security controls integrated into the design. Our battle-tested blueprints and processes ensure rapid, efficient, and effective zero trust deployment.

From developing and deploying modern apps and the secure, scalable platforms on which they run, to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era.

Contact us today.