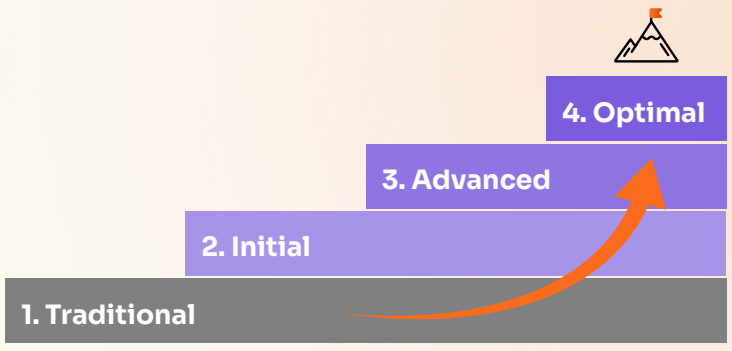
A Visual Guide to Zero Trust 2.0 Encryption Gaps

CISA ZTMM 2.0

The Cybersecurity and Infrastructure Security Agency (CISA) **Zero Trust Maturity Model (ZTMM) 2.0** provides a path for organizations to move from

Traditional → **Optimal**

zero trust architecture.



Legacy Tools Fall Short

ZTMM 2.0 includes guidance specific to networking encryption, but **legacy tools are not equipped** to support these requirements.

Here's a visual guide to those gaps and how, with Aviatrix Cloud Network Security Fabric (CNSF), you can deploy encryption that aligns with ZTMM 2.0.

LEGACY GAPS		THE AVIATRIX CNSF SOLUTION
MACSec decrypts then **re-encrypts frames at each hop**, creating encryption gaps. IPSec doesn't do this, but it does impose a **performance penalty**.	**MACSec Encryption Protocol**	Patented technology using IPSec encryption that matches the line-rate speed of MACSec, **removing the inter-hop vulnerabilities without sacrificing performance.**
TLS/SSL operates **in isolation**, **securing individual applications** rather than providing comprehensive protection across all traffic types.	**TLS/SSL Application-Layer Encryption**	**Encrypts all types of traffic**–east-west, north-south, cloud-to-cloud, and hybrid connections–unifying security policies and collapsing the silos.
Site-to-site VPN technologies and cloud-delivered IPSec VPN technologies create persistent encrypted tunnels **between fixed endpoints for extended periods.**	**Static Configurations** with long-lived credentials	**Scales dynamically** and **enforces access on a per-session basis**, even while site-to-site VPN tunnels remain static and give users far longer access than zero trust allows.
Managing keys/certificates/credentials separately makes it **difficult to enforce consistent encryption policies** or achieve the "cryptographic agility" called for by the ZTMM 2.0 framework.	**Key Management**	**Centralizes key management,** policy control, and telemetry, **delivering consistent encryption governance** across all environments in which it is deployed.
Applying traditional tools in a zero trust model would require you to build an impenetrable wall around **every single workload–it's not scalable.**	**Perimeter-Based Tools**	Is **embedded directly in the cloud fabric**, providing zero trust enforcement inline, everywhere workloads communicate.

Experience Aviatrix for Yourself

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit www.aviatrix.com.