TRINITY CYBER

TRINITY CYBER ZERO TRUST NETWORK ACCESS

Protect your hybrid workforce

Replace legacy VPN. Modernize remote access with threat-centric internet and private application connectivity.

YOUR ZERO TRUST JOURNEY

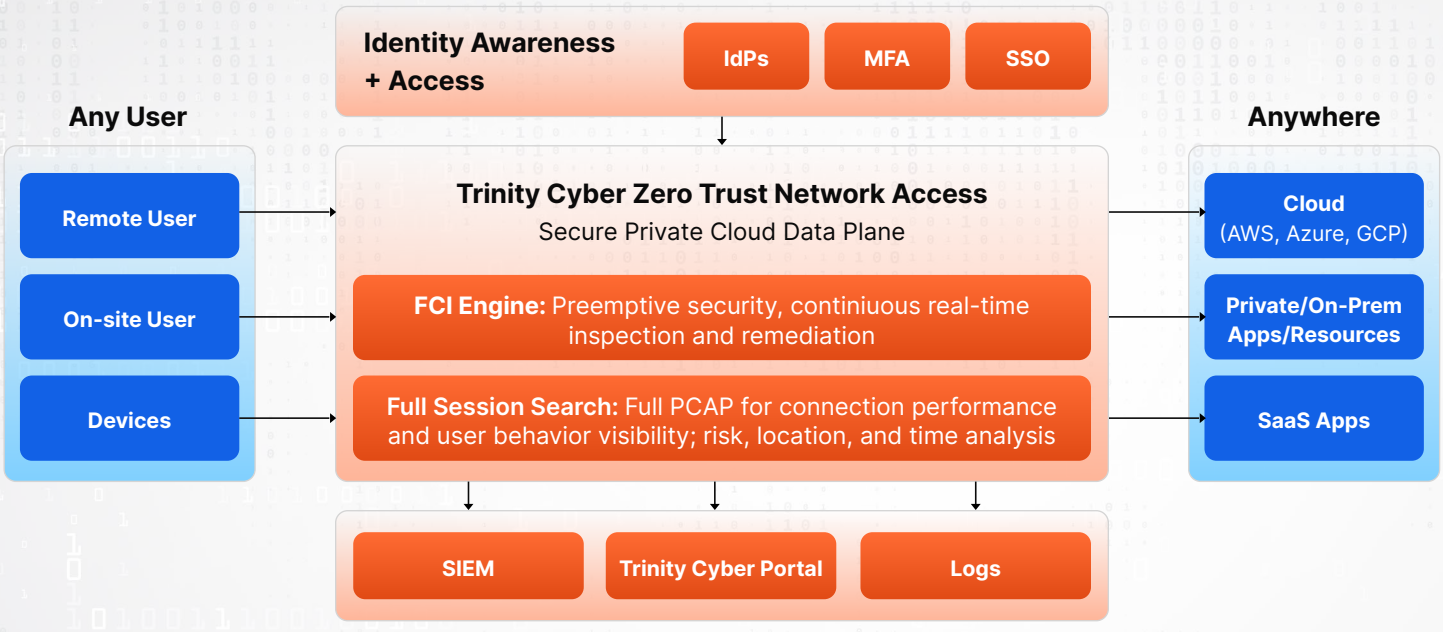
When replacing legacy VPN and ZTNA, you need to:

- ✓ Enable zero trust access to private resources and the internet
- ✓ Ensure an excellent experience for your end-users
- ✓ Deploy and operate with efficiency

Real zero trust

Zero trust should inspect everything. Trinity Cyber takes zero trust further, not only enabling you to connect with confidence to private applications and the internet from everywhere, but also removing threats in real time with preemptive security. Unlike conventional ZTNA, our secure, private cloud Full Content Inspection (FCI) engine, isolated from the internet, transparently removes malware at line speed from your live network sessions. Its alertless threat defense that stops more attacks and reduces security cost. Unique in the industry, its continuous removal of malicious content in real-time enables business continuity.

Only Trinity Cyber fully protects remote access sessions. Alternative solutions typically trust all traffic, so threats can hide in encrypted traffic. Even with SSL inspection, other solutions miss threats that Trinity Cyber FCI stops. With contextual and behavioral understanding, Trinity Cyber's surgical detections meet adversaries precisely where they operate, taking zero trust principles further.



Our AI models defend against new AI-based threats

AI has given attackers new superpowers, accelerating code generation, polymorphic malware development, and deepfake social engineering. Attack volume and sophistication is increasing, compressing the time defenders have to react. Trinity Cyber AI models help defend against unprecedented threat volume and complexity. Our AI models, developed using millions of training data files in a secure air-gapped environment, accelerate identification across the 1.5 trillion files we inspect daily. The result? Stronger threat protection.

Preemptive security: action, not alerts

With conventional network security, attackers operate in your environment before you can even attempt to respond. Competing ZTNA solutions extoll timely "mean time to respond (MTTR)." Whether its meantime to threat remediation, resolution, recovery, or response, new AI-enabled threats make minutes, and even seconds, too long. Legacy detection and response is unsustainable. In contrast, Trinity Cyber remediates in real time, in less than one millisecond, without alerts. The result is preemptive protection before an attack is operating on your endpoints and network. Best of all, the process is invisible to your end users, and with no alerts to manage you get your time back.

A transparent and secure user experience

With Trinity Cyber's approach for preemptive zero trust, worker productivity is enhanced:

Session threat sanitization is transparent to end users

Integrates with your existing IdPs, SSO, MFA

Interoperates, if you require, with third-party VPNs

Simpler management and security operations

Trinity Cyber's approach delivers for IT and security teams:

- **Lowers cost:** stops more threats before an attacker can mount them in your network or on your endpoints, reducing triage and incident response
- **Less stress:** alertless by design, reducing SOC pressure with no day-to-day management required
- **Faster deployment:** Roll out to hundreds of endpoints in minutes; works with your existing endpoint AV/EDR and network architecture

Next steps

See for yourself

Book a demo or, if you are ready, start a 14 day pilot (up to 500 agents)

TRINITY CYBER

info@trinitycyber.com
(844) 853-5933