Zero Trust Admission Control (ZTAC)

Behavioral access enforcement that adapts in real time—without slowing your network

ZTAC, part of the Corero Observability & Resiliency Ecosystem (CORE), delivers out of band behavior based access control that protects remote access to your organization's internal resources from malicious activity without inspecting or redirecting user traffic. As a licensed capability within CORE, ZTAC extends Zero Trust to Internet traffic and services not already covered by ZTNA, delivering transparent admission control without changes to protected applications.

Built for speed, scale, and simplicity, ZTAC stops unauthorized activity at the network edge using telemetry from your existing infrastructure with no agents, proxies, or new appliances required. It continuously evaluates both new and authenticated users to ensure only trusted behavior is allowed.

Adaptive, cost-effective zero trust defense built for what matters now:

Protect access to internal infrastructure and critical resources

Enforce zero trust at the edge with continuous verification

Reduce complexity and latency

ZTAC gives service providers and enterprises real time access control powered by live intelligence from CORE without disrupting performance or operations.

Key Benefits

Ensure secure access to infrastructure: Block threats targeting login portals, APIs, and control planes based on observed behavior.

Enforce dynamic access control: Use live trust signals from authentication data to threat intelligence to decide who gets in every time.

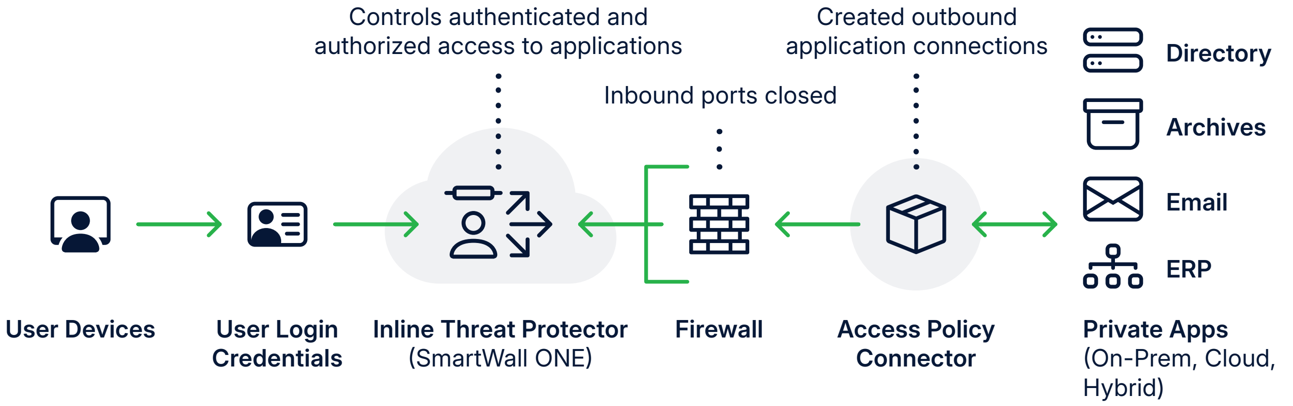
Trolling and disruption: Operates out of band with no added latency and no impact on user traffic.

Scale without friction: Handle millions of connections with zero slowdown and no application changes.

Extortion (RDoS): Uses SmartWall ONE™ or compatible routers and firewalls to enforce policies—no additional enforcement hardware needed.

Automate enforcement: Apply admission decisions automatically through SmartWall ONE or compatible enforcement points, without manual triage.

What is Zero Trust Admission Control (ZTAC)?


Controls authenticated and authorized access to applications
Created outbound application connections
Inbound ports closed
Directory
Archives
Email
ERP
User Devices
User Login Credentials
Inline Threat Protector (SmartWall ONE)
Firewall
Access Policy Connector
Private Apps (On-Prem, Cloud, Hybrid)

Specifications

Platform:	Available through the Corero CORE solution
Deployment:	Requires SmartWall ONE—adds full-spectrum DDoS protection for remote access and critical infrastructure
Access:	Web-based secure dashboard
Delivery Model:	Cloud-based subscription service
Data Sources:	Authentication logs, API telemetry, proxy and infrastructure logs, botnet membership, reputation feeds, geo location, source profiling, and explicit allow or block lists.
Security:	Dedicated login, role-based access, encrypted telemetry
Integration:	Integrated with SmartWall ONE as the enforcement point, with support for additional enforcement options as they are enabled.
Automation:	Driven by live trust indicators, with configurable allow or block actions applied through enforcement points.
Prerequisites:	**Requires SmartWall ONE™; unlocks broader defense capabilities**
Use Cases Supported:	Adaptive access enforcement for internal resources and services independently, or as part of a broader zero trust (ZTNA) architecture Transparent, low-latency, admission control for VPN gateways and other network access points Application layer threat detection for remote access gateways Defense against DDoS, brute force, and scanning attacks Continuous verification post authentication IoT and OT access control VPN Gateway / Firewall vulnerability exploit shielding