# Zero Trust Network Access (ZTNA)

## Today's More Secure Solution

MetTel's ZTNA works with MetTel's FWaaS (Firewall as a Service) to enable secure, granular access to applications no matter if the user is on-net or off-net. Each session is initiated with an automatic, encrypted tunnel from the user's computer to the EMS proxy for user and device verification. If verified, access is granted for that session. Two-Factor Authentication can also be used to provide an additional layer of security. With ZTNA, organizations benefit from both a better remote access solution and a consistent policy for controlled access to applications both on and off the network.

## Key Benefits

### ENDPOINT HYGIENE

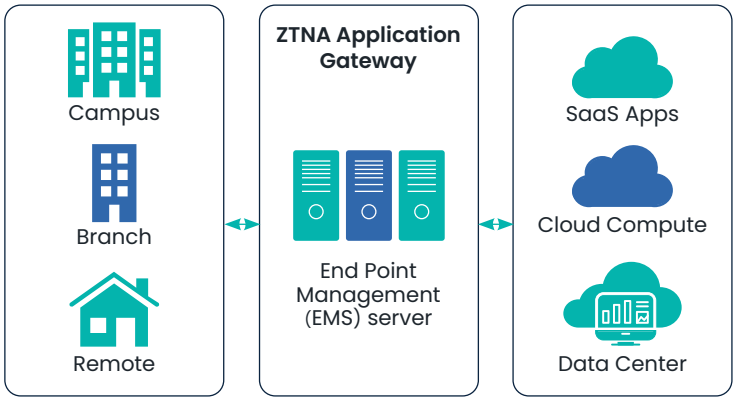
MetTel's ZTNA solution helps organizations reduce attack surface with vulnerability scanning and auto-patching. Combined with zero-trust access principles, this approach can enhance an organization's hygiene and security posture.

### SECURE REMOTE ACCESS

MetTel's ZTNA solution, implemented as part of our Secure Access Service Edge (SASE) solution, provides the ability to integrate ZTNA into a remote access solution, reducing remote workers' access to the network to only what they require for their jobs.

### SECURE CLOUD ACCESS

MetTel's ZTNA solution enables an organization to limit access to their cloud environments and applications based upon business needs. Each user and application can be assigned a role within the ZTNA solution with the appropriate rights and permissions associated with the organization's cloud-based infrastructure.




## Key Features

### WINDOWS AD INTEGRATION

Helps sync your Active Directory (AD) structure into Enterprise Management Server (EMS) for endpoint management.

### REAL-TIME ENDPOINT STATUS

Always provides current information on endpoint activity and security events.

### VULNERABILITY DASHBOARD

All vulnerable endpoints are easily identified for administrative action, helping to manage your attack surface.

### CENTRALIZED ZTNA DEPLOYMENT AND PROVISIONING

Allows administrators to remotely deploy endpoint software and perform controlled upgrades, which makes deploying ZTNA configuration to thousands of clients an effortless task with a click of a button.

### SOFTWARE INVENTORY MANAGEMENT

Provides visibility into installed software applications and license management to remove unnecessary or outdated applications that might have vulnerabilities.

### ENDPOINT QUARANTINE

Helps to quickly disconnect a compromised endpoint from the network and prevent it from infecting other assets.

### AUTOMATED RESPONSE

Helps detect and isolate suspicious or compromised endpoints without manual intervention.

### APPLICATION-BASED SPLIT TUNNEL

Supports source application-based split tunnel, where you can specify application traffic to exclude from the VPN tunnel, such as high bandwidth apps.

For more info, contact your MetTel agent or visit mettel.net.