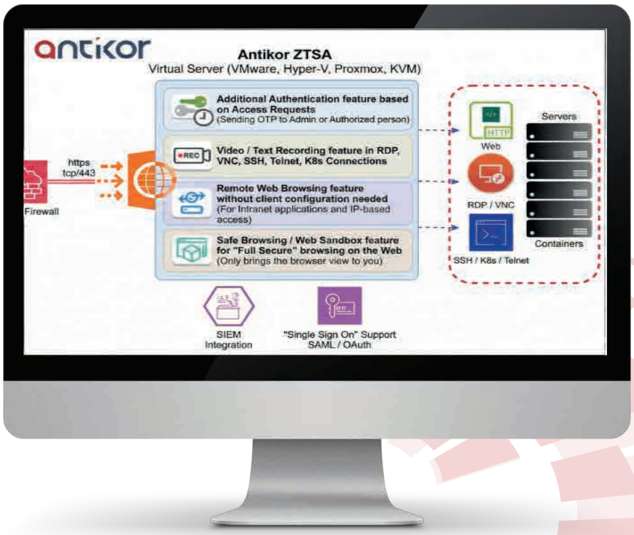
Unified Cyber Security System

EPA-ZTSA-PRO-250

Antikor ZTSA (Next-Gen. PAM)


antikor
Antikor ZTSA
Virtual Server (VMware, Hyper-V, Proxmox, KVM)
Additional Authentication feature based on Access Requests
(Sending OTP to Admin or Authorized person)
Video / Text Recording feature in RDP, VNC, SSH, Telnet, K8s Connections
Remote Web Browsing feature without client configuration needed
(For Intranet applications and IP-based access)
Safe Browsing / Web Sandbox feature for "Full Secure" browsing on the Web
(Only brings the browser view to you)
https
tcp/443
Firewall
HTTP
Web
RDP / VNC
SSH / K8s / Telnet
Servers
Containers
SIEM
Integration
"Single Sign On" Support
SAML / OAuth

Antikor ZTSA (Zero Trust Service Access) software EPA-ZTSA-PRO-250 is an agentless, browser-based ZTSA platform operating over the SSL port, designed as a next-generation Privileged Access Management (PAM) solution. It does not provide users with direct access to services such as RDP, SSH, VNC, Telnet, Kubernetes Console, Remote Web Browsing, SafeBrowsing / Web Sandbox, or File Browser. Instead, it delivers highly secure, low-risk connections by transmitting only screen output and user interactions, thereby preventing direct exposure of internal systems and minimizing attack surfaces.

Authentication and Integration

Antikor ZTSA supports Single Sign-On (SSO) and integrates seamlessly with identity providers using OAuth 2.0, OpenID Connect, and SAML protocols. It can also integrate with authentication sources such as LDAP, RADIUS, TACACS+, and HTTP API–based identity services. In addition, local user accounts can be created and managed within the platform when required.

Safe Browsing / Web Sandbox Feature

Antikor ZTSA enables secure access to web applications operating in both private (closed) and public networks. It launches the web browser within an isolated environment, allowing users to browse websites remotely and securely without exposing the endpoint to potential risks.

Video / Text Session Rec. and OTP Support

For RDP and VNC connections, video session recording is available. For SSH, Telnet, and Kubectl connections, text-based session recording is supported. Additionally, an OTP can be sent to an authorized user for approval. The connection can only be established upon successful authorization, ensuring controlled and auditable privileged access.

Scalability

Antikor ZTSA can be deployed on virtual environments such as VMware, Microsoft Hyper-V, Proxmox VE, and KVM. It is also compatible with modern container architectures such as Kubernetes and Docker Swarm. The platform supports automatic horizontal scaling to meet increasing performance and capacity requirements.

EPA-ZTSA-PRO-250

Product Specifications

Management Interface Features

- HTML5 Responsive Web Interface
- Event Notification Infrastructure
  - SMS, Email, Browser Notifications, and Webhook Support
- Access Logging
- Personalized Favorite Services
- Configuration Override Support Based on Permissions
- Light / Dark Mode Support
- Grid / List View Support
- Service Grouping Support
- Access Request Management Module
- Quick Search Module
- Reporting Module
- Permission Management

Supported Services

- Zero-Configuration, Agentless Web Proxy (HTTP / HTTPS)
- RDP – Remote Desktop Protocol
  - Secure File Sharing
  - Audio, Clipboard, and Printer Sharing
  - Ability to Specify Initial Program
- SSH - Secure Shell
  - Password & Public Key Authentication
- Screen Sharing with Remote Control Capability
- VNC (Virtual Network Computing)
- K8s - Kubernetes Console
- Telnet
- Safebrowsing / Web Sandbox
- Screen Sharing with Remote Control Access via Link
- Proxy Access via Agent (Windows, macOS, Linux Supported)
- File Browser (FTP, SMB/CIFS, SFTP, WebDAV, SCP, AWS S3 and Google Drive)
- Wake on LAN support
- Aktif Oturuma Katılma: Ekran İzleme / Yönetme

Security Features

- Secure Storage of Encrypted Credentials
- Secure File Exchange
  - Antivirus Scanning
  - Optional Sandbox API Integration
- Client-Side RDP Drive Share Isolation
- Session Recording
  - Screen Video Recording
  - Text Session Recording for SSH, Telnet, and Kubernetes (K8s)
  - Session Start and End Logs

Licensing

Asset Count (User + Server × 10)	250
Horizontal Scalability	None
Number of Addressable CPUs	6
Amount of Addressable Memory	16GB

Access Control Features

- Service-, Group-, User-, and Role-Based Access Control
- Access Permission Expiration Date Control
- Access Authorization on Specific Days
- Time-Based Access Authorization (Specific Hours)
- Connection Security with Additional Approval (Sponsored Access)
  - Sending the OTP to an Authorized User
  - Connection Establishment Upon Authorized Approval

Authentication Methods

- Local Users
- Single Sign-On (SSO)
  - SAML2.0
  - OAuth2.0
  - OpenID Connect
- RADIUS with MFA and Challenge Support
- LDAP / Active Directory
- Multi-Factor Authentication (MFA) – OTP and TOTP Support

Integration Features

- SIEM / Syslog Integration
  - CEF and JSON Formats Support
- Audit Log Integration
- External Sandbox Integration
- External Antivirus Integration

Supported Virtualization Platforms

- VMWare ESXi / vSphere
- Microsoft Hyper-V
- Proxmox
- KVM-Based Hypervizors

Minimum Requirements for Virtual Platforms

- VMware ESXi, Hyper-V, Proxmox Hipervisor
- Min 6 Core AESNI Enabled CPU
- Min 16 GB Reserved Ram
- At Least 240GB Storage Area (At Least 10000 IOPS with 4KB Blocks)
- Unubtu Server v24 or Later LTS

* Minimum requirements may vary based on system configuration and hardware.