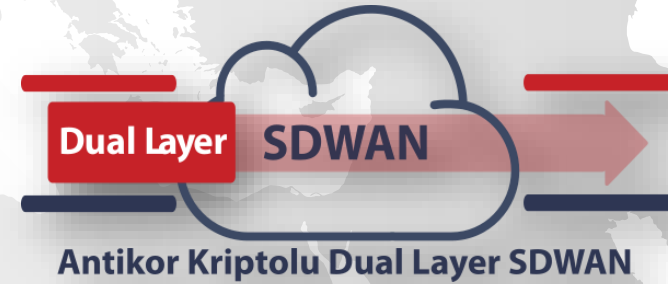


ePATI

ePati Siber Güvenlik A.Ş.



www.epati.com.tr

Kurucu Ortaklar ve Yönetim Kurulu

Öğr. Gör. Dr. Özkan KIRIK

epati

• ePati Siber Güvenlik A.Ş.
Yönetim Kurulu Başkanı



• Mersin Üniv. Bilgi İşl. Arş. Uyg. Mrkz.
Akademisyen



• T.C. Cumhurbaşkanlığı Bilim, Teknoloji
ve Yenilik Politikaları Kurulu
Siber Güvenlik Danışma Kurulu Üyesi



• Türkiye Siber Güvenlik Kümelenmesi
(SSB ve CBDDO Himayelerinde)
Firewall Test Kriterleri Belirleme
Komisyonu Üyesi



• TSE Sertifikalı Beyaz Şapkalı Hacker



• Cisco Certified Trainer



• FreeBSD Project Contributor

epati

Öğr. Gör. Kutluhan KİBRİT

epati

• ePati Siber Güvenlik A.Ş.
Yönetim Kurulu Başkan Vekili



• Mersin Üniv. Bilgi İşlem Daire Bşk.
Akademisyen



• TSE Sertifikalı Beyaz Şapkalı Hacker



• Cisco Certified Trainer

Öğr. Gör. N. Can KIRIK

epati

• ePati Siber Güvenlik A.Ş.
Yönetim Kurulu Başkan Vekili



• Mersin Üniv. Bilgi İşl. Arş. Uyg. Mrkz.
Akademisyen



• PostgreSQL Contributor



• Cisco Certified Trainer



antikor

ePati Siber Güvenlik Hakkında



**TÜRKİYE SİBER
GÜVENLİK KÜMELENMESİ
ÜYESİDİR**

➤ ePati Siber Güvenlik A.Ş.

- 2006 Kasım'da Mersin Teknopark'ında kurularak Mersin Teknopark'ın ilk firması olmuştur
- 2011 yılından bu yana Devlet Malzeme Ofisi kataloğunda yer almaktadır
- Türkiye Siber Güvenlik Kümelenmesi Üyesidir
- İnovasyon odaklı çalışarak, yerli – milli ürünler geliştirmeye ve katma değer üretmeye önem verir



➤ Kuruluş Yapısı

- Kuruluş ortaklarının tamamı Akademisyen olup Mersin Üniversitesi'nde halen görev yapmaktadır. Aynı zamanda 4691 sayılı yasa uyarınca Mersin Üniversitesi tarafından Teknoparkta görevlendirilmişlerdir.

Siber Güvenlikte Milli İrade

Yabancı Çözümlerle
Siber Güvenlik

Yabancı Askerlere Emanet
Sınır Güvenliği

**EŞDEĞER
RİSK!**

Risk: Veri Sızıntısı, Bağımlılık

Risk: Ulusal Güvenlik Tehdidi

Standart ve Sertifikasyonlar

Kurumsal Yönetim Standartları









Ürün Sertifikaları



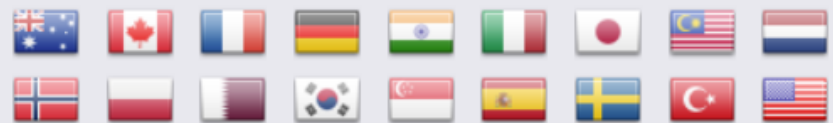
CERTIFIED PRODUCTS

Access Control Devices and Systems – 21 Certified Products

Boundary Protection Devices and Systems – 36 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Schem
Antikor Next Generation Firewall Management v2.0.1188 Certification Report Security Target	Epati Siber Güvenlik Tek. San. ve Tic. A.S.	CCRA Certificate	2023-04-17	2028-04-17	EAL4+ ALC_FLR.1	
Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect Certification Report Security Target	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134-1706 USA	CCRA Certificate	2022-10-07	2027-10-07	EAL4+ ALC_FLR.2	
McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x Certification Report Security Target	Trellix	CCRA Certificate	2022-07-28	2027-07-28	EAL2+ ALC_FLR.2	
ST Engineering Data Diode Model 5282, version 2.2.1055 & Model 5283 version 2.2.1055 Certification Report Security Target	ST Engineering Electronics	CCRA Certificate	2022-07-08	2027-07-08	EAL4+ AVA_VAN.5	
Trend Micro Deep Security 20 Certification Report Security Target	Trend Micro Inc.	CCRA Certificate	2022-05-31	2027-05-31	EAL2+ ALC_FLR.1	
Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7 Certification Report Security Target	Fortinet, Inc.	CCRA Certificate	2021-10-15	2026-10-15	EAL4+ ADV_FSP.3	

Certificate Authorizing Members



Certificate Consuming Members



TÜRKİYE'NİN TEK



COMMON CRITERIA
EAL4+
CERTIFIED

YENİ NESİL GÜVENLİK DUVARI





Test ve Sertifikasyon Sertifikalarının Takdimi



DURUM	A	B	C	P	Toplam
BAŞARILI	24	77	115	31	250
KISMEN BAŞARILI	-	3	-	-	250

- Toplamda 250 madde test edilmiş ve test maddesine ilişkin "BAŞARILI" ya da "BAŞARISIZ" durumu 1.3 Özet Test Sonuçları tablosunda belirtilmiştir.

- Testleri tamamlanan FIREWALL ürün grubunda EPATİ BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ. Firması Antikor ürünü testlerinde herhangi bir zafiyet bulunmamış olup, bu kapsamda yapılan testlerden başarı ile geçtiklerinden dolayı yapılan inceleme ve değerlendirme neticesinde TRTEST tarafından Ürün Uygunluk Sertifikası almaya hak kazanmıştır.

Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
Telefon No:0 850 551 00 00 /25

TRTEST  iştirakidir.

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1 / 250
Yenimahalle / ANKARA
Ulus V.D. 069 03 755 16 52 No:015473
İmarsat No: 0899 0647 9550.0002

Ürün Portföyü



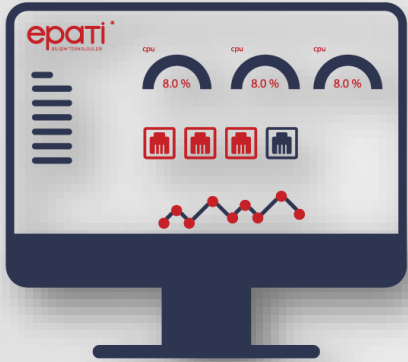
NGFW - Yeni Nesil Güvenlik Duvarı



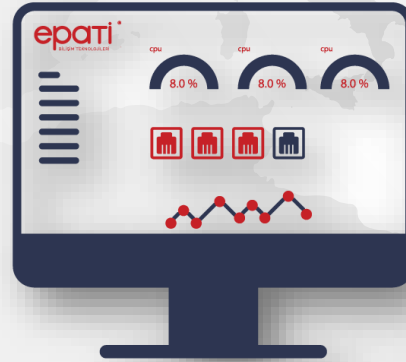
Kriptolu Dual Layer SDWAN



ZTSA - Zero Trust Service Access



- Merkezi NGFW Yönetimi
- Merkezi Log Yönetimi



Merkezi SDWAN Yönetimi



Multi-Zone SSO (SAML & OpenID)
SSLVPN Gateway



ANTİKOR – Başlıca Başarı Hikayelerimiz



T.C. CUMURBAŞKANLIĞI
SAVUNMA SANAYİİ BAŞKANLIĞI



ANTİKOR – Sürdürülebilirlik

➤ Güvenli Ar-Ge Yaşam Döngüsü

- 31 Ülkede gerli Common Criteria EAL4+ sertifikası, ürünlerimizin tasarımından geliştirilmesine, test süreçlerinden dokümantasyonuna kadar **profesyonel bir yaşam döngüsüne sahip** olduğunu doğrular.



COMMON CRITERIA

EAL4+



➤ Ürün Güvenliği Müdahale Ekibi (PSIRT)

- Olası zafiyetlere karşı proaktif bir yaklaşım sergileyen PSIRT portalı, ePati'nin ürün desteğindeki olgunluk seviyesini ve şeffaf profesyonellik anlayışını simgelemektedir.

➤ CI/CD ve Continuous Security Monitoring

- CI/CD süreçleri ile SBOM listesi oluşturma, SAST vb. güvenlik testlerinin uygulanması, Security Monitoring araçlarına gönderme işlemleri gerçekleştirilir.
- Ürünlerimizi **TSE Onaylı Sızma Testi Raporuna sahip** olup sadece düşük seviyeli 1 adet bulgu bulunmaktadır.

lodash - Prototype Pollution Vulnerability

MEDIUM FINAL

Advisory ID EPA-SA-2026-1666	Product Antikor NGFW	Vulnerability Status Fixed	CSAF Download JSON
--	--------------------------------	--------------------------------------	---------------------------------------

Affected Versions

< 2.0.1306

Fixed Versions

2.0.1306

Vulnerabilities

CVE ID	Status	Description	Score
CVE-2025-13465 CWE-1321	FIXED	<p>Lodash has Prototype Pollution Vulnerability</p> <p>Lodash has Prototype Pollution Vulnerability</p> <p>Impact: Lodash versions 4.0.0 through 4.17.22 are vulnerable to prototype pollution in the <code>_.unset` and <code>_.omit` functions. An attacker can pass crafted paths which cause Lodash to delete methods from global prototypes. The issue permits deletion of properties but does not allow overwriting their original behavior.</code></code></p>	6.5

antikor – Continuous Security Monitoring

➤ OWASP Dependency Track - SBOM Analiz Platformu

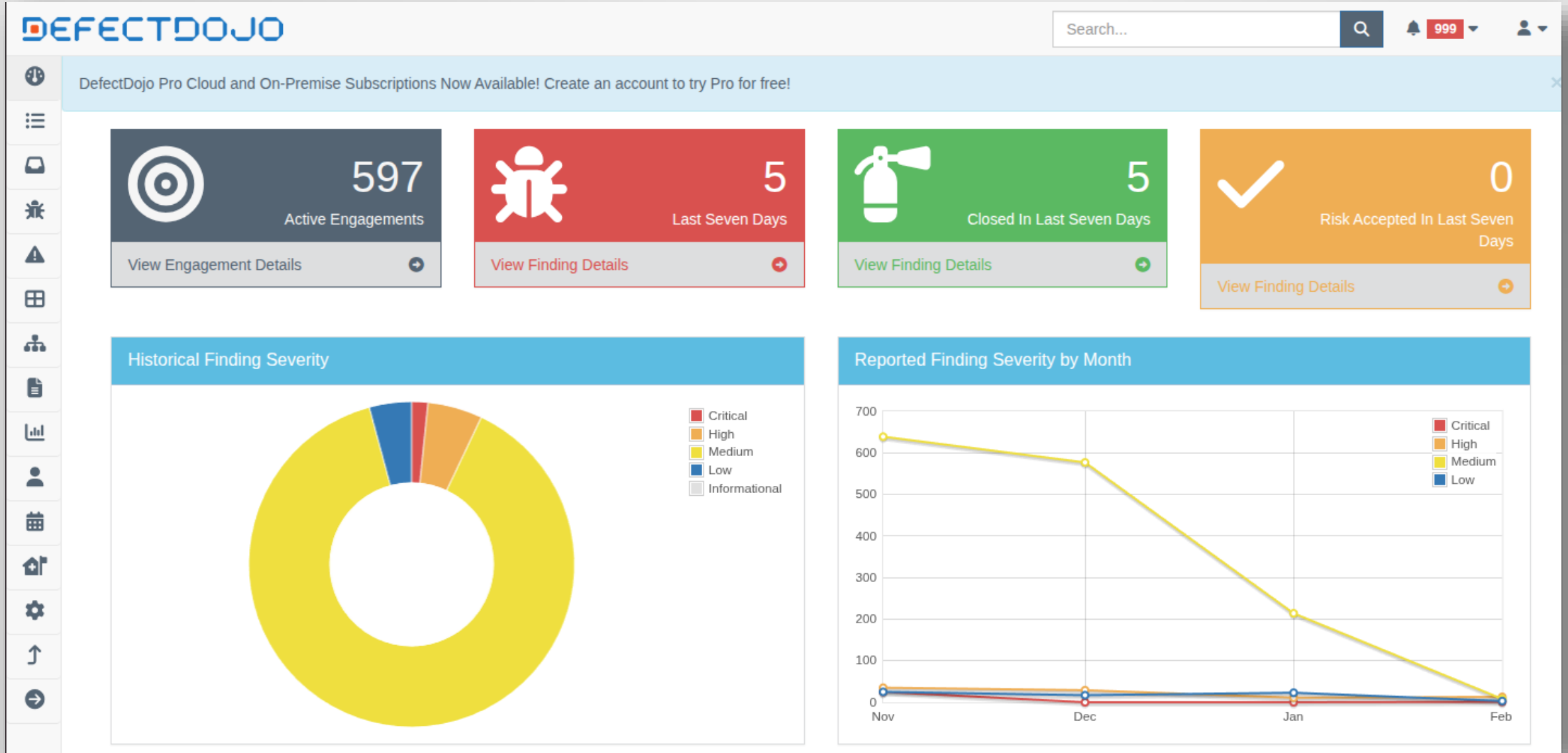


The screenshot displays the Antikor dashboard interface. On the left is a dark sidebar with navigation options: Dashboard, PORTFOLIO (Projects, Components, Vulnerabilities, Licenses, Tags), GLOBAL AUDIT (Vulnerability Audit, Policy Violation Audit), and ADMINISTRATION. The main content area shows a breadcrumb "Home / Projects" and four summary cards with line charts: "87 Portfolio Vulnerabilities", "15 Projects at Risk", "30 Vulnerable Components", and "321 Inherited Risk Score". Below these are filters for "Create Project", "Show inactive projects", and "Show flat project view", along with a search bar and refresh icon. A table lists project details:

Project Name	Version	Latest	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Policy Violations	Vulnerabilities
▶ Antikor NGFW	future		Application	-	-	3	<input checked="" type="checkbox"/>	<div style="width: 100%; background-color: #007bff; color: white; text-align: center;">0</div>	<div style="width: 100%; background-color: #28a745; color: white; text-align: center;">3</div>
▶ Antikor NGFW	f14-rc		Application	-	-	3	<input checked="" type="checkbox"/>	<div style="width: 100%; background-color: #007bff; color: white; text-align: center;">0</div>	<div style="width: 100%; background-color: #28a745; color: white; text-align: center;">3</div>
▶ Antikor NGFW	f14-production	<input checked="" type="checkbox"/>	Application	-	-	3	<input checked="" type="checkbox"/>	<div style="width: 100%; background-color: #007bff; color: white; text-align: center;">0</div>	<div style="width: 100%; background-color: #28a745; color: white; text-align: center;">3</div>

ANTIKOR – Continuous Security Monitoring

DefectDojo - DevSecOps, ASPM (application security posture mgmt.), Vulnerability Mgmt.



epati



Yerli ve Milli Ürünlerin Kullanımı ile İlgili Mevzuatlar

www.epati.com.tr



Yerli ve Milli Ürünlerin Kullanımı ile İlgili Mevzuatlar

19 Mart 2025 de Resmi Gazetede yayımlanan 7545 nolu “Siber Güvenlik Kanunu” 4/d bendinde açıkça belirtilmiştir. İlgili maddeye göre;



“Siber güvenliğin sağlanmasına yönelik çalışmalarda öncelikle yerli ve milli ürünler tercih edilir.”

2.2.1. Bilgi ve İletişim Güvenliği Temel Prensipleri

Yol haritasının planlanması ve uygulanması aşamalarında gerçekleştirilecek tüm çalışmalarda Şekil 8'de yer alan temel prensipler dikkate alınmalıdır.



T.C. CBDDO Bilgi ve İletişim Güvenliği Rehberi



Şekil 8. Temel Prensipler



“Kamuda Açık Kaynak Kodlu Yazılım Kullanımı” konulu Cumhurbaşkanlığı Genelgesi (2023/13)

3. Yazılım tedarikini içeren mal ve hizmet alımlarında, teknik ve/veya ekonomik gerekçelerle uygun olmaması durumu hariç, ticari lisanslı yazılımlar yerine AKKY muadilleri tercih edilecektir. Bu nitelikteki ödenek talepleri için Strateji ve Bütçe Başkanlığına iletilecek proje teklif formlarında, alınması öngörülen ticari lisanslı yazılımlar için AKKY muadillerinin neden tercih edilmediğine yönelik teknik ve ekonomik gerekçeler detaylı şekilde açıklanacaktır.

4. Mevcut AKKY’lerin Türkiye’de faaliyet gösteren yazılım firmalarınca ve Türkiye’de istihdam edilen personel tarafından özelleştirilmesi suretiyle geliştirilen yazılımlar da, yazılım lisanslama usulü itibarıyla AKKY lisanslarını kullanmıyor olsa dahi, AKKY geçiş sürecinde değerlendirmeye alınacaktır. Bu nitelikteki yazılımlar teknik ve mali açılarından ilgili kamu kurum ve kuruluşunun ihtiyacını karşılıyorsa, uygun nitelikte AKKY ürünü bulunmaması durumunda ticari lisanslı yazılımlara tercih edilecektir.

Bilgilerini ve gereğini rica ederim.

28 Temmuz 2023

Recep Tayyip ERDOĞAN
CUMHURBAŞKANI

epati



Antikor ZTSA
Zero Trust Service Access
(Secure Remote Access Gateway
& Next Gen. PAM)

www.epati.com.tr



Antikor ZTSA

Zero Trust Service Access

Genel Tanıtım

Antikor ZTSA, (Zero Trust Service Access) ürünü, agent gerektirmeyen, tarayıcı tabanlı SSL portundan çalışan bir ZTSA platformudur. Kullanıcılara RDP, SSH, VNC, Telnet, Kubernetes Console, Remote Web Browsing, SafeBrowsing / Web Sandbox, File Browser gibi servislere doğrudan erişim vermeden, yalnızca ekran ve kullanıcı etkileşimlerini taşıyarak yüksek güvenli ve düşük riskli bağlantılar sağlayan Yeni Nesil PAM ürünüdür.

Zero Trust Service Access (ZTSA) Nedir?

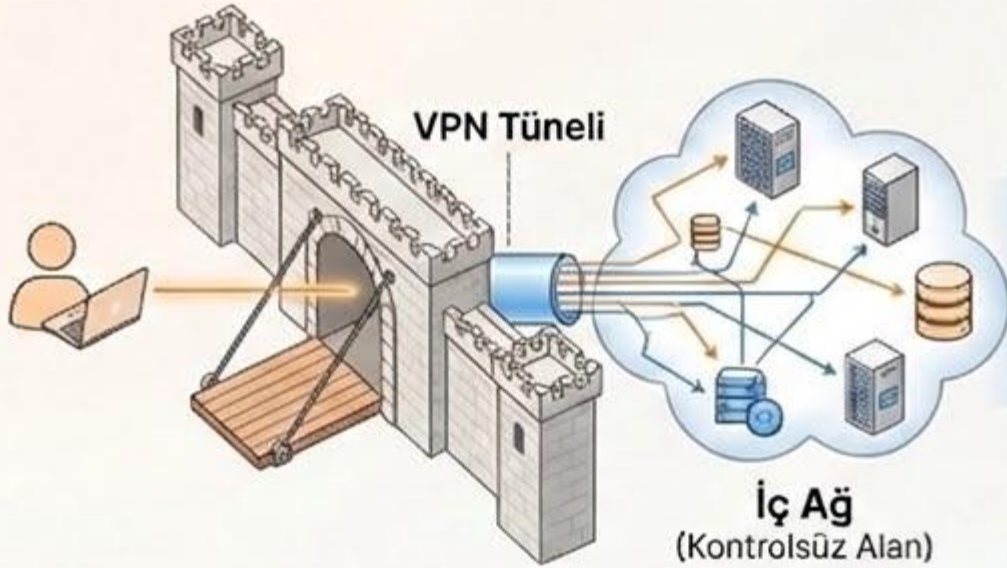
ZTSA (Zero Trust Service Access), “Sıfır Güven” yaklaşımına dayalı bir erişim güvenliği modelidir. Bu modelde, ağdaki hiçbir kullanıcıya ya da cihaza önceden güvenilmez. Her erişim isteği kimlik doğrulama ve yetkilendirme süzgecinden geçtikten sonra izin verilir. Kısaca “Asla güvenme, her zaman doğrula.” mantığındadır.

Ürün Mimarisi

Virtual Appliance (VMWare ESXi / vSphere, Microsoft Hyper-V, Proxmox, KVM Tabanlı Hipervizörler) olarak pazara sunulmuştur ve Tüm Güvenlik Duvarları ile tam uyumludur. Kurum içi sistemlere uzaktan erişimi tamamen yeni bir yaklaşımla sunar. Geleneksel VPN’lerin aksine, kullanıcıların sunucuya doğrudan erişmesine izin vermez. Bu sayede güvenlik açıklarını sıfıra indirir.

Ağ Güvenliğinde Yeni Dönem: Sınırdan “Sıfır Güven”e (Zero Trust) Geçiş

Geleneksel Yaklaşım (VPN Odaklı)



- Sadece ağ sınırlarını korur.
- Kapılar sonuna kadar açılır.
- Kullanıcı doğrudan sisteme dahil olur.
- **RISK:** İçerideki hareketler sorgulanmaz.



Antikor ZTSA (Sıfır Güven Mimarisi)



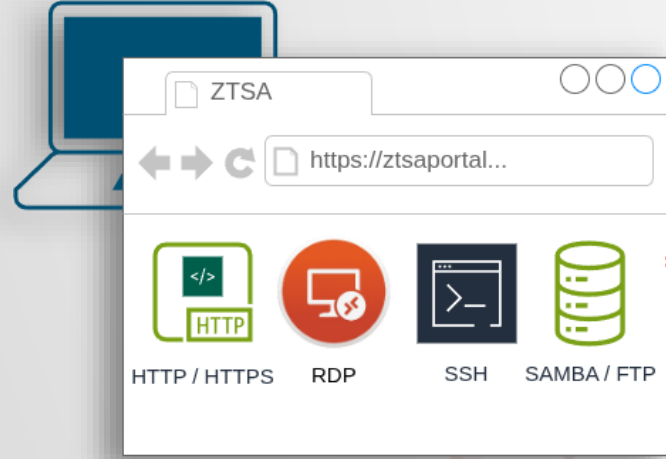
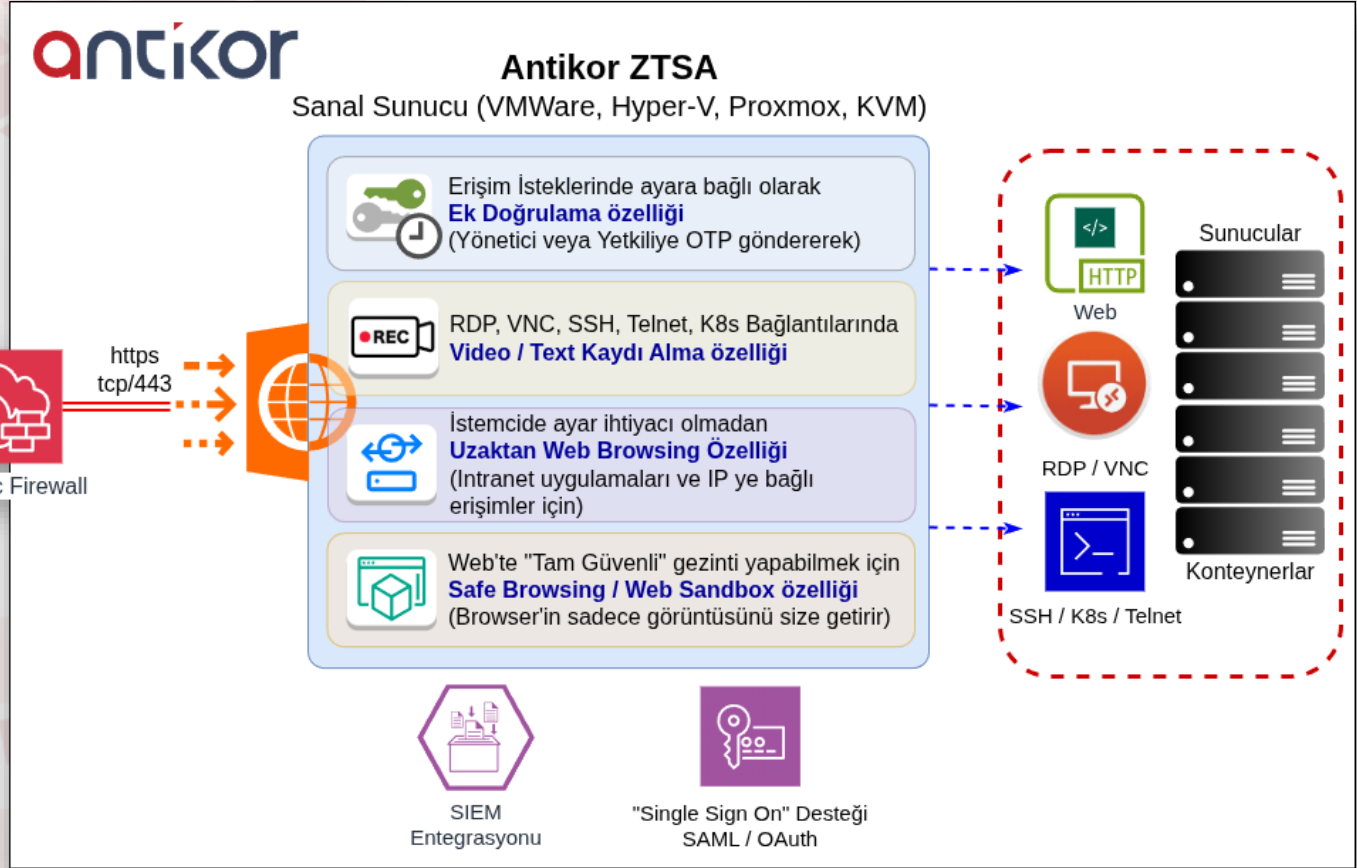
- Ağ içindeki her hareket sorgulanır.
- Saldırı yüzeyi minimuma indirilir.
- Kullanıcı asla doğrudan sisteme dahil olmaz.
- **AVANTAJ:** Hibrit ve Yeni Nesil Erişim Çözümü.

“Asla Güvenme, Her Zaman Doğrula” Prensibi ile Bütünleşik Güvenlik.



Antikor ZTSA

Zero Trust Service Access

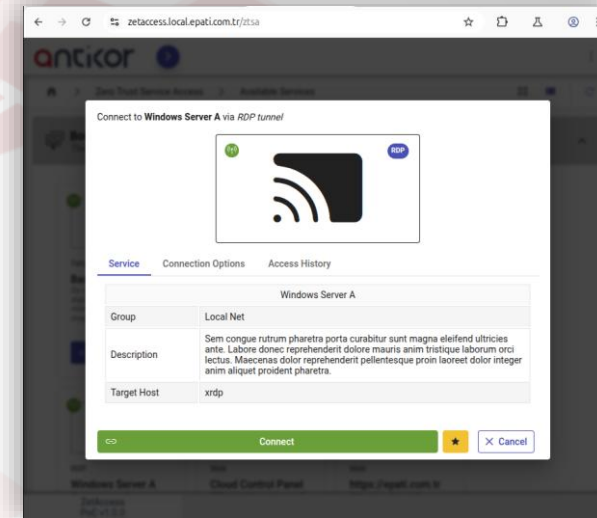




Antikor ZTSA Zero Trust Service Access

Desteklenen Servisler

- Ayarsız, Ajansız Web Proxy (http / https)
- RDP - Remote Desktop Protocol
 - Güvenli Dosya Paylaşımı
 - Ses, Pano ve Yazıcı Paylaşımı
 - Initial Program belirleyebilme
- SSH - Secure Shell
 - Password & Public Key Authentication
- Uzaktan Kontrol Verebilme Özellikli Ekran Paylaşımı
- VNC (Virtual Network Computing)
- K8s - Kubernetes Console
- Telnet
- Remote Web Browsing (İnterneti uzaktan ve güvenli şekilde gezin)
- Safebrowsing / Web Sandbox (Tarayıcıyı izole ortamda aç, risk almadan incele)
- Ekran Paylaşımı (Link ile Uzaktan Kontrol Erişimi)
- Agent (Windows, Mac OS, Linux Destekli) ile Proxy Erişimi
- File Browser (FTP, SMB/CIFS, SFTP, WebDAV, SCP, AWS S3 Uyumlu Storgelar, Google Drive Entegrasyonu)
- Wake on LAN desteği
- Aktif Oturuma Katılma: Ekran İzleme / Yönetme (Birden fazla kişi)





Antikor ZTSA

Zero Trust Service Access

Erişim Denetimi Özellikleri

- Servis, Grup, Kullanıcı ve Rol bazlı Erişim Denetimi
- Erişim izni bitiş tarihi kontrolü
- Belirli günlerde erişim izni sağlama
- Belirli saatler erişim izni sağlama
- Ek Onaylama (Sponsorlu) ile Bağlantı Güvenliği
 - OTP'yi Yetkili bir kullanıcıya gönderilmesi ve
 - Yetkilinin onayı ile bağlantı kurulabilmesi sağlanır.

Güvenlik Özellikleri

- Kriptolu Kimlik Bilgileri (Credentials) Saklama
- Dosya Alışverişi Güvenliği
 - ACL tabanlı, Antivirüs Taraması Desteği
 - İsteğe bağlı Sandbox API Entegrasyonu
- İstemci - RDP drive share izolasyonu
- RDP ve VNC de Oturum Kaydı Alma
 - Ekran Video kaydı
 - SSH, Telnet, K8s için Text Ekran Kaydı
- Kriptolu Kimlik Bilgileri (Credentials) Saklama
 - Oturum Başlangıç ve Bitiş Logları

Entegrasyon Özellikleri

- SIEM / Syslog Entegrasyonu
 - CEF, JSON Formatları
- Audit Log Entegrasyonu
- Harici Sandbox Entegrasyonu
- Harici Antivirüs Entegrasyonu

Kimlik Doğrulama Yöntemleri

- Yerel Kullanıcı
- Single Sign On
 - SAML2.0
 - OAuth2.0
 - OpenID Connect
- RADIUS - MFA ve Challenge Destekli
- LDAP / Active Directory
- MFA - Çok Faktörlü Kimlik Doğrulama (OTP, TOTP)



Antikor ZTSA

Zero Trust Service Access

Yönetim Arayüzü Özellikleri

- HTML5 Responsive Web Arayüzü
- Olay Bildirim Altyapısı
 - SMS, E-posta, Tarayıcı Bildirimi, Webhook
- Erişim Loglama
- Kişiyeye özel Favori Servisler
- Yetkiye Bağlı Kongürasyon Ezme Desteęi
- Light / Dark Modu Desteęi
- Grid / List Görünüm Desteęi
- Servis Gruplama Desteęi
- Erişim Talep Yönetimi Modülü
- Hızlı Arama Modülü
- Raporlama Modülü
- Yetki Yönetimi

Ölçeklenebilirlik

Antikor zetAccess, Kubernetes ve Docker Swarm gibi modern konteyner orkestrasyon mimarileriyle uyumlu olarak tasarlanmıştır. Bu sayede sistem, yoğun kullanıcı yükü altında dahi **yatayda otomatik olarak ölçeklenebilir**.

Altyapının sunduęu kaynaklara baęlı olarak, sistem eş zamanda binlerce kişiyi kesintisiz ve sorunsuz şekilde yönetebilir ve servisler baęlayabilir. Mevcut sanallaştırma, Kubernetes veya Docker Swarm altyapılarına entegre çalışabildięinden, kurumların ek bir donanım yatırımı yapmasına gerek kalmaz.

Yüksek Erişilebilirlik (High Availability) için hem kimlik doğrulama servisleri hem de kullanıcılara sunduęu servisleri, yük dengeleme (Load Balancing) ve failover mekanizmaları ile yönetilir. Bu yapı sayesinde servis süreklilięi garanti altına alınır.



Antikor ZTSA

Zero Trust Service Access

Öne Çıkan Avantajları

- Yüksek Güvenlik — Zero Trust Mimarisi: Kullanıcılara sistemlere doğrudan erişim verilmez. Sadece ekran görüntüsü ve giriş etkileşimleri taşınır. Böylece saldırı yüzeyi en aza indirilir.
- Tarayıcı Üzerinden Erişim — Kurulumsuz Kullanım: Kullanıcı tarafında herhangi bir yazılım veya agent kurulumu gerekmez. Sadece bir web tarayıcısı ile RDP, SSH, VNC, Telnet ve daha fazlasına anında erişim sağlanır.
- VPN'siz Güvenli Alternatif: Antikor ZTSA, VPN'lere kıyasla daha güvenli ve yönetimi kolay bir alternatiftir. Bunun yerine istenirse kendi Agent'i ile bağlantı kurar.
- Gelişmiş Kimlik Doğrulama — SSO Desteği: Mevcut kurumsal kullanıcı hesaplarıyla entegrasyon sağlar: SAML 2.0, OAuth 2.0, OpenID Connect ile güvenli ve tek tıkla oturum açma.
- Kaynak Bazlı Yetkilendirme: Her kullanıcı yalnızca yetkili olduğu sistemleri görebilir ve erişebilir. Erişim kontrolü merkezi panelden kolayca yönetilir.
- Kayıt ve Denetim Mekanizması: Tüm oturumlar izlenebilir ve denetlenebilir. Giriş-çıkış, erişim kayıtları ve sistem davranışları geriye dönük analiz edilebilir.
- Hızlı Kurulum, Kolay Yönetim: Sistemi dakikalar içinde devreye alabilir, tüm erişimleri merkezi olarak yönetebilirsiniz. BT ekipleri için büyük operasyonel kolaylık.
- Esnek Entegrasyon: Farklı veri merkezleri, kimlik sağlayıcılar ve güvenlik çözümleriyle kolayca entegre olur. Mevcut altyapınızı değiştirmeye gerek kalmaz.
- Uzaktan Çalışma için İdeal: Şirket dışından çalışan personelinize güvenli, sınırlı ve izlenebilir erişim sunar. Lokasyon bağımsız çalışmayı güvence altına alır.



Antikor ZTSA

Zero Trust Service Access

Örnek Kullanım Senaryosu

Kampüs Dışından Güvenli, Kurulumsuz ve Denetlenebilir Erişim

Senaryo: Üniversite veya bağlı bir hastanede; Web of Science, Scopus, YÖK Tez, EBYS gibi uygulamalar sadece kampüs içinden erişilebilir. Ancak ihtiyaçlar kampüs dışına taşar.

Akademisyenler için — Kurulumsuz ve Güvenli Erişim

- Akademik kaynaklara (TRDizin, Scopus vb.) güvenli uzaktan erişim
- Kurumsal SSO ile tek tıkla giriş
- Ek şifre veya kurulum gerekmez
- BT desteği azalır, kullanıcı deneyimi artar

Dış Firmalara Verilen RDP Erişimi

- Dış destek erişimleri VPN'siz sağlanır
- Erişim sadece ilgili sisteme verilir
- Tarayıcı tabanlı, güvenli ve izlenebilir

Ağ Cihazlarına (Switch, AP, Güvenlik Duvarı) SSH ve Web Erişimleri

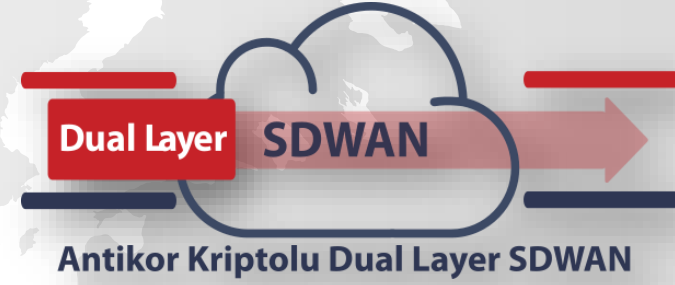
- Sadece yetkili cihazlara erişim tanımı
- SSH ve Web arayüzlerine tarayıcı üzerinden erişim
- Kayıtlı, güvenli ve sınırlandırılmış bağlantı
- Cihaza doğrudan bağlantı yok — saldırı yüzeyi sınırlanır



Antikor ZTSA

Zero Trust Service Access

Özellik	Antikor ZTSA (Yeni Nesil PAM)	PAM (Klasik PAM)
Amaç	Tüm erişimleri kimlik, bağlam ve ilkeye dayalı olarak doğrulayıp mikrosegmente çalışır.	Ayrıcalıklı hesapların güvenliğini sağlamak, yönetmek ve izlemek.
Kullanıcı Profili	Tüm kullanıcılar (çalışanlar, yükleniciler, dış partnerler, IoT, servis hesapları vb.)	Yalnızca ayrıcalıklı kullanıcılar (sistem yöneticileri, root, domain admin, DBA vb.)
Erişim Şekli	Uygulama/servis odaklı, genelde ajan gerektirmeyen, tarayıcı üzerinden erişim	Genelde aracı (agent, vault, proxy, jump host) üzerinden erişim
Kayıt Tutma Farkı	<ul style="list-style-type: none">Erişim loglarıKimlik ve lokasyonSession recording / Text recording	<ul style="list-style-type: none">Session recordingKomut geçmişiEkran görüntüleri
Dinlediği Port	Sadece tek porttan hizmet verir. (443 SSL gibi)	Tüm Portları açmak gerekir.
Bulut ve SaaS Desteği	Çok uygundur	Genellikle veri merkezleri ve şirket içi sistemler içindir, bulut desteği sonradan eklenmiştir
Entegrasyon	SIEM, SSO, MFA, LDAP, Active Directory, RADIUS, zaman gibi faktörlerle erişim kontrolü	LDAP, Active Directory, SIEM, ticketing sistemleri ile entegredir.
Dosya Transferi ve Denetimler	ACL tabanlı, Web Browsing, Virüs taraması desteği, Sandbox Entegrasyonu desteği vardır	Yok



Teşekkürler

epati

ePati Siber Güvenlik A.Ş.

www.epati.com.tr