



CyberArts™

Her ne yaparsak yapalım
içinde “sanat” hep var olacak.

CyberArts Siber Güvenlik Ürünleri

Değerli kurum yetkilisi;

CyberArts’a göstermiş olduğunuz ilgiye ve duyduğunuz güvene teşekkür ederiz.
Görüşmelerimiz neticesinde Siber Güvenlik Çözüm Önerileri dökümanımızı bilginize sunuyoruz.
Lütfen tüm sorularınız için bizimle temasa geçmekten çekinmeyiniz.

Saygılarımızla,

CYBERARTS FELSEFESİ

Söz konusu siber hizmetler olduğunda, tüm kurumlar her şeyin en iyisini talep eder ve her şeyin en iyisini de hak eder. Siber dünyadaki tecrübelerimizi, sanatçı hassasiyeti ve titizliği ile çalışan diğer kurum ve kişilerle bir araya gelerek, sıradanlık değil sanat talep eden kurumların hizmetine sunuyoruz. Her ne yaparsak yapalım içinde “sanat” hep var olacak. CyberArts olarak bu bizim sözümüz.

SİBER GÜVENLİK SANATLARI

CyberArts olarak sanatsal dokunuşları olan teknolojileri, kurumları ve hizmetleri titizlikle seçiyor ve uçtan uca tamamlayıcı bir portföy sunuyoruz. ISO27001, ISO27701, NIST, GDPR, KVKK ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi çerçevelerine uyumu gözeterek, sizinle belirlediğimiz kapsamda, siber güvenlik operasyonlarınızı sizin için yönetiyoruz.

İçindekiler Tablosu

Acalvio ShadowPlex (Deception)	5
Arvis (Biometric Doğrulama).....	6
BeamSec PhisPro (Phising Simulation)	7
Binalyze (Digital Forensic - IR).....	8
Black Duck (Application Security)	9
C-Prot (Mobile Security)	10
CloudFlare Magic Transit (DDoS Protection)	11
Cloudflare ZTNA (Zero Trust Network Access)	12
CrowdStrike Falcon (EDR)	13
CyberWhiz Mobile	14
DNSQ (DNS Security).....	15
FastNAC (Network Access Control - NAC).....	16
FsProtect - Forestall (Active Directory Security).....	17
ICSFusion (OT/ICS Security – Visibility – Threat Detection – Asset Management)	18
Infoblox (DNS Security).....	19
LogRhythm - Exabeam (SIEM & XDR)	20
LogSign (SIEM)	21
LogSign (SOAR).....	22
Mirket Security (MFA- IAM-SSO-Passwordless - ITDR).....	23
Neox Network (Network Visibility Platform)	24
Netscout Arbor (DDoS Protection)	25
Netscout DPI	26
Netwrix (DLP)	27
Nozomi Networks (OT Visibility).....	28
OPSWAT (Data Sanitization)	29
Picus Security (Brige Attack Simullation)	30
Proudsec Cyber Threat Intellgence.....	31
Sceptive BLock (APT/Proactive Threat Intelligence).....	32
SelfHack AI (Penetration Testing Platform)	33
TR7 Application Security Platform (ASP)	34
Vectra AI (NDR).....	35
Veriskop (Veri Keşfi / Veri Sınıflandırma / Veri Maskeleye).....	36
Wallarm (API Security).....	37
Xage Security (IT/OT Identity & Access Managment / PAM)	38
Zscaler AI Security	39

Zscaler (SASE - ZTNA)	40
Fortinet	41
• FortiAnalyzer	41
• FortiAP	41
• FortiAuthenticator	41
• FortiDeceptor	41
• FortiEDR	41
• FortiGateFirewall	41
• Forti Isolator	41
• FortiMail	42
• FortiManager	42
• FortiNac	42
• FortiSandbox	42
• FortiSwitch	42
• SD Branch	42
• FortiNDR	42
• FortiWeb	43
• Fortirecon – CTI	43
• FortiSIEM	43
F5 43	
• BIG-IP Advanced WAF	43
• BIG-IP Local Traffic Manager	43
• BIG-IP DDoS Hybrid Defender	43
• BIG-IP Access Policy Manager	44
• BIG-IP Advanced Firewall Manager	44
• BIG-IP DNS	44
ARISTA 44	
• Backbone Switch	44
• Edge Switch	44
• CloudVision CUE	44
• CloudVision Portal	45
ivanti 45	
• SSL VPN	45
• NAC	45

CITRIX 45

- Citrix Virtual Apps and Desktops..... 45

AUTHTAKE..... 45

- Passwordless Authentication 45
- Single Sign-On (SSO)..... 46

Opinnate NSPM (Network Security Policy Management) 46

- Opinnate 46

CAST DdoS..... 46

- Cast DDoS..... 46
- DDos Saldırı Testi 46

A10 Networks 46

- Thunder Advanced WAF 46
- Thunder ADC (Application Delivery Controller) 47
- Thunder TPS (Threat Protection System)..... 47
- A10 Secure Access (Application Access Control) 47
- Thunder Firewall (CFW - Convergent Firewall) 47
- A10 DNS (Thunder DNS / GSLB) 47

Acalvio ShadowPlex (Deception)

Acalvio ShadowPlex, modern siber tehditleri erken aşamada tespit etmek için gelişmiş deception (aldatma) teknolojisini kullanan yapay zeka destekli bir siber güvenlik platformudur.

Gerçek ortamlardan ayırt edilemeyen sahte varlıklar, kimlik bilgileri ve etkileşim noktaları oluşturarak saldırganları aktif olarak yanıltır; böylece keşif, kimlik bilgisinin kötüye kullanımı, içeriden gelen saldırılar ve yanal hareket gibi saldırı adımlarını daha gerçekleştiren tespit eder.

Bu yaklaşımı sayesinde, saldırıları yayılmadan önce ortaya çıkarır ve güvenlik ekiplerine hızlı ve doğru müdahale imkanı sunar.

Ana Özellikleri

- **Deception Technology** - Gerçek sistemlerle birebir uyumlu sahte varlıklar oluşturarak saldırganları yanıltır.
- **Shadow Assets** - Gerçek sistemlere benzeyen tuzak sistemler oluşturma (OT/IT/IoT cihazları, credentiallar ve veri gibi)
- **Active Directory Deception** - AD ortamında sahte ancak gerçekçi kimlik bilgileri ve erişim izleri oluşturarak credential tabanlı saldırıları erken aşamada tespit eder.
- **Active Directory Atak Yüzeyi Tespiti**
- **Erken Aşama Tehdit Tespiti (Early Threat Detection)** - Tuzaklara yapılan her erişimi yüksek doğrulukla anında tespit eder.
- **Attack Path Visibility** - Saldırganın ağ içindeki hareketlerini ve ilerleme yollarını net şekilde ortaya çıkarır.
- **Entegrasyonlar** - SIEM, SOAR, EDR, AD gibi sistemlerle ile entegrasyon.
- Threat Intelligence – Tespit edilen saldırıların detaylı analizi ve raporlanması.

Sağladığı Katma Değer

- Yapay Zekası sayesinde operasyonel süreçlerin hızlandırılması.
- Saldırıların çok erken aşamada tespiti.
- False-positive oranının minimuma inmesi. (%100'e yakın doğruluk)
- Saldırgan davranışlarının net şekilde analiz edilmesi.
- SOC ekiplerinin daha hızlı aksiyon alması.
- Yapay Zekası sayesinde olay korelasyonu.
- Olay korelasyonu ile birlikte SOC alarm yorgunluğunun minimuma düşürülmesi.
- Saldırı yüzeyinin görünür hale gelmesi.
- Agentsız mimari ile footprint bırakmayan mimari (endpoint dağıtımı dahil)
- APT ve iç tehditlere karşı etkili koruma.
- Active Directory atak yüzeyi çıkartma.
- Active Directory üzerinden gelen atakları tespit etme kabiliyeti.
- Mevcut güvenlik çözümleri ile kolay entegrasyon.

[Tanıtım Broşürü](#)

Arvis (Biometric Doğrulama)

Arvis Biometric Doğrulama, kurumların kullanıcı kimliklerini yüz tanıma, parmak izi, ses tanıma ve davranışsal biyometri gibi gelişmiş doğrulama yöntemleriyle güvence altına alan modern bir biyometrik kimlik doğrulama platformudur. Çözüm, hem güvenlik hem kullanıcı deneyimini artırarak parolasız ve güvenli erişim modelleri sunar.

Ana Özellikleri

- Yüz Tanıma – Yapay zeka destekli hızlı ve yüksek doğrulukta kimlik doğrulama.
- Parmak İzi Doğrulama – Donanım güvenlik modülleriyle güvenli biyometrik doğrulama.
- Ses Tanıma – Kullanıcıya özel ses deseni ile kimlik doğrulama.
- Davranışsal Biyometri – Kullanıcının cihaz kullanım alışkanlıklarını analiz ederek ek güvenlik katmanı sağlar.
- Liveness Detection – Fotoğraf, video veya maske kullanarak yapılan sahte girişimleri engeller.
- Entegrasyon Modülü – IAM, SSO, mobil uygulamalar ve mevcut kurumsal sistemlerle entegrasyon.

Sağladığı Katma Değer

- Parolasız kimlik doğrulama ile kullanıcı deneyimini iyileştirme.
- Yapay zeka destekli biyometrik analiz ile sahtecilik girişimlerinin engellenmesi.
- Regülasyon uyumluluğu (KVKK, GDPR) ve güvenli veri işleme.
- Entegrasyon yetenekleri ile mevcut sistemlere kolay uyum.
- Kimlik doğrulama süreçlerinde hem hız hem güvenlik artışı.
- Çok faktörlü doğrulama için biyometri destekli güçlü ek katman.

[Tanıtım Broşürü](#)

BeamSec PhisPro (Phishing Simulation)

BeamSec PhishPro, kurumların çalışanlarını gerçekçi ortalama (phishing) saldırılarına karşı bilinçlendirmek ve kurumsal güvenlik farkındalığını artırmak için tasarlanmış gelişmiş bir phishing simülasyon ve eğitim platformudur. PhishPro, kurum içi kullanıcıların zafiyetlerini tespit eder, davranışlarını analiz eder ve hedefe yönelik eğitimler sunarak sosyal mühendislik risklerini minimuma indirir.

Ana Özellikler

- Gerçekçi Phishing Simülasyonları – Gerçek saldırı teknikleriyle hazırlanmış hazır senaryolar veya özel tasarım şablonlar.
- Risk Analizi ve Raporlama – Kullanıcı davranışlarının detaylı analizi ve risk puanlaması.
- Otomatik Mikro Eğitimler – Kullanıcıların hatalarına göre atanan kısa, hedefe yönelik farkındalık eğitimleri.
- Spear Phishing ve Whaling Senaryoları – Yönetici seviyesini hedef alan özel saldırı simülasyonları.
- Kampanya Yönetimi – Farklı ekipler için zamanlanabilir ve tekrarlanabilir phishing kampanyaları.
- LMS / Active Directory Entegrasyonu – Kullanıcı yönetimi ve raporlama entegrasyonları.

Sağladığı Katma Değer

- Phishing saldırılarına karşı kurumsal güvenlik farkındalığını artırma.
- Kullanıcı hatalarından kaynaklanan veri sızıntı risklerinin azaltılması.
- Gerçek zamanlı davranış takibi ile çalışan bazlı risk skoru oluşturma.
- Sürekli farkındalık eğitimi ile çalışan güvenliğini güçlendirme.
- Düzenli kampanyalar ile kurumsal sosyal mühendislik olgunluğunu artırma.
- Uyumluluk (KVKK, ISO 27001, PCI) süreçlerine destek.

[Tanıtım Broşürü](#)

Binalyze (Digital Forensic - IR)

Gerçek zamanlı dijital adli analiz ve olay müdahale süreçlerinin yanı sıra *compromise assessment* yeteneğiyle tehdit tespitini hızlandıran kapsamlı bir DFIR ve IR otomasyon platformudur. Açık, kapalı ve uç nokta kaynaklı verileri hızla toplayarak olay müdahale ekiplerine dakikalar içinde derinlemesine analiz imkânı sunar.

Ana Özellikler

- Hız: Manuel toplama işlemlerini saatlerden dakikalara indirir.
- Kapsam: 400+ artefact (delil) tipi ile sektördeki en geniş toplama kapasitesine sahiptir.
- Konsolidasyon: Tek panelden tüm endpoint'lerin durumunu izleme ve analiz etme imkânı.
- Entegrasyon: Mevcut SOC / IR altyapısına kolayca entegre olur.
- Uyumluluk: ISO 27001, NIST, MITRE ATT&CK gibi standartlarla uyumlu raporlama ve 7545 sayılı siber güvenlik kanunu uygunluğu.

Sağladığı Katma Değer

- Dakikalar içinde olay müdahalesi
- Tam görünürlük: tüm uç noktaları tek ekrandan analiz
- Zaman tasarrufu ve operasyonel verimlilik
- Uyumluluk ve denetim kolaylığı
- SOC ve IR ekipleri arasında iş birliği
- Delil bütünlüğü ve zincirleme raporlama (chain of custody)

[Tanıtım Broşürü](#)

Black Duck (Application Security)

Açık kaynak bileşenlerini analiz ederek lisans, güvenlik ve uyumluluk risklerini yöneten gelişmiş bir SCA (Software Composition Analysis) çözümüdür. CI/CD süreçlerine entegre olarak geliştiricilere güvenli kodlama için gerçek zamanlı bildirimler ve otomatik risk raporlaması sunar.

Ana Özellikler

- **Statik Kod Analizi (SAST):** Kodun yazım aşamasında güvenlik açıklarını tespit eder.
- **Dinamik Uygulama Güvenliği Testi (DAST):** Çalışan uygulamalarda güvenlik açıklarını bulur.
- **İnteraktif Uygulama Güvenliği Testi (IAST):** Statik ve dinamik testlerin avantajlarını birleştirir.
- **Yazılım Bileşim Analizi (SCA):** Açık kaynaklı bileşenlerin güvenliğini kontrol eder.
- **Software Risk Manager (SRM):** Uygulama güvenliği test araçlarının (AST) düzenlenmesine, sorunları önceliklendirmesine ve yazılım varlıkları üzerindeki uyumu izlemesine olanak tanır.

Sağladığı Katma Değer

- Açık kaynak zafiyetlerinin erken aşamada tespiti ve giderilmesi.
- Güvenli yazılım geliştirme (SSDLC) süreçlerine güçlü entegrasyon.
- Lisans uyumsuzluklarından kaynaklanan hukuki risklerin azaltılması.
- CI/CD süreçlerinde otomatik güvenlik kontrolleri.
- Kapsamlı SBOM (Software Bill of Materials) üretimi.
- Tedarik zinciri güvenliğini artırma.

[Tanıtım Broşürü](#)

C-Prot Mobile Security, kurumların mobil cihazlarını zararlı yazılımlar, kimlik avı saldırıları, ağ tehditleri ve veri sızıntı risklerine karşı korumak için geliştirilmiş kapsamlı bir mobil güvenlik çözümüdür. Hem kurumsal hem de BYOD cihazlarda güvenli kullanım sağlayarak mobil saldırılara karşı çok katmanlı koruma sunar.

Ana Özellikler

- Mobil Zararlı Yazılım Tespiti – Kötü amaçlı uygulama, trojan, spyware ve ransomware algılama.
- Phishing Koruması – SMS, e-posta ve uygulama içi phishing girişimlerini engelleme.
- Ağ Güvenliği – Güvensiz Wi-Fi ağlarının tespiti ve koruma sağlama.
- Uygulama Güvenliği – Riskli izinler, şüpheli davranışlar ve uygulama açıklarını analiz etme.
- Cihaz Yapılandırma Yönetimi – Cihaz güvenlik ayarlarının politika uyumluluğunu kontrol etme.
- Mobil Veri Koruması – Veri sızıntısı risklerini tespit etme ve önleme.
- MDM/EMM Entegrasyonu – Kurumsal mobil cihaz yönetim platformlarıyla sorunsuz entegrasyon.

Sağladığı Katma Değer

- Mobil cihazlardan kaynaklanan siber risklerin azaltılması.
- Kurumsal verilere uzaktan erişim sağlarken güvenlik seviyesinin artırılması.
- BYOD ortamlarında güvenli çalışma imkânı.
- Regülasyon ve uyumluluk gereksinimlerinin desteklenmesi (KVKK, ISO 27001 vb.).
- Kötü amaçlı uygulamalara ve bağlantılara karşı sürekli koruma.
- Mobil güvenlik görünürlüğü ve merkezi yönetim sayesinde operasyonel verimlilik.

[Tanıtım Broşürü](#)

CloudFlare Magic Transit (DDoS Protection)

Cloudflare Magic Transit, kurumların ađ altyapısını DDoS saldırıları, kötü amaçlı trafik ve performans sorunlarına karşı korumak için tasarlanmış gelişmiş bir ađ güvenliđi ve hızlandırma çözümüdür. Magic Transit, Cloudflare'ın küresel Anycast ađı üzerinden trafiđi yönlendirerek hem güvenlik hem de performans katmanını sağlar.

Ana Özellikler

- DDoS Koruması – Layer 3, 4 ve 7 seviyelerinde yüksek hacimli saldırılara karşı tam koruma.
- Magic Firewall – Ađ trafiđi için gelişmiş paket filtreleme ve kural yönetimi.
- WAN Optimizasyonu – Trafik yönlendirme, paket kaybı azaltma ve gecikme optimizasyonu.
- Anycast Global Network – 320+ veri merkezine sahip küresel altyapı ile düşük gecikme.
- Traffic Acceleration – Trafik performansını artıran Cloudflare optimizasyonları.
- Zero Trust Entegrasyonu – Cloudflare One platformu ile tam güvenlik mimarisi uyumu.

Sađladığı Katma Deđer

- DDoS etkilerini sıfıra indiren global koruma.
- Ađ performansında belirgin iyileşme ve düşük gecikme.
- Ađ katmanında gelişmiş kontrol ve görünürlük.
- Donanım yatırım maliyetlerini azaltan bulut tabanlı mimari.
- Yüksek ölçeklenebilirlik ve anında tehdit hafifletme.
- Magic Firewall ile merkezi trafik yönetimi.

[Tanıtım Broşürü](#)

Cloudflare ZTNA (Zero Trust Network Access)

Kurum içi uygulamalara ve altyapı kaynaklarına erişimi VPN'e ihtiyaç duymadan, her istekte kullanıcı kimliği ve cihaz güvenlik durumu gibi bağlamları doğrulayarak sağlayan modern bir Zero Trust Network Access (ZTNA) çözümüdür.

Cloudflare Access, çalışanlar ve üçüncü taraf kullanıcılar için web, self-hosted, SaaS ve non-web uygulamalara (SSH/RDP gibi) hızlı ve güvenli erişim sunar.

Ana Özellikler

- VPN Replacement / Modern Remote Access – VPN karmaşası olmadan uygulama bazlı erişim.
- Cloudflare Access (ZTNA Gateway) – Self-hosted, SaaS ve non-web uygulamalara erişim kontrolü.
- Granular Policy Enforcement – Her istek için kimlik + cihaz posture kontrolü ile detaylı erişim politikaları.
- Cloudflare Tunnel / WARP Client – Uygulamaları internete açmadan güvenli erişim; kullanıcı tarafında WARP istemcisi ile bağlantı.
- Clientless Access Seçenekleri – Bazı senaryolarda ek istemci gerektirmeden (özellikle web uygulamaları/3rd party erişimi) erişim sağlama imkânı.
- Reusable Access Policies – Tekrarlanabilir ve yönetimi kolay erişim politikaları ile operasyonel hız.
- Third-Party / Contractor Access – Dış kullanıcıları hızlı ve kontrollü şekilde devreye alma.

Sağladığı Katma Değer

- VPN bağımlılığını ortadan kaldırarak saldırı yüzeyini azaltma
- Uygulama bazlı erişim ile “least privilege” yaklaşımını güçlendirme
- Kimlik ve cihaz bağlamı ile her istekte sürekli doğrulama
- Çalışan ve üçüncü taraf erişimlerinde hızlı devreye alma ve kolay ölçeklenebilirlik
- Merkezi politika yönetimi ile operasyonel yükü azaltmaH/RDP gibi) hızlı ve güvenli erişim sunar.

CrowdStrike Falcon (EDR)

CrowdStrike Falcon EDR, uç nokta sistemlerinde gerçekleşen tehditleri gerçek zamanlı olarak tespit eden, davranışsal analiz ve tehdit istihbaratı ile desteklenmiş gelişmiş bir uç nokta tespit ve müdahale (EDR) platformudur. Bulut tabanlı mimarisi sayesinde uç noktalarda minimum ajan kullanarak yüksek görünürlük sağlar ve saldırılara karşı proaktif koruma sunar.

Ana Özellikler

- Gerçek Zamanlı Tehdit Tespiti – Davranışsal analiz ve yapay zeka ile anlık tehdit yakalama.
- Uç Nokta İzolasyonu – Tehdit tespit edildiğinde tek tıkla uç noktayı ağdan izole etme.
- Tehdit Avcılığı (Threat Hunting) – Falcon platformunda gelişmiş IOC/IOA bazlı tehdit araştırması.
- Otomatik Müdahale – Zararlı süreçlerin sonlandırılması, dosya karantinaya alınması gibi aksiyonlar.
- Detaylı Olay Analizi – Saldırının zaman çizelgesi, oluş şekli ve etki kapsamının detaylandırılması.
- Bulut Tabanlı Mimari – Ajan güncellemeleri, veri işleme ve analiz süreçlerinde yüksek performans.

Sağladığı Katma Değer

- Tehditlerin hızlı tespiti ve otomatik müdahale ile riskin azaltılması.
- Gerçek zamanlı uç nokta görünürlüğü ile saldırıların kök neden analizinin hızlanması.
- SOC ekipleri için daha az yanlış pozitif ve daha verimli operasyon.
- Bulut tabanlı mimari sayesinde düşük donanım yükü ve yüksek ölçeklenebilirlik.
- Tehdit istihbaratı entegrasyonları ile saldırı türlerinin daha iyi anlaşılması.
- Uç nokta güvenliği, tehdit avcılığı ve olay analizi için uçtan uca platform yaklaşımı.

[Tanıtım Broşürü](#)

CyberWhiz Mobile

CyberWhiz Mobile, iOS ve Android uygulamalarını tersine mühendislik, kod manipölasyonu, sahte uygulama üretimi ve çalışma zamanı saldırılarına karşı koruyan bir mobil uygulama güvenliği çözümüdür. Uygulamaya entegre edilen güvenlik kütüphaneleri sayesinde uygulamanın çalışma ortamını sürekli kontrol eder; şüpheli cihazları, ağ bağlantılarını ve uygulama üzerinde gerçekleştirilen müdahaleleri tespit eder.

Native iOS ve Android uygulamaların yanı sıra Flutter ve React Native gibi platformları destekler. Güvenlik olayları CyberWhiz Defence Center üzerinden merkezi olarak izlenebilir.

Ana Özellikler

- App Shielding ve Runtime Protection: Uygulamayı çalışma zamanı saldırılarına karşı koruma.
- Root ve Jailbreak Tespiti: Güvenliği değiştirilmiş cihazlarda uygulama çalışmasını kontrol etme.
- Emülatör ve Simülatör Tespiti: Analiz ve otomatik saldırı amacıyla kullanılan sanal ortamları belirleme.
- Uygulama Bütünlük Kontrolü: Kod manipölasyonu, yeniden paketleme ve yetkisiz değişiklikleri tespit etme.
- Anti-Debugging ve Hooking Tespiti: Debugger, Frida ve benzeri müdahale yöntemlerine karşı koruma.
- Kod Gizleme: Uygulama kodunun tersine mühendislikle analiz edilmesini zorlaştırma.
- MITM ve Proxy Tespiti: Uygulama ile sunucu arasındaki trafiğe yönelik müdahale girişimlerini belirleme.
- Güvensiz Ağ Tespiti: Riskli Wi-Fi ve ağ ortamlarını tespit etme.
- SBOM ve Zafiyet Yönetimi: Kullanılan yazılım bileşenlerini takip etme, CVE eşleştirme ve yeni zafiyetleri izleme.
- Merkezi İzleme: Mobil uygulama güvenlik olaylarını CyberWhiz Defence Center üzerinden takip etme.
- Hızlı Entegrasyon: Güvenlik kütüphanesini minimum kod ve mimari değişiklikle uygulamaya dahil etme.

Sağladığı Katma Değer

- Mobil uygulamaların tersine mühendislik ve manipölasyon risklerini azaltır.
- Uygulama kodunu ve hassas iş mantığını korur.
- Güvensiz cihaz ve ağ ortamlarından kaynaklanan saldırıları sınırlar.
- Uygulama güvenlik olaylarında merkezi görünürlük sağlar.
- Native ve cross-platform uygulamaları ortak bir güvenlik yaklaşımıyla korur.
- OWASP Mobile Top 10 ve güvenli yazılım geliştirme gereksinimlerini destekler.
- SBOM ve sürekli zafiyet takibiyle yazılım tedarik zinciri görünürlüğünü artırır.
- Avrupa Birliği Siber Dayanıklılık Yasası kapsamındaki güvenlik ve izleme çalışmalarına katkı sağlar.

[Tanıtım Broşürü](#)

DNSQ, kurumların DNS trafiğini analiz ederek zararlı alan adlarını, veri sızıntılarını ve anormal iletişimleri tespit eden bir DNS güvenliği ve görünürlük çözümüdür. DNS katmanında tehditleri erken aşamada yakalayarak ağ güvenliğini güçlendirir.

Ana Özellikler

- DNS Traffic Analysis – DNS sorgularının detaylı analizi
- Threat Detection – Zararlı domain ve C2 iletişim tespiti
- DNS Tunneling Detection – Veri sızıntısı girişimlerinin belirlenmesi
- Real-Time Blocking – Zararlı sorguların anlık engellenmesi
- Reporting & Visibility – DNS tabanlı tehdit görünürlüğü
- Integration – SIEM, SOAR ve güvenlik sistemleri ile entegrasyon

Sağladığı Katma Değer

- DNS katmanında erken tehdit tespiti
- Veri sızıntısı risklerinin azaltılması
- Ağ görünürlüğünün artırılması
- SOC ekipleri için hızlı aksiyon imkanı
- Düşük false-positive oranı
- Regülasyon uyumluluğu desteği

[Tanıtım Broşürü](#)

FastNAC (Network Access Control - NAC)

FastNAC, kurumsal ağlara bağlanan kullanıcı ve cihazların keşfedilmesini, profillenmesini ve güvenlik politikalarına göre ağ erişimlerinin kontrol edilmesini sağlayan yerli Network Access Control (NAC) çözümüdür.

Agent gerektirmeyen mimarisi sayesinde kullanıcı bilgisayarları, mobil cihazlar, IoT ve diğer ağ bileşenlerini merkezi olarak görünür hale getirir. Ağa bağlanan cihazların kimlik ve güvenlik durumlarını değerlendirerek yetkisiz veya güvenlik politikalarına uygun olmayan cihazların erişimini sınırlandırabilir. Dinamik VLAN yönetimi ve ağ segmentasyonu yetenekleriyle Zero Trust yaklaşımının ağ erişim katmanında uygulanmasına katkı sağlar.

Ana Özellikler

- **Agentless NAC:** Uç noktalara agent kurulmasına ihtiyaç duymadan cihaz keşfi ve erişim kontrolü sağlar.
- **Cihaz Keşfi ve Profilleme:** Ağa bağlanan kullanıcı, bilgisayar, mobil ve IoT cihazlarını otomatik olarak keşfeder ve sınıflandırır.
- **Erişim Politikaları:** Kullanıcı, cihaz tipi ve güvenlik durumuna göre ağ erişim politikalarının uygulanmasını sağlar.
- **Endpoint Posture Control:** İşletim sistemi, antivirüs, domain üyeliği ve benzeri güvenlik kriterlerini kontrol ederek erişim kararlarına dahil eder.
- **Dinamik VLAN Yönetimi:** Cihazları belirlenen politikalara göre uygun VLAN'lara otomatik olarak yönlendirebilir.
- **Active Directory Entegrasyonu:** Kullanıcı ve organizasyon birimi (OU) bilgilerine göre erişim politikalarının uygulanmasını destekler.
- **Ağ Görünürlüğü:** Ağ üzerindeki cihazların ve bağlantı durumlarının merkezi olarak takip edilmesini sağlar.
- **Switch Port Yönetimi:** Switch portlarının merkezi olarak izlenmesi ve yönetilmesine olanak tanır.
- **Entegrasyon:** API desteği sayesinde mevcut ağ ve güvenlik altyapılarıyla entegre çalışabilir.

Sağladığı Katma Değer

- Yetkisiz cihazların kurumsal ağa erişiminin kontrol altına alınması
- Ağ üzerindeki tüm cihazların merkezi görünürlüğünün artırılması
- Zero Trust ve ağ segmentasyonu politikalarının desteklenmesi
- Güvenlik durumuna göre dinamik erişim politikalarının uygulanması
- Agent gerektirmeyen yapı sayesinde operasyonel yükün azaltılması
- Mevcut ağ altyapısına kolay entegrasyon
- Yerli NAC alternatifi ile teknolojik bağımsızlığın desteklenmesi

[Tanıtım Broşür](#)

FsProtect - Forestall (Active Directory Security)

Active Directory ortamlarında ayrıcalıklı erişimleri, konfigürasyon zafiyetlerini ve saldırı yüzeyini sürekli izleyerek kimlik altyapısını güvence altına alan bir güvenlik platformudur. Zararlı değişiklikleri anlık olarak tespit ederek saldırı zincirinin Active Directory üzerinden ilerlemesini engelleyen koruyucu kontroller sunar.

Ana Özellikleri

- AD Vulnerability & Configuration Assessment – AD'deki zafiyetleri, yanlış yetkilendirmeleri ve yapılandırma hatalarını tespit eder.
- Adversary Simulation – Saldırgan TTP'lerini (MITRE ATT&CK) taklit ederek gerçek senaryoları simüle eder.
- Hidden Attack Path Detection – Yetki yükseltme ve yanal hareket yollarını keşfeder.
- Threat Detection & Behavioural Analysis – Kullanıcı davranışlarını, veri hareketlerini ve anormal aktiviteleri analiz eder.

Sağladığı Katma Değer

- Erken aşamada AD zafiyetlerinin tespiti ve giderilmesi.
- Saldırı simülasyonları ile mavi takım performansının ölçülmesi (MTTD/MTTR iyileştirme).
- Yetki zinciri ve lateral movement analizleriyle risk görünürlüğü artışı.
- KVKK, GDPR ve ISO 27001 gibi yasal ve standart uyumluluk süreçlerine katkı sağlama.
- Kullanıcı davranış analizi ile gelişmiş tehdit tespiti.

[Tanıtım Broşürü](#)

ICSFusion (OT/ICS Security – Visibility – Threat Detection – Asset Management)

Endüstriyel kontrol sistemleri (ICS) ve OT ortamlarında (SCADA, DCS, PLC, HMI vb.) varlık görünürlüğü sağlayan, ağ trafiğini pasif olarak izleyerek anomali ve tehditleri tespit eden bir OT güvenliği platformudur. Üretim ve kritik altyapı ağlarında operasyonu kesintiye uğratmadan OT varlıklarını envantere çıkarır, riskleri görünür kılar ve OT güvenlik ekiplerinin olaylara hızlı müdahale etmesini destekler.

Ana Özellikler

- OT/ICS Asset Discovery & Inventory – OT varlıklarını otomatik keşfeder, envanter çıkarır (PLC, SCADA, HMI, switch, gateway vb.).
- Passive Network Monitoring – Ağ trafiğini pasif izleyerek operasyonu kesmeden görünürlük sağlar.
- Threat & Anomaly Detection – OT protokollerindeki anormallikleri, şüpheli hareketleri ve potansiyel saldırı davranışlarını tespit eder.
- Risk & Vulnerability Context – Varlık bazlı risk görünürlüğü, kritiklik ve güvenlik durumu analizi sağlar.
- OT Protocol Awareness – Modbus, DNP3, S7, OPC vb. OT protokollerini anlayarak daha doğru tespit/analiz sunar.
- Alerting & Reporting – SOC/OT ekipleri için alarmlar, raporlar ve denetim kayıtları oluşturur.
- SIEM/SOC Entegrasyonu – SIEM’e log/alert aktarımı ile kurumsal SOC süreçlerine entegre olur.
- Segmentation / Network Zoning Desteği – ISA/IEC 62443 yaklaşımıyla zone & conduit kurgusuna destek verir.

Sağladığı Katma Değer

- OT ağlarında tam görünürlük ve envanter (en kritik ihtiyaç)
- Operasyonu kesmeden güvenlik izleme (pasif yaklaşım)
- OT odaklı tehdit tespiti ile erken uyarı ve hızlı müdahale
- Varlık kritikliğine göre risk yönetimi ve önceliklendirme
- IT-SOC ve OT ekipleri arasında ortak görünürlük ve koordinasyon
- Uyumluluk ve denetim süreçlerini destekleme (IEC 62443, NIST, ISO 27001 vb.)

Infoblox (DNS Security)

Infoblox, kurumların ağı altyapısını daha güvenli, yönetilebilir ve görünür hale getirmek için geliştirilmiş lider DNS, DHCP, IP Address Management (DDI) ve DNS tabanlı güvenlik çözümleri sunan bir platformdur. Infoblox, özellikle kritik ağı hizmetlerini modernleştirerek hem performans hem de güvenlik açısından kurumlara üst seviye koruma sağlar.

Ana Özellikler

- DNS, DHCP ve IPAM (DDI) – Kritik ağı hizmetlerinin merkezi yönetimi.
- BloxOne Threat Defense – DNS tabanlı tehdit algılama ve engelleme.
- BloxOne DDI – Bulut tabanlı IP adres yönetimi ve ağı otomasyonu.
- DNS Firewall – Zararlı alan adlarını çözümlemeyi engelleyen güvenlik duvarı.
- Threat Intelligence Enrichment – DNS sorgularının tehdit verisi ile korelasyonu.
- Network Automation – Ağı yapılandırmaları için otomatik iş akışları.
- Hybrid Infrastructure Support – Hem on-prem hem bulut ağları için yönetim.

Sağladığı Katma Değer

- DNS tabanlı tehditlere karşı güçlü koruma.
- Ağı görünürlüğünün artması ve yönetim kolaylığı.
- Otomasyon ile daha az operasyonel hata ve daha hızlı süreçler.
- Bulut, hibrit ve on-prem altyapılarda tutarlı IP yönetimi.
- Regülasyon uyumluluğunu destekleyen gelişmiş loglama ve raporlama.
- Zero Trust mimarilerini destekleyen güvenlik katmanı.

[Tanıtım Broşürü](#)

LogRhythm - Exabeam (SIEM & XDR)

LogRhythm (Exabeam) SIEM, SOAR, FIM, UEBA ve AI çözümlerini tek bir platformda birleştiren, 7.000+ global referansı ile lider bir güvenlik yönetim platformu sağlayıcısıdır. Yapay zeka destekli olay yönetimi, tehdit avcılığı ve güvenlik operasyonlarının otomasyonunu sunar. Platform; kullanıcı ve varlık davranış analizi , tehdit istihbaratı ve otomasyon yetenekleri ile SOC ekiplerinin tehditleri daha hızlı ve doğru şekilde tespit etmesini sağlar.

Ana Özellikler

- SIEM Platformu – Log toplama, korelasyon ve merkezi güvenlik analizi.
- UEBA (Kullanıcı ve Varlık Davranış Analizi) – Kullanıcı ve varlık davranışlarını analiz ederek anomali tespiti.
- SOAR – Olay müdahale süreçlerinin otomasyonu ve playbook yönetimi.
- Threat Intelligence Entegrasyonu – Tehdit verisi ile zenginleştirme ve korelasyon.
- Case Management – Olay yönetimi, analiz ve raporlama.
- Agentic AI – %100 On-prem (offline) yada bulutta çalışabilen AI co-pilot ile analistlerin manuel süreçlerden kurtularak, tehdit araştırması & avcılığı, olay araştırma, olay müdahale, raporlama vb. süreçlerine saniyeler içerisinde yanıt verebilen bir yapay zeka platformu sunar.

Sağladığı Katma Değer

- Gerçek zamanlı tehdit tespiti ve hızlı olay müdahalesi.
- Davranışsal analiz ile bilinmeyen tehditlerin yakalanması.
- SOC operasyonlarının otomasyon ile hızlanması.
- Farklı güvenlik katmanlarının tek platformda birleşmesi.
- Uyumluluk süreçleri için güçlü log yönetimi ve raporlama.
- False-positive oranını azaltan gelişmiş analiz yetenekleri.
- Bütünleşik mimari ile tek bir platformdan yönetim imkanı.
- Limitsiz Multi-Tenancy: Birden fazla organizasyon için merkezi yönetim.
- BigData Altyapısı: Büyük veri kümelerinde hızlı tehdit avcılığı.
- EPS Lisanslama Modeli: Log kayıplarını önleyen esnek lisanslama.
- On-Prem & Cloud Uyumu: Hem geleneksel veri merkezleri hem de bulut ortamlarında AI destekli analiz.

[Tanıtım Broşürü](#)

Logsign SIEM, kurumların güvenlik olaylarını merkezi olarak toplayıp analiz eden, korelasyon kuralları ve davranışsal analizle gerçek zamanlı tehdit tespiti sağlayan bir Güvenlik Bilgi ve Olay Yönetimi platformudur. Platform, SOC ekiplerinin tehditleri daha hızlı tespit edip etkili şekilde müdahale etmesini sağlayan uçtan uca görünürlük sunar.

Ana Özellikler

- Log Yönetimi – Farklı kaynaklardan gelen logların merkezi olarak toplanması, saklanması ve analizi.
- Korelasyon Motoru – Saldırı göstergelerini ilişkilendiren güçlü ve özelleştirilebilir kurallar.
- Davranışsal Analiz (UEBA) – Kullanıcı ve varlık davranışlarını analiz ederek anormal aktiviteleri ortaya çıkarma.
- SOAR Entegrasyonu – Olay yanıt süreçlerini otomatikleştiren playbook ve aksiyon akışları.
- Dashboard & Görselleştirme – Gerçek zamanlı güvenlik görünürlüğü sunan zengin dashboardlar.
- Olay Yönetimi – SOC ekipleri için vaka yönetimi, atama, analiz ve raporlama özellikleri.

Sağladığı Katma Değer

- Gerçek zamanlı tehdit tespiti ve hızlandırılmış olay müdahale süreçleri.
- Tüm güvenlik verilerinin tek platformda birleşmesiyle uçtan uca görünürlük.
- SOC iş yükünü azaltan otomatik aksiyon ve alarm mekanizmaları.
- Regülasyonlara uygun log saklama ve raporlama (KVKK, ISO 27001, PCI-DSS).
- Makine öğrenimi sayesinde bilinmeyen tehditlerin tespiti.
- Kurum yapısına göre özelleştirilebilen dashboard ve korelasyon kuralları.

[Tanıtım Broşürü](#)

Logsign SOAR (Security Orchestration, Automation and Response), güvenlik operasyon merkezlerinin (SOC) olaylara daha hızlı, otomatik ve tutarlı şekilde yanıt verebilmesini sağlayan bir güvenlik otomasyon platformudur. Sistem, manuel müdahale gerektiren güvenlik süreçlerini otomatikleştirerek hem hız hem de operasyonel verimlilik sağlar.

Ana Özellikler

- Playbook Otomasyonu – Hazır veya özelleştirilebilir otomatik müdahale akışları.
- Olay Yönetimi – Vaka yönetimi, görev atama, analiz notları ve zaman çizelgesi.
- Entegrasyon Yönetimi – SIEM, EDR, Sandbox, Firewall vb. platformlarla çift yönlü entegrasyon.
- Threat Intelligence Enrichment – IOC sorgulama ve tehdit verisi zenginleştirme.
- Otomatik Müdahale – IP engelleme, kullanıcı hesabı kilitleme, cihaz izolasyonu vb. aksiyonlar.
- Raporlama ve Dashboard – Olay performansı, playbook işleyişi ve SOC verimliliği için kapsamlı görünürlük.

Sağladığı Katma Değer

- Olay müdahale süresinde (MTTR) ciddi ölçüde azalma.
- SOC ekiplerinin operasyonel iş yükünün düşürülmesi.
- Her olayda tutarlı ve tekrarlanabilir yanıt süreçleri.
- Güvenlik araçlarının tek merkezden orkestrasyonu.
- Uyumluluk süreçleri için otomatik raporlama.
- Olay yönetiminde görünürlüğün ve kontrolün artması.

[Tanıtım Broşürü](#)

Mirket Security (MFA- IAM-SSO-Passwordless - ITDR)

Kullanıcı doğrulama süreçlerini güçlendiren; esnek çok faktörlü kimlik doğrulama (MFA), kurumsal erişim yönetimi (IAM), tekil oturum açma (SSO) ve parolasız kimlik doğrulama (Passwordless) yetenekleriyle **kurumsal erişim güvenliğini artıran modern bir kimlik güvenliği çözümüdür**. Mobil uygulama, OTP, biyometrik doğrulama ve risk bazlı erişim politikalarıyla hem güvenlik hem de kullanım kolaylığı sağlar.

Buna ek olarak Mirket, **ITDR (Identity Threat Detection & Response)** yaklaşımıyla kimlik altyapısına yönelik saldırıları (hesap ele geçirme, anormal oturumlar, ayrıcalık istismarı vb.) **erken tespit eder ve otomatik müdahale mekanizmalarıyla riski minimize eder**. Böylece MFA/IAM katmanı sadece doğrulama değil, aynı zamanda kimlik tehditlerine karşı proaktif bir güvenlik kontrol noktasına dönüşür.

Ana Özellikler

- Multi-Factor Authentication (MFA) – OTP, push notification, cihaz doğrulama ve daha fazlası.
- Passwordless Authentication – Parolasız, güvenli ve hızlı erişim.
- Single Sign-On (SSO) – Tüm kurumsal uygulamalara tek noktadan giriş.
- Identity Threat Protection (ITDR) – Şüpheli oturumları ve kimlik tabanlı saldırıları tespit eden yapay zeka destekli koruma.
- Risk Bazlı Erişim Politikaları – Kullanıcı, cihaz ve oturum bazlı risk skorlamasıyla dinamik doğrulama.
- Automated Response – Riskli oturumları sonlandırma, ek MFA zorunluluğu, erişim engelleme ve hesap kilitleme gibi otomatik aksiyonlar.
- Self-Service Portal – Kullanıcıların kendi hesaplarını yönetebildiği güvenli panel.
- On-Premise Destek – Tüm veriler kurum içinde kalacak şekilde lokal kurulum seçeneği.
- SIEM/SOAR Entegrasyonu – SOC operasyonlarında olayların merkezi izlenmesi ve aksiyon alınmasını destekler.

Sağladığı Katma Değer

- Kimlik tehditlerine karşı proaktif koruma (ITDR ile erken tespit + müdahale)
- Güvenli ve kesintisiz kullanıcı deneyimi
- Kurumsal uygulamalarda merkezi erişim yönetimi
- Verilerin kurum içinde kalmasını sağlayan on-premise mimari
- Parolasız giriş ile kullanıcı hatalarını ve riskleri azaltma
- Hesap ele geçirme (ATO) ve ayrıcalıklı hesap istismarı riskini düşürme
- Uyumluluk gereksinimlerini karşılama (KVKK, ISO 27001 vb.)

[Tanıtım Broşürü](#)

Neox Network (Network Visibility Platform)

Neox Network Visibility Platform, kurumsal ağılarda geçen tüm trafiği görünür hale getirerek güvenlik, ağ operasyonları ve performans ekiplerine merkezi görünürlük sağlayan gelişmiş bir network visibility platformudur. Platform; Network TAP, Packet Broker, Packet Capture, Deep Packet Inspection (DPI), Network Forensics ve NDR yeteneklerini tek çatı altında sunar.

Neox, ağ üzerindeki trafiği TAP veya SPAN noktalarından toplar, Packet Broker ile filtreler ve ilgili güvenlik araçlarına yönlendirir. Toplanan veriler gerçek zamanlı analiz edilerek ağ performansı, anomali, güvenlik olayları ve adli analiz süreçleri için kullanılır.

Ana Özellikler

- Network TAP - Ağ trafiğini kayıpsız şekilde kopyalar.
- Packet Broker - Trafiği filtreler ve ilgili araçlara yönlendirir.
- Deep Packet Inspection (DPI) - Paket seviyesinde analiz sağlar.
- Packet Capture - Geçmişe dönük trafik inceleme imkanı sunar.
- Network Forensics - Olay müdahale ve adli analiz süreçlerini destekler.
- Network Detection and Response (NDR) - Ağ tabanlı tehditleri tespit eder.
- Observability and Monitoring - Ağ performansını gerçek zamanlı izler.

Kuruma Sağladığı Katma Değer

- Ağ üzerinde uçtan uca görünürlük
- Tehditlerin hızlı tespiti
- Olay müdahale süreçlerinin hızlanması
- Ağ performansının optimize edilmesi
- Güvenlik araçlarından maksimum verim alınması
- Merkezi analiz ve raporlama

[Tanıtım Broşürü](#)

Netscout Arbor (DDoS Protection)

Ağ trafiğini derinlemesine analiz eden, yüksek hacimli DDoS saldırılarını tespit eden ve kesintisiz servis sürekliliği sağlayan gelişmiş bir ağ güvenliği çözümüdür. Küresel tehdit istihbaratı desteği ile saldırı trendlerini öngörerek büyük ölçekli ağlarda görünürlük ve koruma sağlar.

Ana Özellikler

- Gerçek Zamanlı DDoS Tespit – Anormal trafik modellerini anlık algılama.
- Otomatik Mitigasyon – Saldırlara saniyeler içinde otomatik tepki verme.
- ATLAS Threat Intelligence – Küresel saldırı veritabanı ile gelişmiş tehdit analizi.
- Uygulama Katmanı Koruması – L7 saldırılarına karşı gelişmiş savunma mekanizmaları.
- Scrubbing Center Entegrasyonu – Zararlı trafik temizlenerek kuruma geri yönlendirilir.
- Hybrid Koruma – Hem on-prem hem de bulut tabanlı koruma mimarilerini destekler.
- Gelişmiş Trafik Analitiği – Saldırı kökeni, tipi ve etki analizleri.

Sağladığı Katma Değer

- Kesintisiz hizmet sürekliliği.
- Global tehdit istihbaratı ile proaktif savunma.
- İş yükü azaltan otomatik koruma mekanizmaları.
- Ağ görünürlüğü ve detaylı saldırı raporlaması.
- Altyapı kapasitesinin korunması ve maliyet optimizasyonu.

[Tanıtım Broşürü](#)

Netscout DPI

NetScout DPI (Deep Packet Inspection), ađ trafiđini paket seviyesinde analiz ederek uygulama g r n rl đ , performans izleme ve g venlik analitiđi sađlayan geliřmiř bir ađ g r n rl k     m   r. Ger ek zamanlı trafik analizi sayesinde hem performans sorunlarını hem de g venlik tehditlerini tespit etmeye yardımcı olur.

Ana  zellikler

- Deep Packet Inspection (DPI) – Paket seviyesinde detaylı trafik analizi.
- Application Visibility – Uygulama bazlı trafik g r n rl đ  ve sınıflandırma.
- Real-Time Traffic Monitoring – Ger ek zamanlı ađ izleme.
- Encrypted Traffic Analysis – řifreli trafiđin davranıřsal analizi.
- Anomaly Detection – Olađandıřı trafik ve davranıř tespiti.
- Performance Monitoring – Ađ ve uygulama performans analizi.
- Capacity Planning – Trafik eđilimlerine g re kapasite planlama desteđi.
- DDoS Detection Support – Anormal trafik artıřlarının erken tespiti.
- SIEM / SOC Entegrasyonu – Log ve analiz  ıktılarının g venlik sistemlerine aktarımı.

Sađladıđı Katma Deđer

- Ađ  zerinde tam g r n rl k
- Performans ve g venlik olaylarını tek platformda analiz etme
- Servis kesintilerini erken tespit etme
- Anormal trafik ve potansiyel tehditleri g r n r kılma
- Operasyonel verimlilik artıřı
- Kapasite planlamada veri destekli karar alma
- Kurumsal uyumluluk ve denetim s re lerine destek

[Tanıtım Broř r ](#)

Netwrix (DLP)

Netwrix DLP, kurumların hassas verilerini veri sızıntısı, yanlış kullanım ve yetkisiz erişime karşı korumak için geliştirilmiş güçlü bir veri kaybı önleme çözümüdür. Platform; dosya paylaşımları, e-posta trafiği, uç noktalar ve bulut ortamlarında gerçekleşen veri hareketlerini sürekli izleyerek riskli aktiviteleri gerçek zamanlı olarak tespit eder ve otomatik koruma sağlar.

Ana Özellikleri

- Data Discovery – Hassas verilerin dosya sunucuları ve bulut ortamlarında otomatik tespiti.
- Content Inspection – Belgelerdeki PII, PCI, PHI gibi hassas içeriklerin analiz edilmesi.
- Policy Enforcement – DLP politikalarına göre otomatik engelleme, maskeleye veya uyarı oluşturma.
- Endpoint DLP – USB, yazıcı, ekran görüntüsü alma gibi uç nokta veri hareketlerinin kontrolü.
- Email DLP – E-posta yoluyla veri sızıntısının tespiti ve engellenmesi.
- Cloud DLP – Microsoft 365, Google Workspace gibi platformlarda veri koruma.

Sağladığı Katma Değer

- Hassas verilerin nerede olduğunu ve kimler tarafından erişildiğini tam görünürlük.
- Veri sızıntılarına karşı gerçek zamanlı koruma ve otomatik müdahale.
- KVKK, GDPR, PCI-DSS gibi regülasyonlara uyumluluk desteği.
- İç tehditlere ve yanlış kullanıcı davranışlarına karşı güçlü savunma.
- Uç nokta ve bulut ortamlarında bütüncül veri güvenliği.
- Operasyonel verimlilik sağlayan otomatik politika yönetimi.

[Tanıtım Broşürü](#)

Nozomi Networks (OT Visibility)

Nozomi Networks, endüstriyel kontrol sistemleri (ICS), OT (Operational Technology) ve IoT ortamları için gelişmiş görünürlük, tehdit tespiti ve güvenlik sağlayan lider bir siber güvenlik platformudur. Platform; kapsamlı varlık keşfi, derin ağ görünürlüğü, tehdit tespiti, anomali analizi ve risk yönetimi yetenekleri ile operasyonel ortamların güvenliğini uçtan uca güçlendirir. Üretim ve imalat, madencilik, petrol ve gaz, ilaç ve biyoteknoloji, demiryolu, ulaşım, havalimanları, enerji üretim ve dağıtım, sağlık gibi yüksek hassasiyet gerektiren sektörlerde yaygın olarak kullanılmaktadır.

Ana Özellikleri

- **Varlık Keşfi (Asset Discovery)** - OT ve IoT ortamındaki tüm cihazları otomatik olarak tespit eder, zengin ve sürekli güncellenen envanter oluşturur.
- **Pasif ve Güvenli İzleme** - Ağ trafiğini kesintisiz analiz eder, operasyonlara hiçbir etkide bulunmaz.
- **Ağ İzleme ve Protokol Analizi (Network Monitoring)** - Endüstriyel protokoller dahil olmak üzere tüm ağ trafiğini derinlemesine analiz eder.
- **Tehdit Tespiti (Threat Detection)** - Davranışsal analiz ve anomali tespiti ile hem bilinen hem bilinmeyen tehditleri ortaya çıkarır.
- **Zafiyet Yönetimi (Vulnerability Management)** - OT sistemlerdeki zafiyetleri belirler, CVE bazlı analiz ile riskleri önceliklendirir.
- **Yapay Zeka Destekli Analiz** - Varlık sınıflandırma, davranış analizi ve otomatik içgörü üretimi sağlar.
- **Risk Değerlendirme (Risk Assessment)** - Varlık kritikliği, tehditler ve operasyonel etkiye göre çok faktörlü risk skorlama yapar.
- **Kablosuz ve Dağıtık Ortam Görünürlüğü** - Kablolu ve kablosuz varlıkları (Wi-Fi, Bluetooth vb.) tespit eder ve izler.
- **Merkezi Yönetim ve Görselleştirme** - Tüm varlıklar, riskler ve alarmlar tek platformdan izlenir ve raporlanır.
- **Entegrasyon (Integration)** - SIEM, SOAR ve diğer IT/OT güvenlik çözümleri ile sorunsuz entegre olur.

Sağladığı Katma Değer

- **OT ve IoT Ortamlarında Uçtan Uca Görünürlük.** - Sadece bilinen değil, daha önce görünmeyen OT/IoT varlıklarını da ortaya çıkarır.
- **Kritik Altyapılar İçin Kesintisiz Güvenlik Takibi.** - Pasif ve OT uyumlu yaklaşım sayesinde üretim kesintisi riski oluşturmaz.
- **Gelişmiş Tehdit Tespiti (Davranışsal ve İmza Tabanlı)** - Davranış analizi ile bilinmeyen ve hedefli saldırıları erken aşamada ortaya çıkarır, imza tabanlı tespit ile bilinen tehditleri yakalar.
- **Endüstriyel Sistemlerde Güvenli ve Pasif İzleme**
- **Uyumluluk Süreçlerini Kolaylaştırma** - NERC CIP, IEC 62443 ve benzeri standartlara uyumu hızlandırır.
- **Operasyonel Dayanıklılık** - Siber riskleri azaltarak üretim sürekliliğini ve iş güvenliğini artırır.

OPSWAT (Data Sanitization)

OPSWAT, OT ve IT güvenliği alanında dünya çapında lider bir üreticidir. Kritik altyapılar ve yüksek güvenlik gereksinimi olan kurumlar için geliştirilmiş dosya güvenliği platformu ile sayesinde dosya güvenliği sağlar. IT - OT ortamları için, tek yönlü güvenli veri transferi, OT ağ ve varlık yönetimi, endüstriyel güvenlik duvarı, güvenli dosya transferi ve taşınabilir medya güvenliği çözümleri ile zararlı içerik analizi, ağ güvenliği, erişim güvenliği gibi alanlarında çözümler sunan bir siber güvenlik platformudur.

Ana Özellikleri

- MetaDefender Core – Çoklu antivirüs taraması, Deep CDR, Adaptif Sandbox, Proaktif DLP vb. yetenekleri ile gelişmiş dosya güvenliği platformudur.
+30 Çoklu antivirüs motoru ile dosya tarama ve tehdit analizi.
Content Disarm & Reconstruction (Deep CDR) – Dosyalarda içerik silahsızlandırma gerçekleştirerek olası kötü amaçlı etkinlikleri ortadan kaldırır. Sıfıncı gün saldırılarına karşı koruma sağlar.
- MetaDefender Kiosk – USB ve taşınabilir medyalar üzerinden gelen verilerin kontrolü.
- MetaDefender Managed File Transfer – Yönetilen Güvenli Dosya transferi ve depolama.
- MetaDefender IT – OT Access – Cihaz sağlığı kontrolü ve erişim doğrulama.
- OT Security : OT sistemlerinde Ağ ve varlık yönetimi için trafik analizi yaparak gelişmiş görünürlük, izleme, raporlama ve tehdit algılama sağlar.
- Industrial Firewall IDS/IPS (OTFuse): OT Güvenlik duvarıdır. PLC, RTU ya da HMI gibi OT cihazlarına giden trafiği öğrenir kaydeder ve anomali tespit ettiğinde uyarı yaratır ya da ilgili trafiği engeller.
- MetaDefender ICAP : ICAP destekli tüm ağ cihazlarıyla saniyeler içinde entegre olarak çalışır, dosya kaynaklı tehditleri önleyerek ağ trafiğindeki dosya güvenliğini sağlar.
- MetaDefender Email Gateway Security – E-posta tehditlerinin engellenmesi.

Sağladığı Katma Değer

- Veri giriş noktalarında yüksek güvenlik.
- Zero Trust yaklaşımı ile saldırı yüzeyinin azaltılması.
- Çoklu antivirüs motoru ile yüksek tespit ve doğruluk oranları.
- CDR teknolojisi ile sıfıncı gün ataklarına karşı içerik silahsızlandırma
- Regülasyonlara uygun veri transferi.
- Kritik altyapılar için güçlü güvenlik mimarisi.

[Tanıtım Broşürü](#)

Picus Security (Brige Attack Simullation)

Gerçek siber saldırı simülasyonlarıyla güvenlik kontrollerinin etkinliğini sürekli ölçen ve iyileştirme önerileri sunan Breach & Attack Simulation (BAS) çözümdür. Farklı MITRE ATT&CK tekniklerini düzenli olarak çalıştırarak savunma yapılandırmalarındaki zayıf noktaları net bir şekilde ortaya koyar.

Ana Özellikler

- Attack Simulation (BAS) – Gerçek saldırı tekniklerini simüle eder.
- Security Control Validation – Mevcut güvenlik çözümlerinin etkinliğini ölçer.
- Mitigation Guidance – Engellenemeyen saldırılar için üreticiye özel çözüm önerileri sunar (örneğin Palo Alto, Fortinet, CrowdStrike vb. için doğrudan öneriler).
- Purple Teaming – Kırmızı ve mavi ekiplerin ortak çalışmasını kolaylaştırır; saldırı ve savunma ekipleri için aynı platformda senaryo yürütülür.
- Threat Library & Continuous Updates – Güncel tehdit istihbaratına göre sürekli yenilenen saldırı teknikleri.

Sağladığı Katma Değer

- Güvenlik kontrollerinin gerçek zamanlı etkinlik ölçümü
- Sürekli iyileştirme kültürü (Continuous Security Validation)
- Denetim ve uyumluluk raporlaması (ISO, NIST, MITRE ATT&CK)
- SOC ve Blue Team ekiplerinin zaman kazancı
- Güvenlik yatırımlarının ROI'sini net biçimde ölçme

[Tanıtım Broşürü](#)

Kurumlara özel tehdit istihbaratı sağlayarak saldırı yüzeyini görünür kılan ve proaktif savunma kabiliyeti kazandıran bir CTI platformudur. Dark web, açık kaynak ve kapalı kaynak istihbarat akışlarını birleştirerek kuruluşlara erken uyarı mekanizması sağlar.

Ana Özellikler

- Threat Feed & Correlation Engine – Farklı tehdit kaynaklarından gelen verileri birleştirir ve korelasyon analizi yapar.
- Dark Web Monitoring – Şirket verilerinin dark web veya forumlarda paylaşılıp paylaşılmadığını izler.
- Brand Protection – Marka, domain, çalışan e-postaları ve dijital varlıklar için sızıntı ve taklit tespiti sağlar.
- Phishing Detection & Takedown – Sahte domain veya oltalama sayfalarını tespit eder ve kapatma sürecini başlatır.
- Vulnerability Intelligence – Güncel zafiyetleri (CVE) kurum varlıklarıyla eşleştirerek hangi sistemlerin riskte olduğunu gösterir.
- Integration & Automation – SIEM, SOAR, EDR, Firewall gibi sistemlerle entegre çalışarak tehdit istihbaratını aksiyona dönüştürür.

Sağladığı Katma Değer

- Proaktif savunma: Tehditleri gerçekleşmeden önce tespit etme
- Marka itibarı koruma
- Zafiyet önceliklendirme: En kritik açıkları öne çıkarır
- SOC/SIEM entegrasyonu sayesinde hızlı aksiyon
- Dark web görünürlüğü: Veri sızıntısı tespiti
- Uyumluluk ve denetim desteği (ISO 27001, NIST, MITRE ATT&CK)

[Tanıtım Broşürü](#)

Sceptive BLock (APT/Proactive Threat Intelligence)

Sceptive BLock, geleneksel güvenlik yöntemlerinin ötesine geçen, davranışsal parmak izi analizi ile çalışan yeni nesil bir proaktif tehdit koruma sistemidir. Saldırganları statik IP adreslerinden değil, dijital davranış kalıplarından tanıyarak tehditleri sistemlerinize ulaşmadan önce engeller.

BLock, global honeypot ağından topladığı gerçek zamanlı saldırı verilerini yapay zeka destekli davranış analitiği motoru ile analiz eder. Saldırganların niyetlerini ve hareket kalıplarını inceleyerek her biri için benzersiz bir davranışsal parmak izi oluşturur.

IP adresleri değişse bile saldırırganın davranış modeli değişmediği sürece tehdit tespit edilir ve proaktif olarak engellenir.

Ana Özellikler

- Davranışsal Parmak İzi Analizi – IP bağımsız tehdit tespiti.
- AI Destekli Davranış Analitiği – Saldırgan niyet analizi ve proaktif engelleme.
- Global Honeypot Ağı – Gerçek zamanlı tehdit istihbaratı toplama.
- Akıllı ve Dinamik Blocklist'ler – Sürekli güncellenen tehdit listeleri.
- Brute Force Saldırı Engelleme – Parola tahmin saldırılarına karşı koruma.
- Mail Server Koruması – Spam ve phishing saldırılarına karşı savunma.
- Proxy / VPN / TOR Tespiti – Kimlik gizleme kaynaklarını engelleme.
- HTTP & WordPress Koruması – Web servislerine yönelik saldırı önleme.
- D.O.S. Kaynak Tespiti – Kitleseel servis kesinti saldırılarına karşı filtreleme.
- Zero-Day Koruması – Bilinmeyen tehditleri davranış analiziyle yakalama.
- Mevcut Güvenlik Sistemleri ile Entegrasyon – SIEM ve diğer araçlarla uyumlu çalışma.
-

Sağladığı Katma Değer

- Proaktif tehdit engelleme
- IP değiştirerek gelen saldırılara karşı koruma
- Yanlış alarm oranını azaltma
- Bot, VPN ve otomasyon saldırılarını erken durdurma
- İş sürekliliğini ve marka itibarını koruma
- Stratejik tehdit istihbaratı ile karar desteği
- KVKK ve ISO 27001 uyumluluk süreçlerine destek

[Tanıtım Broşürü](#)

SelfHack AI (Penetration Testing Platform)

Yapay zekâ destekli sürekli güvenlik testi ile zafiyetleri öngören, önceliklendiren ve çözüm önerileri sunan otonom güvenlik değerlendirme platformudur. Dinamik tehdit modellerine göre kendi kendine yeni senaryolar üreterek siber dayanıklılığın sürekli olarak güncel kalmasını sağlar.

Ana Özellikler

- AI-simulation – Gerçek saldırgan davranışlarını taklit eden yapay zeka tabanlı saldırı simülasyonları.
- Vulnerability Discovery – Kod, ağ ve uygulama katmanlarında zafiyet tespiti.
- Risk Scoring & Prioritization – Zafiyetleri iş etkisine göre otomatik önceliklendirme.
- Remediation Guidance – Tespit edilen riskler için otomatik çözüm önerileri.
- Continuous Monitoring – Sürekli güvenlik izleme ve yeni tehditlere karşı uyarı mekanizması.

Sağladığı Katma Değer

- Tehditleri gerçekleşmeden önce tespit eden proaktif güvenlik yaklaşımı.
- Yapay zeka hızında saldırı simülasyonu ve zafiyet keşfi.
- Operasyon yükünü azaltan otomatik analiz ve çözüm önerileri.
- Geliştirme ve güvenlik ekipleri arasında daha hızlı iş birliği.
- Sürekli güvenlik doğrulaması (Continuous Security Validation).
- İş riski odaklı önceliklendirme ile verimli kaynak kullanımı.

[Tanıtım Broşürü](#)

TR7 Application Security Platform (ASP)

TR7 Application Security Platform (ASP), kurumların web uygulamalarını ve kritik servislerini korumak, performanslarını artırmak ve yüksek erişilebilirlik sağlamak amacıyla geliştirilmiş yerli bir uygulama güvenliği platformudur. Web Application Firewall (WAF), Load Balancer ve Global Traffic Manager (GTM) yeteneklerini tek platformda birleştirerek hem güvenlik hem de trafik yönetimi ihtiyaçlarını karşılar.

TR7 ASP, kullanıcıların web uygulamalarına gönderdiği trafiği uygulama katmanında analiz eder ve güvenlik politikalarına göre denetler. Gelen trafik yük dengeleme mekanizmaları ile uygun sunuculara yönlendirilirken, WAF motoru tarafından SQL Injection, XSS, Bot ve OWASP Top 10 saldırılarına karşı korunur. Ayrıca uygulama performansını optimize ederek servis sürekliliğini destekler.

Ana Özellikleri

- Web Application Firewall (WAF) – Web uygulamalarını gelişmiş saldırılara karşı korur.
- Load Balancer – Trafiği sunucular arasında dengeli dağıtarak performans ve süreklilik sağlar.
- Global Traffic Manager (GTM) – Kullanıcıları en uygun veri merkezi veya servise yönlendirir.
- SSL Offloading – SSL/TLS işlemlerini uygulama sunucularından alarak performansı artırır.
- High Availability (HA) – Aktif-Aktif ve Aktif-Pasif mimariler ile kesintisiz hizmet sunar.
- Caching & Compression – Uygulama performansını artırmak için önbellekleme ve sıkıştırma sağlar.

Sağladığı Katma Değer

- Web uygulamalarına yönelik saldırılara karşı gelişmiş koruma
- Uygulama performansını ve kullanıcı deneyimini artırma
- Yüksek erişilebilirlik ve iş sürekliliği sağlama
- Veri merkezleri arasında akıllı trafik yönlendirme
- Sunucu kaynaklarının daha verimli kullanılması
- Yerli teknoloji ile güvenlik ve operasyonel bağımsızlık
- KVKK, ISO 27001 ve kurumsal güvenlik gereksinimlerini destekleme

[Tanıtım Broşürü](#)

Vectra AI (NDR)

Vectra AI, yapay zeka destekli Network Detection and Response (NDR) platformu ile ağ içindeki bilinmeyen tehditleri, lateral movement aktivitelerini ve kimlik kötüye kullanımını gerçek zamanlı olarak tespit eden ileri seviye bir güvenlik çözümüdür. Saldırıların erken aşamalarını ortaya çıkararak SOC ekiplerinin tehditlere hızlı ve etkili şekilde müdahale etmesini sağlar.

Ana Özellikleri

- NDR (Network Detection & Response) – Ağ içi saldırı davranışlarını anında tespit eder.
- Identity Threat Detection – Kimlik kötüye kullanımı ve saldırganların hesap ele geçirme girişimlerini analiz eder.
- SaaS & Cloud Detection – M365, AWS, GCP gibi ortamlarda anomali ve saldırı tespiti.
- AI-Powered Triage – Yüzlerce uyarıyı otomatik analiz ederek kritik tehditleri önceliklendirir.
- Attack Signal Intelligence – Tüm uyarıları tek bir saldırı sinyali sisteminde korele eder.
- Incident Response Entegrasyonu – SOAR, EDR ve SIEM ile entegre otomatik müdahale.

Sağladığı Katma Değer

- Lateral movement ve kimlik kötüye kullanımının erken tespiti.
- SOC ekipleri için daha az gürültü, daha yüksek doğruluklu alarmlar.
- Bulut, veri merkezi ve kimlik güvenliği için tek platformda görünürlük.
- Tehdit avcılığı ve olay müdahalesi için derin davranış analizi.
- Saldırı zincirini uçtan uca görme ve hızlı aksiyon alma imkânı.
- False-positive oranının azaltılmasıyla operasyonel verimlilik artışı.

[Tanıtım Broşürü](#)

Veriskop (Veri Keşfi / Veri Sınıflandırma / Veri Maskeleye)

Veriskop, kurumların hassas verilerini keşfetmek, sınıflandırmak ve güvenli şekilde yönetmek için geliştirilmiş veri güvenliği platformudur. Özellikle veri keşfi (data discovery), veri sınıflandırma (classification) ve veri maskeleye (data masking) yetenekleri ile kurumların veri güvenliği süreçlerini merkezi ve kontrol edilebilir hale getirir.

Ana Özellikleri

- Data Discovery – Kurum içindeki hassas verilerin otomatik keşfi.
- Data Classification – Verilerin içerik ve politika bazlı sınıflandırılması.
- Data Masking – Hassas verilerin maskelenmesi ve anonimleştirilmesi.
- Policy Enforcement – Veri erişim ve kullanım politikalarının uygulanması.
- User Activity Monitoring – Veriye erişen kullanıcıların izlenmesi.
- Reporting & Compliance – KVKK, GDPR gibi regülasyonlara uygun raporlama.

Sağladığı Katma Değer

- Hassas verilerin tam görünürlüğü (nerede, kimde, nasıl kullanılıyor).
- Veri sınıflandırma ile risklerin doğru önceliklendirilmesi.
- Veri maskeleye ile veri ihlallerinin etkisinin azaltılması.
- Regülasyonlara (KVKK, GDPR, PCI-DSS) uyumluluk.
- Veri odaklı güvenlik yaklaşımı ile iç tehditlerin azaltılması.
- Merkezi veri güvenliği yönetimi ile operasyonel verimlilik.

[Tanıtım Broşürü](#)

Wallarm (API Security)

Wallarm API Security, modern uygulamaların ve mikroservis mimarilerinin kullandığı API'leri yapay zekâ destekli olarak keşfeden, izleyen ve saldırılara karşı koruyan gelişmiş bir API güvenlik platformudur. Platform, bilinen veya gölge (shadow) API'leri ortaya çıkarır, anormallikleri tespit eder ve saldırıları gerçek zamanlı olarak engeller.

Ana Özellikler

- API Discovery – Bilinen, bilinmeyen ve gölge API'lerin otomatik tespiti.
- API Threat Prevention – API misconfiguration, injection, credential stuffing gibi saldırıların engellenmesi.
- Behavioral Anomaly Detection – API çağrılarında anormal davranışların tespiti.
- Schema Validation – API şeması dışına çıkan istekleri engelleme.
- OWASP API Top 10 Koruması – En kritik API güvenlik risklerine karşı kapsamlı koruma.
- Bot & Abuse Protection – Otomasyon kaynaklı kötü davranışların engellenmesi.

Sağladığı Katma Değer

- API güvenlik risklerinin erken tespiti.
- Shadow API görünürlüğü ile güçlü saldırı yüzeyi kontrolü.
- Yapay zekâ destekli saldırı tespiti ile daha az false-positive.
- API trafik analizi ile anormallik tespiti ve hızlı müdahale.
- Modern DevOps ve Kubernetes ortamlarıyla kolay entegrasyon.
- Uyumluluk süreçlerini destekleyen raporlama ve görünürlük.

[Tanıtım Broşürü](#)

Xage Security (IT/OT Identity & Access Managment / PAM)

Xage Security, özellikle endüstriyel kontrol sistemleri (OT), IoT ve kritik altyapılar için geliştirilmiş Zero Trust tabanlı erişim ve güvenlik platformudur. Merkeziyetsiz güvenlik mimarisi üzerinden kimlik öncelikli siber savunma sağlayarak kullanıcıları, cihazları ve uygulamaları güvenli şekilde doğrular ve kontrol eder. Sistem, kritik varlıkları korumak için güvenli uzaktan erişim, ayrıcalıklı erişim yönetimi (PAM) ve veri değişim güvenliğini tek bir platformda sunar.

Ana Özellikler

- **Güvenli uzak erişim:** Kritik sistemlere kontrollü ve güvenli erişim sağlar.
- **Ayrıcalıklı erişim yönetimi (PAM):** Yetkili hesapların erişimini ve kullanımını güvenli şekilde yönetir.
- **MFA ve SSO desteği:** Erişim güvenliğini çok faktörlü kimlik doğrulama ve tek oturum açma ile güçlendirir.
- **Kimlik tabanlı segmentasyon:** Kullanıcılar, cihazlar ve sistemler arasındaki erişimi politika bazlı sınırlandırır.
- **Güvenli dosya ve veri aktarımı:** Dosya bütünlüğünü korur ve yetkisiz veri hareketini azaltmaya yardımcı olur.
- **Oturum kaydı ve denetim izi:** Erişimleri ve kullanıcı işlemlerini izlenebilir hale getirir.
- **Ajansız mimari:** Uç sistemlerde ajan gerektirmeden devreye alınabilecek şekilde tasarlanmıştır.

Sağladığı Katma Değer

- OT ve IT ortamlarında birleşik güvenlik yönetimi.
- Zero Trust ile güçlü erişim kontrolü.
- Merkeziyetsiz mimari sayesinde yüksek dayanıklılık.
- Kritik altyapılar için kesintisiz güvenlik.
- Uzaktan erişimde yüksek güvenlik seviyesi.
- Regülasyon uyumluluğunu destekleyen güvenlik modeli.

[Tanıtım Broşürü](#)

Zscaler AI Security

Zscaler AI Security, kurumların üretken yapay zekâ uygulamalarını, AI modellerini, ajanlarını ve bu sistemlerle ilişkili veri akışlarını güvenli şekilde keşfetmesini, yönetmesini ve korumasını sağlayan Zero Trust tabanlı yapay zekâ güvenliği platformudur.

Çözüm; çalışanların kullandığı genel amaçlı GenAI uygulamalarından kurum içinde geliştirilen AI servislerine, modellerden API ve ajan trafiğine kadar yapay zekâ yaşam döngüsünün tamamında görünürlük ve kontrol sağlar. Shadow AI kullanımını ortaya çıkarır, hassas verilerin AI sistemlerine aktarılmasını engeller ve AI uygulamalarının güvenlik açıklarını sürekli olarak test eder.

Ana Özellikleri

- **AI Asset Management ve AI-SPM:** AI uygulamalarını, modelleri, ajanları, MCP sunucularını, veri setlerini ve ilişkili servisleri otomatik olarak keşfeder ve envanterler.
- **Shadow AI Tespiti:** Kurumun bilgisi dışında kullanılan AI uygulamalarını ve gömülü AI özelliklerini görünür hale getirir.
- **AI Access Security:** Kullanıcı, grup, uygulama ve risk bağlamına göre AI erişimini izin verme, uyarma, izole etme veya engelleme politikalarıyla yönetir.
- **Prompt ve Response Güvenliği:** Prompt ve model cevaplarını analiz ederek hassas veri paylaşımı, uygunsuz içerik ve politika ihlallerini tespit eder.
- **Inline DLP:** Kaynak kod, kişisel veri, finansal veri, sağlık verisi ve kuruma özel hassas bilgilerin AI uygulamalarına gönderilmesini önler.
- **AI Gateway ve AI Guard:** Model, API ve ajan trafiğine merkezi Zero Trust politikaları, içerik denetimi ve gerçek zamanlı güvenlik kontrolleri uygular.
- **AI Red Teaming:** Prompt injection, jailbreak, veri sızıntısı ve güvenli olmayan model davranışlarına karşı otomatik ve sürekli güvenlik testleri gerçekleştirir.
- **AI Yönetişimi ve Uyumluluk:** AI risklerini NIST AI RMF, MITRE ATLAS, GDPR ve EU AI Act gibi çerçevelerle ilişkilendirerek raporlama ve iyileştirme süreçlerini destekler.

Sağladığı Katma Değer

- Kurumdaki tüm yapay zekâ kullanımının ve Shadow AI risklerinin görünür hale gelmesi.
- Hassas verilerin GenAI uygulamalarına aktarılmasının gerçek zamanlı olarak önlenmesi.
- AI uygulamalarının tamamen engellenmesi yerine güvenli ve kontrollü kullanımının sağlanması.
- AI modelleri, ajanlar, API'ler ve veri kaynakları arasındaki ilişkilerin merkezi olarak yönetilmesi.
- Prompt injection, jailbreak ve veri sızıntısı gibi AI'ya özgü saldırıların azaltılması.
- Güvenlik, veri yönetişimi, hukuk ve uyumluluk ekiplerinin ortak politika uygulayabilmesi.
- AI projelerinin üretime alınma süresinin güvenlik kontrolleriyle birlikte hızlandırılması.

[Tanıtım Broşürü](#)

Zscaler (SASE - ZTNA)

Zscaler, bulut tabanlı Zero Trust Exchange platformu ile Secure Service Edge (SSE) ve SASE mimarisinin öncülerinden biri olarak konumlanan lider bir siber güvenlik çözümüdür. Geleneksel ağ tabanlı güvenlik yaklaşımlarını ortadan kaldırarak, uygulama ve kullanıcı merkezli modern bir güvenlik mimarisi sunar. Tüm trafik, Zscaler'ın global bulut platformu üzerinden denetlenir; kimlik, bağlam ve güvenlik politikaları doğrultusunda kontrol sağlanır.

Bu yaklaşım sayesinde Zscaler, saldırı yüzeyini minimize eder, VPN ve geleneksel güvenlik altyapılarına olan bağımlılığı ortadan kaldırır. Kullanıcı deneyimini iyileştirir ve kurumların modern, dağıtık yapılarında güvenli dönüşümü mümkün kılar.

Ana Özellikleri

- **Zero Trust Exchange Platformu** - Tek bir yönetim platformu ile tüm fonksiyonlar politika tabanlı yönetilebilir.
- **Zscaler Internet Access (ZIA)** - Güvenli internet erişimi sağlayarak SWG, CASB, DNS Security ve Cloud Firewall yeteneklerini tek platformda sunar.
- **Cloud Firewall** - Bulut tabanlı güvenlik duvarı hizmeti.
- **CASB** - Bulut uygulamalarında veri güvenliği ve görünürlük.
- **DLP** - Hassas verilerin korunmasını ve veri sızıntısının önlenmesini sağlar.
- **Zscaler Private Access (ZPA)** - Zero Trust mimarisi ile kullanıcıların iç uygulamalara VPN olmadan, doğrudan ve güvenli erişimini sağlar.
- **Advanced Threat Protection & Sandbox** – Bilinmeyen ve gelişmiş tehditleri analiz ederek zararlı içerikleri engeller.

Sağladığı Katma Değer

- Zero Trust mimarisi ile güçlü erişim güvenliği. - “Trust but verify” yerine “never trust, always verify” yaklaşımıyla erişim güvenliğini yeniden tanımlar.
- VPN’siz modern erişim - Kullanıcıları ağa değil, doğrudan uygulamalara bağlayarak saldırı yüzeyini ortadan kaldırır.
- SSE + SASE ile modern mimari - Güvenliği buluta taşıyarak ağ ve güvenliği tek modelde birleştirir.
- Bulut tabanlı yapı ile yüksek ölçeklenebilirlik.
- Kullanıcı ve uygulama bazlı güvenlik ve görünürlük.
- Veri sızıntılarını önleyen gelişmiş DLP yetenekleri.
- Global altyapı ile düşük gecikme ve yüksek performans.
- Operasyonel Basitlik ve Ölçeklenebilirlik

[Tanıtım Broşürü](#)

Fortinet

- **FortiAnalyzer**

FortiAnalyzer, Fortinet tarafından geliştirilen; ağ güvenliği, log yönetimi ve raporlama için kullanılan merkezi bir analiz platformudur. Fortinet cihazları başta olmak üzere syslog destekli birçok kaynaktan log toplayarak güvenlik ekiplerinin ağda olup biteni detaylı şekilde izlemesini sağlar.

- **FortiAP**

FortiAP, Fortinet tarafından geliştirilen, güvenli ve yüksek performanslı Wi-Fi bağlantısı sağlayan kurumsal kablosuz erişim noktası (Access Point) serisidir. FortiGate ile tam entegre çalışarak hem merkezi yönetim hem de gelişmiş güvenlik sağlar.

- **FortiAuthenticator**

FortiAuthenticator, Fortinet tarafından geliştirilen, kurumların **erişim ve kimlik yönetimini** merkezi şekilde sağlayan bir kimlik doğrulama çözümüdür. Kullanıcıların ve cihazların kimliklerinin doğrulanması, erişim politikalarının uygulanması ve ağ kaynaklarına erişimin kontrol edilmesi amacıyla kullanılır. Fortinet Security Fabric ile tam entegre çalışarak güvenlik olaylarına hızlı müdahale imkânı sunar.

- **FortiDeceptor**

FortiDeceptor, Fortinet tarafından geliştirilmiş yeni nesil bir **aldatma/tuzağa düşürme (deception) ve honeypot çözümüdür**. Amaç, saldırganları gerçek sistemlerden uzaklaştırmak, onları tuzaklara yönlendirerek erken aşamada tespit etmek ve hasar vermeden engellemektir.

- **FortiEDR**

FortiEDR (Endpoint Detection and Response), Fortinet'in bulut tabanlı gelişmiş bir yapay zeka destekli uç nokta güvenlik çözümüdür. Amacı, iş istasyonları, sunucular ve diğer cihazlar dahil olmak üzere uç noktaları (endpoint), siber saldırılara karşı gerçek zamanlı olarak korumaktır. Sadece tespit etmekle kalmaz, aynı zamanda saldırıları durdurur, veri kaybını önler ve olay müdahale/iyileştirme süreçlerini otomatikleştirir. Temel hedefi: ihlal yok, veri kaybı yok, sorun yok.

- **FortigateFirewall**

FortiGate, Fortinet tarafından geliştirilen ve **küçük ofislerden büyük operatörlere kadar** her ölçekte kullanılan, **çok fonksiyonlu (Next-Generation Firewall - NGFW)** bir ağ güvenlik cihazıdır. Tek bir platformda **geniş bir siber güvenlik yelpazesi** sunarak hem ağ trafiğini yönetir hem de gelişmiş tehditlere karşı **yüksek performanslı koruma** sağlar.

- **Forti Isolator**

FortiIsolator, Fortinet'in, web tabanlı gelişmiş tehditlere karşı kritik iş verilerini korumak için tasarlanmış bir **Tarayıcı İzolasyon Platformudur**. Temel amacı, kullanıcıların web'de gezinirken karşılaştıkları potansiyel riskli içeriği (kötü amaçlı yazılımlar, vb.) son kullanıcı cihazından **tamamen uzak tutmaktır**.

- **FortiMail**

FortiMail, Fortinet'in e-posta trafiğine özel, ileri düzeyde güvenlik sağlayan bir **E-posta Güvenlik Ağ Geçidi** çözümüdür. E-posta yoluyla yayılan **spam**, **virüs**, **oltalama (phishing)** ve **veri sızıntısı (DLP)** tehditlerine karşı çok katmanlı koruma sunar. Temel olarak, e-posta sunucusuna ulaşmadan önce tüm e-postaları temizleyerek, kurumların maddi ve itibar kayıplarını önler ve yasal uyumluluğu kolaylaştırır.

- **FortiManager**

FortiManager, özellikle orta ve büyük ölçekli yapılar için tasarlanmış, **Fortinet güvenlik çözümlerini (başta FortiGate ve FortiClient)** tek bir konsoldan **merkezi olarak yönetmek** için kullanılan bir platformdur. Amacı, birden fazla cihazın (birkaç adetten binlerce adete kadar) yönetimini, güncelleme dağıtımını, güvenlik kuralı uygulamasını ve iş akışı kontrolünü **otomasyonla** kolaylaştırmaktır.

- **FortiNac**

FortiNAC (Network Access Control), Fortinet Security Fabric'in **ağ erişim kontrolü** çözümüdür. Temel görevi, ağa bağlanan her cihazı (**geleneksel bilgisayarlar, BYOD, ve özellikle güvensiz IoT cihazları**) tespit etmek, profillemek ve bu cihazların yalnızca kendilerine ait işlevleri yerine getirecek şekilde **rol tabanlı ve dinamik erişim politikalarıyla** ağa dahil edilmesini sağlamaktır. Bu sayede, ağ güvenliği zafiyetleri ve tehditlerin yayılması önlenir.

- **FortiSandbox**

FortiSandbox, Fortinet'in, **sıfırıncı gün (Zero-day)** ve geleneksel sistemlerin atlatılabildiği **gelişmiş/hedefli saldırıları** tespit etmek için kullanılan kum havuzu (Sandbox) çözümüdür. Temel işlevi, şüpheli dosyaları ve uygulamaları **izole edilmiş sanal bir ortamda** güvenli bir şekilde çalıştırmak, davranışlarını analiz etmek ve zararlı olup olmadıklarına karar vermektir. Tespit edildiğinde, oluşturduğu yerel tehdit istihbaratını Security Fabric ile **gerçek zamanlı** paylaşarak otomatik savunma sağlar.

- **FortiSwitch**

FortiSwitch ürün ailesi, küçük, orta ve büyük ölçekli işletmeler ile dağıtık şube yapıları için tasarlanmış **güvenli, basit ve yüksek performanslı** Ethernet anahtarlama çözümleridir. Temel amacı, ağ erişimini güvenli hale getirmek, performansı artırmak ve tüm bu yönetimi Fortinet'in geniş güvenlik mimarisine entegre etmektir.

- **SD Branch**

Secure SD-Branch, Fortinet'in, dijital dönüşümün gerektirdiği **dağıtık şube ofisleri** için geliştirdiği, **ağ erişimi** ile **güvenliği** tek bir platformda birleştiren kapsamlı bir mimaridir. Bu çözüm, Fortinet Security Fabric'in gücünü şubenin en uç noktalarına (erişim katmanına) kadar genişleterek çeviklik, kolay yönetilebilirlik ve daha düşük toplam sahip olma maliyeti (TCO) sağlar.

- **FortiNDR**

FortiNDR (Network Detection and Response), güvenlik operasyonları (SecOps) ekiplerinin karşılaştığı gelişmiş ve öngörülemez siber suçlara karşı geliştirilmiş, **yapay zekâ (YZ)** destekli bir çözümdür. Temel amacı, ağdaki **anormal etkinliği** (davranışsal sapmaları) tespit etmek ve bu tehditlere karşı **otomatik ve hızlı yanıt** vermektir. Böylece güvenlik ekiplerinin **reaktif** (olay sonrası) durumdan **proaktif** (olay öncesi ve anı) bir duruşa geçmesini sağlar.

- **FortiWeb**

FortiWeb, web uygulamalarını ve API'leri, **DDoS**, **kötü amaçlı botlar**, **OWASP Top 10** gibi bilinen ve özellikle **sıfırıncı gün (Zero-day)** açıklarına yönelik saldırılardan koruyan Fortinet'in Web Application Firewall (WAF) çözümüdür. **Makine Öğrenmesi (ML)** destekli gelişmiş algılama yetenekleri sayesinde, saldırıları otomatik olarak tespit eder, yanlış pozitifleri en aza indirir ve kritik iş uygulamaları için çok katmanlı, gerçek zamanlı koruma sağlar.

- **Fortirecon – CTI**

Siber Tehdit İstihbaratı (CTI), bir kuruluşun dijital altyapısına yönelik potansiyel tehditleri belirlemek ve anlamak için iç ve dış kaynaklardan veri toplama, analiz etme ve yorumlama sürecidir. **FortiRecon**, Netsys tarafından sunulan, bu kapsamda yeni nesil bir **Dijital Risk Koruma** hizmetidir. FortiRecon, **makine öğrenimi, otomasyon ve insan zekasını (FortiGuard Labs uzmanlığı)** birleştirerek kurumların harici saldırı yüzeyini izlemesini, marka riskini yönetmesini ve tehditlere karşı proaktif yanıt vermesini sağlar.

- **FortiSIEM**

FortiSIEM, artan saldırı yüzeyi ve yönetim karmaşıklığı ile mücadele eden kuruluşlar için tasarlanmış, **Güvenlik Bilgileri ve Olay Yönetimi (SIEM)** çözümüdür. FortiSIEM, çok sayıda sistem, ağ ve güvenlik cihazından gelen verileri (log/olay) tek bir platformda toplar, ilişkilendirir (**korelasyon**) ve analiz eder. Amacı, tehditleri ve veri ihlallerini **erken keşfetmek, otomatik yanıt** vermek ve güvenlik/ağ operasyonlarının (SOC/NOC) yönetim karmaşıklığını azaltmaktır.

F5

- **BIG-IP Advanced WAF**

BIG-IP Advanced WAF, geleneksel Web Uygulama Güvenlik Duvarlarının (WAF) gözden kaçırdığı gelişmiş ve otomatik saldırıları tanımlamak ve engellemek için tasarlanmıştır. Çözüm, **OWASP Top 10** uyumluluğunu sağlayan özel kontroller sunar, **API güvenliği, Katman 7 DDoS engelleme, davranış analitiği** ve **gelişmiş makine öğrenimi** gibi yeteneklerle web uygulamalarını ve API'leri korur. Amacı, mikro hizmetler dahil olmak üzere tüm uygulamalar için kapsamlı, dinamik ve ayrıntılı güvenlik politikaları oluşturarak uygulama güvenliğini artırmak ve yönetim yükünü azaltmaktır.

- **BIG-IP Local Traffic Manager**

BIG-IP LTM, F5 tarafından geliştirilen, uygulamaların **yüksek kullanılabilirliğini, güvenilirliğini ve performansını** sürekli kılmak için tasarlanmış, **yük dengelemeden daha fazlasını** sunan bir yazılımdır. Tüm trafik talepleri arasında uygulama yükünü yönetir, tek nokta arızalarını ortadan kaldırır ve kullanıcı deneyimini iyileştirmek için **gerçek zamanlı protokol optimizasyonu** ve **güvenlik** hizmetleri sunar.

- **BIG-IP DDoS Hybrid Defender**

BIG-IP DDoS Hybrid Defender, gelişmiş bulut tabanlı ve yerel savunmaları birleştirerek hacimsel ve sofistike dağıtılmış hizmet reddi saldırılarına (**DDoS**) karşı **üstün koruma** sağlayan bir çözümdür. Hedefi, hem **Katman 3/4** hacimsel saldırıları hem de tespiti zor olan **Katman 7 (Uygulama Katmanı)** saldırılarını, özellikle API geçitlerini hedef alanları, **hat hızında** ve gerçek zamanlı olarak engellemektir.

- **BIG-IP Access Policy Manager**

Bu metinde özetlenen çözüm (BIG-IP APM), modern ve dağıtık BT ortamları için **Sıfır Güven Uygulama Erişimi (Zero Trust Application Access)** sağlamaya odaklanmaktadır. Amacı, her uygulama erişim isteğini, **kimlik, bağlam ve uç nokta güvenliğine** dayalı ayrıntılı bir doğrulama modelinden geçirerek güvence altına almaktır. Bu, kullanıcının nerede ve hangi cihazla olursa olsun, yalnızca ihtiyaç duyduğu uygulamalara güvenli, merkezi ve basitleştirilmiş bir şekilde erişmesini sağlar.

- **BIG-IP Advanced Firewall Manager**

BIG-IP Advanced Firewall Manager (AFM), ICSA sertifikalı, yüksek performanslı, tam proxy özellikli bir ağ güvenliği çözümüdür. Uygulama merkezli tasarımı sayesinde hedeflenen ağ altyapısı seviyesindeki saldırılara karşı etkilidir. AFM, **güvenlik duvarı, DDoS hafifletme, DNS güvenliği ve Uygulama Saldırı Önleme Sistemlerini (IPS)** tek bir BIG-IP platformunda birleştirerek yönetim karmaşıklığını azaltırken, **davranışsal analiz ve makine öğrenimi** ile tespiti zor saldırılara karşı üstün koruma sağlar.

- **BIG-IP DNS**

BIG-IP DNS çözümü, DNS sorgu yanıtlarında **(100 milyon RPS'ye kadar) hiper ölçeklendirme** ve üstün **DNS güvenliği** sağlayarak uygulamaların küresel çapta yüksek performanslı ve güvenilir olmasını garanti eder. Temel olarak, kullanıcıları coğrafi konum, iş politikaları ve uygulama performansına dayalı olarak en hızlı ve en güvenilir sunucuya yönlendirir (**GSLB - Global Server Load Balancing**) ve DNS altyapısını DDoS, önbellek zehirlenmesi gibi tehditlere karşı korur.

ARISTA

- **Backbone Switch**

Backbone Switch (Omurga Anahtarı), birden fazla switch arasında **en fazla yükün bulunduğu ve yükü paylaştırmada** görevli olan temel anahtar türüdür. Bir bilgisayar ağındaki çeşitli parçaları (farklı yerel ağları veya binaları) birbirine bağlar ve tüm trafik yükünü bir arada toplar. Kapasitesi genellikle kendisine bağlı olan diğer ağların kapasitesinden daha yüksektir.

- **Edge Switch**

Edge Switch (Uç Anahtar), ağdaki **bilgisayarlar, yazıcılar ve diğer son kullanıcı cihazlarının** birbirleriyle **haberleşmesini** sağlayan ağ aygıtıdır. Cihazlar, ağ kartına takılan bir kablo ile Edge Switch'e bağlanır. Genellikle ofislerde ve veri merkezlerinde kullanılan bu cihazlar, mimari olarak ağın **omurgasına (Backbone Switch)** bağlı olarak çalışır.

- **CloudVision CUE**

CloudVision CUE, ağ yöneticilerine Wi-Fi ağının **kusursuz çalışmasını** sağlamak ve **kullanıcı deneyimini** optimum düzeyde tutmak için gereken araçları sunan, Arista'nın bulut tabanlı bir çözümüdür. Temel hedefi, sorunları **önceden tespit etmek** ve bildirilen arızalar durumunda en kısa **Ortalama Çözüm Süresine (Mean Time To Resolution - MTTR)** ulaşmaktır. Bunu, **yapay zekâ (YZ)** ve **makine öğrenimi** kullanarak gerçekleştirir.

- **CloudVision Portal**

CloudVision Portal (CVP), Arista'nın **CloudVision** platformunun web tabanlı grafik kullanıcı arayüzüdür (GUI). CVP, ağ cihazı provizyonu, uyumluluk yönetimi, değişiklik yönetimi ve ağ izleme dahil olmak üzere tüm ağ operasyonlarını otomatikleştirmek için **anahtar teslim** bir çözüm sunar. Fiziksel ağ katmanı ile hizmet yönetimi katmanı arasında bir **ağ kontrol noktası** (Network Control Point) görevi görür.

ivanti

- **SSL VPN**

SSL VPN (PCS/ICS), çalışanların ve yetkili kullanıcıların dizüstü bilgisayar, akıllı telefon gibi çeşitli cihazlarla **herhangi bir yerden** kurumsal ağ kaynaklarına güvenli bir şekilde erişmesini sağlayan güçlü bir uzaktan erişim çözümüdür. Temel amacı, ağ kaynaklarının **gizliliğini, bütünlüğünü ve kullanılabilirliğini** korurken, esnek ve merkezi yönetilebilir bir uzaktan çalışma ortamı sunmaktır.

- **NAC**

NAC (Network Access Control - Ağ Erişim Kontrolü), bir kuruluşun ağına bağlanan cihazlar için **uç nokta uyumluluğunu** ve **güvenli ağ erişimini** zorlamak için tasarlanmıştır. **Pulse/Ivanti Policy Secure** gibi çözümler, cihazların ağa erişmesine izin verilmeden önce, kuruluşun tanımladığı güvenlik politikalarına (antivirüs güncelliği, işletim sistemi yamaları, güvenlik duvarı ayarları gibi) uyup uymadığını kontrol ederek yetkisiz ve savunmasız cihazların ağa erişimini önler.

CİTRIX

- **Citrix Virtual Apps and Desktops**

Citrix Virtual Apps and Desktops, merkezi sunucular üzerinde çalışan sanal işletim sistemlerine erişim sağlayarak, uygulama ve masaüstü ortamlarını **her türlü cihaz üzerinden, herhangi bir lokasyondan, güvenli ve aynı hız/hissiyatla** kullanılabilir hale getiren bir sanallaştırma teknolojisidir. Kullanıcılar cihazlarına **Citrix Workspace (Receiver) istemci uygulamasını** kurarak erişim sağlar ve cihaz bağımsız çalışır. Bu çözüm, hibrit çalışma ortamları için **DaaS (Desktop as a Service - Bulut)** ve **VDI (Virtual Desktop Infrastructure - Yerinde)** olmak üzere iki ana model sunar.

AUTHTAKE

- **Passwordless Authentication**

AuthTake, siber güvenlik ihlallerinin baş aktörü olan **parolaları tamamen ortadan kaldırmayı** hedefleyen, **FIDO2 (WebAuthn)** standardını ve **Açık Anahtarlı Şifrelemeyi (PKC)** kullanan güvenli bir parolasız kimlik doğrulama hizmetidir. Güvenlik seviyesini artırırken, hızlı oturum açma (ortalama 3 saniye) ve parola yönetim maliyetlerinden kurtulma avantajları sunar. Kuruluşların, **SMS kodu/OTP** gibi paylaşılan sırlardan kurtulmasını ve tam anlamıyla parolasız bir yaşama geçişini sağlar

- **Single Sign-On (SSO)**

Parolasız Tek Oturum Açma (Passwordless SSO), AuthTake'in **SAML** ve **OAuth** protokollerini kullanarak kurumsal ve bulut uygulamalarına (Office 365, Salesforce vb.) **parola kullanmadan, tek bir girişle** hızlı ve güvenli erişim sağlayan çözümdür. Kullanıcılar, bir pano (AuthTake Portalı) üzerinden şifre girme zorunluluğu olmadan uygulamalara erişerek zaman kazanır, kullanım zorluğunu ortadan kaldırır ve üretkenliklerini artırır.

Opinnate NSPM (Network Security Policy Management)

- **Opinnate**

Opinnate, kurumsal güvenlik duvarları için **uçtan uca ağ güvenlik politikası yönetimi** sağlayan bir sistemdir. Temel amacı, günümüzün **karmaşık IT ortamlarında** (çoklu segmentler, hibrit bulut, farklı tedarikçiler) politika yönetimini basitleştirmek ve işletme çalışmalarını analizden otomasyona kadar daha verimli hale getirmektir. Opinnate, **analiz, optimizasyon, denetim, raporlama ve otomasyon** özellikleri sunarak kuruluşların güvenlik durumunu artırmasına ve zaman/çabadan tasarruf etmesine yardımcı olur.

CAST DDoS

- **Cast DDoS**

Cast DDoS, kuruluşların kendi **DDoS önleme sistemlerinin sınırlarını ve verimliliğini** test etmeleri için tasarlanmış **otomatik bir DDoS test platformudur**. Bu platform, gerçek saldırı parametrelerini kullanarak kuruluşa karşı **gerçek DDoS saldırılarını simüle eder**. Web portalı üzerinden saldırı türü, bot miktarı ve süresi gibi parametreler kolayca seçilebilir ve kullanıcılara detaylı raporlama, acil durdurma ve gerçek zamanlı yardım gibi kritik kontrol imkanları sunulur.

- **DDoS Saldırı Testi**

DDoS Testi, bir web mülkünü veya altyapısını **gerçekçi sayıda DDoS saldırısına** tabi tutarak, mevcut savunma sistemlerinin tehditleri beklenen şekilde **hafifletebildiğini kanıtlamak** için yapılan kritik bir süreçtir. Bu, sürekli gelişen İnternet tehdit ortamına karşı savunmalarınızı test etmenin tek yoludur. Amaç, hacker'ların yaptığı gibi, altyapının **zayıf noktalarını bulmak** ve sistemin, performans üzerinde minimum etkiyle hayatta kalmasını sağlamaktır.

A10 Networks

- **Thunder Advanced WAF**

Thunder Advanced WAF, geleneksel WAF çözümlerinin tespit edemediği gelişmiş uygulama katmanı saldırılarını belirlemek ve engellemek üzere tasarlanmıştır. OWASP Top 10 koruması, API güvenliği, bot yönetimi ve davranışsal analiz gibi gelişmiş yetenekler sunar. Makine öğrenimi destekli tehdit analizi ile yanlış pozitifleri azaltırken, uygulama ve API'ler için dinamik ve otomatik güvenlik politikaları oluşturarak operasyonel yükü minimize eder.

- **Thunder ADC (Application Delivery Controller)**

Thunder ADC, A10 Networks tarafından geliştirilen yüksek performanslı bir uygulama teslim ve yük dengeleme çözümüdür. Trafiği akıllı şekilde dağıtarak uygulama sürekliliğini sağlar, tek nokta arızalarını ortadan kaldırır ve kullanıcı deneyimini optimize eder. Gelişmiş SSL offload, trafik optimizasyonu ve içerik yönlendirme özellikleri ile hem performans hem de güvenlik katmanında değer sunar.

- **Thunder TPS (Threat Protection System)**

Thunder TPS, hacimsel ve gelişmiş DDoS saldırılarına karşı gerçek zamanlı koruma sağlayan yüksek performanslı bir çözümdür. Hem Katman 3/4 hem de Katman 7 saldırılarını tespit edip engelleyerek servis sürekliliğini garanti altına alır. Donanım hızlandırılabilir mimarisi sayesinde hat hızında analiz ve müdahale yaparken, otomatik saldırı tespiti ve adaptif savunma mekanizmaları ile operasyonel verimlilik sağlar.

- **A10 Secure Access (Application Access Control)**

A10 Secure Access çözümü, modern BT ortamları için güvenli uzaktan erişim ve Zero Trust yaklaşımı sunar. Kullanıcı kimliği, cihaz durumu ve bağlamsal faktörleri değerlendirerek her erişim isteğini doğrular. Böylece kullanıcıların yalnızca yetkili oldukları uygulamalara güvenli, merkezi ve kontrollü erişimini sağlar, aynı zamanda VPN bağımlılığını azaltır.

- **Thunder Firewall (CFW - Convergent Firewall)**

Thunder CFW, yüksek performanslı, taşıyıcı sınıfı bir ağ güvenlik çözümüdür. Stateful firewall, DDoS koruma, CGNAT ve uygulama farkındalığı özelliklerini tek platformda birleştirir. Gelişmiş tehdit istihbaratı, davranış analizi ve otomasyon kabiliyetleri ile hem ağ hem de uygulama seviyesinde kapsamlı koruma sağlar.

- **A10 DNS (Thunder DNS / GSLB)**

A10 DNS çözümü, yüksek hacimli DNS sorgularını düşük gecikme ile işleyerek uygulamaların global erişilebilirliğini artırır. GSLB (Global Server Load Balancing) yeteneği ile kullanıcıları coğrafi konum, sunucu sağlığı ve performans kriterlerine göre en uygun veri merkezine yönlendirir. Aynı zamanda DNS altyapısını DDoS ve cache poisoning gibi saldırılara karşı korur.