Sentra

UNİFİED EDGE SECURİTY PLATFORM

TEKNİK DATASHEET · FİNANSAL KURUMLAR SÜRÜMÜ

Uygulama ve DNS katmanında bütünleşik güvenlik, trafik ve gözlemlenebilirlik platformu

DNS Firewall · Web Application Firewall (WAF) · Çok katmanlı DDoS savunması · Yük dengeleme · TLS/PKI yönetimi · SIEM-hazır gözlemlenebilirlik — tek kontrol düzleminden, on-prem veya air-gapped kurulumla.

Belge tipi	Teknik Datasheet (v1.0)	Sınıflandırma	Müşteriye Özel / Ticari
Hedef kitle	Güvenlik & Altyapı Mimarisi	Sektör	Bankacılık & Finans
Kapsam	Mimari · Yetenek · Uyum · PoC	Tarih	[Doldurulacak]

Hazırlayan: **[Şirket Adı]** · İletişim: [ad soyad] · [e-posta] · [telefon]
Bu belge alıcı kurumun değerlendirme süreci için hazırlanmıştır ve gizlilik kapsamındadır.

01 — YÖNETİCİ ÖZETİ

Neden Sentra?

Sentra, finansal kurumların internete açık uygulamalarını (internet bankacılığı, mobil API gateway'leri, kurumsal portaller, ödeme uçları) uçtan uca korumak üzere tasarlanmış **bütünleşik bir edge güvenlik platformudur**. Ayrı ayrı tedarik edilen WAF, DDoS, yük dengeleyici, DNS ve log/analitik ürünlerini tek bir kontrol düzleminde birleştirir; böylece operasyonel karmaşıklığı, tedarikçi sayısını ve ortalama müdahale süresini (MTTR) düşürür.

6-in-1	L3–L7	On-Prem	100%
WAF · DDoS · LB · DNS · TLS · Analitik	Ağdan uygulamaya katman kapsamı	Air-gapped & veri egemenliği	Kiracı (tenant) izolasyonu

FİNANS SEKTÖRÜ İÇİN ÖNE ÇIKANLAR

- **Veri egemenliği:** Tüm yığın kurum içinde çalışır; log ve trafik verisi kurumdan çıkmaz.
- **Fail-closed varsayılanlar:** Geo/IP izin listeleri belirsizlikte erişimi *kapatır* — sıkı güvenlik duruşu.
- **Değiştirilemez denetim izi:** Her yapılandırma değişikliği kayıt altında, geri alınabilir (undo).
- **Kontrollü yayınlama:** Değişiklikler önce hazırlanır (staged), onaylı *Deploy* ile üretime geçer.
- **SIEM entegrasyonu:** rsyslog/syslog ile merkezî log iletimi ve ELK tabanlı adli analiz.

ÇÖZDÜĞÜ TEMEL SORUNLAR

- OWASP Top 10 ve otomatik bot/zafiyet tarama trafiğine karşı uygulama katmanı savunması.
- Hacimsel ve uygulama katmanı DDoS ataklarında hizmet sürekliliği.
- Coğrafi ve IP tabanlı erişim politikalarının merkezî uygulanması.
- Sertifika yaşam döngüsü ve TLS sıkılaştırma yönetiminin tek yerden yürütülmesi.
- Güvenlik olaylarının gerçek zamanlı görünürlüğü ve olay müdahalesi.

> Bu belge yalnızca teknik yetenekleri açıklar. Kesin performans rakamları ve kapasite planı, kurumun gerçek trafik profiliyle yürütülecek **PoC (Kavram Kanıtı)** sırasında ölçülür (bkz. §11).

02 — ÇÖZÜM MİMARİSİ

Kontrol düzlemi + akıllı veri düzlemi

Sentra iki katmanlı çalışır: yapılandırmanın yönetildiği **merkezî kontrol düzlemi** ve ziyaretçi trafiğini karşılayan dağıtık **uç (edge/node) sunucuları**. Yönetici tüm ayarları panelde/API'de yapar; değişiklikler yalnızca **Deploy** ile, DataPlane API ve SPOE senkronizasyonu üzerinden filoya güvenle uygulanır.

2.1 İstek Yaşam Döngüsü (Request Lifecycle)

İstemci → TLS Sonlandırma (HAProxy) → L3/L4 hız & bağlantı sınırı (stick-tables) → **ac-agent (SPOE)**: geo/IP kararı + per-pool DDoS → **WAF (ModSecurity/OWASP CRS)**: denetim, learn/block → Yük dengeleme + sağlık kontrolü → **Origin sunucu**. Paralelde: erişim & WAF olayları → rsyslog → Logstash → Elasticsearch.

2.2 Bileşen Envanteri

BİLEŞEN	KATMAN	SORUMLULUK	TEKNOLOJİ
sentradns-admin	Kontrol	Yönetim paneli, REST API, çok kiracılı orkestrasyon, deploy hattı, denetim izi	Go 1.25 · PostgreSQL
lb	Veri (edge)	Yük dengeleme, TLS sonlandırma, sağlık kontrolü, stick-table DDoS	HAProxy 3.3 · DataPlane API v3
waf	Veri (edge)	Uygulama katmanı denetim, learn/block, veri sızıntısı koruması	libmodsecurity 3.0.x · OWASP CRS
ac-agent	Veri (edge)	Gerçek zamanlı geo/IP kararları, per-pool DDoS, GeoIP çözümleme	Go · HAProxy SPOE
sentra-agent	Veri (edge)	Node operasyon/diag API, servis yönetimi, bootstrap	Go · HTTP
sentradns-dns	Veri (edge)	Otoritatif DNS + DNS firewall, harici secondary	Go · NSD/BIND · TSIG
Analytics (ELK)	Kontrol	Log toplama, arama, gerçek zamanlı içgörü panoları	Elasticsearch · Logstash · Metricbeat
AI Assistant	Kontrol	Operasyon asistanı, onaylı işlem önerileri	Çok sağlayıcılı LLM (OpenAI-uyumlu)
Penetra opsiyonel	Federe	AI destekli sızma testi, CVE doğrulama	Federation API · RoE guard

2.3 Yüksek Erişilebilirlik (HA) Topolojisi

VERİ DÜZLEMİ

- Yatay ölçeklenen çok node'lu edge filosu; her node bağımsız trafik karşılar.
- Node başına aktif origin sağlık kontrolü; sağlıksız origin otomatik devre dışı.
- Failover/backup origin ve maintenance modu ile kesintisiz bakım.
- Node arızası trafiği diğer node'lara yönlendirir (upstream LB/anycast ile).

KONTROL DÜZLEMİ

- Kontrol düzlemi kesintisi trafiği *etkilemez*: edge node'lar mevcut yapılandırmayla çalışmaya devam eder.
- PostgreSQL yedekleme/replikasyon ile durum kalıcılığı.
- Deploy hattı kısmî başarıyı raporlar; drift durumunda *force deploy* ile yeniden hizalama.
- Yapılandırma kaynağı merkezîdir; node yeniden kurulunca bootstrap ile otomatik geri yüklenir.

03 — UYGULAMA KATMANI GÜVENLİĞİ (WAF)

ModSecurity + OWASP Core Rule Set

Sentra WAF motoru, endüstri standardı **libmodsecurity** ve **OWASP Core Rule Set (CRS)** üzerine kuruludur. Her pool (uygulama) için bağımsız profil, hassasiyet (paranoia) seviyesi ve mod ataması yapılabilir.

3.1 OWASP Top 10 Kapsama Matrisi

OWASP TOP 10 (2021)	SENTRA KONTROLÜ	DURUM
A01 Broken Access Control	Geo/IP erişim politikaları, IP allow-only, rate limiting, path bazlı kural setleri	✓
A02 Cryptographic Failures	TLS 1.2/1.3 zorlama, HSTS, zayıf cipher engelleme, Full-Strict origin doğrulama	✓
A03 Injection (SQLi/Cmd)	CRS SQLi/RCE/LFI/RFI kural grupları, paranoia 1–4	✓
A04 Insecure Design	Learn modu ile davranış temeli, kademeli sıkılaştırma	✓
A05 Security Misconfiguration	Merkezî politika, zincir/expiry denetimi, güvenli varsayılanlar	✓
A06 Vulnerable Components	Penetra CVE doğrulama (opsiyonel), imza/zafiyet tarama tespiti	✓
A07 Auth Failures	Kimlik bypass tespiti (CRS), rate limiting, IP reputation	✓
A08 Data Integrity Failures	Protocol/method enforcement, deserialization kuralları	✓
A09 Logging & Monitoring	Tam olay logu, ELK analiz, SIEM iletimi, denetim izi	✓
A10 SSRF	Protokol/şema kısıtları, çıkış/istek kalıp kuralları	✓

ÇALIŞMA MODLARI

- **Learn (Gözlem):** Kurallar değerlendirilir, ihlaller loglanır ama *trafik kesilmez* — canlı uygulamada yanlış pozitifleri güvenle kalibre etmek için.
- **Block (Engelleme):** İhlaller anında engellenir.
- Loglarda **LEARN** ve **BLK** ayrımı net görünür; migrasyon riski sıfırlanır.

İNCE AYAR & YANLIŞ POZİTİF YÖNETİMİ

- Paranoia 1–4: koruma sıkılığı ve hassasiyet dengesi.
- Request & Response korumaları: SQLi, XSS, RCE, scanner, veri sızıntısı (SQL/PHP/IIS hata sızıntısı, webshell).
- Hazır **CMS istisnaları** (WordPress/Drupal vb.) ile hızlı devreye alma.
- Log ekranından *tek tıkla* kural devre dışı bırakma (host/global) ve IP block/whitelist.

> Sağlık kontrolü uçları (health check) WAF denetiminden muaf tutulabilir; statik dosyalar için bypass ile gereksiz denetim ve gecikme önlenir.

04 — DDOS SAVUNMASI & ERİŞİM DENETİMİ

Çok katmanlı hız sınırlama ve coğrafi/IP politikaları

4.1 Katmanlı Savunma

KATMAN	MEKANİZMA	ÖRNEK KONTROL
L3 / L4	HAProxy stick-tables	Kaynak IP başına istek/bağlantı hızı; eşik aşımında sessiz reddetme (TCP RST) — WAF'tan önce
Bağlantı	Connection cap	Pool başına eşzamanlı bağlantı tavanı (seviye ön-ayarlı: 8000/4000/2000/1000)
L7 (uygulama)	ac-agent SPOE + WAF	Per-pool koruma seviyesi, challenge, request-rate/anomali
Politika	Geo / IP kuralları	Ülke ve IP/CIDR bazlı allow/deny, block veya log

KORUMA SEVİYELERİ

- **Off · Low · Medium · High · Under Attack** — pool bazında.
- **Inherit (devralma):** Pool, organizasyon varsayılanını devralır; org profili değişince tüm devralanlar bir sonraki deploy'da güncellenir.
- Aksiyonlar: **block · challenge · log**; challenge TTL yapılandırılabilir (5 dk–24 saat).

COĞRAFİ & IP ERİŞİM

- **Geo:** whitelist ("yalnız şu ülkeler") veya blacklist ("şu ülkeler hariç"), ISO kodlarıyla.
- **IP:** allow-only (yalnız izinli IP'ler) veya blacklist; global veya pool kapsamı.
- GeoIP tabanlı çözümleme; karar noktası SPOE'de, mikrosaniye ölçeğinde.

Fail-closed tasarım (finans için kritik avantaj): Geo/IP whitelist modları, eşleşme belirsizse veya coğrafi veri yoksa erişimi *kapatır*. Bu, "şüphede engelle" ilkesini teknik olarak garanti eder — ancak devreye almadan önce en az bir izin kuralı ve (geo için) GeoIP veritabanının yüklü olması gerekir. Sentra bu güvenli duruşu varsayılan yapar.

05 — TLS/PKI, YÜK DENGELEME & DNS

Trafik yönetimi ve şifreleme

TLS / PKI YÖNETİMİ

- Merkezî sertifika deposu: **PEM** ve **PFX/PKCS12** yükleme.
- **ACME-native** otomatik sertifika (HAProxy 3.3 crt_store) — Let's Encrypt uyumlu yenileme.
- Şifreleme modları: **Off · Flexible · Full · Full (Strict)** (origin sertifika doğrulama).
- Minimum TLS sürümü (1.0–1.3), **HSTS**, **HTTP/2**, **0-RTT**.
- Sertifika zinciri denetimi (eksik intermediate / expiry / güvenilmeyen kök) ve Origin CA üretimi.
- Wildcard ve SAN sertifikaları eşleşen hostname'leri otomatik kapsar.

YÜK DENGELEME

- Algoritmalar: **Round Robin · Least Connection · Source IP · URI · URL Param**.
- Aktif sağlık kontrolü: interval, fall/rise eşikleri, özel path/kod/method.
- Ağırlıklı origin dağıtımı, failover/backup, maintenance modu.
- Kaynak-IP kalıcılığı (session persistence) desteği.
- **Quick Pool:** hostname'den origin/port/TLS otomatik keşfi.

5.1 DNS Güvenliği

OTORİTATİF DNS

- Tam kayıt yönetimi: A, AAAA, CNAME, MX, TXT, NS, SRV, CAA.
- Zone import: **BIND · Cloudflare · JSON**; export ve versiyonlu deploy.
- Harici **secondary** (NSD/BIND) desteği; per-zone **TSIG** anahtarlı zone transfer ve notify.

DNS FİREWALL (UÇ NOKTA)

- Kategori bazlı domain filtreleme (kötü amaçlı yazılım, phishing vb.).
- Yeniden kullanılabilir **profiller**, safe search, özel allow/block listeleri.
- İstemci/CIDR bazlı profil ataması, token ile otomatik cihaz kaydı.

06 — GÖZLEMLENEBİLİRLİK & ADLİ ANALİZ

Gerçek zamanlı görünürlük, SIEM entegrasyonu ve denetim izi

ANALİTİK (ELK TABANLI)

- **WAF Güvenlik:** toplam olay, benzersiz saldırgan IP/ülke, saldırı origin haritası, top saldırı türleri ve tetiklenen kurallar.
- **Load Balancer:** istek/hata oranı, gecikme p50/p95/p99, top URL'ler, ülkeler, sonlanma durumları.
- **Sistem Performansı:** Metricbeat ile yanıt süresi, istek oranı, bağlantı ve ağ metrikleri.
- Zaman aralığı (1h/24h/7d) ve pool bazlı filtreleme.

SIEM & LOG İLETİMİ

- **rsyslog/syslog** ile merkezî log node'una iletim (Logstash input).
- Yapılandırılmış WAF/erişim olayları — kurumsal SIEM'e (Splunk/QRadar vb.) syslog üzerinden yönlendirilebilir.
- Log detayında tam olay JSON, eşleşme (match), etiketler; *tek tıkla* müdahale aksiyonları.
- Elasticsearch üzerinde arama (Lucene sorgu dili) ve saklama politikası.

6.1 Değiştirilemez Denetim İzi (Audit Trail)

Panelde, API'de veya AI asistanı aracılığıyla yapılan **her yapılandırma değişikliği** kaynağı (ai/ui/api), durumu, özeti, gerekçesi ve zaman damgasıyla kayıt altına alınır. Uygun işlemler **geri alınabilir (undo)**. Bu, finansal denetim ve olay sonrası inceleme (post-mortem) için tam izlenebilirlik sağlar.

Kim · **Ne zaman** · **Hangi kaynak** (UI/API/AI) · **Ne değişti** (hedef + alan farkı) · **Gerekçe** · **Durum** (applied/undone) — hepsi sorgulanabilir kayıt.

07 — ÇOK KİRACILILIK & YETKİLENDİRME

İzolasyon, roller ve yönetişim

Sentra baştan **çok kiracılı (multi-tenant)** tasarlanmıştır. Her organizasyon; domain, pool, sertifika, kullanıcı ve politika kümesiyle tam olarak izole edilir. Bir kurumun holding/iştirak yapısında farklı birimleri ayrı organizasyonlar olarak yönetilebilir; superadmin filo genelinde görünürlük sağlar.

7.1 Rol Tabanlı Erişim Denetimi (RBAC)

ROL	GÖRÜNTÜLEME	TEMEL İŞLEM	PROFİL/CLİENT/TOKEN	TAM YÖNETİM + DEPLOY	KULLANICI YÖNETİMİ
Viewer	✓	—	—	—	—
User	✓	✓	—	—	—
Manager	✓	✓	✓	—	—
Admin	✓	✓	✓	✓	✓

Ayrıca platform genelinde ayrı bir **superadmin** katmanı; organizasyon oluşturma, filo görünürlüğü ve merkezî domain yönetimi sağlar.

7.2 Değişiklik Yönetişimi

STAGED

Değişiklikler önce hazırlanır; üretime otomatik yansımaz. "N bekleyen değişiklik" göstergesi.

DEPLOY

Onaylı yayınlama; tip bazlı (LB/WAF/Security). Kısmî başarı raporu ve *force deploy*.

AUDİT + UNDO

Her işlem kayıtlı ve geri alınabilir; drift'e karşı orphan temizliği (CLI).

08 — AI OPERASYON & PENETRA

İnsan onaylı otomasyon ve saldırgan güvenlik

AI OPERASYON ASİSTANI

- Çok sağlayıcılı LLM (OpenAI-uyumlu API: Groq/Ollama/Cerebras/DeepSeek — *on-prem/self-host mümkün*).
- **İnsan-döngüde (human-in-the-loop):** Asistan yazma işlemini asla otomatik uygulamaz; *Action Card* ile risk seviyesi ve gerekçe sunar, operatör **onaylar**.
- Her AI kaynaklı işlem denetim izine girer ve geri alınabilir.
- Org-scope korumalı araç kayıt sistemi — kiracı sınırları LLM katmanında da korunur.

PENETRA — CTEM & SIZMA TESTİ PLATFORMU AYRI ÜRÜN

- Üç katmanlı analiz: **pasif** (DNS/TLS/başlık/CT-log keşfi — her zaman güvenli) → **madencilik** (WAF ve erişim loglarından davranış temeli) → **aktif** (SQLi/XSS/SSRF/LFI, Nuclei, portscan, dizin fuzz).
- **RoE (Rules of Engagement) guard:** Aktif tarama yalnızca yazılı izin çerçevesi tanımlıysa çalışır; aksi hâlde reddedilir. Tam denetim izi.
- **Log tabanlı politika madenciliği:** Sentra'nın uç loglarından her URL'nin method/parametre şemasını öğrenip WAF politikası önerir — dışarıdan tarayan rakiplerin göremediği veri.
- Federation ile Sentra'ya entegre; bulgular kurum veritabanında kalır. Tek başına da (Sentra'sız) çalışır.

> Yapay zekâ katmanı isteğe bağlıdır ve **self-host LLM** ile çalıştırılabildiğinden, veri gizliliği hassas kurumlarda dış servise veri göndermeden kullanılabilir.

09 — KURULUM, ENTEGRASYON & ÖLÇEKLEME

Devreye alma modelleri ve sistem gereksinimleri

ON-PREM

Tüm yığın kurum içinde. Veri egemenliği, iç ağ görünürlüğü. Debian paketleriyle (.deb) dağıtım.

AİR-GAPPED / BYOL

İnternetsiz ortam. Offline **Ed25519** imzalı lisans + entitlement motoru. AWS Marketplace BYOL AMI.

SAAS / YÖNETİLEN

Bulut kontrol düzlemi + yönetilen edge. Hızlı devreye alma (değerlendirme/PoC için ideal).

9.1 Entegrasyon Noktaları

ENTEGRASYON	YÖNTEM	DURUM
REST API	Tam yönetim API'si; otomasyon/IaC ve CI/CD ile entegrasyon	**Mevcut**
SIEM / Log	rsyslog/syslog iletimi + ELK; harici SIEM'e yönlendirme	**Mevcut**
API kimlik doğrulama	E-posta/parola oturumu + organizasyon API anahtarı	**Mevcut**
ACME / PKI	Let's Encrypt uyumlu otomatik sertifika; kurumsal CA yükleme	**Mevcut**
SSO (SAML/OIDC)	Kurumsal kimlik sağlayıcı ile tek oturum	**Yol haritası**
MFA / 2FA	Çok faktörlü kimlik doğrulama	**Yol haritası**

9.2 Ağ & Port Matrisi (özet)

YÖN	PORT/PROTOKOL	AMAÇ
Dış → Edge	443/TCP (HTTPS), 80/TCP (yönlendirme)	Ziyaretçi trafiği
Dış → DNS	53/UDP,TCP	Otoritatif DNS / DNS firewall
Kontrol → Edge	DataPlane API (yönetim), SPOE senkron	Yapılandırma dağıtımı
Edge → Log	syslog (rsyslog)	Merkezî log iletimi
Yönetici → Kontrol	Panel/HTTPS + REST API	Yönetim erişimi

Kesin port planı ve segmentasyon (DMZ/iç ağ) kurum mimarisine göre PoC'de netleştirilir.

9.3 Boyutlandırma

Veri düzlemi **HAProxy** tabanlı olup yüksek eşzamanlılık ve düşük gecikme için endüstride kanıtlanmıştır. Node başına kapasite; trafik profili (RPS, eşzamanlı bağlantı, TLS el sıkışma oranı, WAF paranoia seviyesi) ve donanıma göre değişir. Kesin kapasite ve node sayısı planı, kurumun gerçek yük profiliyle **PoC'de ölçülerek** belirlenir.

10 — UYUM & REGÜLASYON

Regülasyon uyumunu destekleyen teknik kontroller

Sentra, aşağıdaki çerçevelerin gerektirdiği teknik kontrolleri **destekler**. (Sertifikasyon; kurumun süreç, politika ve denetim bütünüyle elde edilir — aşağıdaki eşleme, platformun sağladığı teknik yetenekleri gösterir.)

ÇERÇEVE	İLGİLİ GEREKSİNİM	SENTRA'NIN SAĞLADIĞI TEKNİK KONTROL
PCI-DSS	Req. 1/6.4.2 (WAF), 4 (TLS), 10 (log & izleme)	OWASP WAF, TLS 1.2/1.3 zorlama, tam denetim izi + SIEM iletimi
BDDK (Bilgi Sistemleri Yönetmeliği)	Sızma testi, erişim kontrolü, loglama, veri yurt içinde	Penetra pentest, RBAC, kayıt/izleme, **on-prem veri egemenliği**
KVKK	Kişisel verinin güvenliği, erişim sınırlama, iz kaydı	Kiracı izolasyonu, geo/IP erişim, denetim izi, veri kurum içinde
ISO/IEC 27001	A.8/A.12/A.13 erişim, işletim, iletişim güvenliği	RBAC, değişiklik yönetişimi, ağ güvenlik kontrolleri, izleme
GDPR	Bütünlük & gizlilik, veri minimizasyonu	Şifreleme, erişim denetimi, self-host AI ile veri lokalizasyonu

VERİ EGEMENLİĞİ

- On-prem/air-gapped kurulumda trafik ve log verisi **kurumdan çıkmaz**.
- AI katmanı self-host LLM ile dış servise veri göndermeden çalışabilir.

HESAP VEREBİLİRLİK

- Değiştirilemez denetim izi + undo ile "kim, ne, ne zaman" tam kaydı.
- Kontrollü deploy ile değişiklik yönetişimi ve onay zinciri.

> Uyum eşlemesi bilgilendirme amaçlıdır; kurumun mevcut politika ve denetim süreçleriyle birlikte değerlendirilmelidir.

11 — POC METODOLOJİSİ & YOL HARİTASI

Kavram Kanıtı (Proof of Concept) süreci

Sentra PoC'si, kurumun gerçek (veya temsili) trafik profiliyle, kontrollü bir ortamda yürütülür. Tipik PoC 1–2 haftada tamamlanır ve teknik başarı kriterleri baştan yazılı olarak belirlenir.

AŞAMA	İÇERİK	ÇIKTI
1. Hazırlık	Kapsam, hedef uygulamalar, başarı kriterleri, RoE; ağ/port planı	PoC planı
2. Kurulum	On-prem admin + 1+ edge node; DNS/pool/origin tanımı	Çalışan ortam
3. Güvenlik	WAF learn→block kalibrasyonu, DDoS/geo/IP politikaları, TLS	Sıkılaştırılmış profil
4. Gözlem	ELK panoları, SIEM iletimi, denetim izi doğrulama	Görünürlük
5. Doğrulama	Kontrollü saldırı senaryoları, Penetra (opsiyonel), yük testi	Kanıt raporu
6. Değerlendirme	Başarı kriterleri karşılaştırması, boyutlandırma, üretim planı	Sonuç & teklif

11.1 Yol Haritası (Şeffaflık)

YAKIN DÖNEM

- Planlı SSO (SAML/OIDC) ile kurumsal kimlik entegrasyonu.
- Planlı MFA / 2FA yönetici kimlik doğrulaması.

MEVCUT OLGUNLUK

- Üretim WAF, DDoS, LB, DNS, TLS, analitik, RBAC, denetim izi, SIEM iletimi.
- Üretim On-prem/air-gapped kurulum, BYOL lisanslama.

Sonraki Adım

Kurumunuza özel bir PoC planlamak ve teknik derinlemesine oturum (deep-dive) düzenlemek için bizimle iletişime geçin.

[Şirket Adı] · [ad soyad] · [e-posta] · [telefon] · [web]