CYBERPORT

Kontrolsüz AI,

Kurumsal risktir

LLMFORT NEDİR

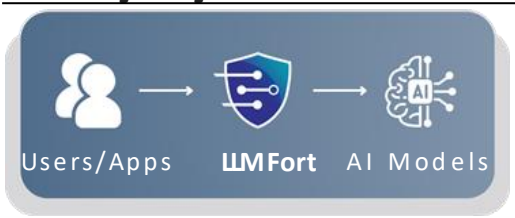
Kurumların LLM ve üretken yapay zekâ kullanımını güvenli hale getiren bir **AI Firewall / LLM Security** çözümüdür.

Kullanıcı ve uygulama trafiğini merkezi olarak denetler; riskli içerikleri modele ulaşmadan önce durdurur.

HANGİ RİSKLERİ ÖNLER?

- Prompt injection ve jailbreak girişimlerini engeller
- PII, gizli ve hassas verileri dışarı çıkmadan önler.
- Kurumsal politika ihlallerini tespit eder ve müdahale eder.
- AI kullanımını güvenli, izlenebilir ve denetlenebilir hale getirir.

NASIL ÇALIŞIR?



Kullanıcıdan veya uygulamadan gelen LLM isteklerini bir **merkezi güvenlik katmanı** üzerinden geçirir; burada çok katmanlı analiz yapar ve riske göre **engelleme, maskeleme veya reddetme** uygular.

Yapay zekâ güvenliğini 4 aşamalı süreçle sağlar:

TEMEL FAYDALARI

1.Veri Güvenliği ve Risk Önleme

- Hassas veriyi (PII) gerçek zamanlı korur
- Prompt injection ve jailbreak saldırılarını engeller
- WAF / NGFW seviyesinin ötesinde AI tehditlerini tespit eder

2. Maliyet ve Kaynak Yönetimi

- AI kullanımını izler, kullanım ve maliyetleri optimize eder
- Token, API ve kullanım bazlı harcamalarda kontrol sağlar
- Kaynakları iş önceliklerine göre yönlendirir

3. Merkezi Yönetim ve Kontrol

- Tüm AI kullanımını tek noktadan yönetir
- Kurumsal politikaları uygular ve ihlalleri engeller
- Active Directory ile entegre çalışır

4. Tam Görünürlük ve Denetim

- Tüm AI etkileşimlerini kayıt altına alır
- Anlık izleme ve raporlama sağlar
- Uyumluluk süreçlerini kolaylaştırır

5. Performans ve Entegrasyon

- Sistemleri yavaşlatmadan çalışır
- Çoklu LLM desteği ile vendor bağımsızdır
- Hızlı ve kolay entegrasyon sağlar

DAĞITIM SEÇENEKLERİ

Inline Mode (Aktif Koruma)

Trafiğin içinde aktif koruma sağlar, tehditleri anında engeller.

Out-of-Band Mode (Pasif İzleme)

Trafiği kesmeden izler, görünürlük ve analiz sağlar.

ENTEGRASYONLAR

- SIEM
- SOAR
- Slack
- Teams
- Webhook
- API
- Jira
- Jenkins
- Azure DevOps

Yapay Zekânızı Koruyun, İşinizi Koruyun.