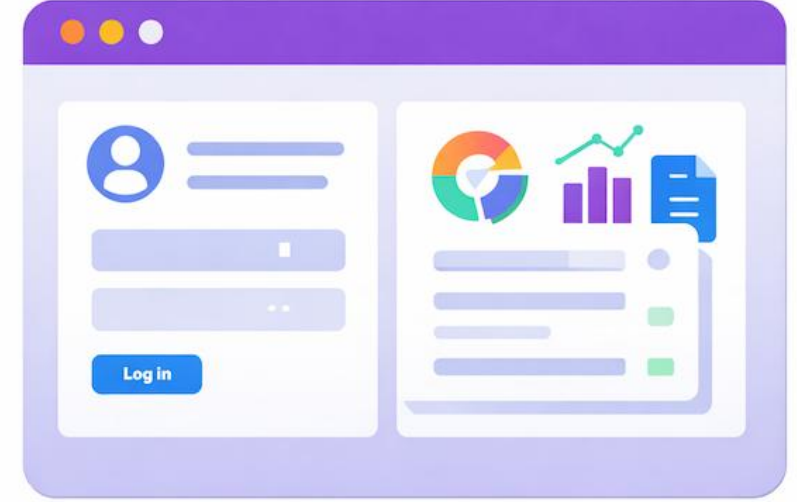


Sigorta Sektöründe Secure Browser ile Zero Trust Yaklaşımı

Sigorta Sektöründe Dijital Çalışma

- İş uygulamalarına erişimin ana noktası tarayıcı
- Poliçe, hasar ve operasyon sistemleri web uygulamaları üzerinden çalışıyor
- Çalışanlar günün büyük bölümünü tarayıcı tabanlı uygulamalarda geçiriyor
- Kritik sistemlerin önemli kısmı hâlâ on-prem ortamda



Güvenlik Perspektifinden Ortaya Çıkan Yeni Gerçek

- Kimlik ve şifre avı saldırıları en büyük risklerden biri
- Saldırıları artık ağı değil kullanıcı davranışını hedefliyor
- Geleneksel güvenlik çözümleri yeni tehditlere karşı yetersiz kalabiliyor
- Hassas müşteri verilerinin büyük bölümü tarayıcı üzerinden işleniyor
- SaaS ve AI araçları ile etkileşim artıyor



Geleneksel Güvenlik Katmanlarının Doğal Sınırı

- Firewall → ağ trafiğini izler
- Proxy → web erişimini kontrol eder
- VPN → uzak bağlantıyı sağlar

Ama bu çözümler:

- Tarayıcı içindeki kullanıcı davranışını göremez
- Kullanıcının hangi veriyi paylaştığını göremez
- Login ekranlarında gerçekleşen riskleri tespit edemez



Neden Secure Browser Öne Çıktı?

Amacımız yeni bir network ürünü eklemek değildi.

Aradığımız şey:

- Kullanıcının gerçekten çalıştığı noktada güvenlik
- Tarayıcı içindeki etkileşimlerin görünürlüğü
- Veri paylaşımının kontrolü
- Kimlik bilgilerinin korunması

Bu nedenle **Secure Browser** yaklaşımını değerlendirmeye başladık.



Kurduğumuz Mimari

Yeni mimaride:

- Mevcut güvenlik katmanları korunuyor
- Tarayıcı seviyesinde yeni bir kontrol katmanı ekleniyor
- Erişim merkezi politikalar ile yönetiliyor

Bu sayede güvenlik kontrol noktası **ağdan tarayıcıya doğru genişlemiş oldu.**

Ek olarak:

- Proxy çözümünü Secure Browser erişim kontrolü ile değiştirdik
- Destek sistemlerine erişimde VPN ihtiyacını kaldırdık
- Daha sade ve daha güvenli erişim alt yapısı oluşturduk
- Lisans maliyetlerimiz azaldı, ürün sayısı azaldı , operasyonel verimlilik arttı.



Tarayıcı Seviyesinde AI Veri Koruması

Secure Browser yaklaşımı sayesinde:

- AI araçlarına gönderilen sorgular analiz edilebilir
- Hassas veri paylaşımı engellenebilir
- Kurumsal veri politikaları uygulanabilir

Böylece çalışanların kullandığı AI araçları da güvenlik kapsamına alınabiliyor.

Bu alan projemizin bir sonraki doğal adımı olacak.



Projeden Elde Ettiğimiz Sonuçlar

Bu yaklaşım bize önemli kazanımlar sağladı:

Güvenlik

- Kimlik avı ve şifre ele geçirme risklerinde görünürlük arttı
- Hassas veri paylaşımları kontrol altına alındı

Mimari

- VPN ihtiyacı azaldı. Erişim mimarisi sadeleşti
- Erişim kontrolleri tarayıcı seviyesine taşındı, Proxy ortadan kalktı.

Kullanıcı Deneyimi

- Çalışanlar mevcut tarayıcılarını kullanmaya devam etti
- Erişim deneyimi değişmeden güvenlik seviyesi yükseldi

Operasyonel

- Lisans maliyetlerimiz azaldı, ürün sayısı azaldı , operasyonel verimlilik arttı.
- **Tarayıcı artık sadece bir erişim aracı değil, kurumsal güvenliğin aktif bir parçası haline geldi.**



Teşekkürler