İÇİNDEKİLER

Antikor Secure Browser.....2
1. Projenin Amacı.....2
2. Kritik Web Uygulamalarını Dünyaya Açmanın Riskleri.....2
2.1. Siber Saldırı Yüzeyi.....2
2.2. Veri Sızıntısı ve Ulusal Güvenlik.....3
2.3. Kimlik Doğrulama Yetersizliği.....3
2.4. Denetim ve İzlenebilirlik Eksikliği.....3
2.5. Bu Proje ile Risklerin Ortadan Kaldırılması.....3
3. Yerli ve Milli Ürün Vurgusu.....4
Neden Yerli Çözüm Zorunludur?.....4
Kritik Önem.....5
4. Temel Güvenlik Mimarisi.....5
Standart Tarayıcı Erişimi Nasıl Engellenir?.....5
Cihaz Kimlik Doğrulama.....5
Çok Katmanlı Güvenlik.....5
5. Temel Yetenekler.....6
5.1. Beş Platform Desteği.....6
5.2. Kullanıcı Deneyimi.....6
5.3. Merkezi Yönetim.....6
5.4. Uyumluluk.....7
5.5. Ölçeklenebilirlik.....7
6. Standart Tarayıcıdan Farkı — Karşılaştırma.....7
7. İş Faydaları.....8
7.1. Güvenlik Faydaları.....8
7.2. Yönetimsel Faydalar.....8
7.3. Ekonomik Faydalar.....8
7.4. Stratejik Faydalar.....8
8. Sonuç ve Değerlendirme.....8

Antikor Secure Browser

1. Projenin Amacı

Güvenli Kurumsal Tarayıcı; kamu kurumlarının kritik web uygulamalarına **yalnızca yetkilendirilmiş cihazlardan, yalnızca bu özel tarayıcı aracılığıyla** erişim sağlanmasını garanti eden, tamamen **yerli ve milli** olarak geliştirilen bir siber güvenlik çözümüdür.

Mevcut durumda kamu personeli, kurumsal web uygulamalarına Chrome, Firefox, Edge gibi yabancı menşeli standart tarayıcılar üzerinden erişmektedir. Bu durum ciddi güvenlik riskleri barındırmaktadır:

- Standart tarayıcılar cihaz kimlik doğrulaması yapmaz
- Herhangi bir kişisel veya yetkisiz cihazdan erişim mümkündür
- Tarayıcı eklentileri ve üçüncü taraf yazılımlar veri sızıntısına zemin hazırlar
- Yabancı menşeli tarayıcıların arka planda hangi verileri topladığı denetlenememektedir

Bu proje ile standart tarayıcılardan kurumsal uygulamalara erişim tamamen engellenmekte; erişim yalnızca Güvenli Kurumsal Tarayıcı üzerinden, kayıtlı ve onaylı cihazlarla mümkün kılınmaktadır.

2. Kritik Web Uygulamalarını Dünyaya Açmanın Riskleri

Kamu kurumlarının kritik web uygulamaları (personel bilgi sistemi, hasta kayıt sistemi, adli sicil sorgulaması, vergi sistemi, nüfus kayıt sistemi vb.) günümüzde internet üzerinden erişime açılmak zorunda kalınmaktadır. Ancak bu uygulamaları **standart tarayıcılar üzerinden herkesin erişimine açık tutmak**, aşağıdaki hayati riskleri doğurmaktadır:

2.1. Siber Saldırı Yüzeyi

- Kurumsal uygulamalar dünyaya açık olduğunda, **dünyanın herhangi bir noktasından** saldırı girişimi yapılabilir
- Brute-force, credential stuffing, SQL injection, XSS gibi saldırılar 7/24 otomatize araçlarla denenebilir
- Sıfır-gün (zero-day) açıkları keşfedildiğinde kamu uygulamaları ilk hedefler arasında yer alır
- DDoS saldırıları ile kritik kamu hizmetleri devre dışı bırakılabilir

2.2. Veri Sızıntısı ve Ulusal Güvenlik

- Başarılı bir sızma sonucunda **milyonlarca vatandaşın kişisel verileri** ele geçirilebilir
- Sağlık verileri, adli sicil bilgileri, nüfus kayıtları gibi hassas bilgiler karanlık ağda (dark web) satışa sunulabilir
- Yabancı devlet destekli APT (Advanced Persistent Threat) grupları kamu sistemlerini hedef almaktadır
- Veri ihlali durumunda KVKK kapsamında ağır idari para cezaları uygulanmaktadır

2.3. Kimlik Doğrulama Yetersizliği

- Standart tarayıcılarla erişimde **yalnızca kullanıcı adı ve parola** ile kimlik doğrulama yapılmaktadır
- Çalıntı kimlik bilgileri ile yetkisiz kişiler sisteme girebilmektedir
- Parola paylaşımı, oltalama (phishing) saldırıları ve sosyal mühendislik ile kimlik bilgileri kolayca ele geçirilebilmektedir
- Hangi cihazdan erişildiği bilinememekte, kayıp/çalıntı cihazlar üzerinden erişim engellenememektedir

2.4. Denetim ve İzlenebilirlik Eksikliği

- Standart tarayıcı kullanıldığında, erişimin hangi cihazdan yapıldığı doğrulanamamaktadır
- Olağandışı erişim desenlerinin tespiti güçleşmektedir
- Bir güvenlik ihlali yaşandığında kök neden analizi yapılamamaktadır
- Yasal denetim ve soruşturmalarda yeterli kanıt sağlanamamaktadır

2.5. Bu Proje ile Risklerin Ortadan Kaldırılması

Güvenli Kurumsal Tarayıcı, yukarıdaki riskleri **kök seviyede** ortadan kaldırır:

Risk	Güvenli Kurumsal Tarayıcı Çözümü
Saldırı yüzeyi	Sertifikasız bağlantılar otomatik reddedilir — saldırgan bağlantı bile kuramaz
Kimlik hırsızlığı	Çalıntı parola yetmez; kayıtlı cihaz + geçerli sertifika zorunlu
Yetkisiz cihaz erişimi	Yalnızca parmak izi doğrulanmış, kayıtlı cihazlar bağlanabilir
Kayıp cihaz	Yönetim Panelinden saniyeler içinde erişim iptal edilir
Denetim eksikliği	Her erişim; cihaz, kullanıcı, zaman damgası ile kayıt altında

Risk	Güvenli Kurumsal Tarayıcı Çözümü
DDoS/Bot saldırısı	mTLS handshake başarısız olan bağlantılar anında düşürülür — uygulama katmanına ulaşamaz

Özetle: Kritik kamu uygulamalarını "dünyaya açık standart web sitesi" olarak sunmak yerine, **yalnızca doğrulanmış cihaz ve tarayıcı ile erişilebilir kurumsal uygulama** haline getirmek; bu projenin temel değer önerisidir.

3. Yerli ve Milli Ürün Vurgusu

Neden Yerli Çözüm Zorunludur?

Kriter	Yabancı Tarayıcı	Güvenli Kurumsal Tarayıcı
Kaynak Kod Sahipliği	Yabancı şirketlerde, denetlenemez	Tamamen yerli, kaynak kodu ulusal kontrolde
Veri Egemenliği	Veriler yurt dışı sunuculara aktarılabilir	Tüm veriler kurum bünyesinde kalır
Arka Kapı Riski	Tespit edilemez	Kaynak kod denetimi mümkün
Güncelleme Kontrolü	Yabancı şirketin insiyatifinde	Kurum kendi güncelleme politikasını belirler
Yaptırım/Ambargo Riski	Hizmet kesintisi olasılığı var	Dışa bağımlılık yok
Milli Mevzuat Uyumu	Uyumsuz olabilir	KVKK, ISO 27001 tam uyumlu

Kritik Önem

- **Dijital egemenlik:** Kamu verilerinin yabancı teknoloji şirketlerinin kontrolüne bırakılmaması
- **Milli güvenlik:** Kritik altyapı erişiminin yabancı yazılıma bağımlı olmaması
- **Ekonomik bağımsızlık:** Lisans bedellerinin yurt içinde kalması, yerli teknoloji ekosisteminin güçlenmesi
- **Yaptırım dayanıklılığı:** Olası uluslararası yaptırımlarda hizmet sürekliliğinin garanti edilmesi

4. Temel Güvenlik Mimarisi

Standart Tarayıcı Erişimi Nasıl Engellenir?

Sistem, **Karşılıklı TLS (mTLS)** teknolojisi ile çalışır. Bu demektir ki:

1. **Kurumsal web uygulamalarına erişim için** sunucu, istemciden (tarayıcıdan) geçerli bir dijital sertifika talep eder
2. **Güvenli Kurumsal Tarayıcı** bu sertifikayı otomatik olarak sunar — kullanıcı hiçbir ek işlem yapmaz
3. **Standart tarayıcılar** (Chrome, Firefox, Edge, Safari) bu sertifikaya sahip olmadığı için bağlantı **anında reddedilir**
4. Yalnızca kayıtlı cihaz + yetkilendirilmiş tarayıcı kombinasyonu erişim sağlayabilir

Sonuç: Kurumsal uygulamalara erişim için tek kapı Güvenli Kurumsal Tarayıcı'dır. Başka hiçbir yol yoktur.

Cihaz Kimlik Doğrulama

Her cihaz sisteme kayıt olurken benzersiz bir "cihaz parmak izi" oluşturulur. Bu parmak izi:

- Cihazın donanım ve yazılım özelliklerinden türetilir
- Dijital sertifikaya gömülür
- Her erişimde otomatik doğrulanır
- Sahte veya klonlanmış cihazların sisteme sızması engellenir

Çok Katmanlı Güvenlik

Katman 1: Kullanıcı Kimlik Doğrulama (Kurumsal kimlik sağlayıcı + MFA)

Katman 2: Cihaz Kimlik Doğrulama (mTLS + Cihaz Parmak İzi)

Katman 3: Sürekli Doğrulama (Her istek otomatik kontrol)

5. Temel Yetenekler

5.1. Beş Platform Desteği

Platform	Desteklenen Sürümler
Windows	10 / 11
macOS	12 Monterey ve üzeri
Linux	Ubuntu 26.04+, Debian 12+, RHEL 9+
Android	10 ve üzeri
iOS	16 ve üzeri

Tüm platformlarda aynı güvenlik seviyesi sağlanmaktadır.

5.2. Kullanıcı Deneyimi

Güvenli Kurumsal Tarayıcı, güvenlik katmanları dışında **normal bir tarayıcı gibi** çalışır:

- Kurumsal sitelere erişimde güvenlik şeffaf biçimde sağlanır (kullanıcı fark etmez)
- Genel internet sitelerine (arama motorları, haber siteleri vb.) serbestçe erişim mümkündür
- Sekme yönetimi, yer imleri, geçmiş, indirme gibi standart tarayıcı işlevleri mevcuttur
- Kurumsal sitelerde güvenlik sertifikası uyarısı gösterilmez

5.3. Merkezi Yönetim

- Web tabanlı Yönetim Paneli ile tüm cihazlar tek noktadan yönetilir
- Anlık cihaz iptali: Kayıp/çalıntı cihazın erişimi saniyeler içinde kesilir
- Kurumsal site listesi merkezi olarak güncellenir — tüm cihazlara otomatik dağıtılır
- Detaylı raporlama: Kim, ne zaman, hangi cihazdan, hangi uygulamaya erişti
- Rol tabanlı erişim kontrolü ile yönetim yetkileri ayrıştırılır

5.4. Uyumluluk

- **KVKK** (6698 sayılı Kanun) tam uyumluluk
- **ISO 27001:2022** Bilgi Güvenliği Yönetim Sistemi uyumlu
- **OWASP ASVS v4.0** Uygulama Güvenliği Standardı uyumlu

- SIEM entegrasyonu ile mevcut güvenlik altyapısına entegre olur

5.5. Ölçeklenebilirlik

- Yatay ölçeklenebilir mimari — ihtiyaç arttıkça kapasite artırılabilir
- Yüksek erişilebilirlik — tek nokta arızası yok
- On-premise dağıtım — tüm veriler kurum içinde kalır

6. Standart Tarayıcıdan Farkı — Karşılaştırma

Özellik	**Standart Tarayıcı (Chrome/Edge/Firefox)**	**Güvenli Kurumsal Tarayıcı**
Kurumsal sitelere erişim	Herkes, her cihazdan	Yalnızca kayıtlı cihaz + yetkili kullanıcı
Cihaz doğrulama	Yok	mTLS + Cihaz Parmak İzi
Kayıp cihaz müdahalesi	Mümkün değil	Anlık uzaktan erişim iptali
Merkezi yönetim	Yok	Tam merkezi kontrol
Veri sızıntısı kontrolü	Yok	Kurumsal politika uygulanır
Denetim izi (audit)	Sınırlı	Her erişim kayıt altında
Yerli/Milli	Hayır (ABD menşeli)	Evet — %100 yerli geliştirme
Kaynak kod denetimi	İmkansız	Talep halinde denetlenebilir
Yaptırım riski	Var	Yok
KVKK uyumu	Belirsiz	Tam uyumlu

7. İş Faydaları

7.1. Güvenlik Faydaları

- Yetkisiz erişimin kök seviyede engellenmesi (sadece kayıtlı cihaz + özel tarayıcı)
- Standart tarayıcılarla kurumsal uygulamalara erişimin kesin olarak kapatılması
- Kayıp/çalıntı cihazlarda anlık müdahale imkanı
- Tüm erişimlerin denetlenebilir kayıt altına alınması
- Milli güvenlik açısından yabancı yazılım bağımlılığının ortadan kaldırılması

7.2. Yönetimsel Faydalar

- Tek merkezden tüm platform ve cihazların yönetimi
- Otomatik sertifika yenileme — operasyonel yük minimum
- Detaylı raporlama ile karar destek bilgisi
- KVKK ve ISO 27001 uyumluluk süreçlerinin kolaylaştırılması

7.3. Ekonomik Faydalar

- Yerli ürün olması sebebiyle lisans bedellerinin yurt içinde kalması
- Kamu teşvik mekanizmalarından yararlanma imkanı
- Uzun vadede bakım ve destek maliyetlerinin öngörülebilir olması
- Yerli siber güvenlik ekosisteminin güçlenmesine katkı

7.4. Stratejik Faydalar

- Dijital egemenlik hedeflerine doğrudan katkı
- Yaptırım ve ambargo senaryolarında hizmet sürekliliği
- Milli teknoloji hamlesinin somut bir çıktısı
- Referans proje olarak diğer kamu kurumlarına örnek teşkil etmesi

8. Sonuç ve Değerlendirme

Güvenli Kurumsal Tarayıcı projesi:

- **Kritik kamu uygulamalarının dünyaya açık bırakılmasının yarattığı riskleri** kök seviyede ortadan kaldırmaktadır
- **Standart tarayıcıların yarattığı güvenlik açığını** kesin olarak kapatmaktadır
- **Yerli ve milli** bir çözüm olarak dijital egemenlik hedeflerimize doğrudan hizmet etmektedir
- **Beş platformda** tutarlı güvenlik sağlayarak kurumsal mobilite ihtiyacını karşılamaktadır
- **On-premise dağıtım** modeli ile verilerin kurum dışına çıkmasını engellemektedir
- **KVKK ve ISO 27001** uyumluluğu ile mevzuat gereksinimlerini tam olarak karşılamaktadır

Kurumsal web uygulamalarına erişimin yalnızca bu özel tarayıcı üzerinden mümkün kılınması, başlı başına bir paradigma değişikliğidir. Artık "kim erişti?" sorusunun yanıtı her zaman net olacaktır: Yalnızca kayıtlı cihaz, yalnızca yetkili kullanıcı, yalnızca Güvenli Kurumsal Tarayıcı.