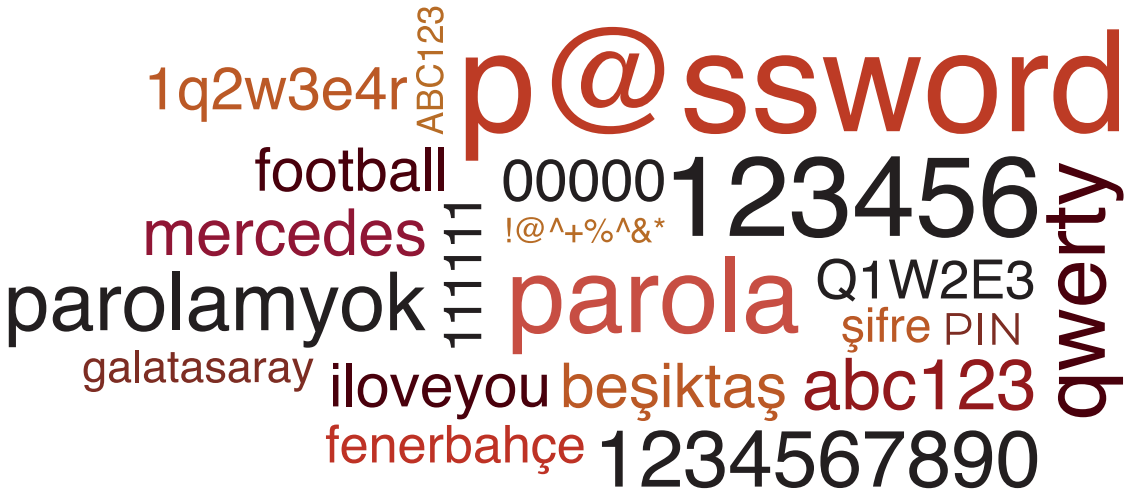
AUTHTAKE

Güvenlik Riskinin

Baş Aktörü

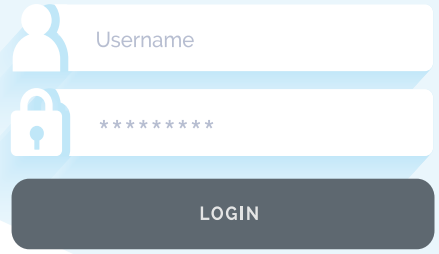
Parolalar



Parolasız Yaşamın Güvenliğini Keşfedin!

Parolaların Hayatımızdaki Yeri

Geçmişten günümüze kadar birçok alanda güvenliği sağlamanın baş aktörü olarak parolalar tercih edildi. Ancak çeşitli saldırılar karşısında parolaların savunmasız kalması ve çok kolay tahmin edilmesi, sırası ile bir dizi önlemler silsilesini de beraberinde getirmiş oldu.



Kurumlar müşteri ve personellerinin doğru ve güvenli erişimlerini sağlamak için öncelikle karmaşık parolaları zorunlu kıldı. Daha sonrasında ise ek bir güvenlik önlemi olarak parola değiştirme sıklığının artırılması şeklinde bir yol izledi. Bu güvenlik artırımları da beraberinde parolaların unutulmasına, bir yerlere yazılmasına ve yardım masasına ekstra yük binerek maliyet artırımına yol açtı.

> Veri ihlallerinin %61'i zayıf ya da çalınan parolalar nedeniyle olmuştur.

Yapılan araştırmalarda her beş kişiden dördünün farklı hesaplarda aynı parolayı yeniden kullandığı saptandı. Bu da hesaplardan herhangi birinin ele geçirilmesi durumunda diğer hesaplarda da böyle bir riskin ortaya çıkacağını gösteriyor.

Güvenlik Riskinin Baş Aktörü: Parolalar

Varonis 2019 Küresel Veri Riski Raporu'na göre kullanıcıların %38'i, geçen yıl %10'luk bir artışla süresi asla dolmayan parolalara sahip. Yine aynı rapore göre şirketlerin %58'inde kullanıcıların tutarsız izinlere sahip oldukları gözlemlendi.

Güvensizdir

Tahmin edilebilir, tekrar kullanılır, farklı noktalar aynı şifre vb.

Paylaşılır

İki kişinin bildiği sır değildir.

Çalınabilir

Basit ataklar ile ele geçirilebilir.

Yorucudur

Kullanıcı adı + Şifre + ...

Unutulur

Kompleks şifre politikası, sık değişime zorlama vb.

Maliyetlidir

Parolaya ilişkin çözümlerin yıllık kullanıcı başı maliyeti 179$

Kullanıcılar günümüzde kullanım zorluklarından dolayı geleneksel kimlik doğrulama yöntemlerini ve bunların güvenlik politikalarını esnetmeye yönelmekteler. Bu da ATO saldırılarının %98 oranında artmasına neden olmakta.

Bu tarz saldırıların önlenmesi amacıyla kurulan siber olaylara müdahale ekiplerinin (SOME) ve yardım masasında parolalara ilişkin çözümlerin maliyetleri de dikkate alındığında parolaların kuruluşlara verdiği maddi zararların çok yüksek boyutlara ulaştığı görülmektedir.

Bunun yanı sıra yaratmış olduğu itibar kaybı ise maddi olarak karşılanamayacak boyutta bir hasar olarak karşımıza çıkmaktadır.

Yapılan araştırmalar ile APT gruplarının en çok devletleri ve global çaptaki şirketleri hedef aldığı tespit edildi.

APT Gruplarının 2020 Yılı İlk 10 Hedef Listesi

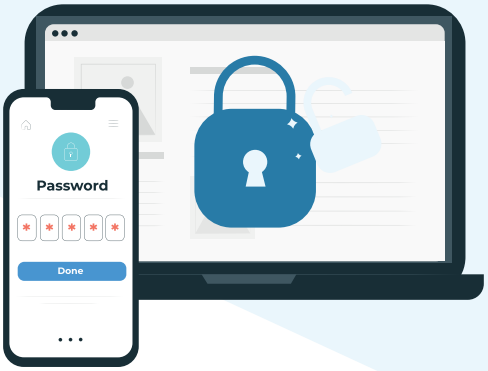
1. Devletler
2. Bankalar
3. Finansal Enstitüler
4. Siyasiler
5. Telekomünikasyon Şirketleri
6. Eğitim Kurumları
7. Savunma Sanayi
8. Enerji Sistemleri/Şirketleri
9. Kolluk Kuvvetleri
10. Bilgi Teknolojileri Şirketleri

Çok Faktörlü Doğrulama ve OTP

Giderek artan güvenlik ihtiyacı parolalara ek ikincil, üçüncül ve fazlası faktörler eklenerek önlemlerin artırılmasına yol açmakla birlikte kullanıcı kolaylığını da kaybetmemize neden oldu.

İki faktörlü doğrulama (2FA) ve çok faktörlü doğrulama (MFA) başlangıç için doğru çözümler olsa da zaman içerisinde oluşabilecek riskler de ortaya çıkmaya başladı:

"*SMS/E-Posta şeklinde iletilen mesajların ele geçirilebilmesi, belirli sayıda elde edilen OTP'lerden daha sonra oluşacak olanların belirlenebilmesi vb.*"



İki faktörlü doğrulama ve çok faktörlü doğrulama sayesinde OTP kullanımı hayatımıza özellikle Finans ve Kamu Kurumları aracılığı ile yerleşti. Fakat zaman içerisinde artırılan tüm bu güvenlik önlemleri yine bir parola ile beraber uygulanmak zorunda.

> Örneklenen tüm kullanıcıların **%38'i** süresi asla dolmayan bir parolaya sahiptir. (Varonis).

> Her **39** saniyede bir siber saldırı gerçekleşmektedir. (2021'de her 11 saniyede)

Veri İhlal İstatistikleri

Güvenliği parolalar ile sağlanan verilerin ihlalinden kaynaklanan mali kayıplar katlanarak artmakta. Siber suçların işletmelere 2019'da 2 trilyon dolardan fazlaya mal olduğu, 2021 yılında ise bu rakamın 6 trilyon dolara ulaşacağı belirtiliyor.

- Veri ihlalleri 2019'un ilk altı ayında 4,1 milyar kaydı açığa çıkardı (Forbes),
- 2019 itibariyle, siber saldırılar küresel istikrarın önündeki en büyük beş risk arasında kabul edilmektedir (Dünya Ekonomik Forumu),

- 2019'da First American Financial Corp., banka işlemleri, sosyal güvenlik numaraları ve daha fazlası dahil olmak üzere 885 milyon kaydı çevrimiçi olarak ifşa etti (Gizmodo),
- 2019 yılında, finans ve ödeme şirketleri ihlal sonrası hisse performansında en büyük düşüşü görürken, fiyatlar bir ihlalin ardından ortalama % 7,27 düştü (Comparitech),
- 2019'da ortalama olarak her çalışanın 17 milyon dosyaya ve 1,21 milyon klasöre erişimi vardı (Varonis),
- Bir veri ihlalinde kaybolan veya çalınan kayıt başına ortalama maliyet 150 ABD dolarıdır (IBM).

Parolasız Yaşamın Güvenliğini Keşfedin!

Gartner'a göre 2023 yılına kadar kuruluşların %30'u en az bir tür şifresiz kimlik doğrulamadan yararlanacak ve statik parolaları ortadan kaldıracak. Bu da bugünün %5'inden büyük bir artış anlamına geliyor.

AuthTake, FIDO2, WebAuthn ve Açık Anahtarlı Şifreleme teknolojilerini kullanarak, kimlik hırsızlarının hedefi olan parola, OTP, SMS Kodları vb. paylaşılan sırlardan kurtulmanıza ve tam olarak şifesiz kimlik doğrulamaya geçiş yapmanıza olanak sağlıyor.

Workstation Oturum Açma

Windows, Linux, Mac cihazlarda şifresiz oturum açma.

E-Posta Güvenliği

Microsoft Exchange, Office 365, Zimbra, ActiveSync, MAPI desteği ile e-posta hesaplarınıza güvenli erişim.

LDAP Service

Şirket içi Active Directory, Azure AD ve Open LDAP gibi dizin servislerine hızlı ve güvenli bağlantı.

Tek Oturum Açma (SSO)

Tek bir kimlik doğrulama ile tüm kurumsal uygulamalara güvenli erişim.

VPN/VDI

Uzaktan kimlik doğrulama yaparak VPN ve VDI bağlantıları sağlama.

SSH

Linux ve Unix sunucularda SSH bağlantılarına güvenli ve parolasız erişim.

Radius

Radius desteği olan tüm ağ cihazları ve yazılımlarla güvenli ve parolasız erişim.

Uygulama Entegrasyonu

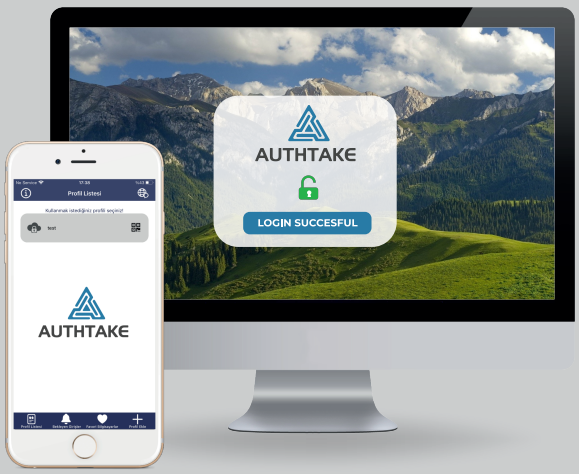
3rd Party ve kurumsal uygulamalara entegrasyon için API desteği.

Cloud & On-Prem Apps

On-Prem veya Cloud üzerinden çalışma seçeneği.

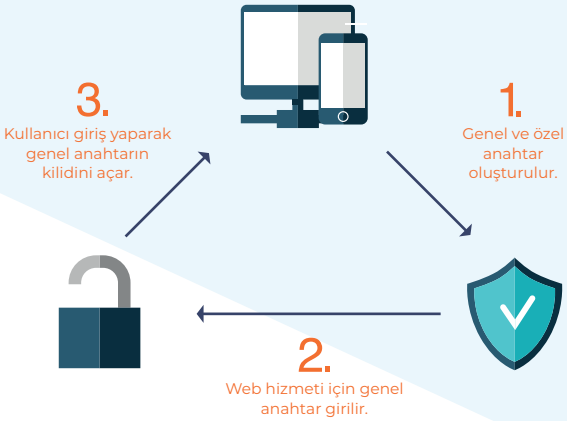
Parolaları Ortadan Kaldırın.

- **Unutulacak sır yok,**
- **Şifreyi bir yere yazmak yok,**
- **OTP yok,**
- **Oltalama yok,**
- **Sniffing yok,**
- **Şifre sıfırlama maliyeti yok.**



Passwordless FIDO2 WebAuthn

FIDO2 WebAuthn, FIDO Alliance'ın web sitelerinin, desteklenen tarayıcı ve platformlarda genel / özel anahtar çiftinden oluşan Public-Key Cryptography (PKC) altyapısını kullanarak güvenli şifresiz kullanıcı doğrulamalarına olanak tanıması amacıyla oluşturmuş olduğu web tabanlı bir API'dir.



Tüm bu doğrulama süreçlerinde kullanıcıdan, mobil cihazının desteğine göre **biyometrik doğrulama** talebinde bulunur.

Neden AuthTake?

AuthTake, güvenlik riskinin baş aktörü parolaları ortadan kaldırarak, Açık Anahtarlı Şifreleme (PKC) ve FIDO altyapısı sayesinde hızlı ve güvenli "Parolasız Kullanıcı Doğrulama" teknolojisi ile kuruluşların güvenlik seviyelerini arttırmalarını ve parola yönetim maliyetlerinden kurtulmalarını sağlar.

- On-Prem ve Cloud Active Directory desteği sayesinde hibrit çalışma olanağı sunar.
- Uzaktan kilitleme özelliği ile kullanıcı nerede olursa olsun verilerinin güvenliğini koruyabilir. (Oturumunuz uzun süre açık kaldığında alarm üretir.)
- Parolaları ortadan kaldırarak unutulması, bir yere not edilmesi ve payaşılması gibi sorunların önüne geçer.
- Hızlı oturum açma ve kolay entegrasyonu sayesinde iyi bir kullanıcı deneyimi sunar. (Oturum açma süresi ortalama 3 saniyedir.)
- Kullanıcı doğrulama işleminin mobilden başlatılması sayesinde PUSH, MITM gibi saldırıların önüne geçilmiş olur.
- Offline kullanılabilir modu sayesinde sisteme bağlı olunmayan çevrimdışı durumlarda da PIN kullanılarak giriş yapılmasını sağlar.

Şifresiz Tekli Oturum Açma (Passwordless SSO)

AuthTake, SAML ve OAuth protokelleri desteği ile kurumsal uygulamalarınıza ve Salesforce, Amazon, Office 365, Dropbox, DocuSign gibi bulut uygulamalarınıza tekli oturum açma desteği sağlayan AuthTake Portalı üzerinden hızlı ve güvenli erişiminize olanak tanır.

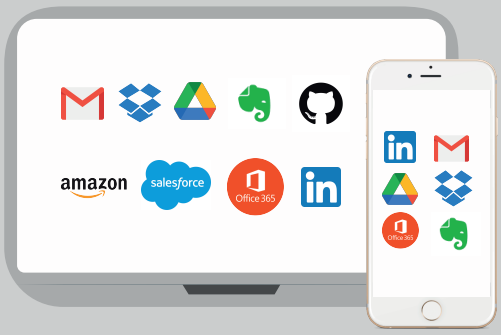
Yerel ve Bulut Uygulamalarına Güvenli Erişim

Kullanıcılar gün içerisinde yerel ve bulutta yer alan birçok uygulamaya erişim sağlamaktadır.
Bu uygulamaların her birine erişim için tekrar tekrar kullanıcı doğrulama işlemi gerçekleştirmek zorunda kalmaları, zaman kaybının yanı sıra kullanım zorluğunu da beraberinde getirmektedir.

AuthTake SSO, kullanıcılarınızın bir pano üzerinden bulutta ve yerelde çalışan uygulamalarınıza güvenli ve hızlı erişim tecrübesi yaşamalarına olanak sağlar. AuthTake SSO kullanıcılarınızın zaman kazanmasını sağlarken, üretkenliklerini arttırır. Tek girişle birçok iş uygulamasına erişmeleri sağlanır.

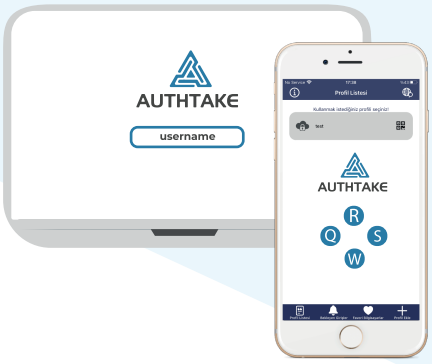
Uygulama Kataloğu

AuthTake SSO önceden yüklenmiş web uygulamalarıyla gelmektedir ve her geçen gün yeni uygulamalar eklenmeye devam etmektedir. Katalog üzerinden hangi uygulamaya ihtiyacınız olduğunu söylemeniz yeterli.



Nasıl Kullanılır?

Bildirim ile Oturum Açma
Kullanıcı sistem erişimlerinde sadece kullanıcı adını yazarak kendine ait cihaza bildirim gönderilmesini sağlar. Mobil cihazında yer alan uygulama sayesinde gelen bildirime onay vererek erişim iznini vermiş ve oturum açmış olur.



Karekod ile Oturum Açma
Kullanıcı erişmek istediği sistemin giriş ekranında yer alan karekodu, mobil cihazındaki AuthTake uygulaması aracılığıyla okutup kendisinden istenen biyometrik doğrulama veya PIN girerek oturumu açar.

Uzaktan Kontrol ile Oturum Açma/Kapatma
Kullanıcı mobil cihazında yer alan AuthTake uygulaması ile eşleştirmiş olduğu bilgisayarlarda mobil cihazı aracılığı ile uzaktan oturum açma ve kilitleme işlemini gerçekleştirebilir.

Çevrimdışı Oturum Açma
Kullanıcı bilgisayar ya da mobil cihazının internet erişiminin olmadığı durumlarda AuthTake uygulamasının Offline Login seçeneğini kullanarak oluşturduğu PIN ile kullanıcı doğrulamasını gerçekleştirip oturum açabilir.

AUTHTAKE

+90 850 303 70 05
info@authtake.com
www.authtake.com

/authtake
/authtake
/authtake