2026 – 2027

Siber Güvenlik Beyaz Kitabı

2026–2027 Döneminde Dijital Korumanın Yeni Zorlukları

Yapay zeka destekli tehditleri anlayın, FIDO2 Passkeys geçiş anahtarlarını devreye alın, riskleri önleyin ve kuruluşunuzu NIS 2, DORA ve Cyber Resilience Act ile uyumlu hale getirin

PASS REVELATOR

Siber Güvenlik Beyaz Kitabı 2026–2027 — Sürüm 2.0 — Kasım 2026

İçindekiler

Ön Söz Intro

1. 2026 Temel Verileri 01

2. Tehdit Manzarasında 2026–2027 02

2.1 Yapay Zeka ve Shadow AI: Yeni Siber Saldırı Sınırı

2.2 Klasik Saldırı Teknikleri ve Oturum Ele Geçirme (AiTM)

2.3 Yeni Tehditler ve Tedarik Zinciri İhlalleri

3. Ekonomik ve Operasyonel Etkiler 03

4. KOBİ ve Orta Ölçekli İşletmeler Odağı: Zafiyetler ve Düzenlemeler (NIS 2, CRA, DORA) 04

5. Koruma Stratejileri, Passkeys ve En İyi Uygulamalar (NIST 2026) 05

6. Siber Savunmada Yapay Zeka ve Yapay Zeka Yönetişimi 06

7. PASS REVELATOR Önerileri ve 9 Araçlık Yazılım Paketi 07

Sonuç ve 2026–2029 Perspektifi 08

Ek Kaynaklar ve Doğrulanmış 2026 Verileri 09

Ön Söz

Siber güvenlik artık yalnızca büyük kurumsal şirketlere özgü teknik bir tercih değildir: her modern kuruluş için hayatta kalmanın ve mevzuata uyumun vazgeçilmez bir koşuludur. 2026 yılında, sanayileşmiş üretken yapay zeka saldırıları, yönetilmeyen 'Shadow AI' (Gölge Yapay Zeka) kullanımındaki patlama ve yoğun tedarik zinciri hedeflemeleriyle yönlendirilen tarihi bir dijital tehdit dönüşümüne tanıklık ediyoruz.

PASS REVELATOR (www.passwordrevelator.net) tarafından hazırlanan bu beyaz kitap, en güncel küresel referans raporlara (IBM Cost of a Data Breach 2026, Verizon DBIR 2026, Sophos State of Ransomware 2026, Microsoft Digital Defense Report 2026 ve NIST SP 800-63B Rev. 4) dayanan kapsamlı bir analiz sunmak üzere Sürüm 2.0 (2026–2027 Baskısı) olarak baştan sona güncellenmiştir.

2026'da Siber Olağanüstü Hal

Küresel siber suç maliyetleri **2026 yılında 11,5 trilyon dolara** ulaşmakta olup **2029 yılına kadar 15,63 trilyon dolara** çıkması öngörülmektedir (yıllık +%15). Küresel ortalama veri ihlali maliyeti tüm zamanların rekoru olan **4,99 milyon dolara** (yıllık +%12) ulaşmış, saldırganların yapay zeka kullandığı durumlarda ise **6,0 milyon dolara** tırmanmıştır. Kuruluşlar haftada ortalama **1.984 siber saldırıyla** karşı karşıya kalmaktadır.

Küçük ve orta ölçekli işletmeler (KOBİ'ler) ön saflarda yer almaya devam etmektedir: **ihlallerin %62'sinde insan faktörü** (sosyal mühendislik, hatalar, çalınan kimlik bilgileri) rol oynamakta, **%48'i üçüncü bir tarafı veya tedarikçiyi** içermekte ve yapay zeka kaynaklı bir güvenlik olayı yaşayan **kuruluşların %92'sinde** yapay zeka araçları ile insan dışı kimlikler üzerinde yeterli erişim kontrolü bulunmamaktadır.

Bu rehber; dayanıklı bir siber strateji kurmak, FIDO2 Passkeys geçiş anahtarlarını benimsemek ve güvenlik denetimi ile meşru erişim kurtarma alanındaki 9 PASS REVELATOR çözümünden oluşan eksiksiz ekosistemden yararlanmak isteyen yöneticiler, CIO'lar, CISO'lar, uyum sorumluları ve profesyoneller için hazırlanmıştır.

> *"Siber güvenlik yalnızca teknik bir beceri değil, temel bir yönetişim ve yaşam becerisidir."*
>
> — Ivan John Uy, Eski Bilgi ve İletişim Teknolojileri Bakanı

1. 2026 Temel Verileri

2026 yılına ait konsolide güvenlik ölçütleri net bir tablo ortaya koymaktadır: yapay zeka destekli savunmalar ve Passkeys teknolojisi ilerlerken, finansal etkiler ve güvenlik açığı sömürü hızları eşi benzeri görülmemiş seviyelere ulaşmıştır.

1.1 Finansal Maliyetler ve Etkiler (2026 Ölçütleri)

4,99 M$
Küresel ortalama veri ihlali maliyeti (yıllık +%12, IBM 2026)

11,50 M$
ABD'deki ortalama veri ihlali maliyeti (2026 tüm zamanların rekoru)

6,00 M$
Kötü amaçlı yapay zeka destekli saldırıları içeren ihlallerin ortalama maliyeti

173 $
Ele geçirilen hassas kayıt başına ortalama maliyet

Gösterge	2026 Değeri	Eğilim	Kaynak
Küresel siber suç maliyeti	11,5 trilyon USD	Yıllık +%15 büyüme	Cybersecurity Ventures 2026
2029 yılı öngörülen küresel maliyet	15,63 trilyon USD	Sürekli artış	Cybersecurity Ventures
Ortalama 'Shadow AI' ihlali maliyeti	5,39 milyon USD	1 yılda >2× olay artışı	IBM Cost of a Data Breach 2026
Ortalama fidye yazılımı kurtarma maliyeti (fidye hariç)	1,70 milyon USD	2025'e göre +%11 (1,53 M$)	Sophos State of Ransomware 2026
Güvenlik Yapay Zekası ve Otomasyon ile tasarruf	-1,93 milyon USD	-%34 ihlal maliyeti azalması	IBM 2026

Temel Çıkarım: Zero Trust ve Şifreleme Açıkları

Olgun bir **Zero Trust (Sıfır Güven)** mimarisi işleten kuruluşlar ortalama ihlal maliyetini **1,76 milyon dolar** azaltmaktadır. Buna karşın IBM 2026 verilerine göre, ihlale uğrayan kuruluşların yalnızca **%37'si** hassas verilerini hem durağan halde hem de aktarım sırasında şifrelemiştir.

1.2 2026'da Saldırı Sıklığı ve Vektörleri

Saldırı Vektörü / Metrik	2026 İstatistiği	Kaynak
Kuruluş başına haftalık ortalama saldırı	Kuruluş başına 1.984 (2 yılda +%58)	WEF / Check Point 2026
Güvenlik açığı sömürüsü (1 numaralı başlangıç vektörü)	İhlallerin %31'i (kimlik bilgisi istismarını geçti)	Verizon DBIR 2026
İnsan faktörünü içeren ihlaller	Analiz edilen tüm ihlallerin %62'si	Verizon DBIR 2026
Üçüncü tarafları / Tedarik Zincirini içeren ihlaller	İhlallerin %48'i (yıllık +%60 artış)	Verizon DBIR 2026
Fidye yazılımı (Ransomware) içeren ihlaller	İhlallerin %48'i (mağdurların %69'u ödemeyi reddediyor)	Verizon DBIR 2026
Yapay zeka destekli kötü amaçlı ihlaller	Kötü amaçlı ihlallerin > %25'i (yıllık +%56)	IBM 2026
Bulut erişim denemelerinde parola püskürtme payı	Hacim bazında ilk bulut erişim denemelerinin > %99'u	Microsoft MDDR 2026

1.3 Tespit, İyileştirme ve Müdahale Süreleri

181 gün
Bir veri ihlalini ortalama tespit etme süresi (MTTI)

241 gün
Bir veri ihlalinin ortalama toplam yaşam döngüsü (tespit + kontrol altına alma)

108 gün
Güvenlik Yapay Zekası ve otomasyon ile ihlal tespitinde kazanılan süre

43 gün
Bilinen sömürülen zafiyetleri (CISA KEV) giderme medyan süresi

2. Tehdit Manzarasında 2026–2027

2026 siber tehdit manzarası üç büyük değişimle tanımlanmaktadır: üretken yapay zeka aracılığıyla saldırı otomasyonu, oturum belirteci hırsızlığı (AiTM) yoluyla geleneksel MFA'nın aşılması ve yamalanmamış uç cihazların hızla sömürülmesi.

2.1 Yapay Zeka ve Shadow AI: Yeni Siber Saldırı Sınırı

2026 yılında kötü amaçlı yapay zeka destekli saldırılar **%56** artarak her dört kötü amaçlı ihlalden birinden fazlasını oluşturmuştur (IBM 2026). Aynı dönemde çalışanların yetkisiz yapay zeka aracı kullanımı (**Shadow AI**) iki kattan fazla artarken, etkilenen **kuruluşların %92'si** yapay zeka modelleri ve bağlayıcıları üzerinde uygun erişim kontrollerinden yoksundu.

2.1.1 Yapay Zeka Destekli Oltalama ve Oturum Ele Geçirme (AiTM)

2026'nın Endişe Verici İstatistikleri

- Geleneksel oltalamada %12 olan tıklama oranına karşın yapay zeka ile kişiselleştirilmiş oltalama tuzaklarında **%54 tıklama oranı**.
- Kusursuz çok dilli oltalama içerikleri saldırgan yapay zeka ajanları tarafından manuel 16 saat yerine **5 dakikanın altında** üretilip başlatılıyor.
- **Adversary-in-the-Middle (AiTM)** oltalama ve Cihaz Kodu Oltalama (Device Code Phishing) saldırıları MFA sonrası oturum çerezlerini çalmak amacıyla **iki kattan fazla arttı** (Microsoft MDDR 2026).
- **Prompt injection** ve model tersine çevirme saldırıları en maliyetli yapay zeka güvenlik olayları arasında yer alıyor (ortalama 5,8 M$–6,0 M$).

2.1.2 Gerçek Zamanlı Deepfake'ler ve Yönetici Taklidi

> *"Gerçek zamanlı ses ve video deepfake'leri, yönetici dolandırıcılığının (BEC 2.0) bir numaralı silahı haline gelerek görüntülü görüşmelerdeki görsel veya işitsel güveni geçersiz kılmıştır."*
>
> — Harvard Law School Forum on Corporate Governance / IBM Threat Intelligence 2026

Dikkat çeken deepfake dolandırıcılığı vakaları:

- **Arup (Hong Kong):** Üst düzey yöneticilerin yapay zeka video ve ses klonlarının yer aldığı canlı bir video konferansın ardından 25 milyon dolar transfer edildi.
- **Türkiye'deki holdingler ve küresel şirketler:** Bant dışı (out-of-band) doğrulama protokolleri sayesinde CEO ses klonlama dolandırıcılığı girişimlerini engelledi.
- 2026'da bir yöneticinin sesini insandan ayırt edilemeyecek doğrulukta klonlamak için yalnızca **3 saniyelik halka açık ses kaydı** ve 20 doların altında bir maliyet yeterli olmaktadır.

2.2 Klasik Saldırı Teknikleri ve Evrimi

2.2.1 Oltalama (Phishing) ve Sosyal Mühendislik

Sosyal mühendislik, artık SMS ve TOTP tek kullanımlık kodlarını gerçek zamanlı yakalayabilen AiTM ters vekil (reverse-proxy) kitleriyle birleştirilerek ilk ele geçirmelerin merkezinde yer almaktadır.

Saldırı Türü	2026 Mekanizması	Başarı Oranı / Etki
Kitlesel Yapay Zeka Oltalaması	Yazım hatası veya statik imza içermeyen dinamik üretilmiş e-postalar	%12–18 tıklama oranı
Bağlamsal Hedefli Oltalama (Spearphishing)	LinkedIn ve sosyal medya taramasıyla otomatik hedefleme	%35–50 başarı oranı
Whaling / Yönetici Dolandırıcılığı	C-level yöneticilere, CFO'lara ve BT yöneticilerine yönelik saldırılar	Doğrulama protokolü yoksa %55–65
Vishing ve Sesli Deepfake	Gerçek zamanlı yönetici ses klonlaması kullanan telefon aramaları	%25–35 başarı oranı
AiTM ve BEC (Kurumsal E-posta İhlali)	MFA sonrası oturum belirteçlerini yakalayan ters vekil sunucu	Olay başına medyan kayıp > 150.000 $

2.2.2 Fidye Yazılımı (Ransomware) ve Üçlü Şantaj

Verizon DBIR 2026 raporuna göre fidye yazılımı tüm veri ihlallerinin **%48'inde** görülmektedir. Yedekleme dayanıklılığı arttıkça (**mağdurların %69'u artık ödeme yapmayı reddediyor**), şantaj grupları üçlü şantaja başvurmaktadır: şifreleme, fikri mülkiyet hırsızlığı (%31) ve marka itibarının silah olarak kullanılması (%41).

%48
Fidye yazılımı içeren tüm veri ihlallerinin payı (Verizon DBIR 2026)

%69
Dayanıklı yedeklemeler sayesinde fidye ödemeyi reddeden mağdurlar

1,70 M$
Fidye hariç ortalama kurtarma maliyeti (yıllık +%11, Sophos 2026)

%71
Fidye ödeyip 6 ay içinde ikinci bir saldırıya uğrayan kuruluşlar

2.2.3 Kaba Kuvvet Saldırıları, Parolalar ve İnsan Dışı Kimlikler

Parola Uzunluğu	Karmaşıklık / Entropi	Kırma Süresi (2026 GPU Kümeleri)
8 karakter	Yalnızca küçük harfler (26^8)	< 1 saniye (anında)
8 karakter	Büyük + küçük harfler (52^8)	~15 saniye
8 karakter	Harfler + rakamlar + semboller (94^8)	~4 saat
12 karakter	Büyük + küçük harf + rakam + sembol	~1.500 yıl
16+ karakter	Karmaşık parola cümlesi veya rastgele üretim	> 30.000 yıl (kaba kuvvete dayanıklı)

2026'da İnsan ve İnsan Dışı Kimlik Gerçeği

- **İhlallerin %39'u** bir aşamada çalınmış veya ele geçirilmiş kimlik bilgilerini içermektedir (Verizon DBIR 2026).
- **Passkeys** ve oltalamaya dayanıklı MFA benimseyen kuruluşlarda doğrudan parola saldırılarında **%26 düşüş** (Microsoft MDDR 2026).
- Geçerli hesapların kullanıldığı **izinsiz girişlerin %52,2'si** yanal hareket için ardından gelen oturum belirteci hırsızlığını içermektedir.
- Kuruluşların yalnızca **%46'sı insan dışı kimliklerini** (API anahtarları, servis hesapları, yapay zeka ajanları) yeterince güvence altına almaktadır.

2.3 Yeni Tehditler ve Tedarik Zinciri

2.3.1 SIM Kart Saldırıları (Simjacking ve SIM Swapping)

Simjacking: Yamalanmamış fiziksel SIM kartlardaki operatör uygulamacıklarında bulunan eski güvenlik açıklarının sömürülmesi.

SIM Swapping: Kurbanın numarasını saldırgan kontrolündeki bir SIM/eSIM'e taşımak ve tüm SMS tabanlı MFA kodlarını ele geçirmek için telekom operatörlerinde sosyal mühendislik veya içeriden rüşvet kullanımı.

2.3.2 Air-Gapped Saldırılar ve Gizli Kanallar

- **Lantenna Attack:** İzole ağlardan veri sızdırmak için Ethernet kablolarının radyo frekansı anteni olarak kullanılması.
- **LED-it-Go:** Donanım LED durum ışıklarındaki mikro dalgalanmalar üzerinden optik veri sızdırma.
- **Power Hammering:** Elektrik hatları üzerindeki güç tüketimini modüle ederek ikili veri iletimi.
- **Bluejacking ve BLE İstismarları:** Bluetooth Low Energy açıklarından yararlanan yakın mesafe ele geçirmeleri.

2.3.3 Zero-Day, Zero-Click İstismarları ve Üçüncü Taraf İhlalleri (%48)

2026 yılında yazılım güvenlik açığı sömürüsü, yoğun biçimde VPN ağ geçitlerini, çevre güvenlik duvarlarını ve SaaS platformlarını hedef alarak **1 numaralı başlangıç erişim vektörü (%31)** haline gelmiştir. Üçüncü taraf ve tedarik zinciri ihlalleri yıllık %60 artarak **tüm ihlallerin %48'ine** ulaşmıştır (Verizon DBIR 2026).

> *"Zero-click istismarları saldırgan sofistikasyonunun zirvesini temsil eder: kurban hiçbir işlem yapmazken ele geçirme sessizce gerçekleşir."*
>
> — Citizen Lab, Toronto Üniversitesi

3. Ekonomik ve Operasyonel Etkiler

Büyük bir siber saldırı, teknik veri kaybının ötesinde nakit akışını, tedarik zinciri operasyonlarını ve müşteri güvenini aylarca sekteye uğratır.

3.1 Doğrudan ve Dolaylı Maliyet Dağılımı (IBM 2026)

Maliyet Kategorisi	Operasyonel Açıklama	Toplam Maliyet Payı
Tespit ve eskalasyon	Adli bilişim incelemesi, acil denetim, kriz yönetimi	%29
Bildirim ve uyum	KVKK/GDPR/NIS 2 bildirimleri, hukuki danışmanlık, paydaş iletişimi	%13
İhlal sonrası müdahale	BT iyileştirme, mağdur desteği, kimlik/kredi izleme	%23
İş ve itibar kaybı	Operasyonel kesinti, müşteri kaybı, marka hasarı	%35

2026'da Fidye Yazılımının Gerçek Maliyeti

Fidye ödemesi, **toplam olay maliyetinin yalnızca %15–20'sini** oluşturur. Ortalama iyileştirme ve kurtarma maliyetleri **1,70 milyon dolara** ulaşırken (Sophos 2026), **ödeme yapan kuruluşların %71'i** 6 ay içinde ikinci kez saldırıya uğramaktadır.

3.2 Kesinti Süresine Göre Operasyonel Etkiler

Kesinti Süresi	Operasyonel Etki	Tahmini Ortalama Maliyet
< 24 saat	Küçük aksaklık, kısıtlı manuel prosedürlere geçiş	50.000 $ – 200.000 $
1 ila 3 gün	Faturalama ve lojistiğin durması, anında gelir kaybı	200.000 $ – 1 M$
3 ila 7 gün	Kısmi felç, sözleşme cezaları, kamuoyu krizi	1 M$ – 5 M$
> 1 hafta	Varoluşsal kriz, kalıcı müşteri kaybı, KOBİ iflas riski	> 5 M$

Kritik operasyonel ölçütler:

- 2026 DBIR raporunda kaydedilen fidye yazılımı mağdurlarının hacim bakımından büyük çoğunluğunu küçük kuruluşlar oluşturmaktadır.
- Fidye yazılımı sonrası tam operasyonel iyileşmeye kadar geçen ortalama süre: **24 gün**.

- Şantaj saldırılarının **%41'inde** tehdit aktörleri doğrudan marka itibarını silah olarak kullanmaktadır (IBM 2026).

3.3 Siber Güvenliğin Yatırım Getirisi (ROI)

Savunma Yatırımı	İhlal Maliyeti Azalması	Tahmini 3 Yıllık ROI
Güvenlik Yapay Zekası ve SOC otomasyonu	-1,93 M$ (-%34)	%380
Zero Trust mimarisi ve Passkeys	-1,76 M$	%320
Olay Müdahale Ekibi ve test edilmiş IRP	-1,50 M$	%280
Sürekli eğitim ve yapay zeka oltalama simülasyonları	-1,20 M$	%450

Önlemenin Ekonomik Avantajı

Önleme ve siber hijyene yatırılan her dolar, ortalama **5 dolarlık müdahale ve kurtarma maliyetinden** tasarruf sağlar. Yüksek olgunluğa sahip kuruluşlar finansal ihlal kayıplarını **%42** oranında azaltmaktadır.

4. KOBİ ve Orta Ölçekli İşletmeler Odağı: Zafiyetler ve Düzenlemeler

KOBİ'ler ve orta ölçekli işletmeler siber suçluların hedefinin tam merkezindedir: değerli finansal varlıklara ve B2B bağlantılarına sahip olacak kadar dijitalleşmiş, ancak çoğu zaman 7/24 özel bir SOC ekibinden yoksundurlar.

2026'da KOBİ'lerin Gerçeği

- **Siber saldırıların %43'ü** doğrudan küçük ve orta ölçekli işletmeleri hedef almaktadır.
- KOBİ'ler tedarik zinciri ihlallerinde birincil giriş noktasını oluşturmaktadır (**tüm ihlallerin %48'i**).
- KOBİ'lerin yalnızca **%14'ü** olgun ve test edilmiş bir siber güvenlik duruşuna sahip olduğunu bildirmektedir.
- Küçük işletmelerin **%47'si** hâlâ resmileştirilmiş bir siber güvenlik yol haritasından yoksundur.

4.1 KOBİ'ler ve Orta Ölçekli Firmalar Neden Öncelikli Hedeftir?

Yapısal Zafiyet	Açıklama	Saldırı Etkisi
Kısıtlı BT kaynakları	Sınırlı siber güvenlik bütçesi ve personeli	7/24 izleme eksikliği ve gecikmiş tespit
Özel CISO olmaması	Güvenliğin günlük BT desteğiyle birlikte yürütülmesi	Yapay zeka ve üçüncü taraf risklerini değerlendirme zorluğu
Tedarik zinciri bağlantısı	Büyük kurumsal müşterilerle VPN/API bağlantıları	Yüksek değerli hedeflere ulaşmak için sıçrama tahtası
Açıkta kalan uç teknik borç	48 saat içinde yamalanmayan VPN, NAS veya güvenlik duvarları	KEV açıklarının otomatik sömürüsü (ihlallerin %31'i)

4.2 Güvenlik Denetimlerinde Gözlemlenen Yaygın Açıklar

> *"'Hedef alınmak için fazla küçüğüz' düşüncesi siber güvenlikteki en maliyetli yanılsama olmaya devam ediyor: otomatik saldırı tarayıcıları şirket büyüklüğüne bakmaksızın savunmasız her IP adresini vurur."*
>
> — Verizon DBIR 2026

%37
Tüm kritik erişim noktalarında oltalamaya dayanıklı MFA bulunmayan KOBİ'ler

%52
Belgelenmiş bir Olay Müdahale Planı (IRP) olmayan KOBİ'ler

%68
Parola yönetişimi veya insan dışı kimlik koruması olmayan KOBİ'ler

%41
Çevrimdışı yedeklerinden tam geri yüklemeyi hiç test etmemiş KOBİ'ler

4.3 Şirket Büyüklüğüne Göre Orantısız Finansal Etki

Şirket Büyüklüğü	Ortalama Büyük Olay Maliyeti	Yıllık Cirodaki Payı (%)	İyileşme Süresi
Mikro işletme (< 10 çalışan)	25.000 € – 100.000 €	Cironun %20–50'si	6–12 ay (yüksek iflas riski)
Küçük işletme (10–50 çalışan)	100.000 € – 500.000 €	Cironun %10–30'u	3–6 ay
Orta ölçekli işletme (50–250 çalışan)	500.000 € – 2 M€	Cironun %5–15'i	2–4 ay
Mid-Market / ETI (250–5.000 çalışan)	2 M€ – 10 M€	Cironun %2–8'i	1–3 ay

4.4 2026–2027 Yasal Yükümlülükleri (KVKK, Ulusal Siber Güvenlik, NIS 2 & CRA)

Türkiye ve Uluslararası Alanda Sıkı Denetlenen Yasal Çerçeve

- **Türkiye Siber Güvenlik Düzenlemeleri (USOM / BTK / Cumhurbaşkanlığı DDO Rehberi) ve AB NIS 2 Uyumu:** Kritik altyapılar, KOBİ'ler ve AB ile ticaret yapan ihracatçı kuruluşlar için zorunlu risk yönetimi, **24 saat içinde USOM/SOME siber olay bildirimi** ve **yönetim kurulu düzeyinde doğrudan sorumluluk** getirir.
- **6698 Sayılı KVKK (Kişisel Verilerin Korunması Kanunu):** Veri ihlallerinin **en geç 72 saat içinde Kişisel Verileri Koruma Kurulu'na (KVKK)** bildirilmesi, güncel VERBİS kaydı ve yurt dışı veri aktarımı güvenceleri.
- **BDDK, SPK ve DORA Finansal Siber Dayanıklılık Kuralları:** Finans, bankacılık, fintek ve kritik BT/Bulut tedarikçileri için zorunlu sızma testleri ve üçüncü taraf risk denetimi.
- **Siber Dayanıklılık Yasası (CRA) ve Yapay Zeka Yönetişimi:** Dijital ürünler için 24 saat içinde aktif zafiyet bildirimi (Eylül 2026) ve kurumsal yapay zeka sistemleri için erişim kontrolleri.

4.5 Öncelikli KOBİ Önerileri

Yüksek Etkili Hızlı Kazanımlar (Bütçe < 5.000 €)

Öncelikli Eylem	Tahmini Maliyet	Güvenlik Etkisi	Devreye Alma Süresi
Oltalamaya dayanıklı MFA ve Passkeys	Ücretsiz – 500 €	Otomatik hesap ele geçirmelerin > %99,9'unu engeller	1 hafta
Kurumsal Parola Yöneticisi	3–5 € / kullanıcı / ay	Parola tekrarını ortadan kaldırır ve sızıntıları tespit eder	1 hafta
Test Edilmiş Değiştirilemez / Çevrimdışı Yedekler	500 € – 2.000 €	Fidye ödemeden kurtarmayı garanti eder	2 hafta
Yapay Zeka Oltalama Simülasyonu ve Eğitimi	50 € / çalışan / yıl	Oltalama tıklama oranlarını %70 azaltır	2 hafta

5. Koruma Stratejileri, Passkeys ve En İyi Uygulamalar

Başarılı siber saldırıların %80'inden fazlası, 2026 standartlarına göre güncellenmiş temel siber hijyen kurallarının titizlikle uygulanmasıyla önlenebilir.

5.1 Modern Parola Yönetimi (NIST SP 800-63B Rev. 4)

> **2026 NIST Standart Devrimi**
>
> **NIST SP 800-63B** Revizyon 4; **uzunluğu (en az 15–16+ karakter)**, mutlak benzersizliği ve sızdırılmış parola veritabanlarına karşı otomatik taramayı önceliklendirirken, zayıf ve tahmin edilebilir değişikliklere yol açan **keyfi periyodik parola değiştirmeyi yasaklamaktadır**.

2026 Temel Kuralı	Teknik Gerekçe	Pratik Uygulama
En az 16+ karakter	GPU ile kırmaya karşı matematiksel direnç (> 30.000 yıl)	Parola cümleleri veya uzun rastgele diziler
Her hizmet için benzersiz	Üçüncü taraf ihlalleri sonrası credential stuffing'i önler	Şifreli kasa (Bitwarden, 1Password, Proton Pass)
Sızdırılmış parola taraması	Dark web'de ifşa olmuş tüm parolaları engeller	HaveIBeenPwned API / PASS REVELATOR denetimi
90 günlük zorunlu değişime son	Tahmin edilebilir kalıpları önler (Kis2026!)	Yalnızca ihlal kanıtı veya uyarısı durumunda değiştirin

2026'da Önerilen Parola Yöneticileri:

- **Bitwarden** — Açık kaynak, bağımsız denetimden geçmiş, tam Passkey desteği — *En iyi KOBİ önerisi*
- **1Password** — Sezgisel kullanıcı deneyimi, Watchtower uyarıları, gelişmiş Passkey ve SSH/API gizli anahtar yönetimi
- **Proton Pass** — Yerleşik takip önleyici e-posta takma adlarıyla açık kaynak uçtan uca şifreleme
- **Dashlane** — Proaktif dark web izleme ve entegre oltalama karşıtı uyarılar
- **NordPass** — XChaCha20 şifrelemesiyle güçlendirilmiş sıfır bilgi (zero-knowledge) mimarisi

5.2 Çok Faktörlü Kimlik Doğrulama (MFA) ve FIDO2 Passkeys

AiTM ters vekil kitlerinin 6 haneli OTP kodlarını yakalaması nedeniyle, **Passkeys (FIDO2/WebAuthn kriptografik anahtarları)** geçişi 2026'da 1 numaralı kimlik önceliğidir. Microsoft, Passkey ve MFA benimsenmesi sayesinde parola saldırılarında **%26 azalma** bildirmiştir.

MFA Yöntemi	AiTM Oltalama Direnci	Kullanıcı Deneyimi	2026 Önerisi
SMS / Sesli arama	Düşük (SIM swap ve AiTM'ye karşı savunmasız)	Basit	Tüm hassas hesaplarda kullanımdan kaldırın
TOTP Doğrulama Uygulaması	Orta (AiTM vekil sunucusuyla yakalanabilir)	Kolay	Bağlam istemleriyle birlikte asgari temel düzey
Passkeys (FIDO2 / WebAuthn)	Çok Yüksek (kriptografik alan adı bağlama)	Sorunsuz (yerel biyometri)	Tüm kullanıcılar için 2026 ÖNERİLEN STANDART
Donanım FIDO2 Anahtarı (YubiKey / Titan)	Maksimum (oltalanamaz donanım belirteci)	Fiziksel USB/NFC anahtarı gerektirir	Yöneticiler, BT ve üst düzey yöneticiler için ZORUNLU

Pratik Rehber: Sosyal Medya / Bulut Hesabını Güvenceye Alma (Instagram ve Meta Hesaplar Merkezi)

1. Instagram'ı açın → **Profil** → Sağ üst menü ☰.
2. **Hesaplar Merkezi** → **Şifre ve güvenlik** bölümüne girin.
3. **İki faktörlü kimlik doğrulama**'yı seçin (ve cihazınızda **Passkey** ile girişi etkinleştirin).
4. **Kimlik doğrulama uygulaması (TOTP)** veya **Güvenlik anahtarı** seçin (SMS yedeğini devre dışı bırakın).
5. **Kurtarma kodlarınızı** oluşturun ve güvenli bir çevrimdışı konumda saklayın.

> **Kurtarma Kodlarının Kritik Önemi**
>
> Yedek kurtarma kodlarınızı yazdırın veya çevrimdışı saklayın. Telefonunuz kaybolur veya hasar görürse, kurtarma kodları ve meşru erişim kurtarma araçları hesabınıza geri dönmenin tek yoludur.

5.3 Güvenlik Açığı ve Yama Yönetimi (2026'da 1 Numaralı Vektör)

İhlallerin %31'inin yazılım güvenlik açığı sömürüsüyle başlaması (Verizon DBIR 2026) ve CISA KEV açıkları için medyan giderme süresinin 43 gün olması nedeniyle maruz kalma pencerelerini daraltmak hayati önem taşımaktadır.

Varlık / Sistem	Kritiklik	Doğrulama Sıklığı	Maksimum Giderme SLA'sı
VPN Ağ Geçitleri, Güvenlik Duvarları, Açık Sunucular	KRİTİK	Sürekli (CISA KEV / CERT uyarıları)	Aktif sömürülen CVE'ler için 24–48 saat
İş İstasyonları (Windows, macOS, Linux)	YÜKSEK	Haftalık (otomatik MDM dağıtımı)	< 7 gün
İş Uygulamaları, ERP ve CMS Eklentileri	KRİTİK	Sürekli üretici bültenleri	Kritik güvenlik yamaları için 72 saat
Web Tarayıcıları ve Uzantılar	YÜKSEK	Otomatik sessiz güncellemeler	Anında (24 saat içinde zorunlu yeniden başlatma)

5.4 Veri Güvenliği, Şifreleme ve Yedeklemeler

Altın 3-2-1-1-0 Fidye Yazılımı Karşıtı Yedekleme Kuralı

- Tüm kritik iş verilerinin **3 farklı kopyası**.
- **2 farklı depolama ortamı** veya teknolojisi (ör. yerel NAS + Nesne Bulutu).
- Ayrı bir coğrafi konumda **1 tesis dışı (offsite) kopya**.
- Ele geçirilmiş bir yönetici tarafından bile değiştirilemeyen **1 değiştirilemez (WORM / Object Lock) veya Air-Gapped kopya**.
- Üç aylık süreli geri yükleme tatbikatlarında doğrulanan **0 hata**.

> **Ölümcül Hata: Test Edilmemiş Yedekler**
>
> Fidye yazılımına maruz kalan **kuruluşların %34'ü** yedeklerinin bozuk veya eksik olduğunu ancak geri yükleme yapmaya çalışırken keşfetmektedir. Ayrıca hassas verileri hem durağan halde hem de aktarım sırasında şifreleyin (2026'da ihlale uğrayan kuruluşların yalnızca %37'si her ikisini de yapmıştır).

5.5 Saldırgan Yapay Zekaya Karşı Kullanıcı Eğitimi

İnsan faktörü **ihlallerin %62'sinde** yer aldığı için güvenlik farkındalığı, ses/video deepfake'lerini ve sorumlu yapay zeka kullanımını kapsayacak şekilde gelişmelidir.

Eğitim Modülü	Sıklık	Sunum Formatı	Operasyonel Hedef
Siber Başlangıç ve Yapay Zeka Tüzüğü	İşe girişte	90 dk etkileşimli e-öğrenme	Passkeys, veri sınıflandırma ve Shadow AI kurallarına hakimiyet
Yapay Zeka ve AiTM Oltalama Simülasyonları	Aylık	Gerçekçi hedefli kampanyalar	Tıklama oranını < %5 tutmak ve bildirimleri > %70 artırmak
Yönetici ve Finans Deepfake Tatbikatı	Üç aylık	C-level ve finans masa başı tatbikatı	Tüm para transferleri için bant dışı doğrulamayı zorunlu kılmak
Yeni Tehditler Mikro-Öğrenme	Haftalık	3–5 dakikalık video kapsülleri	Sürekli güvenlik teyakkuzunu korumak

Güvenlik Farkındalık Eğitiminin Kanıtlanmış ROI'si

Olgun eğitim programları oltalama tıklama oranlarını **%70** azaltmakta ve önlenen ihlal başına ortalama **1,2 milyon dolar** tasarruf sağlamaktadır (çalışan/yıl başına 50–150 € yatırımla).

5.6 Olay Müdahale Planı (IRP)

KOBİ'lerin %52'sinde bulunmasa da test edilmiş bir Olay Müdahale Planı ihlal yaşam döngüsünü **54 gün** kısaltır ve maliyetli karar felcini önler.

USOM / KVKK ve NIST Uyumlu Bir Olay Müdahale Planının (IRP) 6 Temel Aşaması

1. **Hazırlık:** Çevrimdışı basılı kriz iletişim listesi, ön anlaşmalı CSIRT desteği, doğrulanmış değiştirilemez yedekler.
2. **Tespit ve Triyaj:** EDR/SIEM uyarı değerlendirmesi, başlangıç vektörünün belirlenmesi, kriz ekibinin aktive edilmesi.
3. **Acil Kontrol Altına Alma:** Ele geçirilen sistemlerin ağ izolasyonu, aktif oturum belirteçlerinin ve API anahtarlarının iptali.
4. **Kökten Temizleme:** Kalıcılık mekanizmalarının kaldırılması, sömürülen açıkların yamalanması, tüm gizli anahtarların döndürülmesi.
5. **Aşamalı Kurtarma:** Değiştirilemez yedeklerden temiz geri yükleme, sıkılaştırılmış izleme ve yasal bildirimler (USOM / TR-CERT'e 24 saat içinde siber olay bildirimi, KVKK'ya 72 saat içinde veri ihlali bildirimi).
6. **Olay Sonrası Çıkarılan Dersler:** Kök neden analizi ve kontrollerin sıkılaştırılması.

5.7 2026'da Siber Sigorta: Gereksinimler ve Kapsam

Küresel siber sigorta değerlendirmesi artık katı teknik ön koşullar dayatmaktadır: doğrulanmış temel kontroller olmadan sigortacılar teminatı reddetmekte veya tazminat taleplerini kapsam dışı bırakmaktadır.

Kapsam Alanı	Kapsanan Hizmetler	Tipik KOBİ/Mid-Market Limiti
Olay Müdahalesi ve Adli Bilişim	7/24 CSIRT uzmanları, hukuki danışmanlık, GDPR/NIS 2 bildirimleri	100.000 € – 500.000 €
Sistem ve Veri Kurtarma	Altyapının yeniden inşası, zararlı yazılım temizliği	250.000 € – 1 M€
İş Kesintisi (Business Interruption)	Operasyonel kesinti süresince brüt kâr marjı tazminatı	500.000 € – 2 M€
Siber Üçüncü Şahıs Sorumluluğu	Müşteriler veya iş ortakları tarafından talep edilen hukuki savunma ve tazminat	1 M€ – 5 M€

2026'da sigortacıların şart koştuğu 6 zorunlu teknik kontrol:

- Tüm uzaktan erişim noktalarının (VPN, M365, Google Workspace) ve yönetici hesaplarının %100'ünde oltalamaya dayanıklı MFA.
- Tüm sunucular ve uç noktalarda devreye alınmış yönetilen EDR (Uç Nokta Tespit ve Müdahale).
- En az üç ayda bir test edilen değiştirilemez veya çevrimdışı yedeklemeler.
- Belgelenmiş yama yönetimi politikası (internete açık kritik açıklar için < 48 saat yama).
- Yıllık olarak test edilen resmileştirilmiş Olay Müdahale Planı (IRP).
- Tüm personel için yıllık güvenlik farkındalığı eğitimi ve oltalama simülasyonları.

6. Siber Savunmada Yapay Zeka ve Yapay Zeka Yönetişimi

Otomatikleştirilmiş saldırganlara karşı manuel savunma artık yeterli değildir. IBM 2026'ya göre Güvenlik Yapay Zekası ve otomasyonu kapsamlı biçimde kullanan kuruluşlar **ihlal başına 1,93 milyon dolar (-%34) tasarruf etmekte** ve ihlalleri **108 gün daha hızlı** tespit etmektedir.

6.1 Modern SOC'ta Savunma Amaçlı Yapay Zeka Uygulamaları

Savunma Yapay Zekası Teknolojisi	Operasyonel Kullanım Alanı	Ölçülen Fayda
UEBA (Davranışsal Analitik)	Ele geçirilen hesapların ve çalınan oturum belirteçlerinin tespiti	Yanal hareketi ve insan dışı kimlik istismarını belirler
NDR / ML Ağ Trafiği Analizi	Şifreli akışların ve API'lerin sürekli denetimi	C2 geri aramalarını ve sessiz veri sızdırmayı tespit eder
Davranışsal EDR / XDR	Polimorfik zararlı yazılımları ve dosyasız fidye yazılımlarını engelleme	Şifrelemeden önce yürütmeyi durdurur (%95 doğruluk)
SOAR (Orkestrasyon ve Otomasyon)	Sınırlama oyun kitaplarının (playbooks) anında yürütülmesi	Sistemleri izole eder veya ele geçirilen belirteçleri saniyeler içinde iptal eder
Üretken Yapay Zeka SOC Yardımcı Pilotları	Uyarı triyajı, betik deobfuskasyonu ve günlük korelasyonu	Analist yorgunluğunu %70 ve yanlış pozitifleri %80 azaltır

-1,93 M$
Kapsamlı Güvenlik Yapay Zekası ve otomasyon ile ortalama ihlal maliyeti tasarrufu (IBM 2026)

108 gün
Güvenlik ihlallerini tespit ve kontrol altına alma süresindeki azalma

%95
Davranışsal ML EDR kullanarak polimorfik zararlı yazılım tespit doğruluğu

%80
Akıllı korelasyon yoluyla yanlış pozitif uyarılarda azalma

6.2 Yapay Zeka Yönetişimi ve 'Shadow AI' Kontrolü

Kurumsal Yapay Zeka Kullanımı	Verimlilik Artışı	Zorunlu Güvenlik Kontrolü
YARA / KQL / Sigma kuralları yazımı	5× daha hızlı tespit kuralı mühendisliği	Üretime almadan önce zorunlu insan incelemesi
Günlük özetleme ve olay raporları	Milyonlarca olay arasında anında korelasyon	Sıfır veri saklamalı özel yapay zeka örnekleri
Kod üretimi ve denetimi (DevSecOps)	Daha hızlı geliştirme ve hata keşfi	Yapay zeka tarafından üretilen kodun otomatik SAST/DAST taraması
Otonom yapay zeka ajanları ve MCP/API bağlayıcıları	Karmaşık iş akışı otomasyonu	Katı en az ayrıcalık, denetim günlüğü ve prompt-injection korumaları

2026 Yapay Zeka Yönetişimi Aciliyeti: Shadow AI'ı Ortadan Kaldırmak

IBM 2026'ya göre yapay zeka güvenlik olayı yaşayan **kuruluşların %92'sinde** yapay zeka erişim kontrolleri, **%68'inde ise yapay zeka yönetişimi** bulunmamaktaydı; bu durum Shadow AI ihlal maliyetlerini **5,39 M$** seviyesine çıkardı. Yapay zeka politikanız şunları tanımlamalıdır:

- Kurumsal yapay zeka araçlarından oluşan onaylı bir izin listesi (kurumsal verilerin asla model eğitimi için kullanılmayacağına dair sözleşme garantileriyle).
- Gizli anahtarların, tescilli kaynak kodların veya kişisel müşteri verilerinin halka açık LLM'lere yapıştırılmasının kesin olarak yasaklanması.
- Yapay zeka ajanları tarafından kullanılan API anahtarlarının, OAuth belirteçlerinin ve insan dışı kimliklerin otomatik keşfi ve döndürülmesi.
- Üretken yapay zeka hizmetlerine giden istemlerde (prompt) DLP (Veri Kaybı Önleme) denetimi.

6.3 2026'da Saldırgan ve Savunma Yapay Zekası Dengesi

Saldırgan Yapay Zeka Tehdidi	Savunma Önlemi	2026 Güç Dengesi
Üretken Oltalama ve AiTM Vekil Sunucuları	FIDO2 Passkeys + semantik LLM e-posta filtreleri	Passkeys ile donatılmış savunucular avantajlı
Gerçek Zamanlı Ses/Video Deepfake'leri	Biyometrik deepfake dedektörleri + bant dışı doğrulama	Saldırganlar önde — insan doğrulama protokolleri şart
Yapay Zeka Üretimli Polimorfik Zararlı Yazılım	Davranışsal EDR/XDR ve çekirdek izolasyonu	Savunucular hafifçe önde
Otomatik Zero-Day / KEV Sömürüsü	Sürekli Tehdit Maruziyeti Yönetimi (CTEM) ve otomatik yama	Kritik yarış (KEV'lerin yalnızca %26'sı zamanında gideriliyor)

> *"Yapay zeka siber güvenlik profesyonellerinin yerini almayacak; ancak savunma amaçlı yapay zeka ile güçlendirilen kuruluşlar, yalnızca manuel savunmaya güvenenlerden daha uzun süre ayakta kalacaktır."*
>
> — Küresel CISO Uzlaşısı, 2026

6.4 Yapay Zeka ROI'si ve KOBİ'ler İçin Uygulama Yol Haritası

1,93 M$
Yapay zeka destekli güvenlikle elde edilen ortalama maliyet tasarrufu

%380
Ortalama 3 yıllık yatırım getirisi

-108 g
Toplam ihlal yaşam döngüsü süresindeki azalma

-%70
BT/SOC ekipleri için tekrarlayan uyarı triyajı iş yükünde azalma

Aşamalı Yapay Zeka ve Güvenlik Yol Haritası (0 ila 24 Ay)

Aşama 1 — Temeller ve Shadow AI Yönetişimi (0–6 Ay):

- Çalışanların yapay zeka aracı kullanımını denetleyin ve yönetin (Shadow AI politikası).
- E-posta paketinizde yerleşik yapay zeka oltalama korumasını etkinleştirin ve FIDO2 Passkeys dağıtın.
- Tüm insan dışı kimliklerin (API anahtarları, webhook'lar, servis hesapları) envanterini çıkarın.

Aşama 2 — Davranışsal Tespit (6–12 Ay):

- Uç noktaların ve sunucuların %100'üne davranışsal makine öğrenimi tabanlı EDR/XDR kurun.
- Kimlik anomali tespitini (UEBA) ve otomatik oturum belirteci iptalini devreye alın.

Aşama 3 — Otomasyon ve Sürekli Dayanıklılık (12–24 Ay):

- Bir dakikanın altında otomatik kontrol altına alma için SOAR oyun kitaplarını entegre edin.
- KOBİ/Mid-Market kapsamı için 7/24 yapay zeka destekli MDR (Yönetilen Tespit ve Müdahale) hizmetinden yararlanın.

7. PASS REVELATOR Önerileri ve Yazılım Paketi

Kimlik güvenliği, parola denetimi ve meşru erişim kurtarma alanındaki uluslararası uzmanlığıyla PASS REVELATOR, eksiksiz 9 araçlık yazılım paketinin yanı sıra acil bir 30 günlük eylem planı sunmaktadır.

7.1 Acil Eylem Planı (İlk 30 Gün)

Kritik Eylemler — 1. ila 4. Haftalar

Bu 6 öncelikli önlemin disiplinli biçimde uygulanması, 2026'da sömürülen **başlangıç sızma vektörlerinin %85'inden fazlasını** minimum maliyetle ortadan kaldırır.

Öncelik	Somut Eylem	Sorumlu	Süre	Tahmini Maliyet
P0	Tüm yönetici ve uzak hesaplarda oltalamaya dayanıklı MFA / Passkeys etkinleştirme	CIO / BT Yöneticisi	48 saat	Ücretsiz / Dahil
P0	Ayrıcalıklı hesapların ve insan dışı kimliklerin (API anahtarları) envanterini çıkarma ve koruma	CIO / CISO	3 gün	İç kaynak süresi
P0	Kurumsal parola yöneticisi kurma ve zayıf/tekrarlanan parolaları denetleme	BT + Yönetim	1 hafta	3–5 € / kullanıcı / ay
P1	Yedeklerin değiştirilemezliğini doğrulama ve tam canlı geri yükleme tatbikatı yapma	BT Yöneticisi	2 hafta	İç kaynak süresi
P1	VPN'ler, güvenlik duvarları ve uç sunuculardaki kritik CISA KEV açıklarını yamalama	BT / MSP	1 hafta	İç kaynak süresi
P1	Yöneticileri ve finans ekiplerini deepfake, BEC ve NIS 2 görevleri konusunda eğitme	Yönetim + İK	2 hafta	500 € – 2.000 €

7.2 Siber Güvenlik Yatırımı Önceliklendirme Matrisi

Stratejik Kadran	2026–2027 Temel Önlemleri	Eylem
Hızlı Kazanımlar (Yüksek Etki / Düşük Efor)	• Oltalamaya dayanıklı MFA ve FIDO2 Passkeys • Kurumsal parola yöneticisi • Test edilmiş değiştirilemez / çevrimdışı yedekler • Shadow AI tüzüğü ve oltalama eğitimi	DERHAL DEVREYE ALIN (Maksimum ROI)
Büyük Projeler (Yüksek Etki / Yüksek Efor)	• Yönetilen EDR / XDR kurulumu (7/24 MDR) • Zero Trust mimarisi ve mikro segmentasyon • Tam NIS 2 / DORA / CRA uyumu • İnsan dışı kimlik yönetişimi	6–18 AY İÇİN PLANLAYIN
Sürekli İyileştirmeler (Orta Etki / Düşük Efor)	• Sistem yapılandırmasının sıkılaştırılması • Aylık yapay zeka oltalama simülasyonları • DNS filtreleme ve yetkisiz Device Code akışlarını engelleme • Yıllık masa başı kriz tatbikatları	AŞAMALI ENTEGRE EDİN
Kaçınılması Gerekenler (Düşük Etki / Yüksek Efor)	• Yönetecek personeli olmayan karmaşık araçlar • 90 günlük zorunlu parola değişiklikleri • Yönetişimi olmayan denetimsiz yapay zeka araçları	KAÇININ

7.3 2026–2027 İçin Önerilen Siber Güvenlik Bütçesi

NIS 2 yükümlülüklerini karşılamak ve otomatik tehditlere karşı koymak için siber güvenlik bütçeleri **toplam BT harcamalarının %10–15'ini** (veya yıllık cironun yaklaşık %0,5–1'ini) temsil etmelidir.

Kuruluş Büyüklüğü	Yıllık BT Bütçesi	Önerilen Siber Bütçe	Hedef Dağılım
Mikro (< 10 çalışan)	5.000 € – 15.000 €	1.000 € – 3.000 €	%70 araçlar ve yedekler / %30 eğitim
Küçük KOBİ (10–50 çalışan)	20.000 € – 100.000 €	5.000 € – 25.000 €	%55 araçlar / %30 hizmet ve denetim / %15 eğitim
Orta KOBİ (50–250 çalışan)	100.000 € – 500.000 €	25.000 € – 80.000 €	%45 araçlar / %35 MDR ve denetim / %20 yönetişim
Mid-Market (250–5.000 çalışan)	500.000 € – 5 M€	80.000 € – 750.000 €	%40 araçlar / %35 siber personel / %25 yönetilen hizmetler

Örnek Optimize Edilmiş Bütçe — 50 Çalışanlı KOBİ: 25.000 € / yıl

Harcama Kategorisi	Yıllık Bütçe
Uç noktalar ve sunucularda yönetilen profesyonel EDR / XDR	5.500 €
Kurumsal parola yöneticisi ve FIDO2 Passkey dağıtımı	2.000 €
Değiştirilemez bulut yedeklemeleri + çevrimdışı replikasyon	4.000 €
Yeni Nesil Güvenlik Duvarı (NGFW) ve VPN/ZTNA sıkılaştırması	3.000 €
Sürekli yapay zeka oltalama ve deepfake eğitimi (50 kullanıcı)	2.500 €
Yıllık harici güvenlik denetimi, KEV taraması ve sızma testi	5.500 €
KOBİ siber sigorta poliçesi	2.500 €
YILLIK TOPLAM	25.000 €

500 € / çalışan / yıl — büyük bir KOBİ siber olayının ortalama maliyetinin (> 500.000 €) yalnızca çok küçük bir kısmı.

7.4 Aylık İzlenecek Temel Performans Göstergeleri (KPI'lar)

Teknik ve Operasyonel KPI'lar

KPI	2026–2027 Hedefi	Ölçüm Yöntemi
Kritik güvenlik açığı giderme (CISA KEV)	48 saat içinde > %95 yamalanmış	Sürekli güvenlik açığı tarayıcısı
Oltalamaya dayanıklı MFA / Passkey kapsamı	%100 yöneticiler, VIP'ler ve uzaktan erişim	Aylık IAM / Entra ID denetimi
İnsan dışı kimlik güvenliği (API'ler/Botlar)	Gizli anahtar rotasyonu ile %100 envanterli	Servis hesabı ve gizli kasa denetimi
Değiştirilemez yedek geri yükleme testleri	Çeyrek başına kritik sistemlerin %100'ü	İmzalı geri yükleme test raporu
Ortalama Tespit (MTTD) / Müdahale (MTTR) Süresi	MTTD < 24 saat / MTTR < 48 saat	EDR / MDR / SIEM konsolu

İnsan ve Yönetişim KPI'ları

KPI	2026–2027 Hedefi	Ölçüm Yöntemi
Yapay zeka oltalama simülasyonlarında tıklama oranı	< %5	Aylık simülasyon platformu
Şüpheli e-posta proaktif bildirim oranı	> %70	E-posta istemcisi bildirim düğmesi
Siber eğitim ve Yapay Zeka tüzüğü tamamlama	Personelin %100'ü (yöneticiler dahil)	LMS takibi ve NIS 2 uyum günlüğü
Shadow AI kontrolü	Kurumsal verilere erişen 0 onaysız yapay zeka aracı	CASB / Proxy / DNS günlükleri

7.5 2026–2027 Uyum Kontrol Listeleri

KVKK (ve GDPR) Veri Koruma — Temel Kontrol Listesi

- Güncel Kişisel Veri İşleme Envanteri ve VERBİS kaydı (yapay zeka veri işleme süreçleri dahil).
- Yüksek riskli veri işleme ve üretken yapay zeka projeleri için Veri Koruma Etki Değerlendirmesi.
- Hassas verilerin hem durağan halde HEM DE aktarım sırasında şifrelenmesi (TLS 1.3 / AES-256).
- Tedarikçi veri işleme sözleşmelerinin yapay zeka güvenlik maddeleriyle güncellenmesi.
- Veri ihlallerinin 72 saat içinde KVKK'ya (ve ilgili durumlarda AB otoritelerine) bildirilmesi prosedürü.

USOM / SOME, CBDDO Rehberi ve NIS 2 — KOBİ Uyumluluk Listesi

- Sektörel düzenleyici kapsamın (USOM / BTK / BDDK ve AB ihracatçıları için NIS 2) doğrulanması.
- Üst yönetim ve yönetim kurulu üyeleri tarafından siber güvenlik farkındalık eğitiminin tamamlanması.
- Resmi risk analizi, olay müdahale (SOME) ve İş Sürekliliği / Felaket Kurtarma (BCP/DRP) politikaları.
- Önemli siber olayların 24 saat (erken uyarı) ve 72 saat içinde USOM / TR-CERT'e bildirim iş akışı.
- Tedarik zinciri güvenliği denetimi (kritik yazılım tedarikçileri, MSP'ler ve bulut sağlayıcıları).
- Yapay zeka yönetişim politikası (Shadow AI) ve insan dışı kimliklerin (API anahtarları) envanteri.

7.6 Eksiksiz PASS REVELATOR Ekosistemi (9 Çözümün Tamamı)

> **Resmi PASS REVELATOR 2026–2027 Paketi**
>
> PASS REVELATOR; erişim gücünü değerlendirmek, BT güvenliğini denetlemek ve parola kaybı ya da güvenlik olaylarının ardından meşru hesapları kurtarmak için **9 uzman araçtan** oluşan kapsamlı bir paket geliştirmektedir.

www.passwordrevelator.net adresinde bulunan 9 resmi çözümümüz:

- **PASS REVELATOR** — Microsoft, Outlook ve MSN ortamları için amiral gemisi BT güvenlik denetimi ve erişim kurtarma çözümü.
- **PASS FINDER** — Kişisel ve kurumsal Facebook hesapları için özel parola gücü denetimi ve erişim kurtarma aracı.
- **PASS RECOVERY** — Ele geçirilmiş veya kilitlenmiş X (eski adıyla Twitter) hesapları için özel erişim kurtarma ve geri yükleme çözümü.
- **PASS DECRYPTOR** — Instagram hesapları için gelişmiş şifre çözme ve meşru erişim kurtarma teknolojisi.
- **PASS BREAKER** — Gmail hesapları ve Google ekosistemi için güvenlik denetimi ve erişim geri yükleme modülü.
- **PASS ACCESS** — Yahoo! hesapları için güvenlik tanılama ve parola kurtarma çözümü.
- **PASS WIFI** — Altyapınızdaki Wi-Fi anahtarlarını (WPA/WPA2/WPA3) denetlemek ve kurtarmak için kablosuz ağ güvenlik analizörü.
- **PASS UNLOCKER** — TikTok hesapları için meşru hesap kilidi açma, koruma denetimi ve erişim kurtarma aracı.
- **PASS DECODER** — Snapchat hesapları için güvenli tanılama ve erişim kurtarma çözümü.

Zorunlu Etik ve Yasal Kullanım Taahhüdü: PASS REVELATOR paketindeki tüm yazılımlar yalnızca yasal ve etik kullanım için tasarlanmıştır: kendi altyapınızı denetlemek, parola dayanıklılığını test etmek ve meşru olarak sahip olduğunuz ya da denetlemek için açık yazılı yetkiye sahip olduğunuz hesaplara erişimi kurtarmak. Üçüncü taraf sistemlere yönelik her türlü yetkisiz kullanım kesinlikle yasaktır.

> *"Siber güvenlik durağan bir varış noktası değil, sürekli bir disiplindir. PASS REVELATOR ekosistemi dijital varlıklarınızı denetlemek, korumak ve geri yüklemek için her adımda yanınızdadır."*
>
> — PASS REVELATOR Team

Sonuç ve 2026–2029 Perspektifi

2026 yılında BT güvenliği ile iş sürekliliği arasındaki sınır kalıcı olarak ortadan kalkmıştır. Üretken yapay zeka saldırılarının sanayileşmesi, tedarik zinciri ihlallerindeki artış (tüm ihlallerin %48'i) ve NIS 2, DORA ile Cyber Resilience Act'in sıkı biçimde uygulanması stratejide acil bir değişim gerektirmektedir.

2026 verileri tartışmasızdır: rekor seviyedeki küresel ortalama **4,99 milyon dolar** (ve yapay zeka destekli saldırılar için **6,0 milyon dolar**) ihlal maliyetine karşılık, savunma yapay zekası, Zero Trust ve FIDO2 Passkeys benimseyen kuruluşlar için kanıtlanmış **1,93 milyon dolarlık maliyet azalması**.

2026 İçin 4 Temel Çıkarım

%62
İnsan faktörünü içeren ihlaller — ekipleri yapay zeka oltalaması ve deepfake'lere karşı eğitin

-%26
Oltalamaya dayanıklı MFA ve FIDO2 Passkeys sayesinde parola saldırılarında düşüş

-1,93 M$
Savunma yapay zekası ve SOC otomasyonu ile ihlal başına ortalama maliyet tasarrufu (IBM 2026)

%80
Titiz hijyen ile etkisiz hale getirilen siber saldırı oranı (< 48 saat yamalar, Passkeys, 3-2-1-1-0 yedekler)

2026–2027 İçin Siber Güvenliğin 10 Emri

1. **Oltalamaya dayanıklı MFA ve FIDO2 Passkeys devreye alın** — AiTM vekil kitlerini boşa çıkarmak için tüm hassas ve yönetici hesaplarında.
2. **Benzersiz 16+ karakterli parola cümleleri kullanın** — NIST SP 800-63B Rev. 4 ile uyumlu şifreli bir parola yöneticisinde saklayın.
3. **İnternete açık cihazları ve sistemleri 48 saat içinde yamalayın** — çünkü güvenlik açığı sömürüsü artık 1 numaralı başlangıç erişim vektörüdür (%31).
4. **İnsan dışı kimlikleri ve Shadow AI'ı yönetin** — API anahtarlarını, servis hesaplarını ve kurumsal LLM erişimini kontrol altında tutarak.
5. **Değiştirilemez yedekleri (3-2-1-1-0) üç ayda bir test edin** — dayanıklı mağdurların %69'u gibi fidye taleplerini reddedebilmek için.
6. **En az ayrıcalık ve Zero Trust uygulayın** — hem çalışanlar, hem üçüncü taraf yükleniciler hem de otonom yapay zeka ajanları için.
7. **Yöneticileri ve finans ekiplerini deepfake'lere karşı eğitin** — tüm finansal işlemler için bant dışı doğrulamayı zorunlu kılarak.
8. **Tedarik zincirinizi denetleyin** — çünkü ihlallerin %48'i artık üçüncü taraf bir satıcıyı veya yazılım entegrasyonunu içermektedir.

9. **Bir Olay Müdahale Planı (IRP) resmileştirin ve prova edin** — kontrol altına alma sürelerini kısaltarak ve 24/72 saatlik NIS 2 & GDPR sürelerini karşılayarak.
10. **Savunma yapay zekasını ve PASS REVELATOR denetim araçlarını entegre edin** — siber güvenliği kalıcı bir rekabet avantajına dönüştürerek.

Üst Düzey Yöneticilere Stratejik Mesaj

> *"Siber güvenlik artık yalnızca BT departmanına devredilen teknik bir konu değildir: artık yasalarla güvence altına alınmış doğrudan bir yönetim kurulu sorumluluğudur."*
>
> — Temel Yönetişim İlkesi, AB NIS 2 Direktifi

Ulusal NIS 2 düzenlemeleri ve Cyber Resilience Act kapsamında şirket yöneticileri kişisel sorumluluk taşır ve tamamlanmış siber güvenlik eğitimini ile aktif risk gözetimini kanıtlamak zorundadır.

Yönetim Kurulu için acil eylemler:

- Siber güvenlik KPI'larını ve yapay zeka yönetişimini aylık yönetim kurulu gündemine alın.
- Toplam BT harcamalarının %10–15'ini temsil eden özel bir siber güvenlik bütçesi ayırın.
- Zorunlu üst düzey yönetici siber güvenlik eğitimini tamamlayın (NIS 2 uyumu).
- Yılda bir kez simüle edilmiş bir siber kriz tatbikatına (fidye yazılımı / veri sızıntısı) katılın.
- Deepfake yönetici dolandırıcılığını önlemek için katı bant dışı çift yetkilendirmeyi zorunlu kılın.

2026 Siber Dayanıklılık Denklemi

CYBER-RESILIENCE =

(Passkeys & Zero Trust × Savunma Yapay Zekası × Değiştirilemez Yedekler) + İnsan Eğitimi + Yönetici Yönetişimi

Bu denklemdeki hiçbir çarpan sıfır olamaz: bir yönetici sesli deepfake üzerine para transferini onaylarsa en iyi teknoloji başarısız olur ve en iyi eğitim yamalanmamış bir VPN ağ geçidini sömüren otomatik bir tarayıcıyı durduramaz.

2026–2029 Perspektifi: Bir Sonraki Dalgaya Hazırlık

2026–2029 Eğilimi	Beklenen Etki	Bugün Önerilen Hazırlık
Otonom saldırgan yapay zeka ajanları ve Shadow AI	Kendi kendine uyarlanan çok aşamalı saldırılar ve LLM veri sızıntıları	Katı yapay zeka yönetişimi, insan dışı kimlik güvenliği, AI EDR/NDR
Yaygın gerçek zamanlı ses/video deepfake'leri	Aramalarda ve toplantılarda rutin yönetici taklidi	Kriptografik doğrulama, sözlü kod kelimeleri ve çok kanallı onay
Kuantum Sonrası Kriptografiye (PQC) geçiş	Uzun ömürlü sırlar için 'Şimdi Topla, Sonra Çöz' tehdidi	Kriptografik envanter (2026'da yalnızca %34'ünde var) ve NIST FIPS 203/204/205 geçişi
Sıkı NIS 2, DORA, CRA ve AI Act uygulaması	Mevzuat denetimleri, ağır para cezaları ve B2B ihale dışı kalma	Proaktif uyum, 24/72 saatlik raporlama ve üçüncü taraf denetimleri
Küresel siber güvenlik yetenek açığı	Milyonlarca nitelikli uzman eksikliğinin sürmesi	SOAR otomasyonu, yapay zeka SOC yardımcı pilotları ve 7/24 MDR hizmetleri

Eylemsizliğin Maliyeti

Gerçek Dünya Senaryosu: Hazırlıksız 50 Çalışanlı KOBİ

- **1. Gün:** Yamalanmamış bir VPN açığının otomatik sömürülmesi veya Passkey bulunmayan bir hesapta AiTM oltalaması.
- **2. Gün:** Segmentlere ayrılmamış düz bir ağ üzerinde oturum belirteci hırsızlığı ve servis hesabı ele geçirilmesi.
- **3. Gün:** Müşteri verilerinin sızdırılması ve ardından fidye yazılımı dağıtımı. Bağlı çevrimiçi yedekler de şifrelenir.
- **1. Hafta:** Operasyonlar ve faturalama tamamen durur. Şantajcılar müşteri verilerini sızdırmakla tehdit eder (üçlü şantaj).
- **2–3. Haftalar:** Acil adli bilişim maliyetleri, sunucuların manuel yeniden kurulumu, KVKK ve USOM'a zorunlu yasal bildirimler.
- **2.–6. Aylar:** Tedarik zinciri uyumsuzluğu nedeniyle B2B müşterilerinin %30'unun kaybı, > 750.000 € toplam kayıp, ciddi iflas riski.

Bu felaketi önleyebilecek yıllık bütçe: 25.000 € / yıl (Passkeys/MFA + EDR + Değiştirilemez Yedekler + Eğitim).

Bugün Harekete Geçin

Kuruluşunuzu 2026–2027 döneminde güvenceye almak için sonraki 6 adımınız:

1. **Acil Değerlendirme (1. Gün):** Bölüm 7.5'teki kontrol listelerini kullanarak hızlı bir denetim yapın.
2. **Kimlik Hızlı Kazanımları (1. Hafta):** Oltalamaya dayanıklı MFA / Passkeys'i etkinleştirin ve kurumsal bir parola yöneticisi kurun.
3. **Shadow AI Yönetişimi ve Yama (2. Hafta):** İnternete açık cihazları yamalayın ve bir yapay zeka kullanım tüzüğü oluşturun.
4. **Yedekleme Dayanıklılığı (3.–4. Haftalar):** Canlı bir geri yükleme tatbikatıyla 3-2-1-1-0 mimarinizi doğrulayın.
5. **2026–2027 Bütçesi:** BT bütçenizin %10–15'ini siber güvenliğe ve NIS 2 uyumuna ayırın.
6. **Denetim ve Araçlar:** Meşru hesaplarınızı denetlemek ve kurtarmak için PASS REVELATOR yazılım paketinden yararlanın.

PASS REVELATOR Taahhüdü

PASS REVELATOR olarak misyonumuz, güvenlik denetimini ve meşru erişim kurtarmayı hem işletmeler hem de yetkili bireyler için erişilebilir, güvenilir ve şeffaf kılmaktır:

- 9 yazılım çözümümüzü en yüksek 2026–2027 teknolojik standartlarına göre geliştirmek ve sürdürmek.
- Siber güvenlik ve etik hacking uzmanlığımızı uluslararası rehberler aracılığıyla ücretsiz olarak paylaşmak.
- KOBİ'leri, orta ölçekli firmaları ve profesyonelleri dijital kimliklerini güvenceye alma konusunda desteklemek.
- Güvenlik denetimi ve kurtarma araçlarının kesinlikle etik, yasal ve sorumlu kullanımını teşvik etmek.

> **Yardıma veya Yazılım Çözümlerimize mi İhtiyacınız Var?**
>
> 9 güvenlik denetimi ve erişim kurtarma aracımızın tamamını keşfedin veya uzman ekibimizle iletişime geçin:
> www.passwordrevelator.net
> info@passrevelator.net

Son Söz

> *"2026'nın dijital ekonomisinde siber güvenlik küresel şirketlere özgü bir lüks değil, her kuruluş için güvenin temelidir. Otomatik tehditlere karşı gecikilen her gün maruziyetinizi artırır. İyi haber: siber dayanıklılığın %80'i bugün devreye alabileceğiniz yapılandırılmış, erişilebilir önlemlere dayanmaktadır. Şimdi başlayın."*
>
> — PASS REVELATOR Ekibi — Kasım 2026

Ek Kaynaklar ve Doğrulanmış 2026 Verileri

Resmi Kurumlar ve Uluslararası Çerçeveler

Kurum / Çerçeve	Rol ve Referans Rehberler	Resmi Web Sitesi
USOM / TR-CERT (Türkiye)	Ulusal Siber Olaylara Müdahale Merkezi — Tehdit Bildirimleri ve Zararlı Bağlantı Listesi	https://www.usom.gov.tr
KVKK (Türkiye)	Kişisel Verileri Koruma Kurumu — Veri İhlali Bildirim Rehberleri ve Teknik Tedbirler	https://www.kvkk.gov.tr
CISA (ABD / Küresel)	Cybersecurity & Infrastructure Security Agency — İstismar Edilen Zafiyetler Kataloğu (KEV)	https://www.cisa.gov
ENISA (Avrupa Birliği)	AB Siber Güvenlik Ajansı — Tehdit Raporları, NIS 2 ve Siber Dayanıklılık Yasası	https://www.enisa.europa.eu
NIST (Uluslararası)	Cybersecurity Framework (CSF 2.0), SP 800-63B Rev. 4 ve Kuantum Sonrası Kriptografi	https://www.nist.gov/cyberframework
OWASP & MITRE ATT&CK	Küresel uygulama güvenliği standartları (Top 10) ve saldırgan taktikleri bilgi tabanı	https://owasp.org

Tehdit İstihbaratı ve Güvenlik Bültenleri

- **USOM (TR-CERT)** — Resmi Türkiye siber güvenlik uyarıları ve tehdit istihbaratı: www.usom.gov.tr
- **Krebs on Security** — Derinlemesine siber suç araştırmaları: krebsonsecurity.com
- **The Hacker News** — Günlük zafiyet ve siber tehdit haberleri: thehackernews.com
- **Bleeping Computer** — Teknik güvenlik uyarıları, fidye yazılımları ve kritik yamalar: bleepingcomputer.com

Bu 2026–2027 Baskısı İçin Doğrulanmış Kaynaklar

Sürüm 2.0, en güncel küresel sektör yayınlarından elde edilen doğrulanmış veriler üzerine inşa edilmiştir:

- IBM & Ponemon Institute — *Cost of a Data Breach Report 2026* (21. Baskı)
- Verizon — *Data Breach Investigations Report (DBIR) 2026*
- Sophos — *The State of Ransomware 2026*
- Microsoft — *Microsoft Digital Defense Report (MDDR) 2025–2026*
- Cybersecurity Ventures — *Global Cybercrime Economy & Almanac 2026–2029*
- World Economic Forum (WEF) — *Global Cybersecurity Outlook 2026*

- NIST — *Special Publication 800-63B Revision 4 (Digital Identity Guidelines)* ve PQC Standartları FIPS 203/204/205
- Avrupa Birliği — Direktif (AB) 2022/2555 (NIS 2), DORA Tüzüğü, Cyber Resilience Act (CRA) ve EU AI Act
- PASS REVELATOR Teknik Dokümantasyonu ve Özgün Araştırmaları (2026)

PASS REVELATOR

Siber Güvenlik, Kimlik Denetimi ve Etik Hacking Uzmanları

www.passwordrevelator.net | info@passrevelator.net

© 2026 PASS REVELATOR — Tüm hakları saklıdır.
Bu beyaz kitap yalnızca bilgilendirme ve eğitim amaçlı sunulmaktadır. Öneriler her kuruluşun kendi özel ortamına göre uyarlanmalıdır.
Siber Güvenlik Beyaz Kitabı 2026–2027 — Sürüm 2.0 — Kasım 2026 — www.passwordrevelator.net kaynak gösterilerek ücretsiz halka açık dağıtım serbesttir