OSIRIUM **PAS**

Privileged Access Security

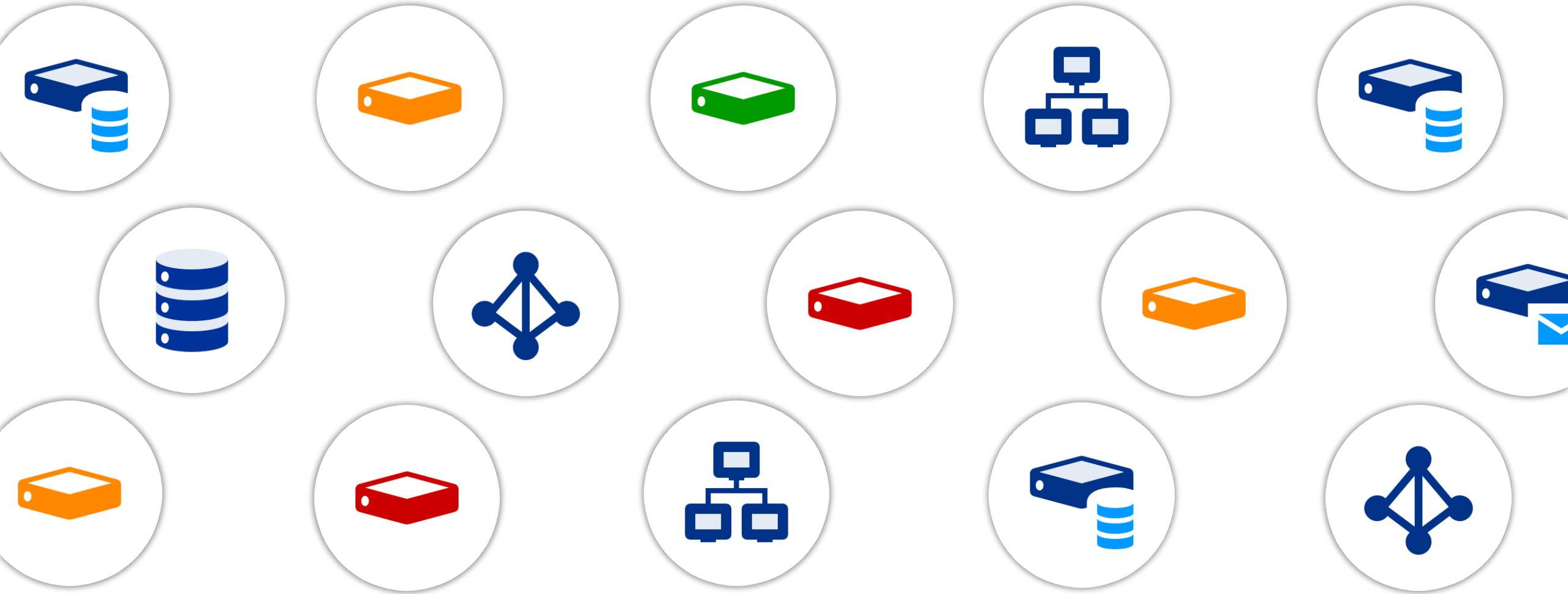
Ayrıcalıklı Erişim Güvenliği

Değerli IT varlıklarınızı koruyun,
operasyonunuzu hızlandırın

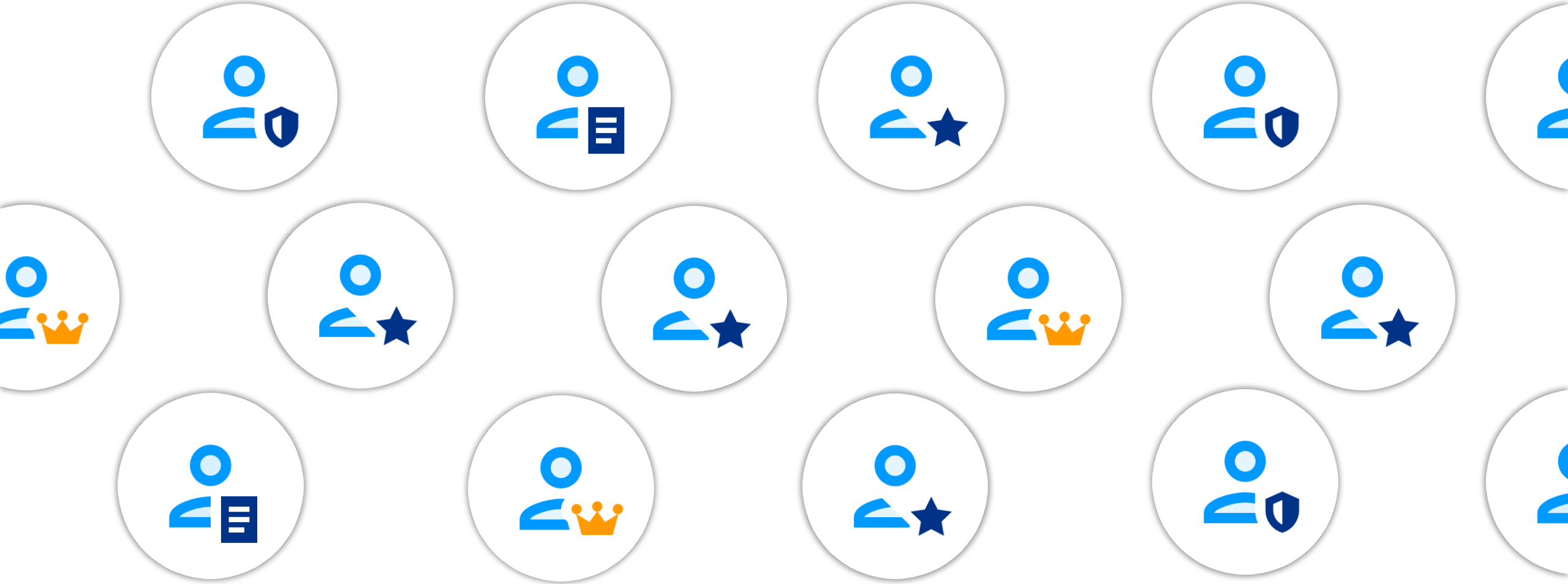
TeSlakom

OSIRIUM

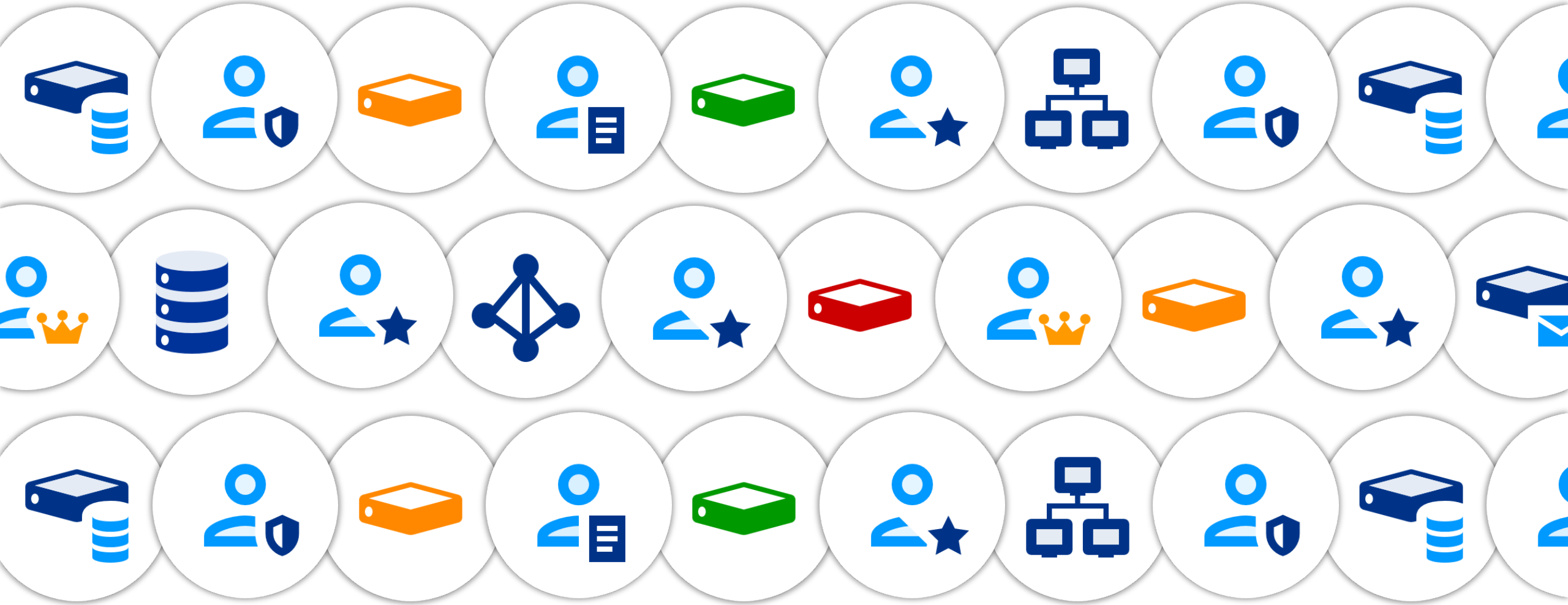
Yönetilmesi gereken çok sayıda servis ve cihaz



Çok sayıda admin hesabı



Güvende ve verimli olmak çok zor

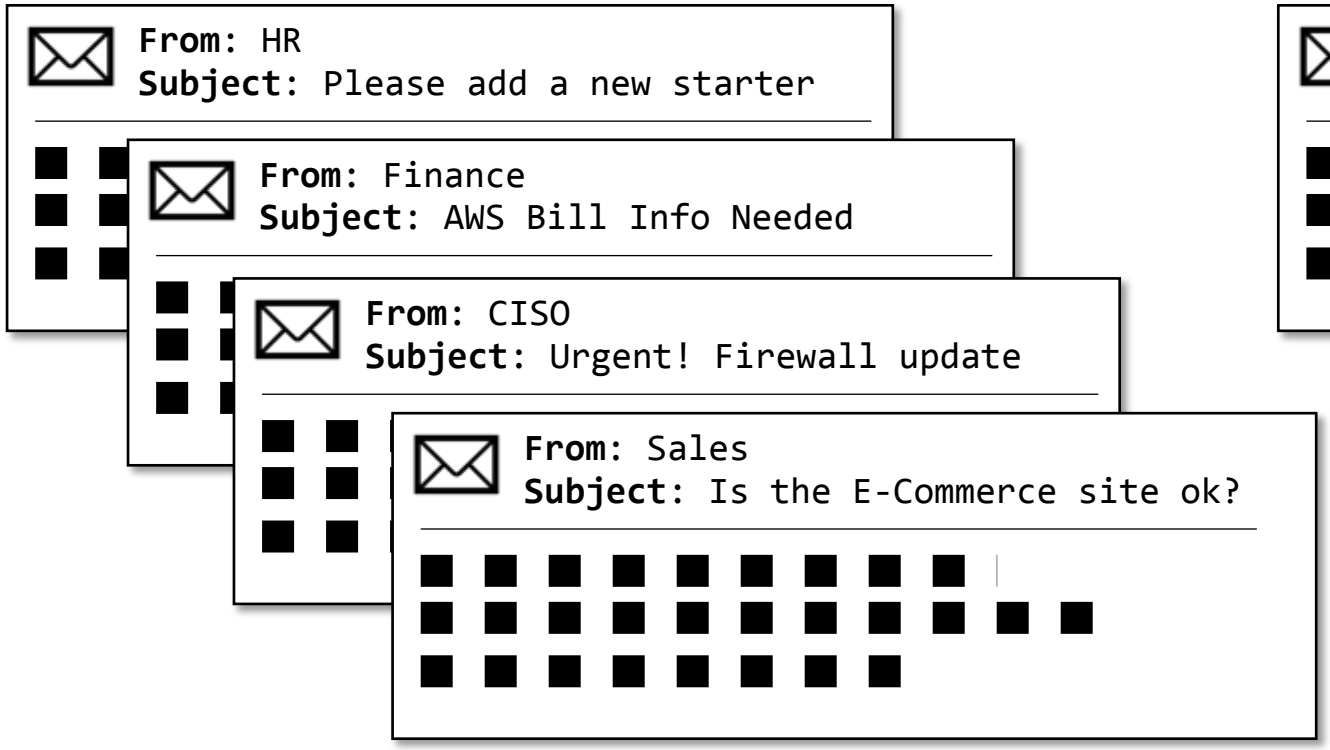


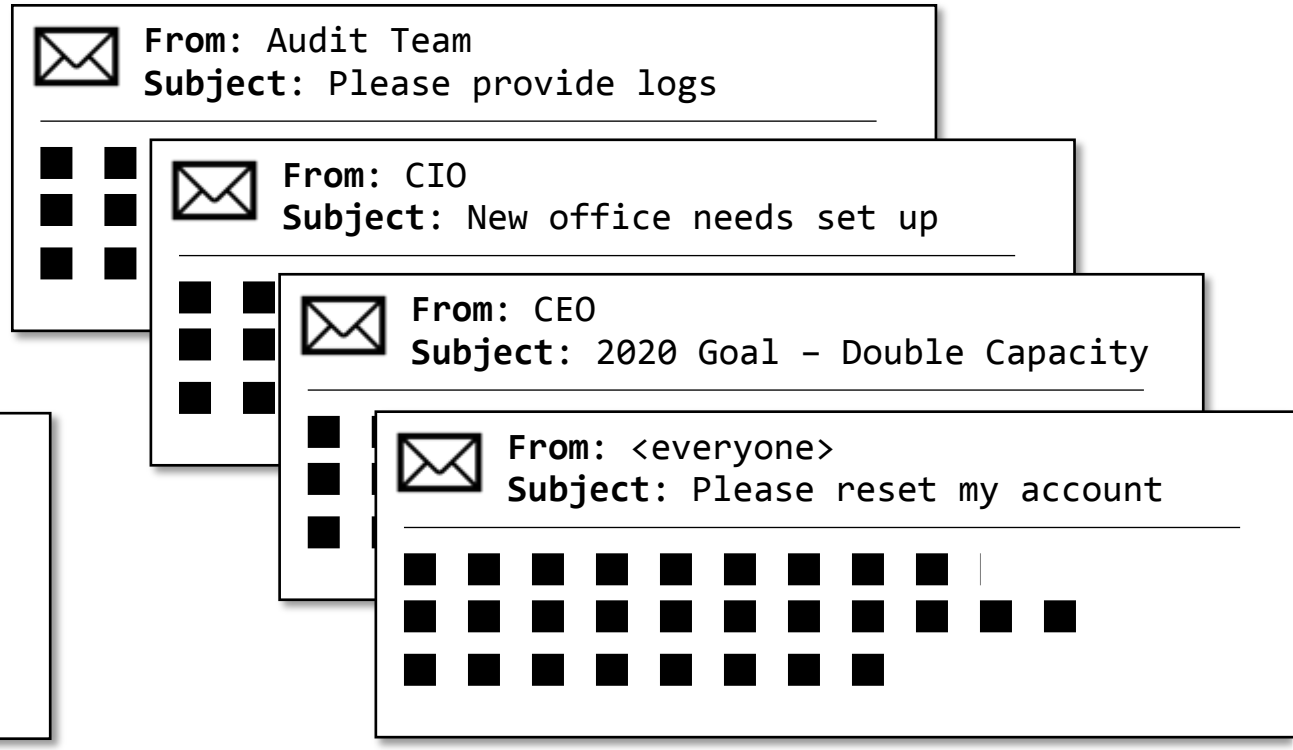
Desktop cihazlarda ayrıcalıklı hesaplar

Lokal admin hesapları siber saldırganlar için cazip ve savunmasız giriş noktalarıdır...

IT Operasyon ekipleri aşırı yoğunluktan şikayetçi

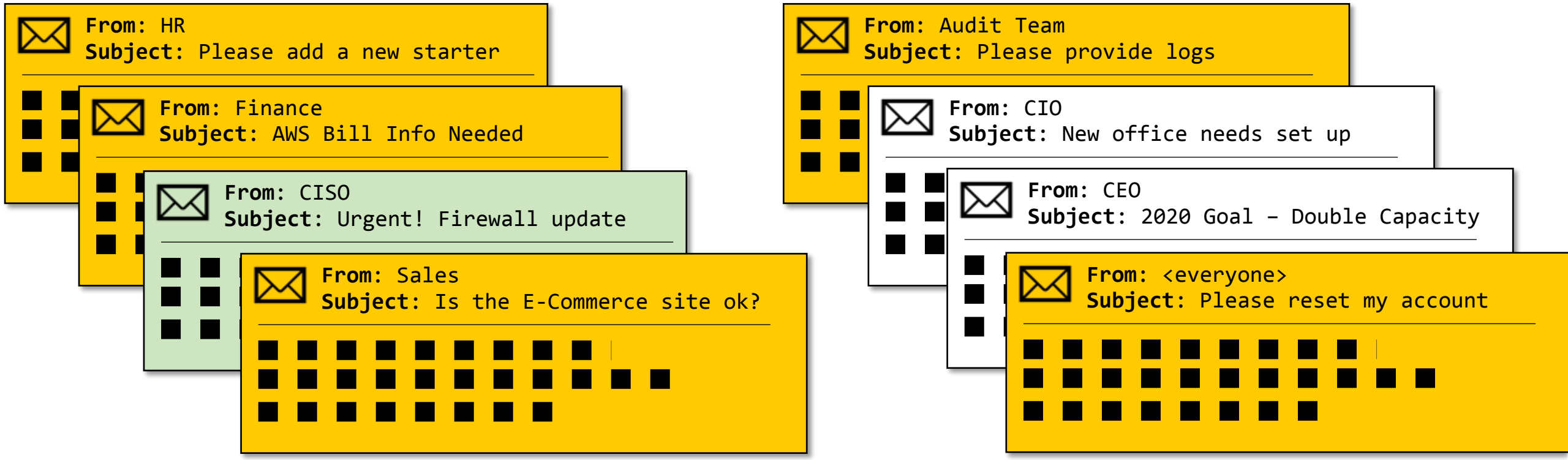
Sonu gelmeyen talepler ve güncellemeler…





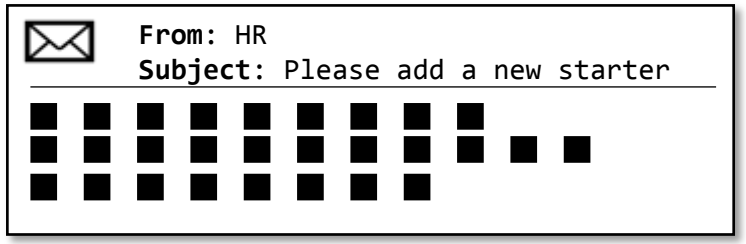
IT Operasyon ekipleri aşırı yoğunluktan şikayetçi

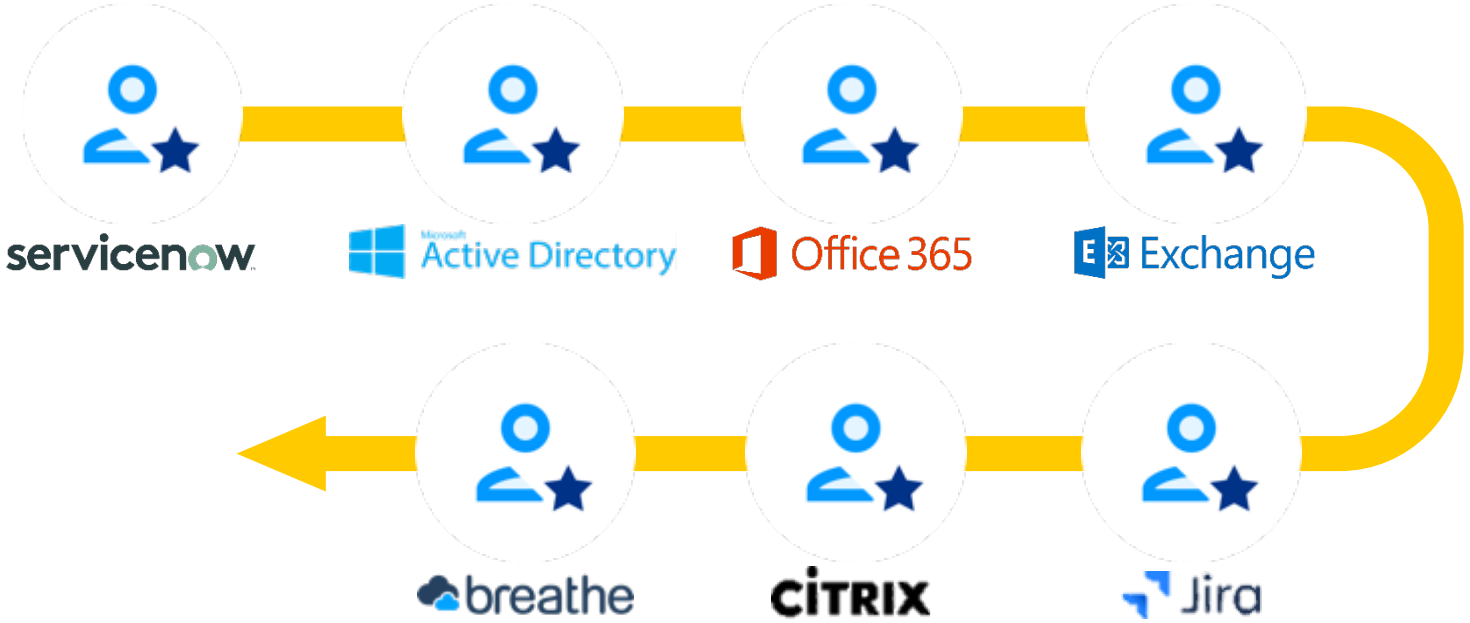
Oysa bazı talepler hızlı ve hatasız şekilde çözümlendirilebilir



Ancak otomasyonun avantajları verimli kullanılamaz

Talepler birden fazla uzman admin'in onayını gerektirir





- ☹ **Çok fazla admin**
- ☹ **Çok fazla giriş yetkisi kontrolü**
- ☹ **Çok fazla gecikme**

OSIRIUM **PAS**

Ayrıcalıklı Erişim Güvenliği - Değerli IT varlıklarınızı koruyun, operasyonunuzu hızlandırın

OSIRIUM **PPA**

IT ve iş süreçlerini otomatikleştirin

OSIRIUM **PAM**

Paylaşımlı servis, uygulama ve cihazlarınızı koruyun

OSIRIUM **PEM**

Yardım masalarının yükünü azaltın, lokal adminleri kaldırın

OSIRIUM **PAM**

Paylaşımlı servis, uygulama ve cihazlarınızı koruyun

KULLANICILARI ŞİFRE ve KİMLİKLERDEN **AYRI TUTUN**

SADECE BELİRLİ UYGULAMARA **ERİŞİM İZNİ VERİN**

DENETİM ve ARAŞTIRMALAR İÇİN OTURUMLARI **KAYDEDİN**

GENEL ve ORTAK GÖREVLERİ **OTOMATİKLEŞTİRİN**

OSIRIUM **PPA**

IT ve iş süreçlerini otomatize edin

KARŞILIKLI SİSTEM SÜREÇLERİNİ **OTOMATİKLEŞTİRİN**

KULLANICI ve YARDIM MASASINA GÖREVLER **DELEGE EDİN**

KİMLİKLERİ **GÜVENDE TUTUN**

POTANSİYEL RİSK ve MALİYETLERİ **AZALTIN**

OSIRIUM **PEM**

Yardım masalarının yükünü azaltın, lokal adminleri kaldırın

LOKAL ADMIN HESAPLARINI **KALDIRIN**

KULLANCILARI **UYGULAMA BAZLI** YETKİLENDİRİN

ADMIN OLARAK ÇALIŞTIRILACAK UYGULAMALARI **ONAYLAYIN**

YARDIM MASASININ YÜKÜNÜ **AZALTIN**

OSIRIUM

- Yenilikçi Ayrıcalıklı Erişim Yönetim hakkında uzun süreli bilgi birikimi
- Gartner Cool Vendor
- Güvenlik süreç otomasyonunda lider
- 2008’de kuruldu
- Genel Merkez İngiltere

OSIRIUM **PAM**

Privileged Access Management

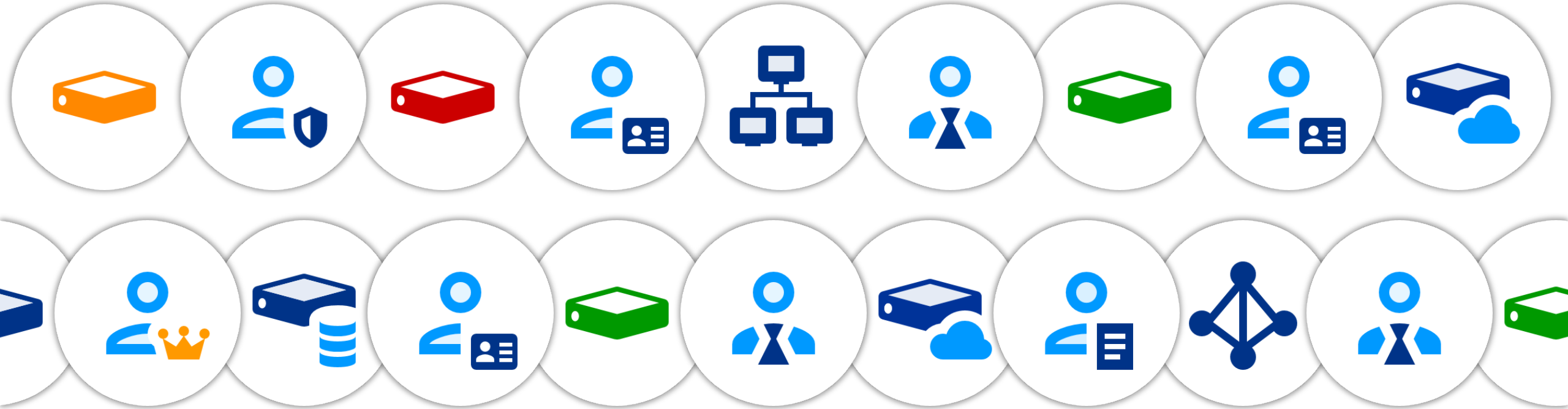
Ayrıcalıklı Erişim Yönetimi

Paylaşımlı servis, uygulama ve cihazlarınızı koruyun

TeSlakom

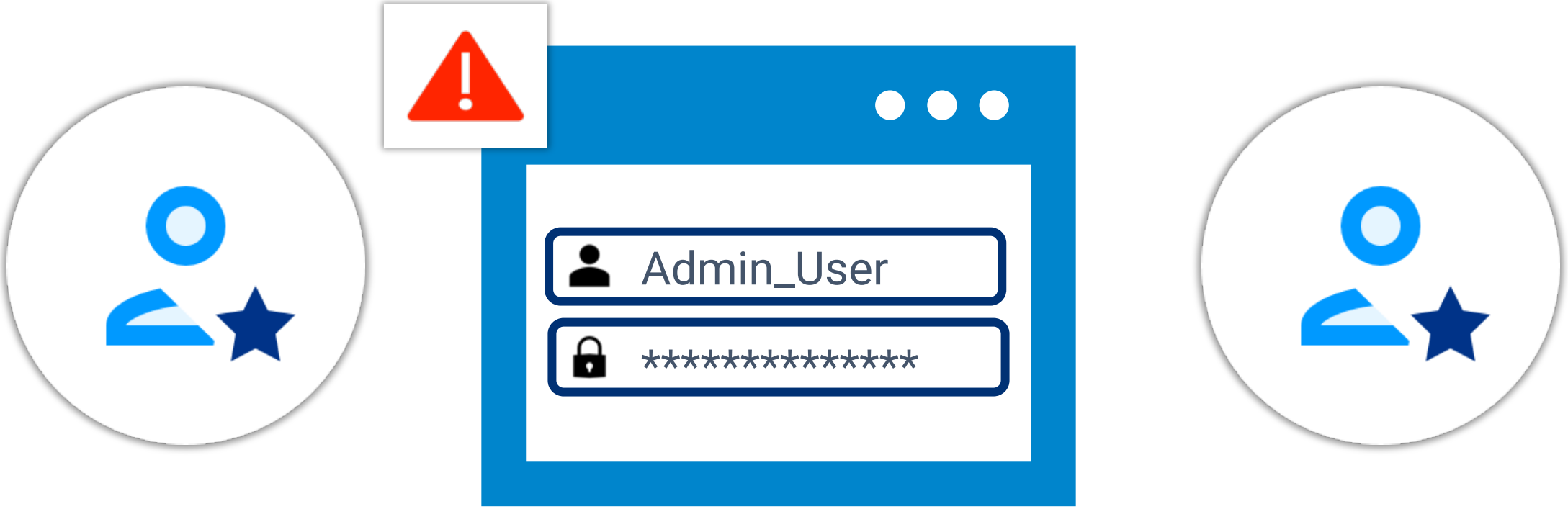
OSIRIUM

Pek çok farklı cihaz/hizmetin ve yönetici hesabının karmaşıklığı göz önüne alındığında, çoğu kuruluşun **hangi ayrıcalıklı hesaplara** sahip olduklarını, bunlara **kimin eriştiğini** veya bu erişimi **nasıl kontrol edeceğini** bilmemesi şaşırtıcı değildir.

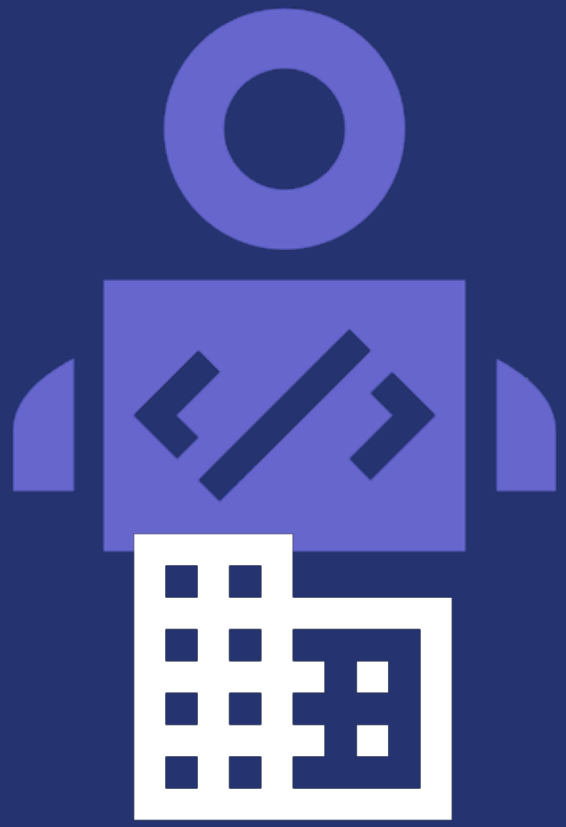


Hesap kullanıcı ad ve şifreleri **paylaşılır**, şifreler yeterince sık **güncellenmezse**, denetçiler sistemlerin **ne kadar güvenli olduğunu kanıtlayamaz….**

Admin hesaplarının **kontrolü sizde değilse**, diğer güvenlik araçları **güvensizdir**, çünkü bunların nasıl yönetileceğini kontrol edemezsiniz.



DIŞ KAYNAK TEHDİTLERİ

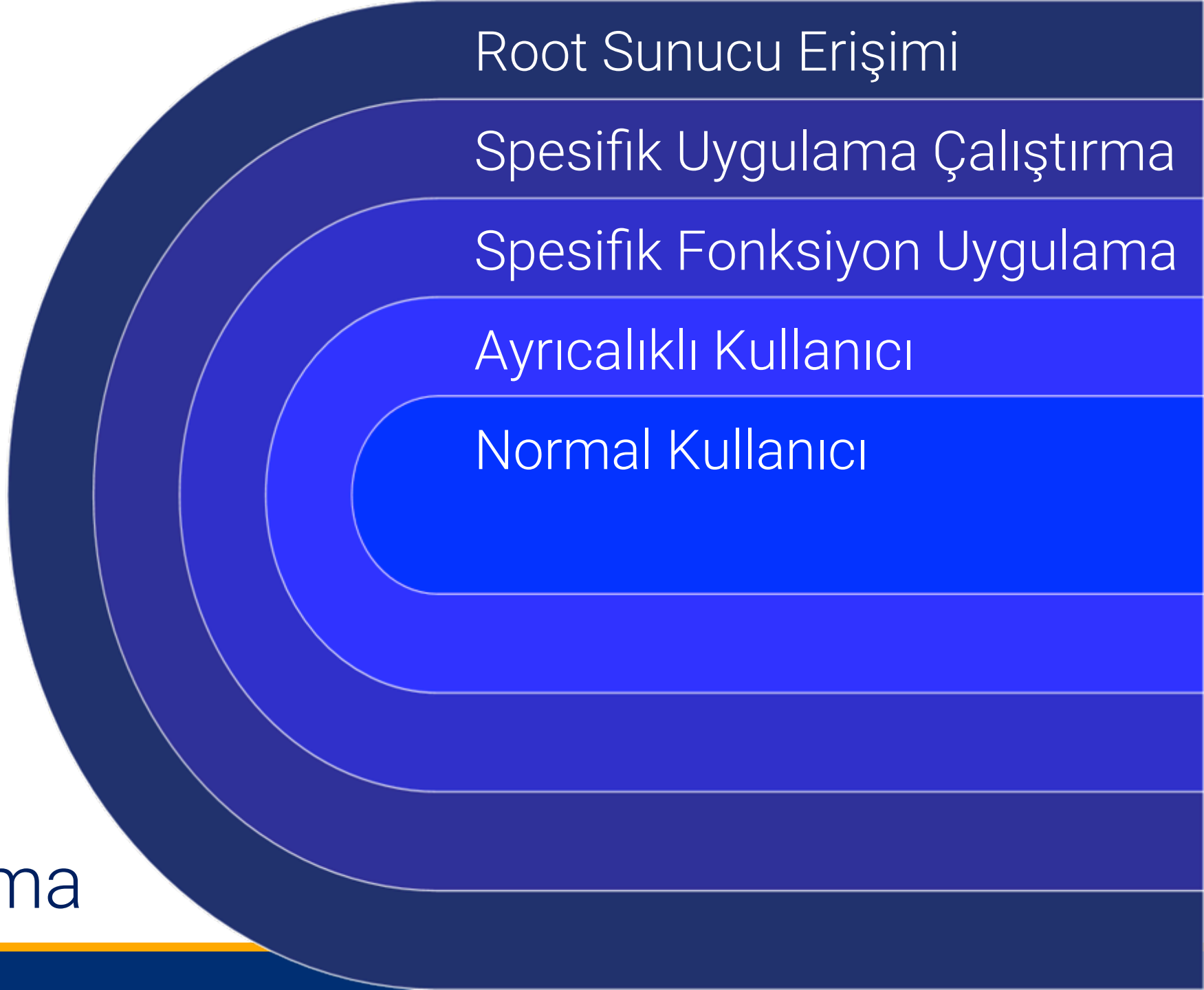


İÇ KAYNAK TEHDİTLERİ

3RD PARTY TEHDİTLERİ

Siber saldırıların %80'i ayrıcalıklı kimlikleri adreslerler.

Tüm IT sorunlarının %95'i ayrıcalıklı kimlikler ile alakalıdır.



Doğru Ayrıcalık
Doğru Kişiler
Doğru Zamanlama

İhtiyacınız olan çözüm: **Ayrıcalıklı Erişim Yönetimi (PAM)**
Geleneksel PAM çözümlerini uygulamaya almak ve yönetmek kadar son kullanıcı verimliliği ile ilişkilendirmek de zordur.

Yeni nesil PAM çözümü **Osirium'un PxM platformu** bu sorunları çözüyor. Kurulumu çok **kolaydır** ve **minimum altyapı** gereksinimine sahiptir.
PxM, kullanıcılar ve sistemler arasında oturur, böylece kullanıcılar gerçek ayrıcalıklı hesap detaylarına asla erişemez ve tüm ayrıcalıklı hesaplar için bir komut ve kontrol noktası vardır.

PxM platformu kullanıldığında, denetçi ve yönetişim uzmanlarının ihtiyaçlarını karşılamak için **analitik çözümler, oturum kaydı, görev otomasyonu** ve zengin **denetim araçları** gibi gelişmiş yeteneklerin temelini oluşturur.

ANALİTİK ÇÖZÜMLER

DENETİM VE KONTROL

OSIRIUM **PAM**

OTURUM KAYDI

GÖREV OTOMASYONU

OSIRIUM **PPA**

Privileged Process Automation

Ayrıcalıklı Süreç Otomasyonu

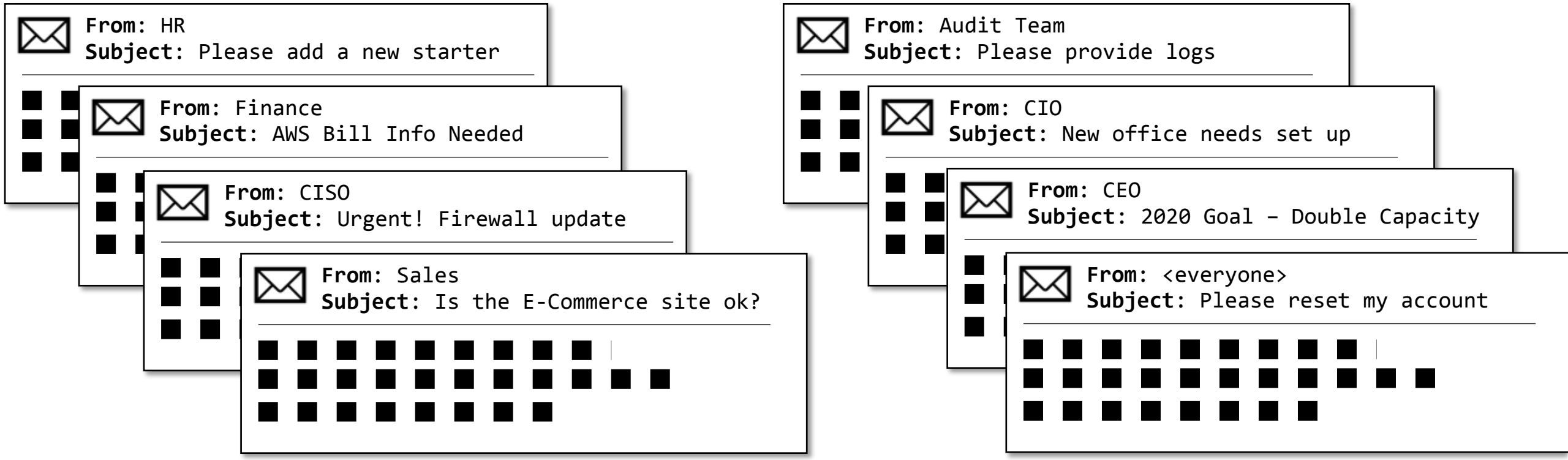
Otomatize IT ve iş süreçleri ile IT yoğunluğunu azaltın

TeSlakom

OSIRIUM

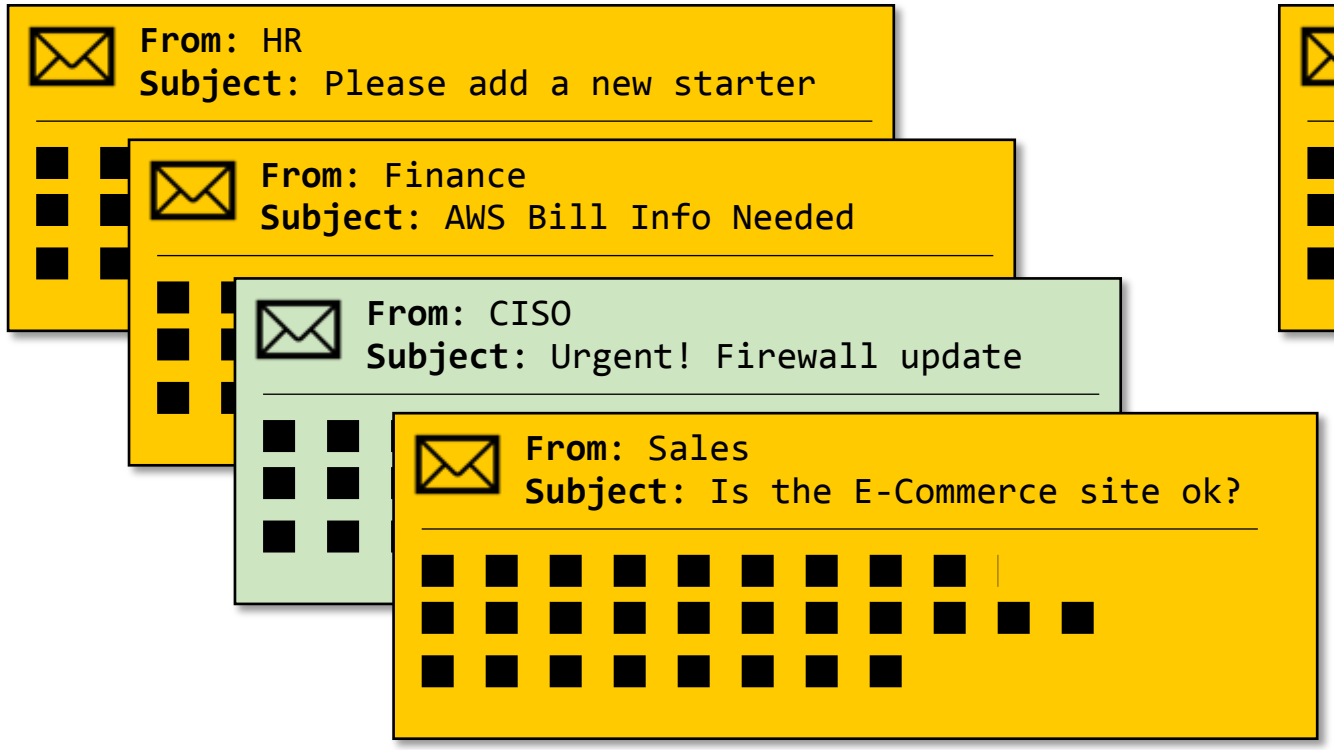
IT Operasyon ekipleri aşırı yoğunluktan şikayetçi

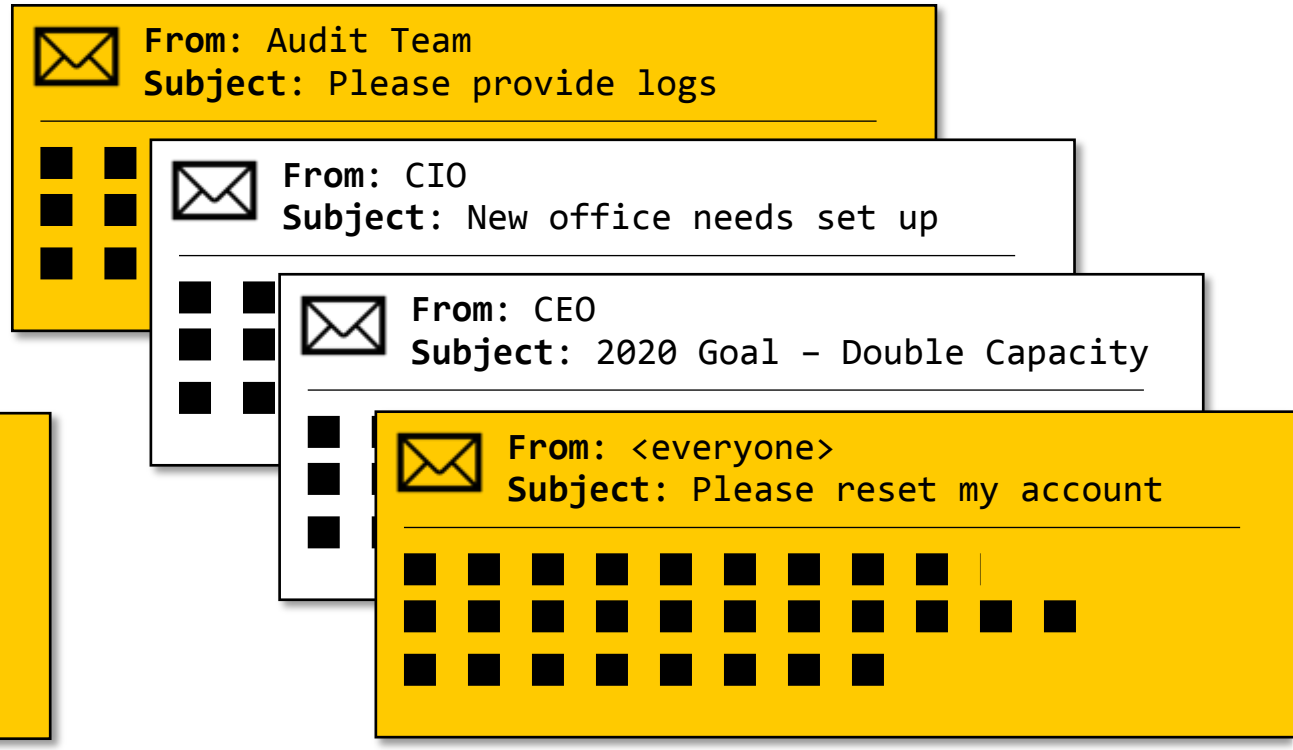
Sonu gelmeyen talepler ve güncellemeler…



IT Operasyon ekipleri aşırı yoğunluktan şikayetçi

Bazı talepler hızlı ve hatasız şekilde çözümlendirilebilir... **EĞER KONTROL EDERSENİZ!**

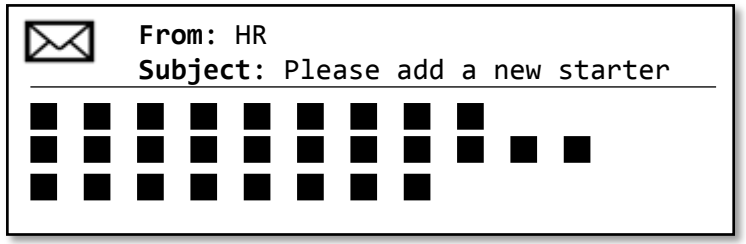


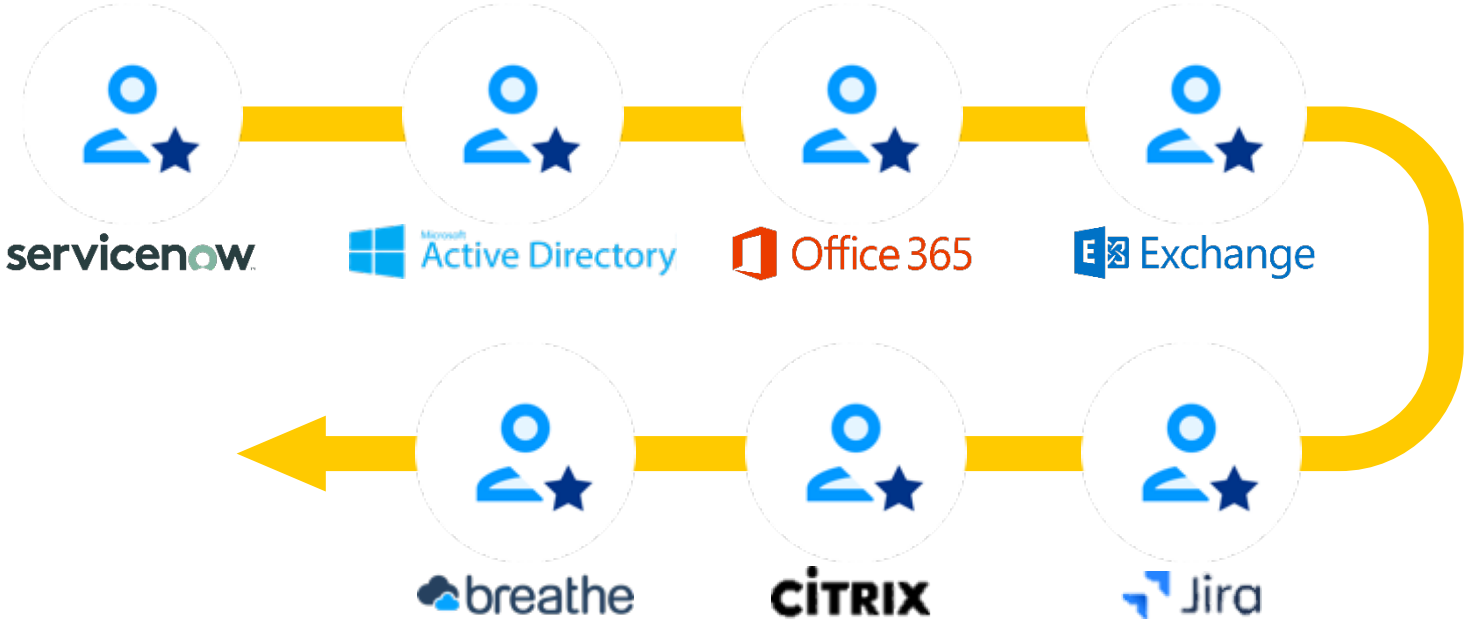


SONUÇ: **DEĞERLİ İŞLERE ODAKLANIN, RİSKİ DÜŞÜRÜN, MALİYETİ AZALTIN**

Süreçler neden otomatize edilmez?

Talepler birden fazla uzman admin'in onayını gerektirir





- ☹ **Çok fazla admin**
- ☹ **Çok fazla giriş yetkisi kontrolü**
- ☹ **Çok fazla gecikme**

Geleneksel otomasyonun limitleri vardır

Komut Yazma

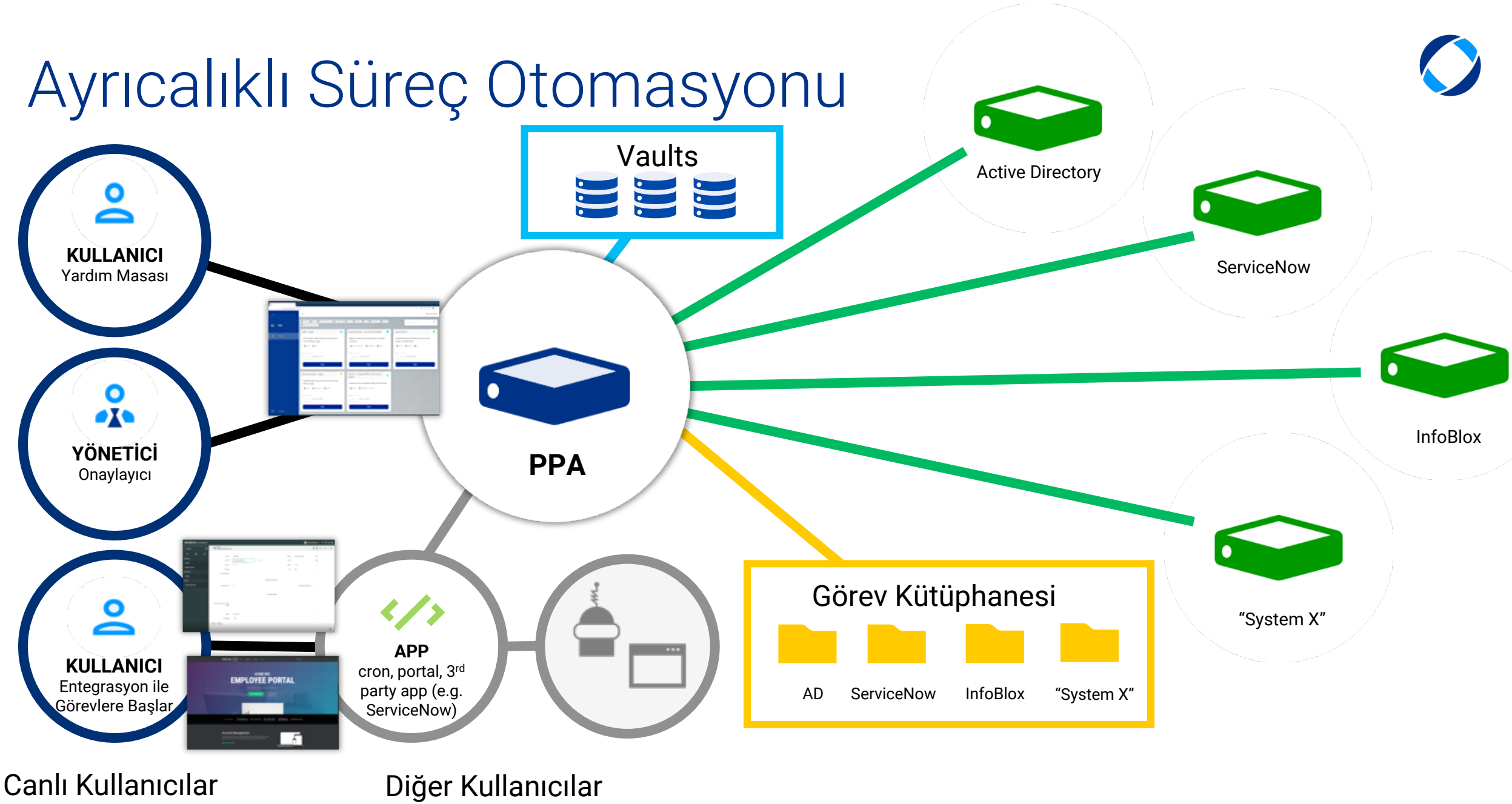
IT yöneticileri bash veya PowerShell kullanabilirler. Ama bu riskli senaryoları nasıl çalıştıklarını kimin bildiğini kim bilebilir?
Admin hesabı kullanıcı adı ve şifresini göstermeden sunuculara giriş yapmayı nasıl yönetiyorlar?
Bir admin, hepsini otomatik hale getirmek için bir süreçte dokunulması gereken birden fazla sistem hakkında yeterli bilgiye sahip mi?

RPA

RPA araçları OCR ve belge taramalarına sahip olabilirler, ancak Active Directory gibi karmaşık bir araca nasıl bağlanacaklarını ve bu araçlarda nasıl gezineceklerini bilmiyorlar.
Ayrıca, sürekli olarak işlenen belgeler ile beslenen makine olmaları da amaçlanmıştır. IT Yöneticisinin görevleri daha farklıdır ve değişken girdiler sağlamak veya bir araçtan sonuçları doğrulamak için genellikle operatör müdahalesine ihtiyaç duyar (örneğin, Active Directory'de güncellenen kullanıcının doğru olduğunu doğrulamak).

Çözüm: AYRICALIKLI SÜREÇ OTOMASYONU (PPA)

Ayrıcalıklı Süreç Otomasyonu

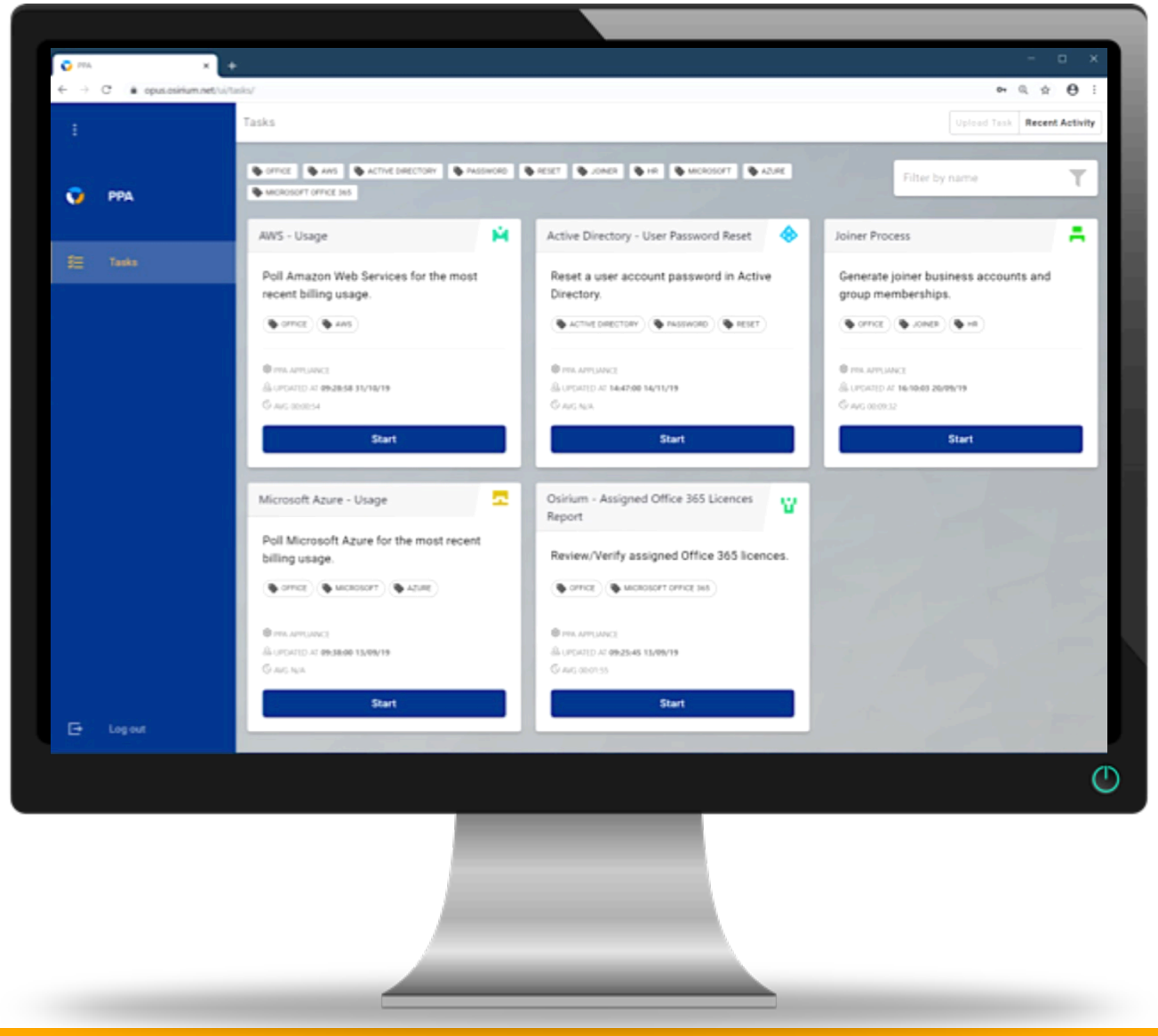


PPA Dashboard Ekranı

Görev erişimi role bağlıdır

Kullanıcılar sadece izin verilen işlemleri yapabilir

Sunucuya veya tam uygulamaya erişmeye gerek yok



PPA Görevler Ekranı

Etkileşimli arayüz

PPA tarafından belirlenen kimlik bilgileri - kullanıcılara veya ağa hiçbir zaman yayılmaz

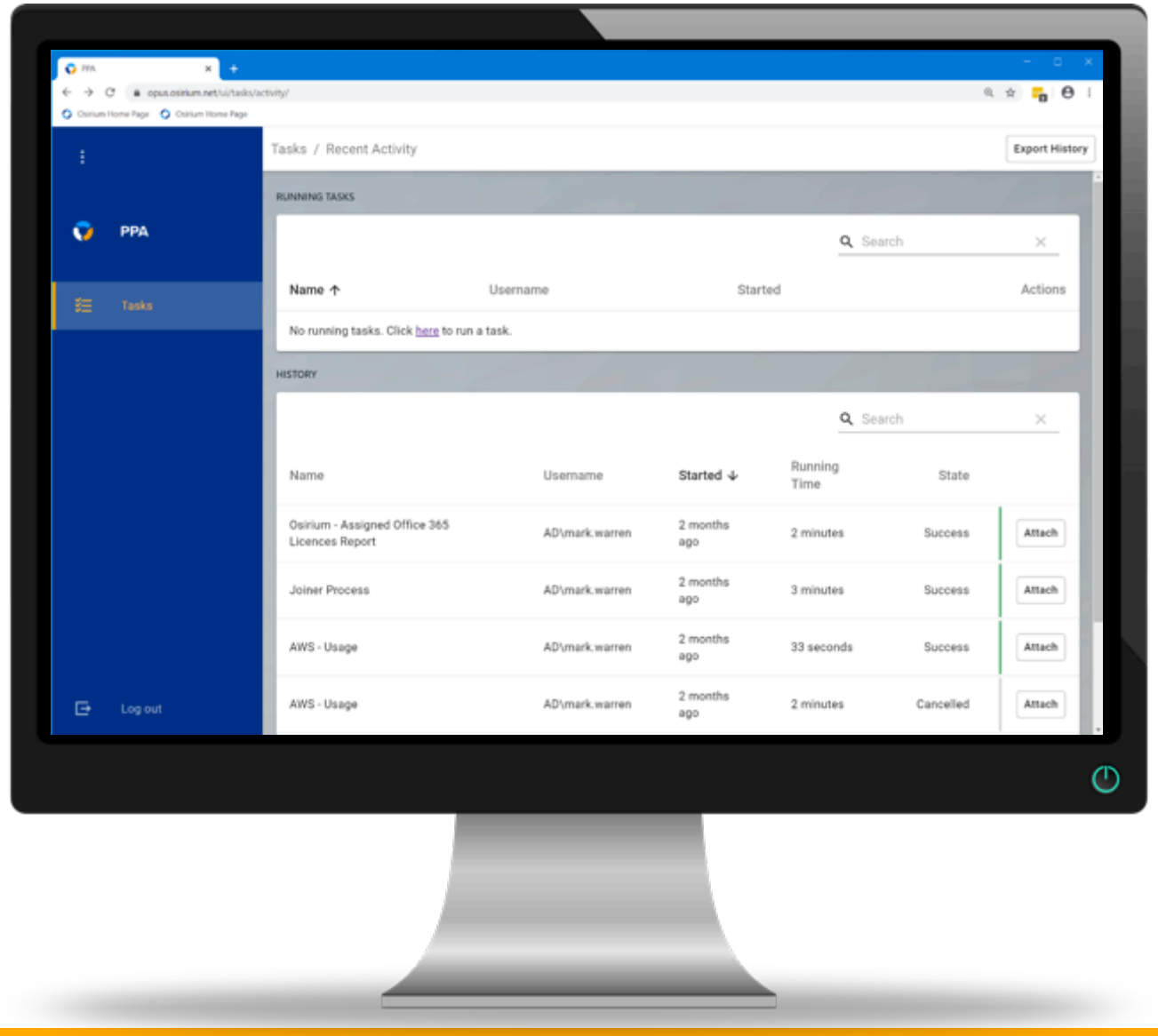
Kullanıcı geri bildirim alır ve seçim yapabilir

PPA Aksiyon Log Ekranı

Görev süreçlerinin uçtan uca geçmişi

Tam süreci izlemek için bir göreve ekleyin

Birden çok sistemde zengin denetim izi



PPA’den ÖNCE

Günlük sağlık kontrolü
30 Dakika

Senede **808** saat

PPA’den SONRA

Günlük sağlık kontrolü
10 Saniye

Osirium’un Sağladığı Otomasyon ile Kazanılan Zaman:
Senede **226 gün**

Kaynak: Osirium müşteri verisi

OSIRIUM **PEM**

Privileged EndPoint Management

Ayrıcalıklı Son Kullanıcı Yönetimi

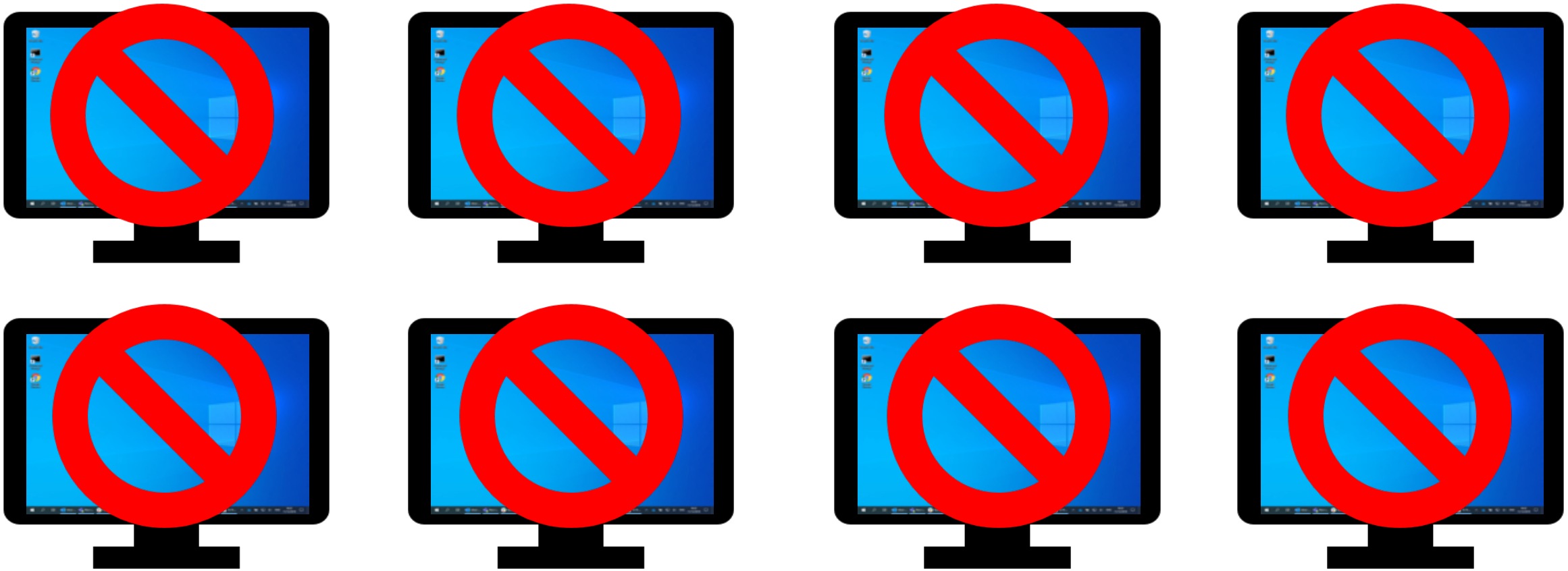
Yardım masalarının yükünü azaltın,
lokal adminleri kaldırın

TeSlakom

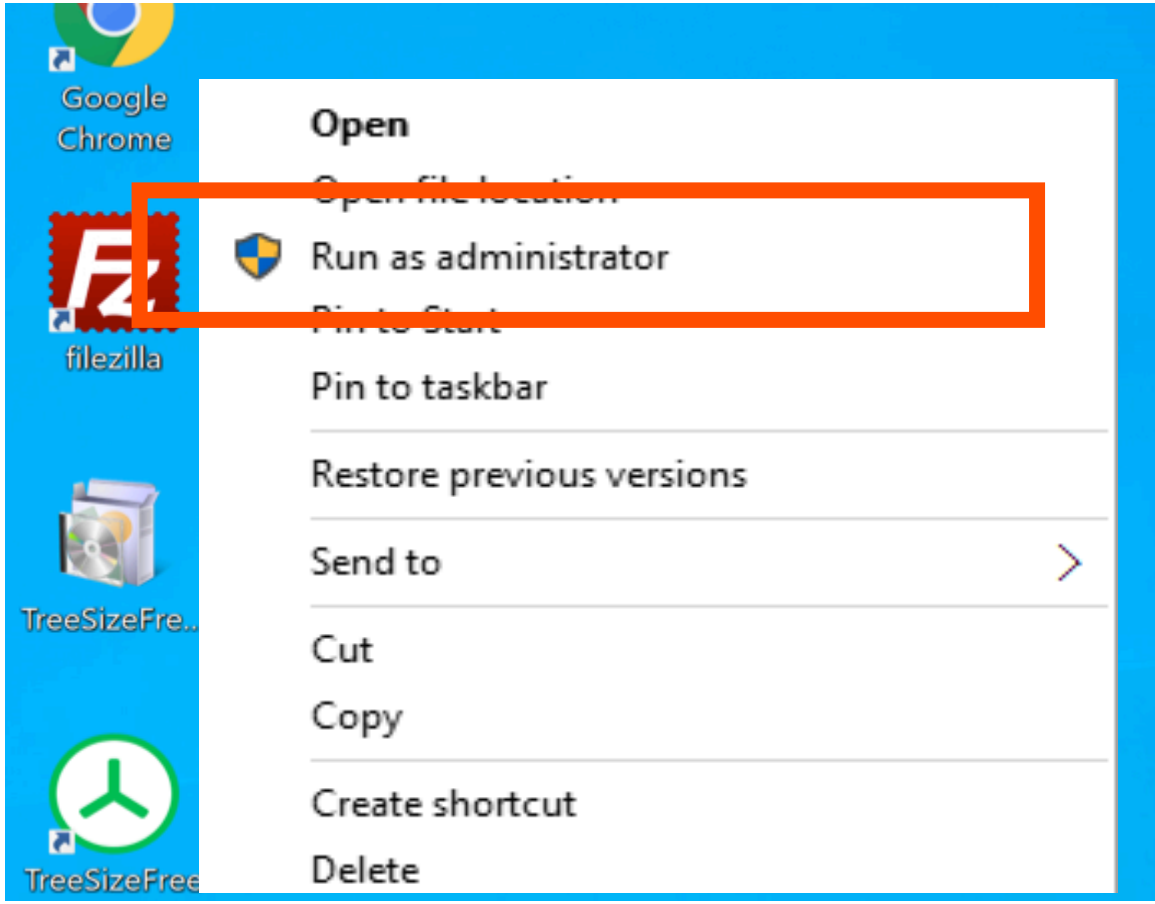
OSIRIUM

IT yöneticilerinin işletmelerini ve çalışanlarını üretken tutma sorumluluğu vardır. Ancak genellikle “**daha fazla güvenlik sağlamak**” veya “**kullanıcılar için hayatı kolaylaştırmak**” arasında seçim yapmak zorunda kalırlar..

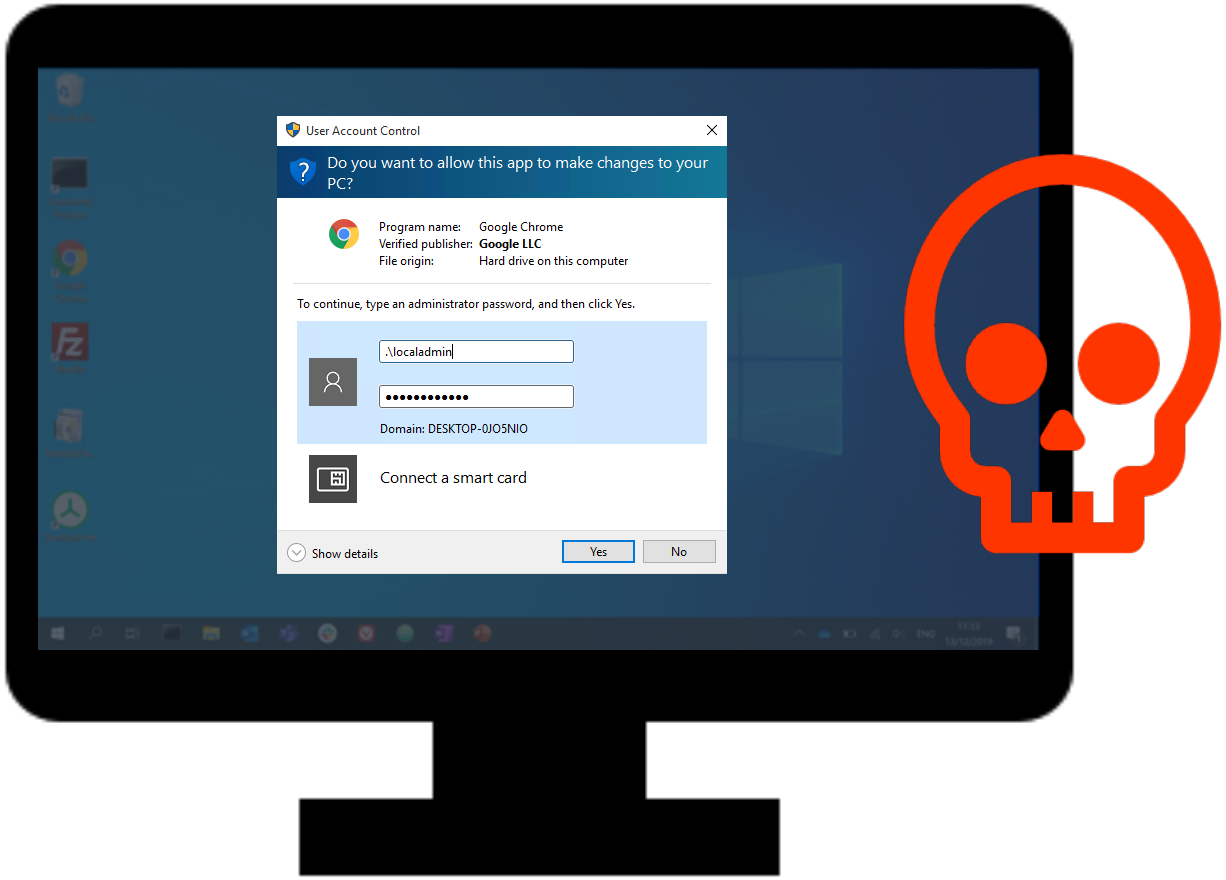
Örneğin, çoğu IT ekibi için büyük bir zorluk, kullanıcıların **güvenilmeyen uygulamaları** yüklemelerini veya çalıştırmasını engellemektir.
Bunu, kullanıcıların admin ayrıcalıklarına erişimini kısıtlayarak sağlarlar.
Bu **güvenlik için iyi**, ancak **kullanıcılar için çok kötü** bir deneyim.



İşte bir örnek: Burada kullanıcının bir uygulamayı **admin olarak çalıştırması** gerekir, bunun için sağ tıklama veya içerik menüsünü kullanırlar. Daha sonra "**Admin Olarak Çalıştır**" tıklanır.



Windows, **admin ayrıcalıklarına** sahip kimlik bilgileri gerektiren Kullanıcı Erişim Denetimi penceresini sunar. Kullanıcı bu yetkiye sahip olmadığı için **IT yardım masasına** ulaşması önerilir. Bu **çağrıları önlemek için** IT birimleri genellikle kullanıcının makinesinde **yerel bir admin** hesabı oluşturur.



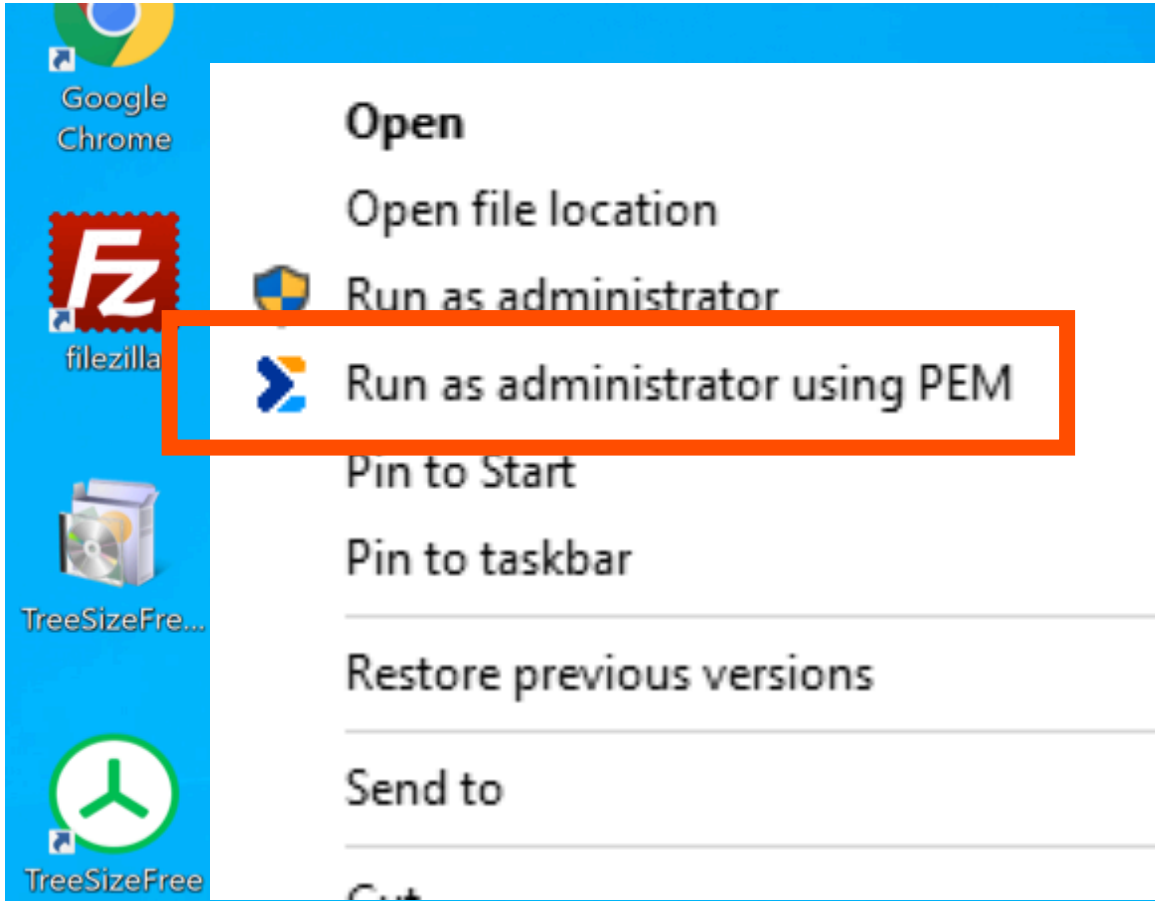
Yerel admin çözüm gibi görünse de çok önemli bir **güvenlik açığıdır**.

Artık, IT hangi uygulamaların yüklendiğini veya çalıştırıldığını **bilemeyecek**.

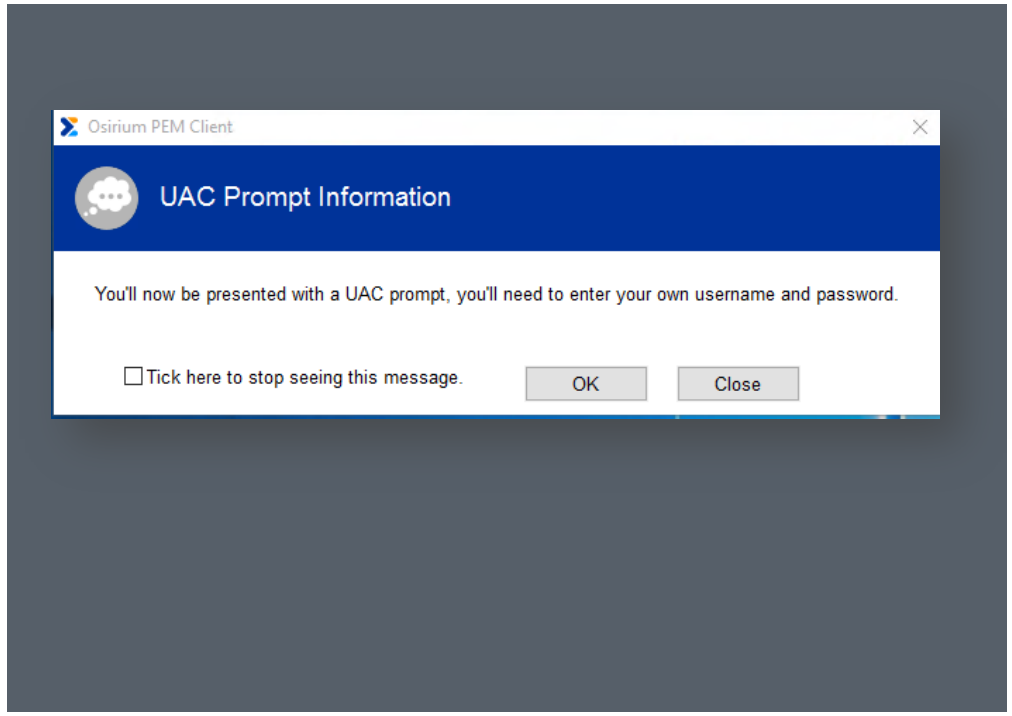
Ve bu şekilde potansiyel saldırılara maruz bırakan **kötü amaçlı yazılım** dahi yüklenebilecek...

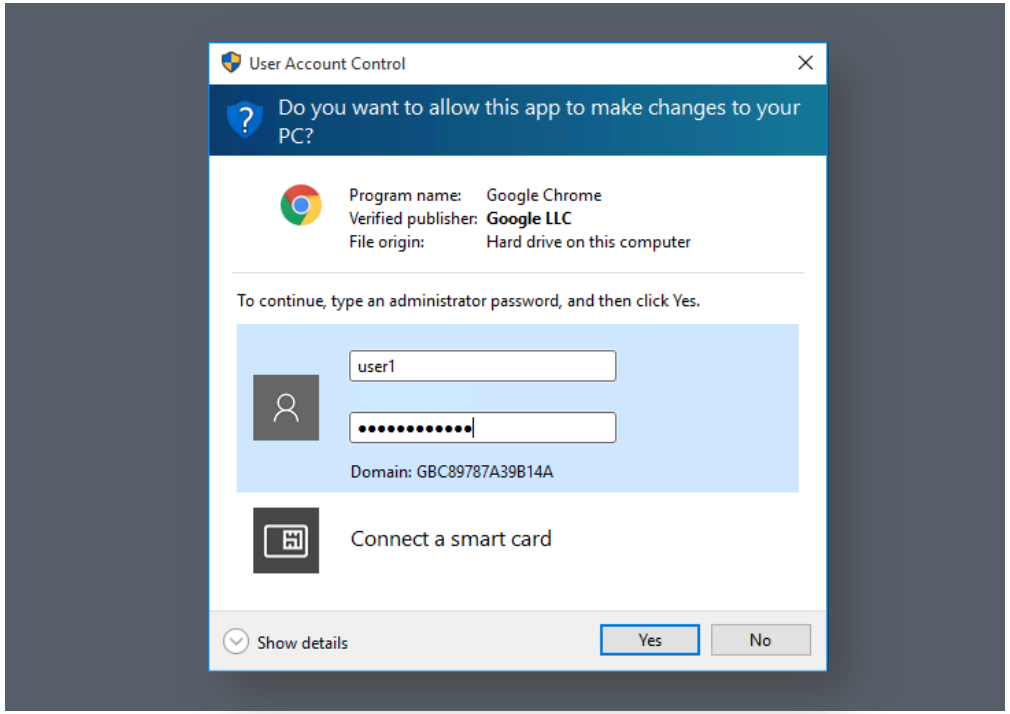
AYRICALIKLI SON KULLANICI YÖNETİMİ (**PEM**) TAM İHTİYACINIZ OLAN ÇÖZÜM

Osirium PEM kullanıcısı için işler her zamankinden daha kolay. Sağa tıkladıktan sonra **“Admin Olarak Çalıştır”** yerine **“PEM Kullanan Admin Olarak Çalıştır”** seçilecek.



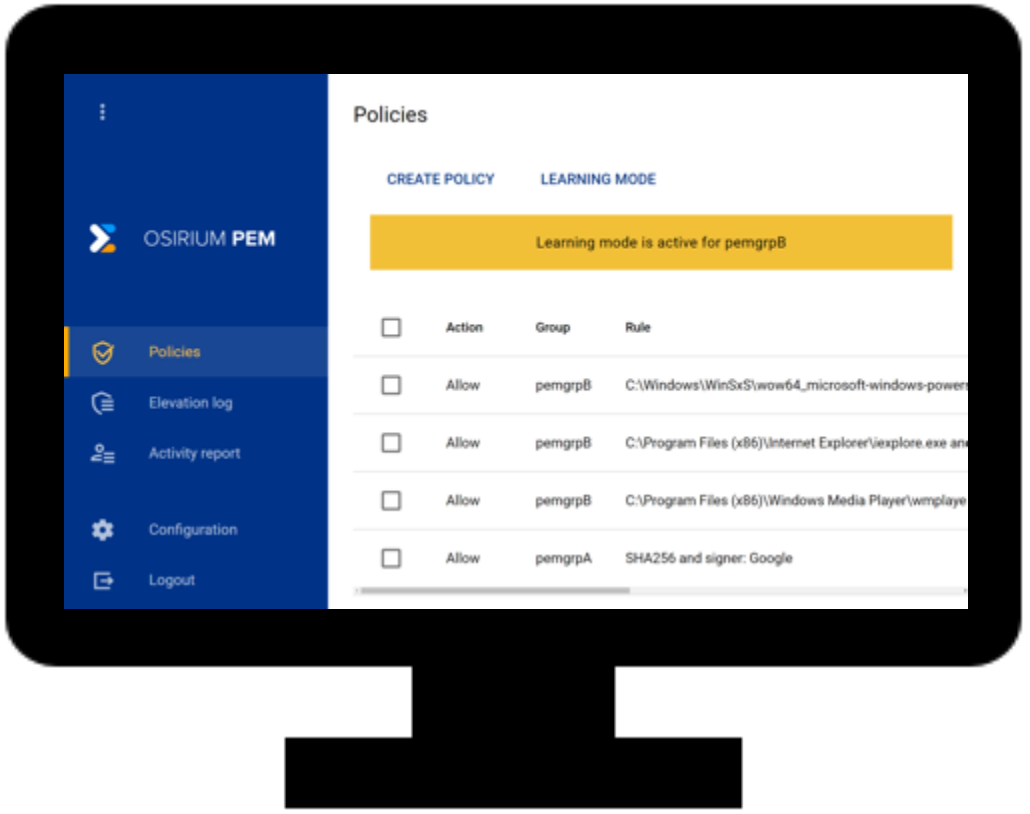
UAC istemi göründüğünde, **normal kullanıcı hesabı kimlik bilgilerini** girerler.
Bu, **onaylanan bir uygulama** ise, normal şekilde çalışmaya devam ederler.
Yeni bir uygulamaysa, IT'den politikalarına eklemesini isteyebilir ve daha sonra çalışmaya devam edebilirler; ve uygulamayı bir daha çalıştırmak istediklerinde tekrar onay istemek zorunda kalmazlar.
Böylece kullanıcıyı admin yapmak yerine **uygulamanın ayrıcalığını artırılmış** olur.





IT yöneticisi açısından durum nasıl?

PEM, kullanıcıların hangi uygulamaları kullandıklarını takip etmek için bir süre çalışır. Uygulamalar incelenir ve belirli sürümlerin kullanımına izin vermek için politikalar oluşturulur. Bu, PEM'in öğrenme modundan uygulamaya geçisinde, tüm kullanıcıların favori uygulamalarının yardım masasından bağımsız kurulduğu anlamına gelir.



OSIRIUM **PAS**

Ayrıcalıklı Erişim Güvenliği - Değerli IT varlıklarınızı koruyun, operasyonunuzu hızlandırın

Daha fazla bilgi için hemen bizimle iletişime geçin:

E-posta: iletisim@teslakom.com
Telefon: 0212 356 4646

Teslakom
Find Unique Solutions