VERİ SAYFASI

One Identity Safeguard

Ayrıcalıklı erişimi güvenli bir şekilde depolar, yönetir, kaydeder ve analiz eder

Avantajlar

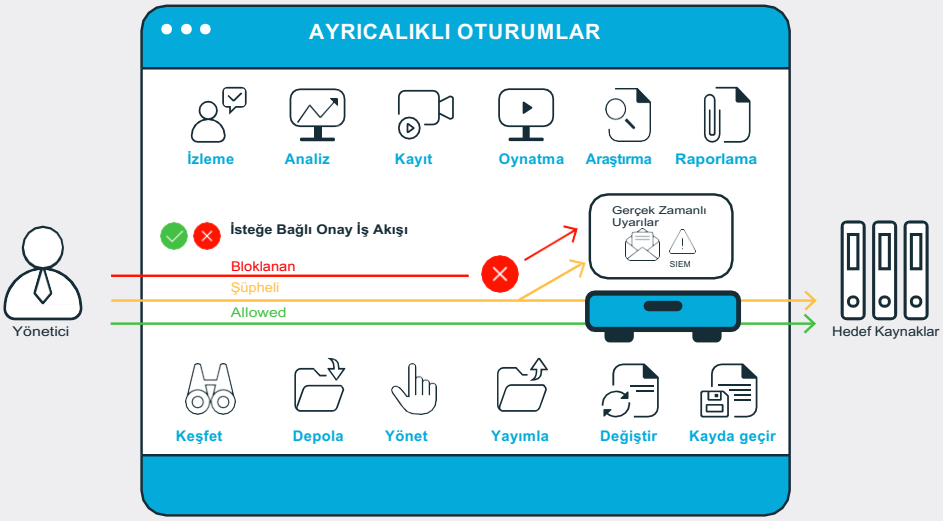
- Güvenlik ihlallerinin olası zararlarını azaltır
- Uyumluluk gereksinimlerini karşılar
- Basitleştirilmiş dağıtım ve yönetim ile hızlı yatırım getirisi sağlar
- Verimli denetim raporu oluşturur
- Yüksek riskli ayrıcalıklı kullanıcıları, riskli davranışları ve olağandışı olayları belirler
- Ayrıcalıklı hesap yönetimini basitleştirir

Giriş

Bilgisayar korsanları, sistemlere ve verilere erişmek için kullandıkları yöntemleri sürekli olarak geliştirirler. Sonuç olarak, ayrıcalıklı hesaplara ulaşmayı hedeflerler. Neredeyse her yüksek profilli ihlalde, kritik sistemlere ve verilere erişmek için ayrıcalıklı hesapların gizliliği ihlal edilmiştir. Bir ihlal nedeniyle oluşacak hasar, ayrıcalıklı hesaplara erişim için güvenli, verimli ve uyumlu bir yol sunan çözümleri kullanmak suretiyle sınırlandırılabilir.

BT yöneticileri için, bu tam erişimli hesapların yönetilmesi çeşitli nedenlerle zordur. Bunlara, ayrıcalıklı hesapların çok sayıda olması ve yine bu hesaplara erişmesi gereken kişi sayısı da dahildir. Bu zorlukların ötesinde, geleneksel ayrıcalıklı erişim yönetimi (PAM) çözümleri karmaşık mimarileri, uzun dağıtım sürelerini ve külfetli yönetim gereksinimlerini içerir.

Evet, PAM çok zor olabilir, ama bu bir zorunluluk değildir. “One Identity Safeguard” güvenli ve zorlaştırılmış bir şifreyi, oturum yönetimini ve tehditleri algılayan ve analiz eden bir izleme çözümünü birleştiren entegre bir çözümdür. Ayrıcalıklı erişimi güvenli bir şekilde depolar, yönetir, kaydeder ve analiz eder.



Ödün vermeden ayrıcalıklı erişimi güvence altına alın

“One Identity Safeguard” ile yöneticileri ve denetçileri tatmin ederken, ayrıcalıklı erişimi güvenli bir şekilde depolayarak, yöneterek, kaydederek ve analiz ederek ayrıcalıklı hesapları korumanın stresi ortadan kaldırılabilir.

Safeguard for Privileged Passwords

“One Identity Safeguard for Privileged Passwords”, rol tabanlı erişim yönetimi ve otomatikleştirilmiş iş akışları ile ayrıcalıklı kimlik bilgileri verme sürecini otomatikleştirir, denetler ve güvence altına alır. "Safeguard for Privileged Passwords" ürününün kullanıcı merkezli tasarımı, azaltılmış bir öğrenme eğrisi anlamına gelir. Ayrıca, çözüm, şifrelerin her yerden yönetilmesine ve neredeyse tüm cihazlarda kullanılmasına olanak tanır. Sonuç, kurumları güvence altına alan ve ayrıcalıklı kullanıcılara yeni bir özgürlük ve işlevsellik düzeyi sağlayan bir çözümdür.

Safeguard for Privileged Sessions

“One Identity Safeguard for Privileged Sessions” ile yönetici, uzak satıcı ve diğer yüksek riskli kullanıcıların ayrıcalıklı oturumları kontrol edilebilir, izlenebilir ve kaydedilebilir. Kaydedilen oturumların içeriği, daha sonra oturum olaylarını bulmayı kolaylaştıracak ve raporlamayı basitleştirip otomatikleştirmeye yardımcı olacak şekilde endekslenir. Her iki işlev de denetim ve uyumluluk gereksinimleri kolaylaştırır. Ek olarak, "Safeguard for Privileged Sessions" proxy olarak hizmet eder ve uygulama düzeyindeki protokol trafiğini denetler ve protokolü ihlal eden herhangi bir trafiği reddederek saldırılara karşı etkili bir koruma sağlar.

Safeguard for Privileged Analytics

“One Identity Safeguard for Privileged Analytics” ile yapılacak kullanıcı davranışı analizleri, hangi ayrıcalıklı kullanıcıların en fazla risk teşkil ettiğini bilebilir, önceden bilinmeyen iç ve dış tehditleri keşfedebilir ve şüpheli faaliyetleri bularak onları durdurabilir. “Safeguard for Privileged Analytics” tehditlerin potansiyel risk seviyesini sıralar; böylece verilecek cevap öncelik sırasına konulabilir, en yakın tehditlere karşı hemen harekete geçilebilir ve sonuç olarak veri ihlalleri önlenebilir.

Özellikler

Politika tabanlı sürüm kontrolü

Mobil cihazları destekleyen güvenli bir web tarayıcısı kullanarak, ayrıcalıklı şifreler ve oturumlar için erişim talep edilebilir ve onay verilebilir. Talepler otomatik olarak onaylanabilir veya kuruluş politikasına bağlı olarak çift / çoklu onay gerektirebilir. Dolayısıyla, politikalar istekte bulunanın kimliğini ve erişim düzeyini, istek girişiminin saatini ve gününü ve istenen belirli kaynağı (veya bunların tümünü) göz önünde bulundursa da özel ihtiyaçların karşılanması için "One Identity Safeguard" yapılandırılabilir. Ayrıca, neden kodları girilebilir ve / veya biletleme sistemleriyle entegre edilebilir.

Tam oturum denetimi, kayıt ve oynatma

Tuş darbesinden, fare hareketine ve görüntülenen pencerelere kadar tüm oturum faaliyetleri bir video gibi izlenebilen ve bir veri tabanı gibi aranabilen kurcalanmaya karşı korumalı denetim izlerinde tespit edilir, dizine eklenir ve depolanır.

Güvenlik ekipleri tarafından oturumlar arasında belirli olaylar aranabilir ve arama kriterlerinin karşılandığı yerden başlanarak kayıt oynatılabilir. Denetim izleri şifreli ve zaman damgalıdır ve adli tıp ve uyumluluk amacıyla şifreli olarak imzalanmıştır.

Değişim Kontrolü

Zamana ve son kullanıma dayalı ve manuel veya zorla yapılan değişiklik de dahil olmak üzere paylaşılan kimlik bilgilerinin yapılandırılabilir, ayrıntılı değişiklik kontrolünü destekler.

Kullanıcı davranışsal biyometrisi

Her kullanıcı, klavye ile yazı yazma ya da fareyi hareket ettirme gibi klasik eylemleri gerçekleştirirken bile kendine özgü bir davranış modeline sahiptir. "Safeguard for Privileged Analytics" içerisine yerleştirilen algoritmalar, ("Safeguard for Privileged Sessions" tarafından tespit edilen) bu davranışsal özellikleri inceler. Tuş darbesi dinamikleri ve fare hareketi analizi, ihlallerin belirlenmesine yardımcı olur ve ayrıca sürekli, biyometrik bir kimlik doğrulaması işlevi de görür.

Her yerden onay

"One Identity Starling Two-Factor Authentication" kullanılarak, VPN'de olmadan herhangi bir yerden - ve hemen hemen her cihazdan - gelen istekler onaylanabilir veya reddedilebilir.

Favoriler

En sık kullanılan şifrelere giriş ekranından hemen erişilebilir. Birden fazla şifre talebi tek bir favori olarak gruplandırılabilir, böylece tek bir tıklamayla ihtiyaç olan tüm hesaplara erişilebilir.

Keşif

Ana bilgisayar, dizin ve ağ bulma seçenekleriyle ağdaki ayrıcalıklı hesaplar veya sistemler hızla keşfedilebilir.

Gerçek zamanlı uyarı ve engelleme

“Safeguard for Privileged Sessions” trafiği gerçek zamanlı olarak izler ve komut satırında veya ekranda belirli bir şekil düzeni belirirse çeşitli eylemleri gerçekleştirir. Önceden tanımlanmış şekil düzenleri, metin odaklı bir protokolde riskli bir komut veya metin veya grafiksel bir bağlantıda şüpheli bir pencere başlığı olabilir. Şüpheli bir kullanıcı eylemi tespit edilmesi durumunda, Safeguard olayı günlüğe kaydedebilir, bir uyarı gönderebilir veya oturumu hemen sonlandırabilir.

Riskli kullanıcıların tespiti

Safeguard yüksek riskli hesapları tespit etmek için yetkilendirme haklarını risk sınıflandırma kurallarına göre değerlendirir. Yetkilendirme haklarındaki değişiklikler, bir kullanıcının profilini yüksek riskli bir duruma getirdiğinde proaktif bildirimler gönderilir. Bu, birisi onları kötüye kullanmadan veya sömürmeden önce, gereksiz ya da kullanılmayan yetkilerden kaynaklanan riski ortadan kaldırır.

Komut ve uygulama kontrolü

“Safeguard for Privileged Sessions” komut ve pencere başlıklarının hem kara hem de beyaz listesini destekler.

Anında açık

“Safeguard for Privileged Sessions” kullanıcı iş akışlarında değişiklik yapılmasını gerektirmeyen şeffaf modda kullanılabilir. Proxy ağ geçidi görevi gören Safeguard, ağda bir yönlendirici gibi çalışabilir - kullanıcıya ve sunucuya görünmez. Yöneticiler, aşina oldukları istemci uygulamalarını kullanmaya devam edebilir ve günlük rutinlerini bozmadan hedef sunuculara ve sistemlere erişebilirler.

Geniş protokol desteği

SSH, Telnet, RDP, HTTP(s), ICA ve VNC protokolleri için tam destek sunar. Ek olarak, güvenlik ekipleri, yöneticiler için protokollerdeki hangi ağ servislerini (örneğin dosya transferi, kabuk erişimi, vb.) etkinleştireceklerine / devre dışı bırakacaklarına karar verebilirler.

Tam metin araması

Optik Karakter Tanıma (OCR) motoru ile denetçiler hem komutlar hem de kullanıcı tarafından oturumların içeriğinde görülen herhangi bir metin için tam metin araması yapabilirler. Hatta dosya işlemlerini listeleyebilir ve aktarılan dosyaları incelenmek üzere genişletebilir. Oturum içeriği ve meta verileri arama yeteneği, adli tıp ve BT sorunlarının giderilmesini hızlandırır ve basitleştirir.

Parazit karakter kullanımı

Hızlı bir cihaz tabanlı kullanımı ve trafiğin basitleştirilmiş yeniden yönlendirmesiyle, "One Identity Safeguard", kullanıcıları rahatsız etmeden birkaç gün içinde oturumların kaydedilmesini sağlayabilir.

RESTful API

Safeguard, diğer uygulamalara ve sistemlere bağlanmak için REST'e dayalı modern bir API kullanır. Her işlev, ne yapılmak istendiğine veya uygulamaların hangi dilde yazıldığına bakılmaksızın hızlı ve kolay entegrasyon sağlamak için API üzerinden gösterilir.

One Identity Hybrid Subscription

Bulut tarafından sunulan özelliklere ve hizmetlere anında erişim sağlayan “One Identity Hybrid Subscription" ürünü ile Safeguard’ın yetenekleri çoğaltılabilir. Bunlara, Safeguard erişimini korumak için istenildiği kadar "Starling Two-Factor Authentication" ve "Starling Identity Analytics & Risk Intelligence for Safeguard" dahildir. Böylece riskli kullanıcılar ve yetkiler önceden etkin bir şekilde tespit edilebilir. Tek bir abonelik, tüm "One Identity" çözümü kullanımlarını mümkün kılar.

Ayrıcalıklı erişim yönetimine One Identity yaklaşımı

One Identity portföyü, endüstrinin en kapsamlı ayrıcalıklı erişim yönetimi çözümleri setini içerir. "One Identity Safeguard" ürünümüzün yapabildikleri, Unix temel hesabının ve Aktif Dizin yönetici hesabının ayrıntılı yetkilendirmesi için çözümler, açık kaynaklı Sudo’yu kuruma hazır hale getirmek için eklentiler ve Unix temel aktiviteleri için tuşa basma kayıtlarının alınması ile geliştirilebilir. Ve bunların hepsi sektörün önde gelen Aktif Dizin köprü çözümüyle sıkı bir şekilde entegre edilmiştir.

Profelis Hakkında

Profelis Bilişim ve Danışmanlık, kadrosunda bulunan sertifikalı mühendisleri ile One Identity bünyesindeki ürünlerinin desteğini ve danışmanlığını sunmaktadır. Detaylı bilgi için bizimle iletişime geçebilirsiniz.

Profelis Bilişim ve Danışmanlık Tic. ve San. A.Ş.
Vali Dr. Reşit Sokak No:6/1 Çankaya - Ankara
Telefon: +90 312 482 8021
Faks: +90 312 482 8040
bilgi@profelis.com.tr
www.profelis.com.tr