

VERİ SAYFASI

Safeguard for Privileged Sessions

Ayrıcalıklı erişimi kontrol ederek, izleyerek ve kaydederek riski azaltır

Avantajlar

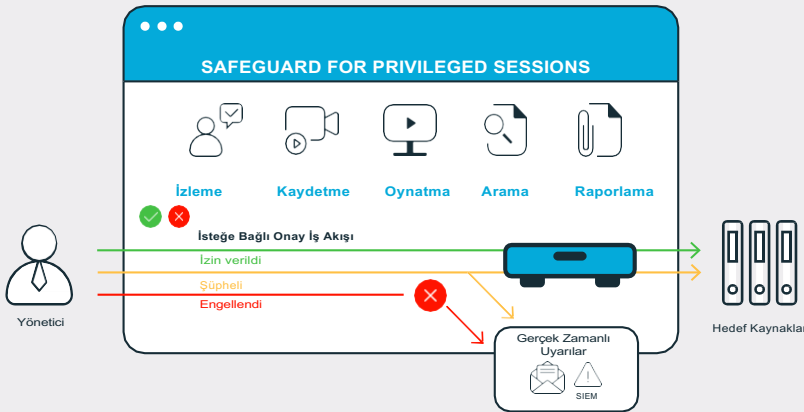
- Hassas BT varlıklarına erişimi kontrol ederek güvenlik ihlali riskini azaltır
- Ayrıcalıklı erişimi izlemek için uyumluluk gereksinimlerini kolayca yerine getirir
- Basit dağıtım ve yönetim ile ödenen paranın karşılığını daha hızlı bir şekilde alınır
- Sistemleri yönetmek için bilinen araçların kullanımını sağlayarak yöneticileri mutlu eder
- Küçük bir öğrenme eğrisi ve şık bir Kullanıcı Ara Yüzü tasarımı ile üretkenliği en üst düzeye çıkarır
- İhtiyaç duyulan tüm bilgilere hızlı erişim ile denetim raporları için harcanacak çabaları azaltır
- Ana bilgisayardan bağımsız, aracısız tasarım sayesinde her türlü sisteme erişimi izler
- Kayıtlı oturumlarda hızlı ve tüm metin araması yaparak olaylara müdahaleyi hızlandırır

Giriş

Şirket içi yöneticilere, üçüncü taraf satıcılara, yüklenicilere ve servis sağlayıcılara kontrolsüz ayrıcalıklı erişim verilmesi, önemli bir risk oluşturabilir. Bu, ayrıcalıklı hesapları ele geçiren saldırganlara ve dolandırıcı yöneticilere olanak tanır. Bu tür bir riskin talihsiz ve de maliyetli etkisi, son zamanlarda bildirilen son olaylar ile tekrar tekrar kanıtlanmıştır. Gerçek anlamda güvenlik ve uyumluluk elde etmek için, ayrıcalıklı kullanıcı hesaplarını kontrol etmekten daha fazlasının yapılması gerekir. Ayrıcalıklı erişim ile yapılanlar izlenmeli ve kaydedilmelidir.

"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 olayların aranmasını kolaylaştırmak için dinlenir ve ayrıca raporlamanın otomatik hale getirilmesine yardımcı olur, böylece denetim ve uyumluluk gereksinimleri kolayca karşılanabilir.

"Safeguard for Privileged Sessions" ayrıca, uygulama seviyesindeki protokol trafiğini inceleyen bir proxy olarak da hizmet verir. Bu, protokolü ihlal eden tüm trafiği reddederek saldırılara karşı etkili bir kalkan görevi görür. Şeffaf modda, ağ üzerinde minimum değişiklik yapılması gerekir ve kullanıcıların mevcut iş akışını veya istemci uygulamalarını değiştirmeleri gerekmez; bu da uygulamayı kolaylaştırır. Bununla birlikte, iş akışı kuralları, kullanıcının önceden yetkilendirilmesini gerektirme, belirli kaynaklara erişimi sınırlama ve bağlantıların önceden belirlenmiş zaman sınırlarını aşması halinde uyarı alma da dahil olmak üzere daha katı olacak şekilde yapılandırılabilir. Safeguard ayrıca oturumları gerçek zamanlı olarak izleyebilir ve çeşitli eylemler gerçekleştirebilir: Riskli bir komut veya uygulama ortaya çıkarsa, "One Identity Safeguard" bir uyarı gönderebilir veya oturumu hemen sonlandırabilir.



Tüm ayrıcalıklı erişimi kaydetme ve izleme

Tüm metin araması, gerçek zamanlı uyarı ve engelleme özelliği ile Safeguard, riskleri azaltırken uyumluluk gereksinimlerinin yerine getirilmesini de kolaylaştırır.

Özellikler

Tam oturum denetimi, kayıt ve oynatma

Tüm oturum aktiviteleri - her bir tuş darbesi, fare hareketi ve görüntülenen pencerelere kadar - bir video şeklinde izlenebilir ve bir veri tabanı gibi aranabilen güvenli denetim kayıtlarına yakalanır, dizinlenir ve saklanır. Güvenlik ekipleri, belirli olayları oturumlar içerisinde arayabilir ve arama kriterlerinin tanımlandığı yerden başlayarak kaydı oynatabilir. Denetim kayıtları şifreli ve zaman damgalıdır. Ayrıca adli bilişim ve uyumluluk amacıyla kriptoyla imzalanmıştır.

Gerçek zamanlı uyarı ve engelleme

Trafiği gerçek zamanlı olarak izler ve komut satırında veya ekranda belirli bir örüntü belirirse çeşitli eylemleri gerçekleştirir. Önceden tanımlanmış örüntüler, metin odaklı bir protokolle riskli bir komut, 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.

İki işlem modu

Gereksinimlere en uygun mod seçilebilir.

- **İş Akışı Motoru** – Zaman kısıtlamalarını, birden fazla onaylayanı, gözden geçirenleri, acil durum erişimini ve politikanın süresinin dolmasını destekleyen bir iş akışı motoru. Ayrıca, neden kodlarını girme ve/veya doğrudan biletleme sistemlerine entegre olma özelliğini de içerir. Bir şifre talebi otomatik olarak onaylanabilir veya herhangi bir düzeyde onay gerektirebilir.
- **Anında Açılma** - Saydam modda konuşlandırılır, böylece kullanıcı iş akışlarında değişiklik yapılması gerekmez. Ağdaki bir yönlendirici gibi çalışan bir proxy ağ geçidi işlevi görebilir. Kullanıcıya ve sunucuya görünmezdir. Yöneticiler bilinen istemci uygulamalarını kullanmaya devam edebilir ve günlük rutinlerini bozmadan hedef sunuculara ve sistemlere erişebilirler.

Proxy erişimi

Kullanıcılar kaynaklara doğrudan erişime sahip olmadığından kurum, hassas veri ve sistemlere yetkisiz ve sınırsız erişime karşı korunur. "Safeguard for Privileged Sessions" Proxy işlevi görebilir ve UNIX / Linux, Windows, ağ cihazları, güvenlik duvarları, yönlendiriciler ve daha fazlası dahil olmak üzere birçok hedef kaynağa kaydedebilir.

Komut ve uygulama kontrolü

"Safeguard for Privileged Sessions" komutların ve pencere başlıklarının hem kara listesini hem de beyaz listesini destekler.

İstenilen şekilde çalışma imkânı

İş akışı etkin olsa bile, yöneticiler ayrıcalıklı oturumlara erişirken müşterilerini, araçlarını ve tercihlerini belirleyebilirler. Bu, yöneticilere uyum ve güvenlik yönetmeliklerinin şartlarını yerine getirirken ihtiyaç duydukları erişimi sağlayan ve ihtilaf içermeyen bir çözüm yaratır.

Tüm metin arama

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

Otomatik kullanıcı girişi

Parola enjeksiyonu işlevi ile erişim, parolayı kullanıcıya asla göstermeden güvenliği ve uyumluluğu artıran otomatik oturum açma için yapılandırılabilir.

Geniş protokol desteği

SSH, Telnet, RDP, HTTP(s), ICA ve VNC protokolleri için tam destek. Ek olarak, güvenlik ekipleri, yöneticiler için protokoller içinde hangi ağ servislerini (örneğin dosya transferi, kabuk erişimi vb.) etkinleştirmek / devre dışı bırakmak istediklerine karar verebilirler.

Anında Kapanma

"One Identity Safeguard", sanal bir güvenlik duvarı gibi davranarak neredeyse anında sorgulanabilir veya kötü niyetli erişimleri sonlandırır ve sunucuların korunmasını artırır. Kazara yanlış yapılandırma ve diğer insan hatalarından kaçınmanın yanı sıra, çözüm, izleme yöneticisinin oturumu herhangi bir zamanda sonlandırabileceği four-eyes yetkilendirme ilkesini desteklemektedir.

Habersiz dağıtım

Hızlı bir araç tabanlı dağıtım ve basitleştirilmiş trafik yönlendirmesi ile "One Identity Safeguard", kullanıcıları rahatsız etmeden birkaç gün içinde oturumların kaydedilmesini sağlayabilir.

Hazır analiz

Ayrıcalıklı kullanıcıları ve davranışları analiz etmek, iç ve dış tehditleri tespit etmek için ihtiyaç duyulan tüm bilgileri toplar.

Eski sistemlere güvenli erişim

Sistemlere güvenli erişim sağlamak için akıllı kart, 2FA (iki faktörlü kimlik doğrulama) veya diğer güçlü kimlik doğrulama yöntemlerini kullanır. Safeguard sisteme bir proxy ağ geçidi işlevi gördüğünden, bu yöntemleri yerel olarak destekleyemeyen veya desteklemeyen hedeflere güçlü kimlik doğrulaması sağlar.

Ayrıcalıklı erişim yönetimine One Identity yaklaşımı

One Identity portföyü, endüstrinin en kapsamlı ayrıcalıklı erişim yönetimi çözümleri setini içerir. Ayrıcalıklı parola güvenli ve ayrıcalıklı analitik çözümlerimizle, "Safeguard for Privileged Sessions" ürünümüzün güçlü oturum yönetimi işlevi geliştirilebilir. Ürünümüz 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 alınmasını içermektedir. 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