

safetica

VERİ KAYBINI ÖNLEME

Safetica ONE Genel Bakış

eset TECHNOLOGY ALLIANCE

safetica ONE

Zahmetsiz **veri kaybı önleme** ve
iç tehditlere karşı koruma

- ✓ Kullanıcılar ve altyapı açısından **kolaylık**
- ✓ tehditlere ve veri kaybına karşı **sağlamlık**
- ✓ Yasal düzenlemelere uygunluk için **aktif destek**



Operasyonel verimliliğinizi artırırken verilerinizi güvende tutun

Safetica ONE, KOBİ'lerin ve şirketlerin ölçeklenebilirliği ve ihtiyaçları için tasarlanmış tek olgun veri güvenliği çözümüdür. Kısa sürede değer elde ederek değerli verilerinizi kontrol altına alın. İç tehditleri daha erken algılamak ve bu tehditler olaya dönüşmeden önce tepki vermek için bütünsel davranış analizi ile veri kaybını önlemenin ötesine geçin. Maliyetleri optimize etmek üzere şirket çalışma alanına, dijital varlıklara ve operasyonlara ilişkin öngörülerden yararlanın.

Kişiler ve veriler, şirketlerin ilerlemesi için gereklidir. Hassas verilerin kaybolması veya çalınması şirketin itibarını, rekabet avantajını ve kârlılığını etkiler.

Bir veri ihlalinin ortalama maliyeti **3,86 milyon ABD dolarıdır**.*

Büyük bir veri ihlalden sonra küçük şirketlerin %60'ı **6 ay içerisinde** kapanma tehlikesiyle karşı karşıya kalıyor.**

*2020 Veri İhlali Raporu, Ponemon Institute; ** National Cyber Security Alliance, Ekim 2012

Tüm kuruluşlar verilerini güvende tutabilir

Şirket içi güvenlik her zamankinden çok daha kolay. Verilerinizi korumanıza, çalışanlarınızı yönlendirmenize ve şirketinizin yasal düzenlemelerle uyumluluğunu desteklemenize yardımcı oluyoruz. Safetica ONE, şirketinizi insan hatasından veya kötü amaçlı davranışlardan koruyarak veri ihlallerini önler ve şirketinizin veri koruma yönetmeliklerine uyumluluğunu kolaylaştırır.

UZMAN VERİ GÜVENLİĞİ

Şirket içi veri riskinin tüm alanlarını kapsar ve değerli verileri insan hatasına ve kötü amaçlı etkinliklere karşı koruma sağlarız.

KISA SÜREDE DEĞER ELDE ETME

Güvenlik asla üretkenliğin önüne geçmemelidir. Safetica ONE, çalışanlar veya BT bölümü için fazladan bir zorluk oluşturmaz. Değer elde etme süresi rakip tanımaz.

SORUNSUZ ENTEGRASYON

Yalnızca sorunsuz bir şekilde entegre edilmiş bir güvenlik çözümü verimli çalışabilir. Teknoloji ortaklarımızla birlikte tüm cihazlardaki, tüm başlıca işletim sistemlerindeki ve buluttaki verileri koruyoruz.

Temel **Veri Güvenliđi** senaryoları

VERİ AKIŞI KEŞFİ VE RİSK ALGILAMA

Safetica, hassas bilgilerin nerede saklandığına veya bunlara kimin eriştiğine bakılmaksızın, kasıtlı veya kasıtsız olarak veri sızdırma girişimlerini denetler ve kaydeder. Safetica'nın risk analizi, verilerinizin nasıl sızdırılabileceğini veya çalınabileceğini tespit etmenize ve araştırmanıza yardımcı olur.

YASAL DÜZENLEMELERE UYGUNLUK

Safetica ONE GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001 veya CCPA gibi yasal düzenlemelere ve veri koruma standartlarına uyum sağlamak için bunlara ilişkin ihlalleri tespit edip önlemenize ve olayları araştırmanıza yardımcı olur.

VERİ KORUMASI VE ÇALIŞAN REHBERİ

Herhangi bir çalışan, işinizi riske atabilecek bir hata yapabilir. Safetica ONE ile şirket içi riskleri analiz edebilir, tehditleri tespit edebilir ve bunları hızla ortadan kaldıracaktır. Hassas verilerin nasıl ele alınacağına ilişkin bildirimler, veri güvenliği konusunda farkındalığı artırmaya ve çalışanları eğitmeye yardımcı olabilir.

ÇALIŞMA ALANI VE DAVRANIŞ ANALİZİ

Çalışma alanı ve kullanıcı davranışı analizi, şirket içi riskleri tespit etmek için daha ayrıntılı bilgiler sunar. Ayrıca, çalışanlarınızın nasıl çalıştığını, neler yazdığını ve hangi pahalı donanım ve yazılım lisanslarını kullandığını anlayarak maliyetlerinizi optimize edebilir ve operasyonel verimliliği artırabilirsiniz.

SAFETICA ONE ŞUNLARI KORUR

- Kişisel verileriniz
- Stratejik şirket belgeleriniz
- Müşteri veritabanlarınız
- Kredi kartı numaraları gibi ödemeyle ilgili verileriniz
- Fikri mülkiyet haklarınız - endüstriyel tasarımlar, ticari sırlar ve teknik bilgiler
- Sözleşmeleriniz



Safetica ONE
Discovery



Safetica ONE
Protection



Safetica ONE
Enterprise

Safetica UEBA

Safetica Mobile

Ürün Katmanları

Modüller

Referans Mimarisi



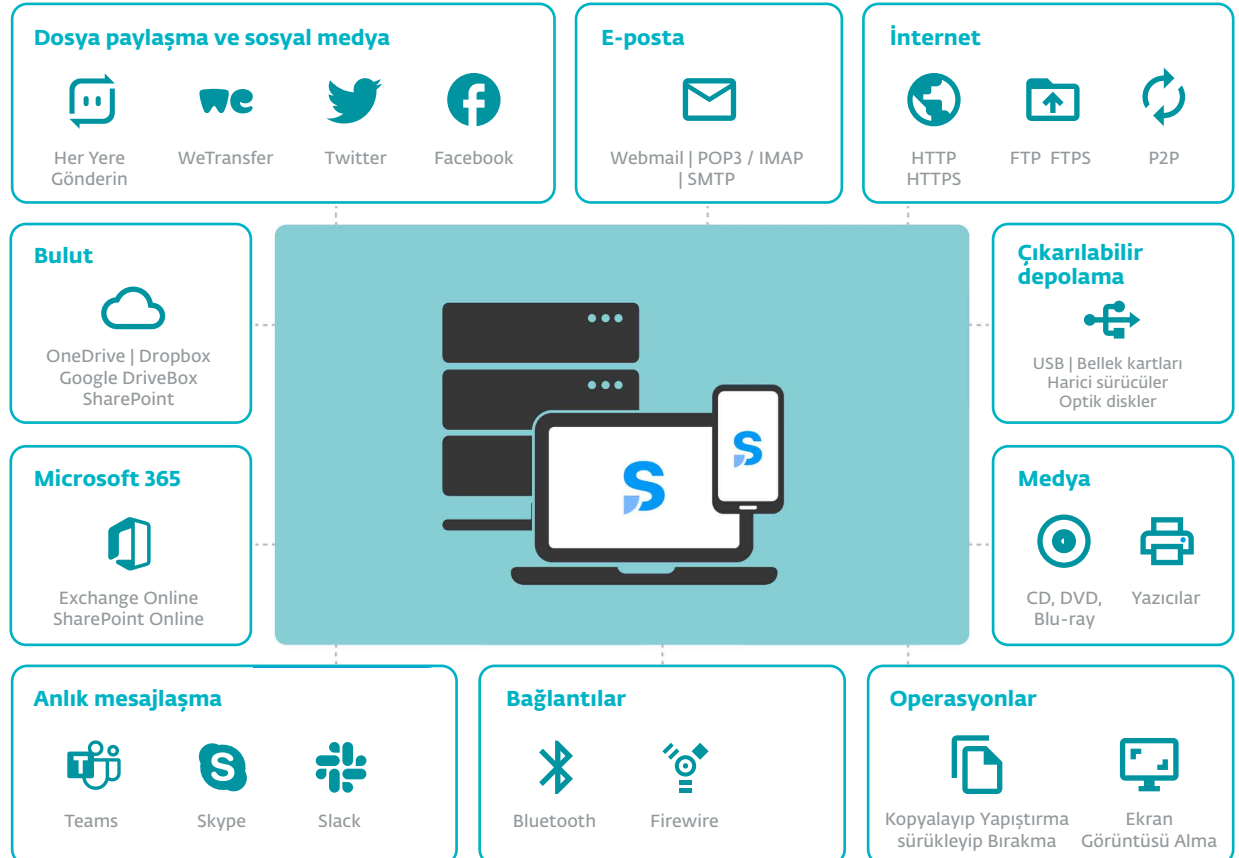
Fiziksel veya sanal sunucu, uç nokta etkinliği ve güvenlik kayıtları olan bir veritabanı çalıştırır. Safetico Yönetim Konsolu, yöneticilerin güvenlik politikalarını yönetmesini ve toplanan bilgileri görüntülemesini sağlar.

Tüm etkinlikler kaydedilir ve Safetico İstemcisi ile masaüstü bilgisayarlar, dizüstü bilgisayarlar ve diğer uzak ve hatta çevrimdışı mobil cihazlarda (yalnızca akıllı telefonlar MDM) güvenlik politikaları uygulanır.

Hassas veriler tüm kanallarda korunur.

Veri kanalları kapsam altındadır

Safetico, verilerin çok sayıda kanal ve platformda korunmasını sağlar, böylece verileriniz saklandığı veya aktarıldığı her yerde güvende olur.



Discovery'nin Temel Avantajları

Safetica ONE Discovery, kuruluşunuzdaki tüm veri akışlarını denetler ve sınıflandırır. Optik karakter tanıma (OCR) ile içerik incelemesini kullanarak hassas bilgileri ve güvenlik risklerini belirler. Gerçek zamanlı olarak çalışma alanınızda neler olduğuna dair hızlı bir genel bakış elde edin. Veri güvenliğinizi ve şirket içi verimliliğinizi artırmak için tüm şirket içi etkinlikleri, süreçleri ve veri risklerini daha iyi anlayın.



Veri güvenliği olaylarının yanı sıra **yasal düzenlemelere uygunlukla** ilgili ihlallere tepki vermek ve bu ihlallerin etkilerini ortadan kaldırmak üzere bilgi sahibi olun



Verilerinizin hangi noktada kaybolma veya çalınma riski altında olduğunu öğrenmek üzere tüm kanallardaki veya etkinliklerdeki hassas veri akışınızı **denetleyin ve sınıflandırın**



Okuması kolay risk seviyesi değerlendirmesi ve olay genel bakışı sayesinde **anında bildirimler** ve eyleme dönüştürülebilir **yönetim raporları** alın



İstenmeyen veya gereksiz yazılımları, bulut hizmetlerini veya donanımları/ çevre birimleri **keşfedin ve kaldırın**



Microsoft 365 ile tek tıkla entegrasyonun sağladığı **dağıtımı kolay** çözüm, mevcut süreçlere saygı duyar ve günler içerisinde ilk raporları sunar

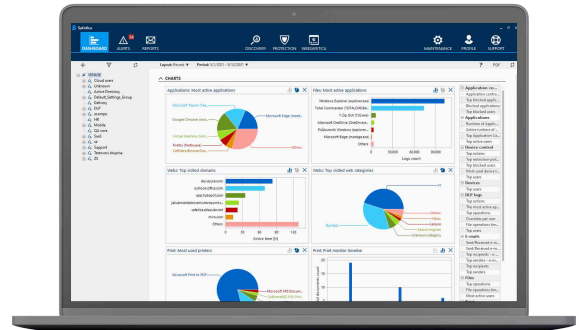


Ortaminizdeki **kullanıcı etkinliklerini analiz edin** ve şirket ekipmanlarının ve ağının **doğru kullanılıp kullanılmadığına** objektif bir şekilde karar verin

Öne çıkan özellikler

Şirket verilerinizin bulunduğu yer veya veri akışının nerede olduğu fark etmeksizin bu verilerin nasıl kullanıldığını, nerede saklandığını veya nereye gönderildiğini belirleyin.

- ✓ Windows ve macOS desteği
- ✓ Microsoft 365 ile tek tıkla entegrasyon
- ✓ Dosya içerik incelemesi ve sınıflandırması
- ✓ Tüm özelliklere sahip veri güvenlik platformuna kolaylıkla yükseltme
- ✓ Çıplak makine üzerinde veya sanallaştırılmış, şirket içinde, buluttaki VM'de çalışır



Safetica ONE Discovery için Safetica Yönetim Konsolu, kolay bir şekilde yorumlayabilmek için farklı görüşler sağlatarak kaydedilen tüm dosya operasyonlarıyla ilgili derin analizler sunar.

Protection'ın Temel Avantajları

Safetica ONE Protection, riskleri belirler, çalışanlarınızı eğitir ve verilerinizi korumak için insanların hatalarını ve kötü amaçlı davranışlarını önler. Veri analizi, veri sınıflandırması ve veri kaybı önleme (DLP) ile iç tehdit korumasının birleşimi, verimli iş operasyonlarını sürdürürken güvenli bir ortam oluşturur.



Davranış analizi ve içerik incelemesi sayesinde **hassas veri akışı** ve **şirket içi riskler** konusunda tam kontrole sahip olun



Düzenli **güvenlik raporları** and ve gerçek zamanlı olay **bildirimleri** alın



Basitleştirilmiş yüksek seviyede veri güvenliği için **Safetica Zones'u** kullanın



Daha fazla araştırma için adli kanıtları saklamak üzere sızan verilerin **Birebir Kopyasını** oluşturun

TÜM KULLANICILAR VE VERİ KANALLARI İÇİN NET POLİTİKALAR BELİRLEYİN

Belirli gruplar veya bireyler için güvenlik politikaları belirleyin. Sessiz denetimden kullanıcı bildirimlerine ve sıkı engellemeye kadar yapılandırılabilir eylemlerle istediğiniz iş akışını seçin.

OLASI TEHDİTLERİ ALGILAYIN VE İÇ RİSKLERİ ANALİZ EDİN

Kuruluşunuzdaki davranış anormalliklerinin ve veri akışı risklerinin erken keşfedilmesi sayesinde, tehditlere büyük bir olay olmadan önce tepki verin. Safetica ONE, görüntü dosyalarında ve taranmış PDF belgelerinde hassas verileri algılamak üzere gelişmiş içerik sınıflandırması ve OCR kullanır.

Öne çıkan özellikler

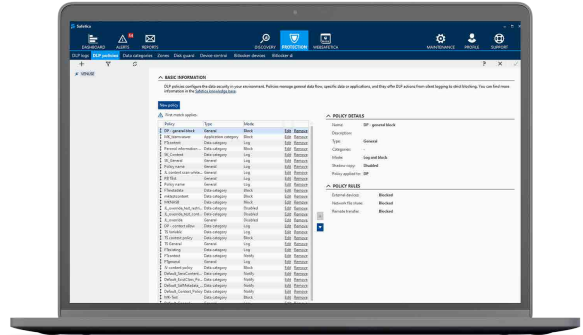
Safetica ONE Protection, içerik incelemesine, şirket içi risk analizine ve tüm veri kanalları için belirlenmiş net politikalara dayanarak, birileri bir hata yaptığında veya hassas verilerinizin riske girdiğinde bunu algılayabilir. Safetica ONE'in hangi modda çalıştığına bağlı olarak, riskli etkinliği engelleyebilir, yöneticiyi bilgilendirebilir veya çalışana kuruluşun güvenlik yönergelerini hatırlatabilir.

HASSAS VERİLERLE ÇALIŞIRKEN ÇALIŞANLARINIZI YÖNLENDİRİN

Politika ihlali riski olduğunda çalışanlara bilgi vermek veya böyle bir ihlalin olup olmadığına karar vermek için eğitim bildirimlerini görüntüleyin. En değerli verileri korumak için belirli süreçleri uygulayın.

ÇEVİRİM İÇİ VE ÇEVİRİMDIŞI TÜM CİHAZLARI KONTROL ALTINA ALIN

Taşınabilir çevre birimlerinin veya yetkisiz ortamların kullanımını kısıtlayın. Kurumsal mobil cihazları kontrol edin ve Microsoft 365'ten çıkan verileri takip edin. Safetica, ağ bağlantısından bağımsız olarak tamamen aktif kalır. Toplanan tüm kayıtlar, bağlantı yeniden kurulduğunda senkronize edilir.



Safetica Yönetim Konsolu DLP politikalarının, veri kategorilerinin veya raporların ayrıntılı ve kolay yapılandırılmasını sağlar.

Enterprise'in Temel Avantajları

Safetica ONE Enterprise, ilave iş akışı kontrolü, otomasyon ve üçüncü taraf ağ güvenliği çözümleri, SIEM'ler ve veri analizi araçlarıyla sorunsuz entegrasyon sayesinde veri kaybı önlemeyi ve iç tehditlere karşı korumayı genişletir. Kurumsal BT güvenlik yığınızı kolaylıkla oluşturun.



Otomatik **üçüncü taraf entegrasyonu** ve gelişmiş kullanım durumları için özellikler



Şirket uç noktalarında **iş akışı kontrolü** için politikalar



Birden çok etki alanı olan ortamlarda Active Directory için destek



Uç noktalarda kullanıcı güvenlik bildirimlerinin **özel markalanması**

SORUNSUZ ENTEGRASYONLAR

Güvenlik politikalarının otomasyonu ve BT yığınızıza entegrasyon sayesinde varlıklarınızı karmaşık ortamlarda bile koruyabilirsiniz.

Microsoft 365 veya **Fortinet** ağ cihazları ile yerel entegrasyon, bilinmeyen cihazlar üzerinde genişletilmiş kontrol sağlar ve uç noktadan ağa sağlam bir güvenlik çözümü oluşturur.

Denetlenen tüm olaylar ve günlükler, daha fazla araştırma için **Splunk**, **IBM QRadar**, **LogRhythm** veya **ArcSight** gibi SIEM çözümlerine otomatik olarak gönderilebilir. REST API, gelişmiş analiz için **Power BI** veya **Tableau** gibi araçlara toplanan verileri sunar.

GÜÇLÜ İŞ AKIŞI KONTROLÜ

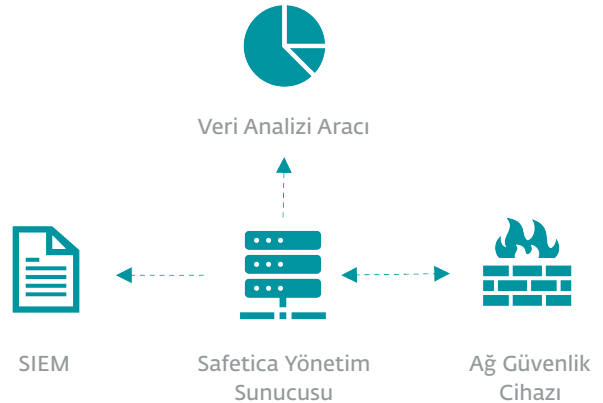
Kontrol özellikleri seti, ilgili verilerden bağımsız olarak kullanıcıların nasıl çalışmasına izin verildiğini tanımlamanıza olanak tanır.

İş akışı denetimiyle, belirli bir güvenli süreç uygulayabilir ve bir eylemi gerçekleştirmenin diğer tüm yollarını engelleyebilirsiniz.

İş akışı kontrolü, CRM veya IM gibi çeşitli uygulama türlerinin davranışını yönetmek için **uygulama DLP politikası** ve farklı ağlara, yerel yollara veya ayrıcalıklı kullanıcılar için özel erişime uygulanan özel yapılandırmalarla **DLP politika kurallarını** içerir.

Öne çıkan özellikler

- ✓ Windows ve macOS desteği
- ✓ Microsoft 365 ile tek tıkla entegrasyon
- ✓ Fortinet ağ cihazları entegrasyonu
- ✓ Power BI veya Tableau ile API entegrasyonu
- ✓ Gelen kutunuza iletilen anında bildirimler
- ✓ Önceden tanımlı şablonlarla dosya içeriği incelemesi
- ✓ Çeşitli yaklaşımlara göre içerik sınıflandırma



UEBA Module'ün Temel Avantajları

Bilgi, şirketinizin iş akışını, çalışanlarınızın çalışma alışkanlıklarını ve üretkenliğini anlamanın ilk ve en önemli adımudur. Kullanıcı etkinliklerini ayrıntılı bir şekilde görmek ve davranış anormalliklerini ortaya çıkarmak için Safetica ONE ürününüzü Kullanıcı ve Varlık Davranışı Analizi modülüyle zenginleştirin. Uzaktan çalışırken bile sorunsuz iş operasyonları sağlayın.



İstenmeyen kullanıcı etkinliklerini tespit etme

İş etkinliği denetimi ve kullanılan uygulamaların ve belirli kullanıcılar tarafından ziyaret edilen web sitelerinin otomatik olarak etiketlenmesi ve sınıflandırılmasıyla istenmeyen kullanıcı etkinliklerini tespit edin



E-posta iletişimiyle ilgili ayrıntılı bilgi edinme

Çalışanın gizliliğine ilişkin olarak gelen ve giden tüm e-postaların kayıtları ile e-posta iletişimiyle ilgili daha derin bilgiler edinin



Kullanıcı davranışındaki değişiklikleri izleme

Ağınızdaki kullanıcı davranışındaki eğilimlerin ve değişikliklerin genel görünümü ve görselleştirilmesiyle zaman içinde kullanıcı davranışındaki değişiklikleri izleyin



Kaynak kullanımını denetleme

Satın alınan donanım ve yazılım lisanslarının dağıtılıp dağıtılmadığına ve verimli bir şekilde kullanılıp kullanılmadığına dair kesin bir genel bakış elde etmek için kaynak kullanımını denetleyin



Kapsamlı raporlar ve gerçek zamanlı uyarılar alma

Uzak masaüstü vb. aracılığıyla uzaktan çalışırken bile, bireysel kullanıcı etkinlikleri hakkında kapsamlı raporlar ve gerçek zamanlı uyarılar alın



İş aramalarını denetleme

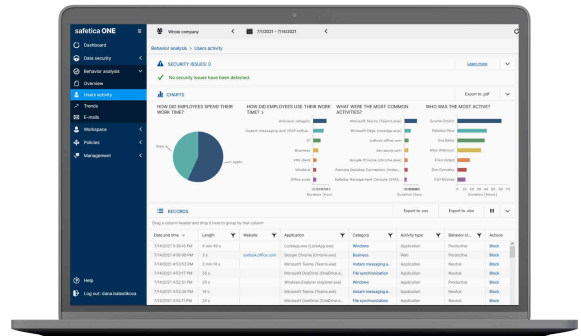
Gelecekte veri güvenliği riski oluşturabilecek belirli kullanıcılar tarafından ziyaret edilen iş portallarını belirlemek için iş aramalarını denetleyin

ANOMALİLERİN KÖK NEDENLERİNİN BELİRLENMESİ

Güvenlik veya iş verimliliğiyle ilgili endişeleri gidermek için daha derine inin ve ortamınızdaki sorunlu öğeleri kesin olarak belirleyin. Bireysel çalışanların işle ilgili etkinliklerini ayrıntılı bilgilerle objektif olarak analiz edin. Bir çalışanın tehlikeli web sitelerini ziyaret edip etmediğini veya istenmeyen uygulamaları kullanıp kullanmadığını öğrenin.

UZAKTAN ÇALIŞIRKEN BİLE ŞEFFAF ÇALIŞMA

Üst yönetimin ve bölüm liderlerinin, bireysel raporlarının nasıl işlediğini görmelerine izin verin. Çalışanlarınız evden çalışırken veya hareket halindeyken bile her şeyi kontrol edin. Verimsiz çalışanları, iş aramayı ve şüpheli davranış kalıplarını belirleyerek güvenlik risklerini önleyin ve çalışanların verimliliğini yönetin.



WebSafetica, olası tüm tehditlere ilişkin anlaşılması kolay bir genel bakış sağlar. Gösterge tablosunda önemli istatistikler alın, özel kayıt görüntüleri ve raporlar belirleyin.

Mobile Module'ün Temel Avantajları

Safetica ONE Mobile, akıllı telefonlarda ve tabletlerde veri güvenliğini artırarak, bu cihazları BT ortamınızın güvenilir bir parçası haline getiren hafif bir Mobil Cihaz Yönetimi (MDM) aracıdır. Güvenlik risklerini belirlemek ve bu risklere hızlı bir şekilde tepki verebilmek için mobil cihaz durumuna genel bir bakış sunar. Hepsine tek bir panodan ulaşabilirsiniz.



Mobil cihazlarda veri koruması

İşle ilgili uygulamaları ve verileri, korumalı bir çalışma alanına ayırın, belirli cihazlardaki zararlı uygulamaları tanımlayın, kaybolan veya çalınan cihazları uzaktan engelleyin veya silin.



Kullanıcı ve cihaz durumuna genel bakış

Uzaktan yerelleştirme ile cihaz güvenliğini ve bağlantısını izleyin, kaybolan cihazları takip edin ve bulun.



Merkezi uzaktan yönetim

Uygulama ayarlarını ve davranışlarını kontrol etmek, cihaz grupları için güvenlik politikaları belirlemek ve bunları tek bir yerden otomatik olarak yapılandırmak ve yönetmek için gelişmiş uygulama yönetimini kullanın.

TÜM MOBİL CİHAZLARI KORUYUN VE YÖNETİN

Tüm şirket cihazlarınızı kontrol edin ve tek bir bakışta güvenlik risklerini fark edin. Uzaktan Wi-Fi hesaplarında bile cihaz politikaları belirleyin. Şirket cihazlarında ayrı bir çalışma alanları oluşturmak ve bu alanları uzaktan çalışma ve özel amaçlar için kullanmak üzere Android EMM ve iOS Yönetilen Uygulamalar'dan yararlanın.

ANDROID'TE GELEN DOSYALARI DENETLEYİN

Kurumsal mobil cihazlarda da verilerinizin nerede saklandığına dair bir genel bakış edinin (Android 6-10 için mevcuttur). WebSafetica özelliğine sahip Safetica ONE Mobile kullanarak telefonunuzda, bilgisayarınızda veya Microsoft 365 bulutunda meydana gelen güvenlik olaylarını tek bir pencerede görebilirsiniz.

HIRSIZLIĞA KARŞI KORUMA

Şirket mobil cihazlarının kaybolması ve çalışanların iş değiştirmesi, hassas verilerinizi riske atabilecek yaygın sorunlardır. Safetica ONE Mobile, kurumsal mobil cihazları bulabilir ve bu cihazlara ulaşılmasını durumunda cihazları uzaktan silebilir. Altyapınızın güvenliğini sağlamanıza ve kritik verileri varlıklarınız arasında tutmanıza yardımcı olur.

Öne çıkan özellikler

- ✓ MDM ve güvenlik: güvenli çalışma alanı, cihaz politikaları, uzaktan yapılandırma ile uygulama yönetimi, güvenlik durumu
- ✓ Hırsızlığa karşı koruma: yerelleştirme, parola güçlendirme, uzaktan kilitleme, uzaktan veri silme

SİSTEM GEREKSİNİMLERİ

- Android: min. Android 6 ve üzeri ile Google Play Hizmetleri
- iOS: min. iOS 10 ve üzeri

Ayrıntılı Özellikler Liste I

Şunlarla uyumludur: Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Protection	Safetica ONE Enterprise
Güvenlik Denetimi	✓	✓	✓
Veri akışı güvenlik denetimi Harici cihazlar, web yükleme, e-posta, anında mesajlaşma, yazıcı ve bulut sürücülerini dahil tüm kanallardaki veri akışı için güvenlik denetimi.	✓	✓	✓
Office 365 dosya ve e-posta denetimi Office 365'teki dosya operasyonlarını ve giden e-posta iletişimini denetleyin.	✓	✓	✓
Yasal düzenlemelere uygunluk denetimi Tüm yerel varyasyonları dahil olmak üzere PCI-DSS, GDPR veya HIPAA gibi yaygın kullanılan çoğu yasal düzenlemelerle ilgili ihlalleri fark edin.	✓	✓	✓
Çalışma alanı güvenliği denetimi Şirket cihazlarının, uygulamalarının, ağların, ve yazıcının kullanımını denetleyin. Çalışma alanını korumak, sürekliliğini sağlamak ve maliyetleri azaltmak için kullanılan veya kötüye kullanılan kaynakları fark edin.	✓	✓	✓
İçerik inceleme Önceden tanımlanmış şablonlar veya özel kurallar ve sözlüklerle güçlü içerik incelemesi yaparak hassas dosyaları ve e-postaları sınıflandırın.	✓	✓	✓
Şüpheli etkinliklerin algılanması Şüpheli etkinliklerin gerçek zamanlı algılanması ve anında e-posta uyarıları sayesinde hızlı bir şekilde harekete geçin.	✓	✓	✓
Uç Nokta Veri Koruması	✗	✓	✓
E-posta ve ağ koruması E-posta, web yükleme, anında mesajlaşma ve ağ paylaşımları için veri koruma	✗	✓	✓
Cihazlar ve yazıcı koruması Harici cihazlara veri akışını yönetin ve hassas verileri yerel, ağ veya sanal yazıcılarda yasaklanmış yazdırmaya karşı koruyun.	✗	✓	✓
Uzaktan çalışma koruması Uzaktan uç noktadaki veya uzaktan masaüstü bağlantılarındaki veri sızıntılarından kaçının. Birçok uzaktan erişim çözümünü destekler.	✗	✓	✓
Gelişmiş veri sınıflandırma Kaynak, iş akışı bağlamı veya dosya türüne göre hassas verileri algılamak ve etiketlemek için gelişmiş teknolojileri kullanın. Üçüncü taraf sınıflandırmalarını kullanmak için meta veri algılamadan yararlanın. Kullanıcıların dosyaları sınıflandırmasına izin verin.	✗	✓	✓
Farklı ortadan kaldırma politikaları Çalışanlarınızı yönlendirmek ve eğitmek için algılanan olaylara esnek bir şekilde tepki verin. Olaylar günlüğüne kaydedilebilir, engellenebilir veya geçersiz kılma ile gerekçelendirilebilir/engellenebilir.	✗	✓	✓
Olayın Birebir Kopyası Sızan verilerin birebir kopyalarını oluşturarak olaylara ilişkin adli kanıtları saklayın. Birebir kopyalar tamamen şifrelenir ve bir ortadan kaldırma politikasıyla yerel bilgisayarlarda tutulabilir.	✗	✓	✓

Ayrıntılı Özellikler Liste II

Şunlarla uyumludur: Windows, macOS, Microsoft 365, Android, iOS	Safetlica ONE Discovery	Safetlica ONE Protection	Safetlica ONE Enterprise
Uç Nokta Veri Koruması	✗	✓	✓
Çalışma alanı kontrolü Güvenli çalışma alanınızı belirleyin ve uygulama ve web sitesi kontrolü ile çevreyi azaltın. Şirketinizdeki istenmeyen davranışlardan kaçınin ve güvenlik yönetimi maliyetini azaltın.	✗	✓	✓
Safetlica Zones Veri koruma politikalarının sayısını önemli ölçüde azaltan benzersiz Safetlica Zones ile güvenli veri çevresinin kolay yönetimi.	✗	✓	✓
BitLocker şifreleme yönetimi BitLocker şifreleme ile yerel sürücülerin ve harici cihazların merkezi yönetimi.	✗	✓	✓
Bulut Veri Koruması	✗	✓	✓
Uç nokta bulut senkronizasyonu koruması OneDrive, Google Drive, Dropbox, Box gibi uç nokta bulut sürücülerini için veri koruma.	✗	✓	✓
Uç Nokta Microsoft 365 koruması Uç noktadaki Microsoft 365 ve SharePoint için koruma. Buluttan uzak tutmak istediğiniz verileri paylaşmayı veya yüklemeyi engelleyin.	✗	✓	✓
Azure Bilgi Koruması Şifrelenmiş halde bile olsalar, Microsoft Azure Information Korumasında veri sınırlandırmalarının algılanması.	✗	✓	✓
Exchange Online Koruması Uç noktadaki ve bulut e-postalarındaki e-posta politikalarının aynı olmasını sağlayın. Uç noktalardan ve Exchange Online'dan giden verileri yönetin ve filtreleyin.	✗	✓	✓
Enterprise Özellikleri	✗	✗	✓
Bildirimlerin markalanması Son kullanıcı bildirimlerinde özel markalama (logo).	✗	✗	✓
İş akışı kontrolü Uç nokta iş akışını şirket süreçleriyle uyumlu hale getirmek için uygulama politikaları ve uzman politika ayarları.	✗	✗	✓
Birden fazla etki alanı desteği Active Directory için birden fazla etki alanı kurumsal desteği.	✗	✗	✓
Güvenlik Otomasyonu	✗	✗	✓
SIEM entegrasyonu Olayların SIEM çözümlerine (Splunk, QRadar, LogRhythm, ArcSight, vb.) otomatik olarak raporlanması.	✗	✗	✓
FortiGate entegrasyonu Uç nokta ve ağ arasında sağlam bir çözüm oluşturmak için FortiGate ağ cihazları ile otomatik güvenlik entegrasyonu.	✗	✗	✓
API raporlama Safetlica verilerini analiz ve görselleştirme hizmetlerine raporlamak için API.	✗	✗	✓

Teknolojik Özellikler ve Gereksinimler

SUNUCU

- 2,4 GHz dört çekirdekli işlemci
- 8 GB ve üzeri RAM
- 100 GB boş disk alanı
- Sanal makineleri ve bulutu destekleyen paylaşılan veya bu amaca özel sunucu
- MS SQL 2012 ve üzeri veya Azure SQL ile sunucuya bağlantı gerektirir
- MS Windows Server 2012 ve üzeri

VERİ TABANI

- MS SQL Server 2012 ve üzeri veya MS SQL Express 2016 ve üzeri veya Azure SQL.
- MS SQL Express, evrensel bir yükleyicinin bir parçasıdır ve 200'den fazla korunan uç nokta için önerilir.
- 200 GB boş disk alanı (toplanan verilerin çeşitliliğine bağlı olarak 500 GB veya daha fazlası en uygundur).
- Sanal makineleri ve bulutu destekleyen paylaşılan veya bu amaca özel sunucu. Safetica sunucusuyla birlikte kullanılabilir.

WINDOWS İSTEMCİ

- 2,4 GHz çift çekirdekli işlemci, 2 GB ve üzeri RAM
- 10 GB boş disk alanı
- MS Windows 7, 8.1, 10 (32 bit [x86] veya 64 bit [x64])
- MSI kurulum paketi
- .NET 4.7.2 ve üzeri

MACOS İSTEMCİ

- 2,4 GHz dört çekirdekli işlemci, 2 GB ve üzeri RAM
- 10 GB boş disk alanı
- macOS 10.10 ve üzeri (tam DLP özellik seti için 10.15 ve daha yüksek önerilir)

MOBİL İSTEMCİ

- Android: min. Android 6 ve üzeri ile Google Play Hizmetleri
- iOS: en az iOS 10 ve üzeri

DESTEKLENEN BULUT SAĞLAYICILAR

- Microsoft Azure, Microsoft 365

SEÇKİN SERTİFİKALAR

- ISO 9001 ve ISO/IEC 27001
- Cybersecurity Tech Accord Üyesi
- Microsoft Gold Partner
- ESET Technology Alliance Üyesi
- Fortinet Technology Alliance Üyesi

safetica

Safetica, küçük büyük tüm kuruluşa Veri Kaybını Önleme ve İç Tehdit Koruması çözümleri sunan bir Çek yazılım şirkettir. Safetica olarak herkesin verilerinin güvende olduğunu bilmeyi hak ettiğine inanıyoruz.

eset TECHNOLOGY ALLIANCE

ESET Technology Alliance, birçok tamamlayıcı BT güvenlik çözümüyle şirketleri daha iyi korumayı amaçlıyor. Kanıtlanmış ve güvenilir teknolojimizi, türünün en iyisi diğer ürünlerle birleştirerek, sürekli değişen güvenlik ortamında korunmaya devam etmeleri amacıyla müşterilerimize daha iyi bir seçenek olarak sunuyoruz.

