

**Proofpoint ile, İçeriden Tehdit Yönetimi**

**Modern İşletmeler için, İnsan Merkezli İçeriden Tehdit Yönetimi**

## **TEMEL AVANTAJLAR**

* Riskli şirket içi eylemleri tespit edin ve uç noktadaki veri kaybını önleyin!
* İçerden tehdit ve veri kaybı vakalarının müdahale süreçlerini basitleştirin!
* Modern bulut- yerel bağlantı tarafından desteklenen yüksek düzeyde ölçeklenebilir SaaS dağıtımı süresini hızlandırın!
* Uç nokta aracısıyla kullanıcılarınızın verimliliğini artırın!

**ANAHTAR ITM KULLANIMI**

* Kullanıcı riskini belirleme
* Uç noktadan veri kaybına karşı koruma
* Kullanıcı kaynaklı olaylara müdahaleyi hızlandırma
* İçeriden tehdit programlarını geliştirme

Proofpoint İçeriden Tehdit Yönetimi (ITM),firmaların çalışanlarının sebep olduğu veri kaybına, kötü niyetli eylemlere ve marka değer kaybına karşı korumak için, insan merkezli bir yaklaşım benimsemektedir. Proofpoint olarak, bu çözümle sizi kötü niyetle, veya bilmeden hareket eden yetkili kullanıcılara karşı koruyoruz. Ve firmanızı içeriden gelen veri ihlallerinden korumak için kullanıcı eylemleri ile veri hareketini ilişkilendiriyoruz. Ayrıca, yanlış davranışlara dair size kolay anlaşılır kanıtlar sunmak için, riskli davranışları da gerçek zamanlı olarak tespit ediyoruz.

## **Çalışanlarınızın Riskli Davranışlarını Gerçek Zamanlı Olarak Algılayın ve Önleyin!**

ITM ile uygulamalar, dosyalar, masaüstleri, sunucular ve sanallaştırılmış ortamlar üzerindeki riskli davranışları meydana gelirken ilişkilendirebilirsiniz. Bu, sadece olay gerçekleştikten sonra değil, kullanıcı olayı gerçekleştirirken olur. Gerçek zamanlı görünürlüğümüz, içeriden gelen tehdit vakalarını ilişkilendirmeniz, tespit etmeniz ve çözmeniz için size güçlü yeni yöntemler sunar.

### **Gerçek Tehdit Senaryoları**

Riskli davranışları gerçek zamanlı olarak tespit edebilirsiniz. Bunlara aşağıdakiler dahildir:

* Veri hırsızlığı
* Riskli veri hareketi
* Yetkinin / uygulamanın kötüye kullanılması
* Yetkisiz Erişim
* Bilmeden gerçekleştirilen riskli eylemler

ProofPoint’in Boolean mantık tabanlı kural oluşturucusu ile, ortamınıza göre uyarlanmış kural ve tetikleyicileri kolaylıkla belirleyebilirsiniz. Kullanıma hazır tehdit senaryolarıyla başlayabilir ve mevcut olanları değiştirebilirsiniz. Ya da sıfırdan senaryo yaratabilirsiniz. Çok çeşitli içeriden tehdit kurallarımız, Carnegie Mellon’un CERT Bölümü, NITTF, NIST ve müşterilerimizin ortak bilgi birikimine dayanmaktadır.

### **İşaretle ve Tıkla Arayüzü**

Tehdit avı sadece dış tehditlerden ibaret değildir. ITM ile, şirketinizde bilerek yada bilmeyerek riskler alan kişileri kolayca tespit edebilirsiniz. ‘İşaretle ve tıkla’ arayüzümüz, anormal davranışları proaktif olarak tespit etmenize yardımcı olur.

‘İşaretle ve tıkla’ tehdit avıyla şunları yapabilirsiniz:

* Çevrenize göre uyarlanmış riskli davranışları ve etkinlikleri gözden geçirme
* İlişkili olmayan binlerce eylemi filtrelemek ve ilişkili olanlara odaklanmak için, gruplamaları kullanma
* Zaman çizelgesi ve ekran görüntüsüne dayalı kanıtlar aracılığıyla anormal davranışları belirli bir sisteme oturtma

### **Veri Sınıflandırma Desteği**

Bu çözüm, Microsoft Bilgi Koruması (MIP) ile entegre çalışır. ITM aracımız, kullanıcı dosyayla etkileşim kurarken duyarlılık etiketlerini gerçek zamanlı olarak okur. Dosya MIP duyarlılık etiketi, dosya kaynağı, dosya türü ve dosya hedefine göre algılama ve önleme kurallarını belirleyebilirsiniz.

### **Veri Kaybını Önleme**

ITM, ortak uç nokta kanallarından hassas veri hırsızlığını önleyebilir. Buna yerel senkronizasyon klasörleri, ağa bağlı depolama, flaş bellekler, multimedya cihazları ve telefonlar gibi USB bağlantılı cihazlar da dahildir. Hatta bu yapı, kullanıcı çevrimdışıyken bile çalışır.

USB tabanlı eylemleri kullanıcıya, gruplara ve ana bilgisayarlara göre aşağıdaki şekilde yönetebilirsiniz:

* USB’ye veri yazmayı engelleme
* Bazı USB cihazlarını güvenli listeye alma
* Dosya adı modelleriyle eşleşen dosyaları engelleme
* Dosya türlerini/ kaynaklarını engelleme

Proofpoint Kurumsal DLP paketi, korumayı e-posta ve bulut uygulamalarını da içerecek şekilde genişletebilir.

### **Olay Müdahaleyi Hızlandırma**

Birçok firma, içeriden tehditle ilgili aksiyonları, bir güvenlik sorunu yaşadıktan sonra alır. Ve çoğu, mevcut güvenlik araçlarının genel iş akışlarının içeriden tehditler açısından işe yaramadığını fark eder. Şirket içi bilgiler hassastır ve siber güvenlik dışı ekiplerle daha yüksek seviyede işbirliği yapmayı gerektirir.

###  **İç süreçlerde Yardımcı Çözüm**

Firmaların iş akışları, kullanıcı odaklı eylemler için özel olarak hazırlanmıştır. Proofpoint ITM ile, toplanan tüm meta veriler ve ekran görüntüleri genelinde anahtar sözcükler ve filtrelerle güvenlik olayları arasında arama yapabilirsiniz. Diğer bir deyişle, tamamen yeni bir sorgulama dilini öğrenmenize gerek yoktur. Filtreleri proaktif tehdit avı için veya herhangi bir araştırmada ileride başvurmak üzere kaydedebilirsiniz.

### Araştırmalarla ilgili kritik vakaları ve uyarıları belirledikçe, bunları etiketleyebilir ve kategorilere ayırabilirsiniz. Kanıt paylaşmanız gerektiğinde, ilgili vakaları ve uyarıları bu etiketler aracılığıyla bulabilirsiniz. Ve bunları PDF gibi yaygın dosya formatlarında dışa aktarabilirsiniz. Bu raporlar ekran görüntüsü kanıtlarını ve kim, ne, nerede ve ne zaman sorularına yanıt veren ilgili bağlamı içerir. Bunun siber güvenlik açısından yönetilmesi çok daha kolaydır ve İK, hukuk, uyum ekipleri ve araştırmacılar tarafından anlaşılması da daha kolaydır.

## **ITM Mimarisinin Avantajları**

Bulut tabanlı mimarimiz ölçek, kullanım kolaylığı, güvenlik ve genişleme yeteneği için oluşturulmuştur. Eylem verilerini toplamak için sektör lideri olan hafif uç nokta aracılarımızdan faydalanır. Kullanıcının işini engellemeden sisteminde ne yaptığına dair güçlü ve uygulamadan bağımsız bir görünürlük elde edersiniz.

### **Modern SaaS Platformu**

Proofpoint Uç Nokta DLP; analiz, güvenlik, gizlilik ve genişleme özelliği ile, oluşturulmuş modern bir SaaS platformudur. Bu, uçta kurulum süresini ve maliyeti azaltırken, güvenlik yöneticileri için süreci basit hale getirir.

### **İki Sorun, Tek Çözüm**

Uç Nokta DLP ve İçeriden Tehdit Yönetimi, tek, yaygın ve hafif bir araç ve modern bir SaaS mimarisi kullanır. Birlikte kullanıldıklarında, Uç Nokta DLP, günlük kullanıcılarda veri kaybı risklerine karşı koruma sağlar. Ve ITM de bu korumayı kötü niyetli ve yüksek riskli kullanıcıların tüm riskli davranışlarını kapsayacak şekilde genişletir.