Forcepoint

Hassas Verilerin Bir Günü

Bir çalışan. Sıradan bir sabah. Katlanarak büyüyen veri riski. Nasıl gerçekleştiği ve nasıl durdurulacağı şu şekilde gerçekleşiyor.

Risk Zaten Burada

53%

İÇERİDEN KAYNAKLANAN OLAYLAR KAZAYLA YA DA İHMAL SONUCU GERÇEKLEŞMEKTEDİR

DTEX 2026 İç Tehdit Riskleri Maliyeti

13%

OLAYLAR 30 GÜNDEN KISA SÜREDE KONTROL ALTINA ALINMAKTADIR

DTEX 2026 İç Tehdit Riskleri Maliyetis

200+ Gün

İÇERİDEN KAYNAKLANAN OLAYLARIN (KÖTÜ AMAÇLI VE KAZAYLA) ÇÖZÜLMESİ İÇİN ORTALAMA SÜRE

IBM 2025 Veri İhlali Maliyeti Raporu

$19,5 Mn

İÇERİDEN KAYNAKLANAN OLAYLARIN TOPLAM ORTALAMA YILLIK MALİYETİ

DTEX 2026 İç Tehdit Riskleri Maliyeti

Alice ile Tanışın

Alice, çok önemli bir iş ortağı toplantısına hazırlanan bir satış temsilcisidir. İşini yapıyor. Bir güvenlik olayına neden olmaya çalışmıyor. **Toplantıya hazırlanırken hassas verilere ne olduğunu izleyin.**

Salesforce → Excel

Alice, Salesforce'ta en önemli stratejik hesaplarına ilişkin bir rapor çalıştırır ve bunu bir Excel dosyası olarak indirir. Veriler hesap adlarını, kişi bilgilerini ve gelir rakamlarını içerir.

Düzenlemeye tabi KBB, fikri mülkiyet ve stratejik hesap verileri kontrollü bir CRM ortamından çıkıyor.

Excel → Bulut

Dosyayı ekibiyle paylaşmak için bir işbirliği platformuna yükler. SharePoint. Box. OneDrive. Hangisi olduğu fark etmez.

Kritik veriler artık birden fazla konumda mevcut ve izni olan herkes tarafından erişilebilir durumda.

Excel → Kamuya Açık Yapay Zeka

Alice, trendleri özetlemek ve konuşma noktaları oluşturmak için kamuya açık bir yapay zeka aracı kullanır. Excel dosyasını doğrudan komuta yükler.

Kritik veriler, riskli bir komut ile Gölge Yapay Zeka'ya yüklendi.

Yapay Zeka Çıktısı → Slack

Yapay zeka tarafından oluşturulan özeti, ekibiyle Slack üzerinden paylaşır. Kritik veri unsurları içeren yeni içerik bir işbirliği kanalına yayılır.

New content that includes elements of critical data spreads to a collaboration channel.

Slack → Harici E-posta

Alice, özeti kuruluş dışındaki bir iş ortağına e-postayla gönderir.

Kritik veriler, erişim veya denetim kontrolü olmaksızın en riskli kanal üzerinden dışa aktarılır.

Az önce ne oldu?

KBB. Fikri mülkiyet. Stratejik bilgiler. Tek bir günde bunların tümü işbirliği platformlarına, bulut depolama alanlarına, yapay zeka araçlarına ve dış güven sınırlarına yayıldı. Alice bir sorun yaratmak istemiyordu. Sadece daha akıllı ve hızlı çalışmaya çalışıyordu. İçeriden kaynaklanan riski yönetmek bu yüzden bu kadar zor: çoğunun arkasında kötü bir niyet yok. Bunun sebebi tamamen insani.

Yeni Bir Yaklaşım: Veriyi Takip Eden Güvenlik

Hassas verilerin korunması, gerçek zamanlı olarak uyum sağlayan sürekli bir yaklaşım gerektirir. Bir kontrol listesi değil. Statik politikalar bütünü değil. Bir döngü. **Forcepoint bu yaklaşımı Data Security Everywhere olarak adlandırmaktadır.**

Keşfet
Hassas verilerin nerede bulunduğundan bağımsız olarak görünürlük sağlayın

Sınıflandır
Verinin türünü, iş kullanımını ve hassasiyet düzeyini belirleyin

Önceliklendir
Riskin en yüksek olduğu alanlara odaklanın

Hassas verileri korumak bir kontrol listesi değildir. **Sürekli bir döngüdür. cycle.**

Koru
Riski azaltmak için politikaları tüm kanallarda tutarlı biçimde uygulayınız

İyileştir
Güvenlik açıklarını ihlale dönüşmeden önce giderin

Forcepoint Data Security Cloud

Beş adımın tamamı tek bir birleşik platformda buluşur: Forcepoint Data Security Cloud. Tek platform. Tek politika seti. Verilerin yaşadığı, hareket ettiği ve kullanıldığı her ortamda tam görünürlük.

Daha Fazla Bilgi

Forcepoint