IBM Connected 2013

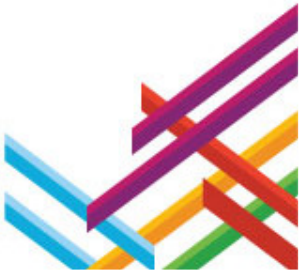
Her Deneyim Bir Kazanım

#connected

Kursad YILDIRIM
10 Ekim 2013

UÇ NOKTALARDA GÜVENLİK ÇÖZÜMLERİ

IBM Endpoint Manager



Çözüm Yapısı

IBM Endpoint Manager

Yaşam Döngüsü Yönetimi

- Yama Yönetimi
- Donanım ve Yazılım Envateri
- Yazılım Dağıtımı
- İşletim Sistemi Kurulumu
- Uzak Bağlantı

Yazılım Envanter Yönetimi

Güç Yönetimi

Mobil Cihaz Yönetimi

Yama Yönetimi

- Yama Yönetimi
- Güvenlik Konfigurasyon Yönetimi
- Zaafiyet Analizi
- Uyumluluk Analizş
- Diğer firmalara ait ürünlerin yönetimi

Güvenlik ve Uyumluluk

UçNokta Korunması

- Zararlı Yazılım
- Güvenlik Duvarı
- DLP

Uç Noktalarda Yönetim Zorlukları

Sistem ve uygulama zaafiyetlerinin en fazla saatler mertebesinde kapatılması

Hızlı, iteratif ve olabildiğince otomatik aksiyonlar

Mobil ve hareketli cihazlar

Yeni ortam ve platformlar

Şahsi cihazlar ve kurum verileri

Uyumluluğun sürekli sağlanması ve gerçek zamanlı takip edilmesi

IEM: Güvenlik ve Uyumluluk

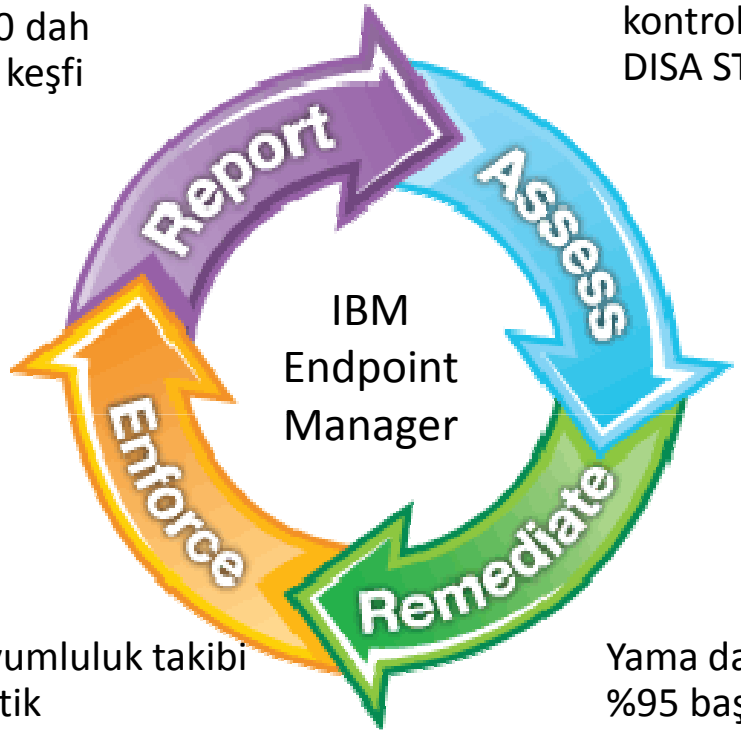
- Varlıkların keşfi
- Uyumluluk Analizi
- Yama Yönetimi
- Güvenlik Konfigurasyonu
- Zaafiyet Analizi
- Diğer firmaların ürünlerinin yönetilmesi

Available Separately:

- Entegre AntiVirus
- DLP

Bilinen varlık verisinin %10 - %30 dah fazlasının keşfi

5000'den fazla uyumluluk kontrol kuralı: FDCC SCAP, DISA STIG



Sürekli uyumluluk takibi ve otomatik konfigurasyon

Yama dağıtımında ilk fazda %95 başarı oranı

Common Criteria Certified EAL3

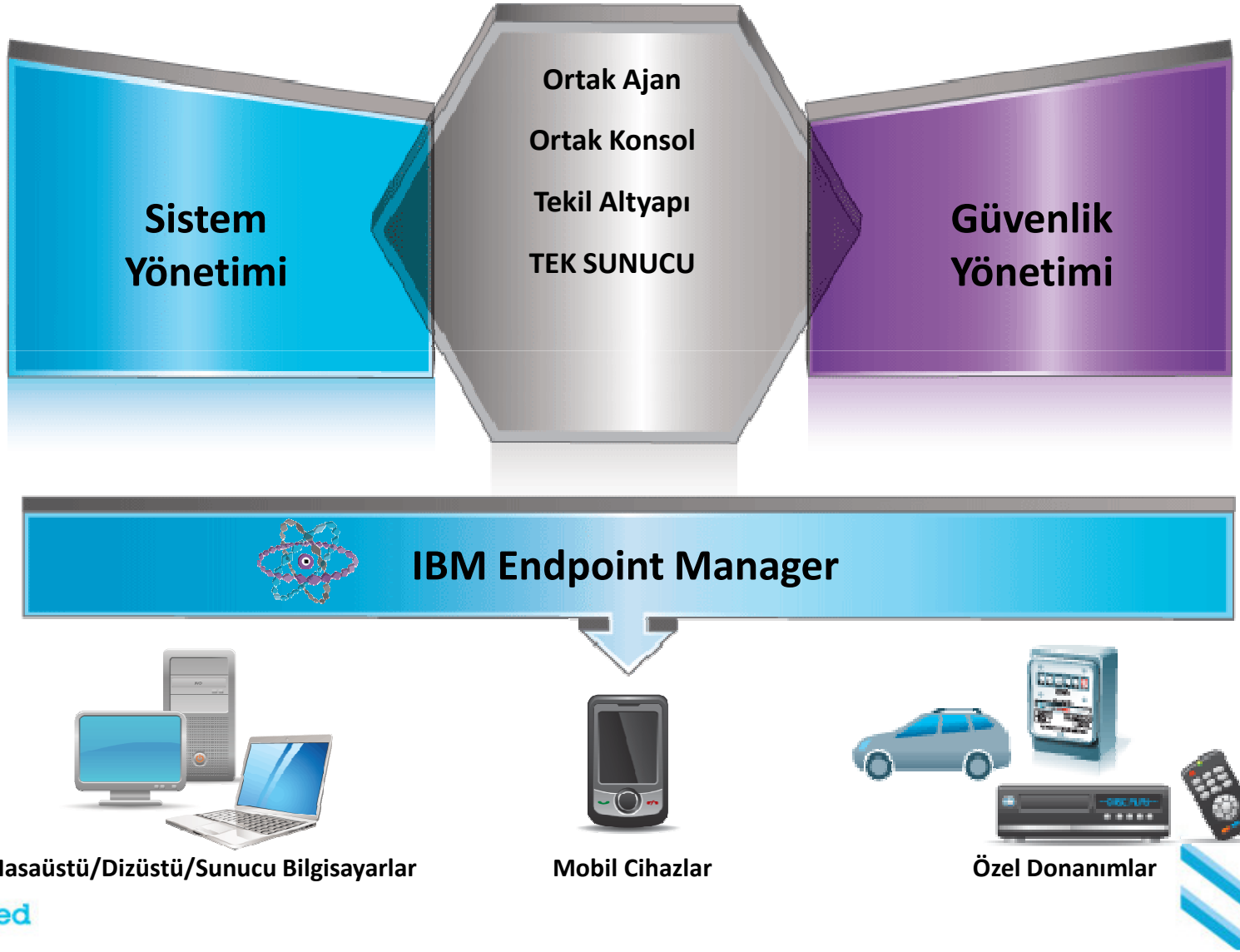
oval.mitre.org

cve.mitre.org

FIPS VALIDATED 140-2
FIPS 140-2 Inside

Operasyon ve Güvenlik

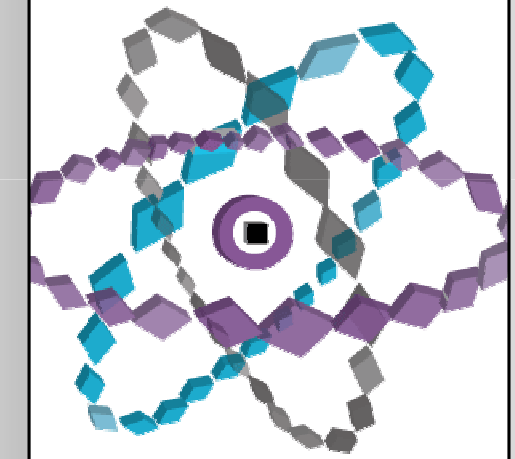
Düzgün Yönetim = Güvenli Sistem



Operasyon ve Güvenlik

Operasyonel Bileşenler

- Yaşam Döngüsü Yönetimi
- Mobil Cihaz Yönetimi
- Yama Yönetimi
- Güç Yönetimi
- Yazılım Varlıklarının Yönetimi

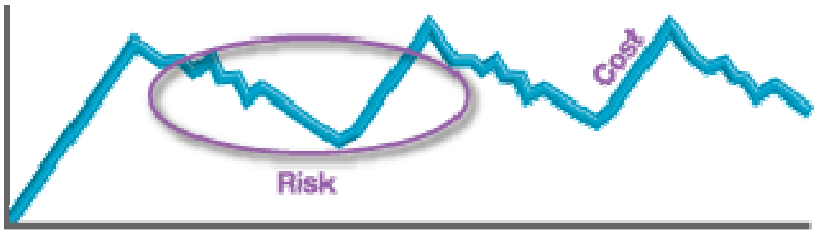


Güvenlik Bileşenleri

- Güvenlik ve Uyumluluk
- Uç Nokta Koruma
- Mobil Cihaz Yönetimi
- Yama Yönetimi

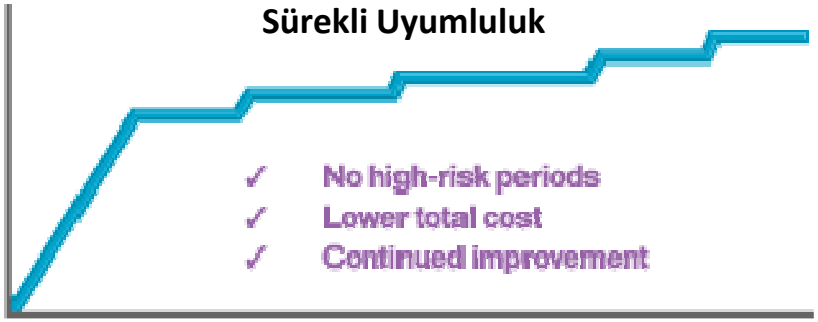
Uyumluluk Takibi ve Yönetimi

Geleneksel Yöntem



1. Güvenlik ekibi politikaları geliştirir.
2. Güvenlik ekibi araç(lar) ile uç noktalarda politikaları kontrol eder
3. Güvenlik ekibi bulguları operasyona iletir
4. Operasyon ekibi bulguları düzetlmeye başlar. Güvenlik ile aynı ürün kullanılmadığından bulgular teker teker ele alınır.
5. Zaman içerisinde sistemlerin uyumluluk düzeyi aşağı iner. Eksik yamalar, yeni regulasyonlar, kullanıcı hareketleri
6. Bütün süreç en başından tekrar yaşanır.

Sürekli Uyumluluk

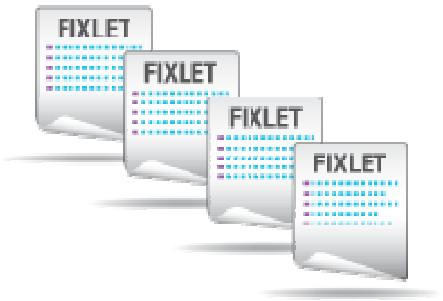


1. Güvenlik ve operasyon ekipleri birlikte politikaları ve düzeltici aksiyonları geliştirir.
2. Operason ekibi ortaya çıkan politikayı bütün uç noktalarda uygular.
3. Uyumluluk sürekli izlenir ve gerektiğinde uç noktada otomatik uygulanır. Bütün değişiklikler ve aksiyonlar gerçek zamanlı rapor edilir
4. Güvenlik ekibi herhangi bir anda güncel politika uyumluluk düzeyini kontrol edebilir.
5. Zaman içerisinde değişen şartlar doğrultusunda güvenlik ve operasyon ekipleri gerektiğinde politika güncelleme işlemi yapar.

Teknik Bileşenler

Çok amaçlı ortak ajan

- Gerçek zamanlı izleme
- Sürekli otomatik/manuel aksiyonlat
- Düşük işlem yükü (<2% CPU, <10MB RAM)



Esnek politika geliştirme dili

- Binlerce hazır kontrol
- Operasyon ve güvenlik için en iyi pratikler
- Özel politikaların basit bir şekilde oluşturulması
- Geliştirilebilir/Genişletilebilir ortam desteği

Tekil sunucu ve konsol

- Yüksek güvenlik ve erişilebilirlik
- Veri toplama, analiz ve raporlama
- Tek sunucu 250000 uç nokta

Virtual infrastructure

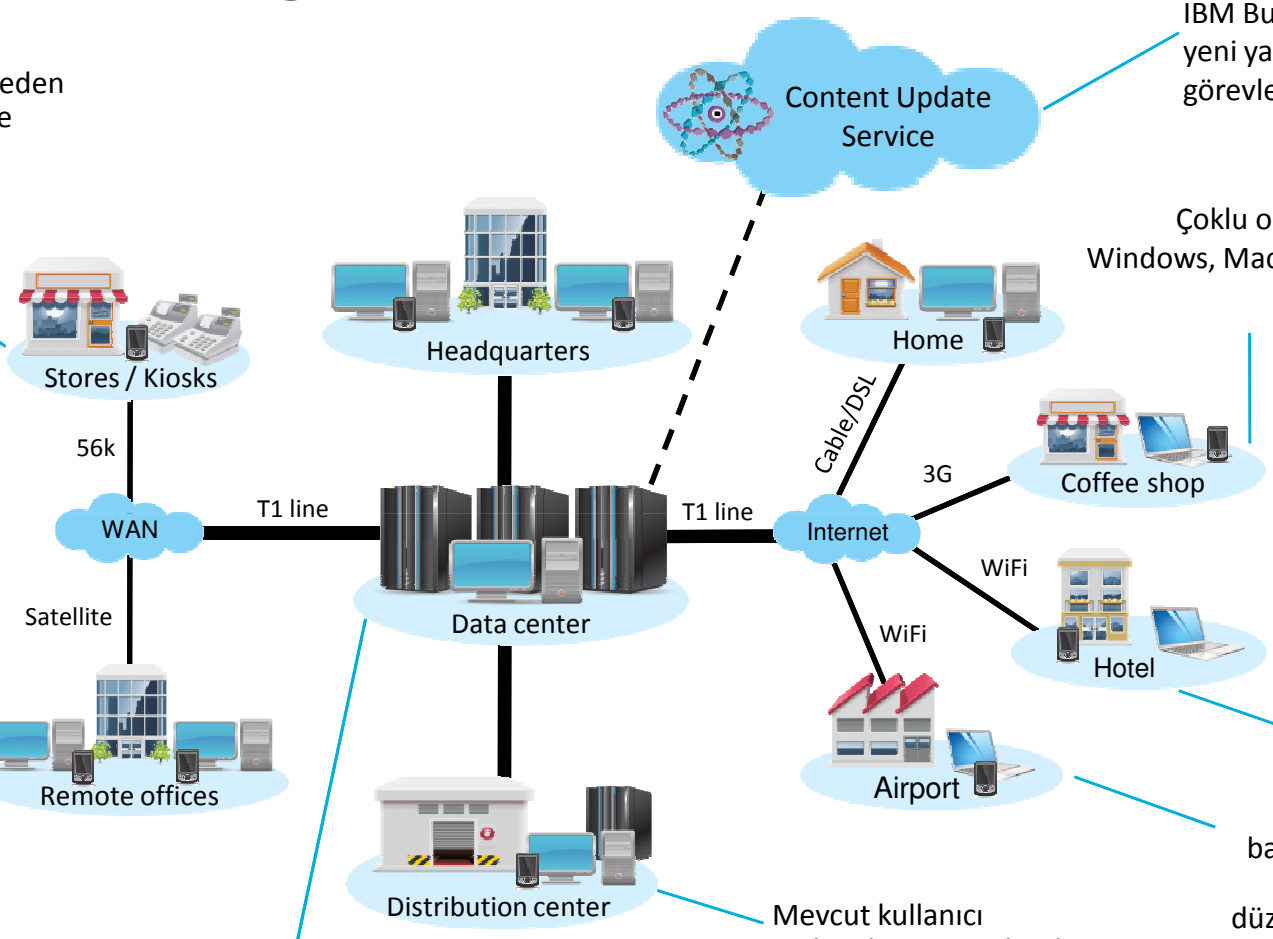
- Merkezden tek hareketle ajanları relay yapma özelliği
- Yüksek erişilebilirilk yapısı
- Relay için özel donanım ihtiyacı olmadığından

Mevcut altyapının kullanılabilmesi

Dağıtık Mimari

Çalışan uygulamarı etkilemeden büyük paketleri dağıtabilme yeteneği

IBM Bulut üzerinden yeni yamaların ve görevlerin alınması



Çoklu ortam desteği: Windows, Mac, Unix, Linux, mobile

Tek bir ajan ve düşük sistem yükü

Internet üzerinde bağlanan cihazların kurum içi ile aynı düzeyde yönetilmesi

Tek sunucu ile 250000 noktanın yönetilmesi

Mevcut kullanıcı makinelerinin yönlendirme istasyonu olabilmesi

Düşük Sahip Olma Bedeli

	Eski Çözüm	IBM Endpoint Manager
90K Ajan Kurulumu	6 Ay	1 Hafta
Yönetim için kullanılan sunucu sayısı	25	1
Yıllık elektrik maaliyeti	$6.9M	$4M
Yama değerlendirme	7 Gün	5 Dakika
Yazılım Envateri (Lisanslama ve Kontrat)	3 Hafta	20 Dakika
Zaafiyet Analizi	6 Ay	3 Gün
Güvenlik Ekibi	5 Ay, 6 Kişi	2 Hafta, 1 Kişi

Geniş Ortam Desteği

IBM

Achieving a substantial reduction in endpoint security issues

The need:

With a growing number of nonstandard endpoints and the increasing sophistication of security threats, IBM evaluated new approaches to effectively protect its internal infrastructure under changing operating conditions.

The solution:

Using Tivoli Endpoint Manager, IBM moved from a reactive correction model to a model based on continuous compliance with internal security policies that provides real-time visibility into endpoints, automatically remediates issues across over 500,000 endpoints, and supports multiple policies based on employee role and data access.

The benefit:

- Realized a **78 percent** decrease in endpoint security issues in the first quarter of global use.
- Reduced internal support costs for savings well above **US$10 million.**
- Enabled **three FTEs** to support **over 500,000** endpoints.

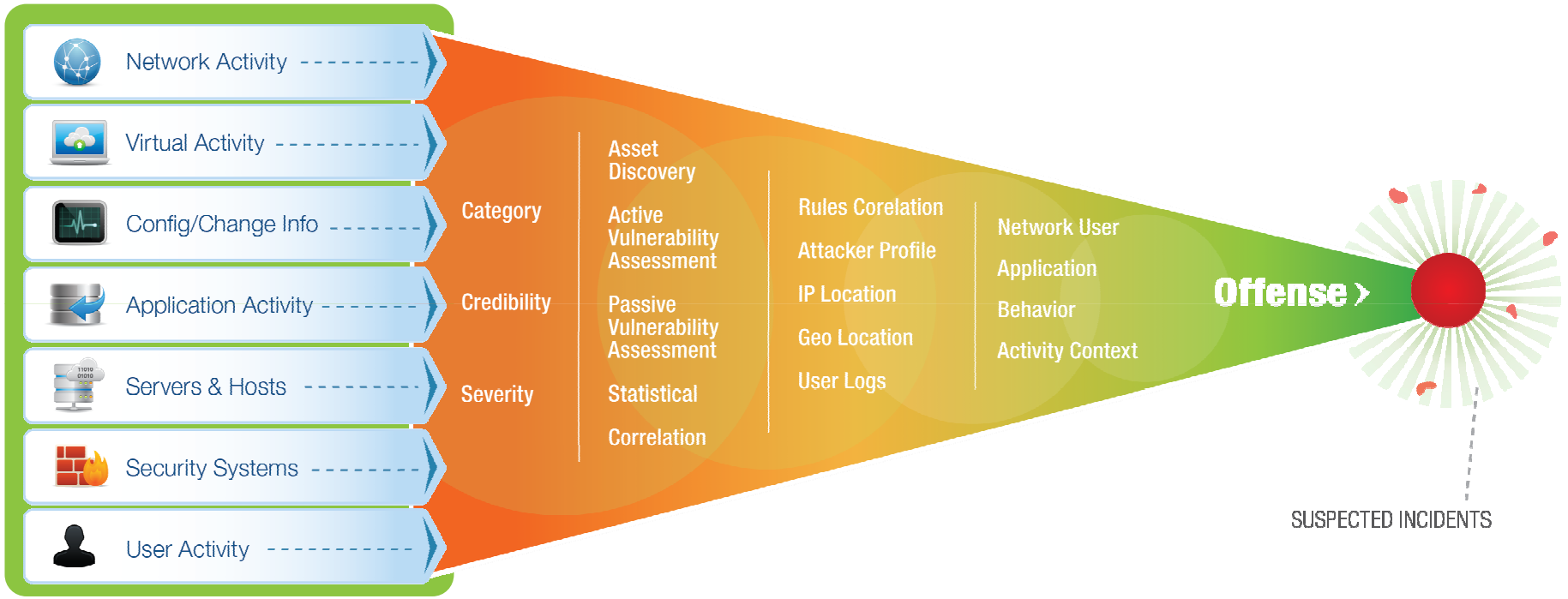
"After deploying Tivoli Endpoint Manager we have realized a 78 percent decrease in endpoint security problems in the first quarter of global use, which is significantly better than our pilot estimate. This should drive savings well above our initial US$10 million estimate—and I believe that we'll see the savings increase as we complete the deployment to all 750,000 endpoints."

—David Merrill, Strategist, Chief Information Security Office, IBM

Solution components:

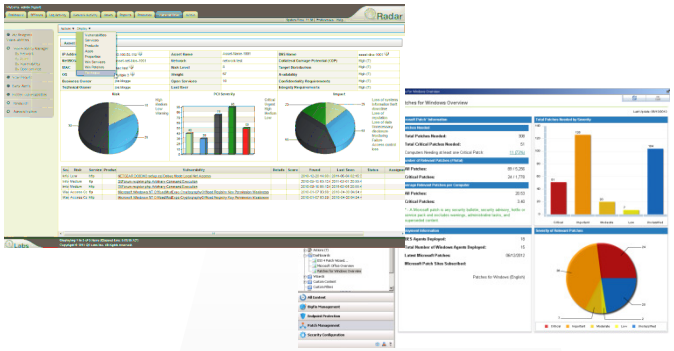
- IBM® Tivoli® Endpoint Manager, built on Bigfix® technology
- IBM System x®

QRadar



Bilgi Kaynakları + Akıllı Yorum = Sonuç ve Aksiyon

QRadar ve IBM Endpoint Manager



QRadar ve IEM birlikte maaliyet ve riski düşürürken uyumluluk düzeyini üst seviyeye çıkarır

Sürekli İzleme

Politika tabanlı uyumluluk

Uç nokta, Network, Güvenlik Olayları ve Zaafiyet İlişkileri

Yüksek Risk noktlarının tespiti

Mobil cihazlar ile birlikte 80'den fazla ortamın desteklenmesi

- Network Cihazları (Cyberscope raporlama), Sunucular ve İş istasyonları uçtan uca gerçek zamanlı izleme
- Uç nokta değerlendirme ve aksiyonlarında network mimarisi doğrultusunda önceliklendirme
- Qradar ve IEM içerisinde bulunan kesin ve güncel veri sayesinde varlıkların durumuna 360 derece bakış açısı.
- İzlenmeyen.Yönetilmeyen sistemlerin tespiti ve gerektiğinde IEM ajan kurulumu ile güveniğin sağlanması

Durum: Zaafiyet bilgisinin QRadar'a sağlanması

IBM Endpoint Manager

1. Qradar, CVE ID sine sahip zaafiyet tanımlarını IEM üzerinden alır.

2. Zenginleştirilmiş zaafiyet veritabanı ile QRadar analizleri üst seviyede etkin ve verimli bir hale gelmiş olur.

QRadar SIEM

IEM Aksiyonlarının Sonuçlarının QRadar'a Sağlanması

IBM Endpoint Manager

1. QRadar aksiyon sonuçlarını IEM üzerinden alır.

2. Konfigurasyon değişiklikleri, Virus tespiti, DLP aktivite bilgileri, başarısız girişler, vs gibi QRadar için önem taşıyan bilgiler hazır bir şekilde sağlanmış olur.

QRadar bu bilgileri network logları, alarmlar gibi diğer kayıtlar ile ilişkilendirir.

QRadar SIEM

Gerçek Yaşam Örnekleri

- Şüpheli kullanıcı hareketleri
  - DLP üzerinden bir FTP bağlantısı girişimi tespiti QRadar'a yönelendirilir. Özellikle mobil veya hareketli cihazlar için bu bilginin başka bir kanaldan edinilmesi kolay olmayacaktır.
- Zararlı Yazılımlar
  - Virus ve diğer zararlı uygulama tespitleri QRadar'a gönderilir. Bu bilgi network aktiviteleri ile ilişkilendirilir. Bu sayede virus aktivitelerinin kaynakları çok daha erken bir safhada saptanabilir..
- İlişkili olayların izlenmesi
  - Üst üste başarısız girişler, takip eden başarılı bir giriş, takip eden şifre değişimi işlemi ve nihayetinde şüpheli network aktivitesi ile sorun çıkaracak muhtemel durumlar cok daha erken tespit edilip gerekli aksiyonlar alınabilir.

IBM

IBM Connected 2013

Her Deneyim Bir Kazanım

Teşekkürler

#connected