Yeni Nesil Bilgi Toplama ve Olay Yönetimi

Bülent S. KARAMAN
Security Systems
Brand Specialist
bulentk@tr.ibm.com

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

Gündem

- ✓ Günümüzde BT güvenliği gereksinimi
- ✓ IBM nasıl yardımcı olabilir?

- ✓ Müşteri başarı öyküleri
- ✓ Sorular ve yanıtlar

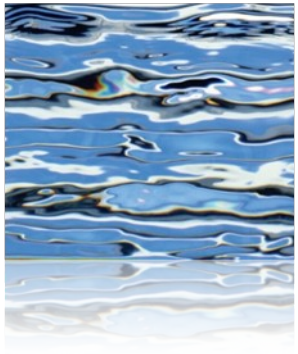
Dünya giderek daha donanımlı, birbiriyle bağlantılı ve zeki hale geliyor

Akıllı Tedarik Zincirleri

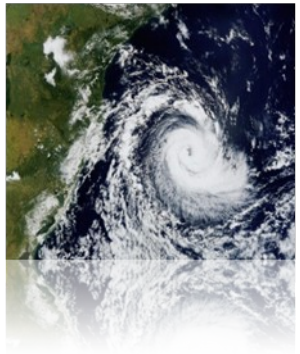
Akıllı Ülkeler

Akıllı Perakendecilik

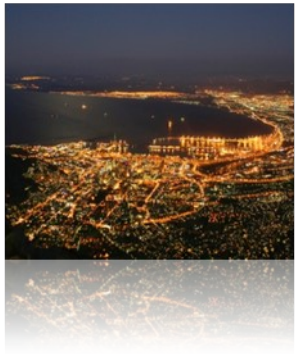
Akıllı Su Yönetimi



Akıllı Hava



Akıllı Enerji Şebekeleri



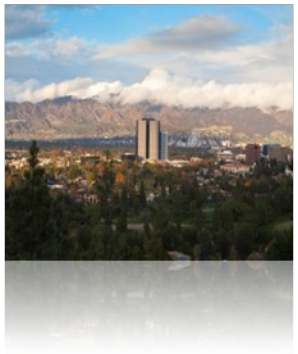
DONANIMLI

BİRBİRİYLE BAĞLANTILI

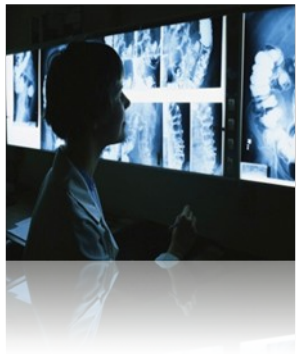
ZEKİ

Akıllı Petrol Sahası Teknolojileri

Akıllı Bölgeler



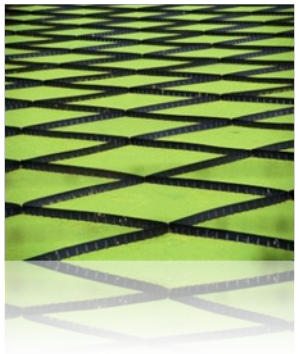
Akıllı Sağlık Hizmetleri



Akıllı Trafik Sistemleri

Akıllı Şehirler

Akıllı Gıda Sistemleri



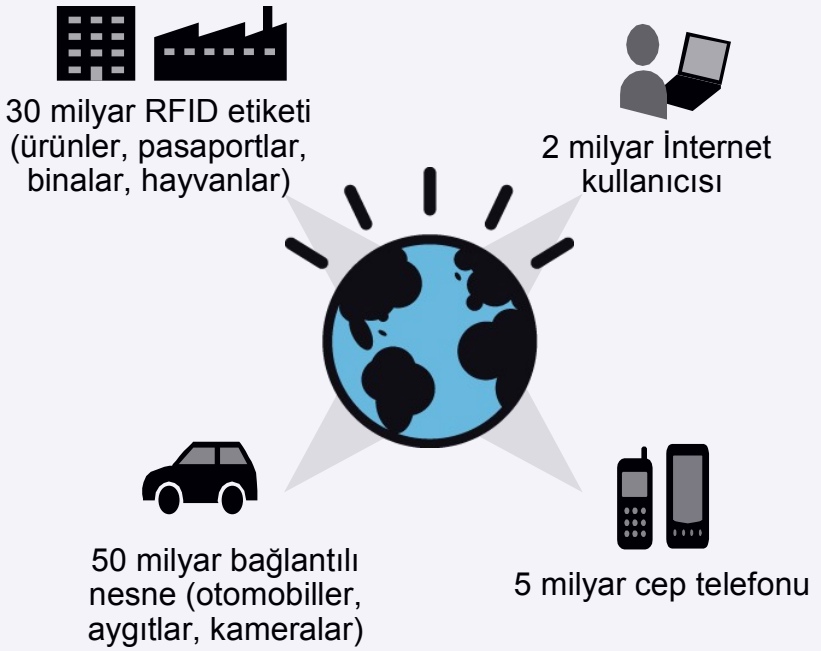
Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

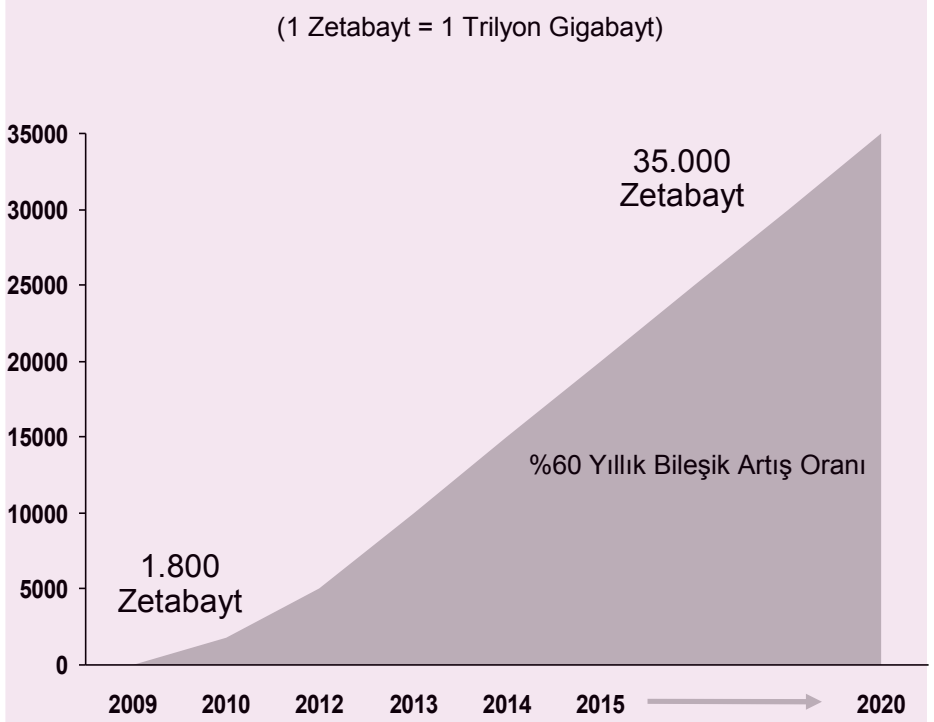
Grand Hyatt İstanbul

Bununla birlikte daha fazla hedef ve güvenlik açığı ortaya çıkıyor

Çok sayıda hedef içeren ortam



Dünya çapındaki veri patlaması



"Mobil tarayıcılarla bağlantılı olarak, henüz yeterince bilgi sahibi olmadığımız güvenlik sızıntıları bulunuyor."
Bilgi Teknolojileri Yöneticisi, Medya Şirketi

Kuruluşların güvenlik yatırımlarını artırmalarına neden olan 4 temel iş sorunu bulunuyor

VERİ PATLAMASI

Hassas verilerine kimlerin baktığını bilmek bir yana, sadece tüm hassas verilerinin nerede bulunduğunu bilen müşteri sayısı bile çok az olduğundan, mevzuata uygunluk önemli bir zorluk oluşturmaktadır.

BT'NİN ÜRÜN HALİNE GETİRİLMESİ

Şirket 2.0'ın ve sosyal işin yaygınlaşması, önemli ölçüde yeni iş risklerinin ortaya çıkmasına neden olmaktadır.

HER ŞEY HER YERDE

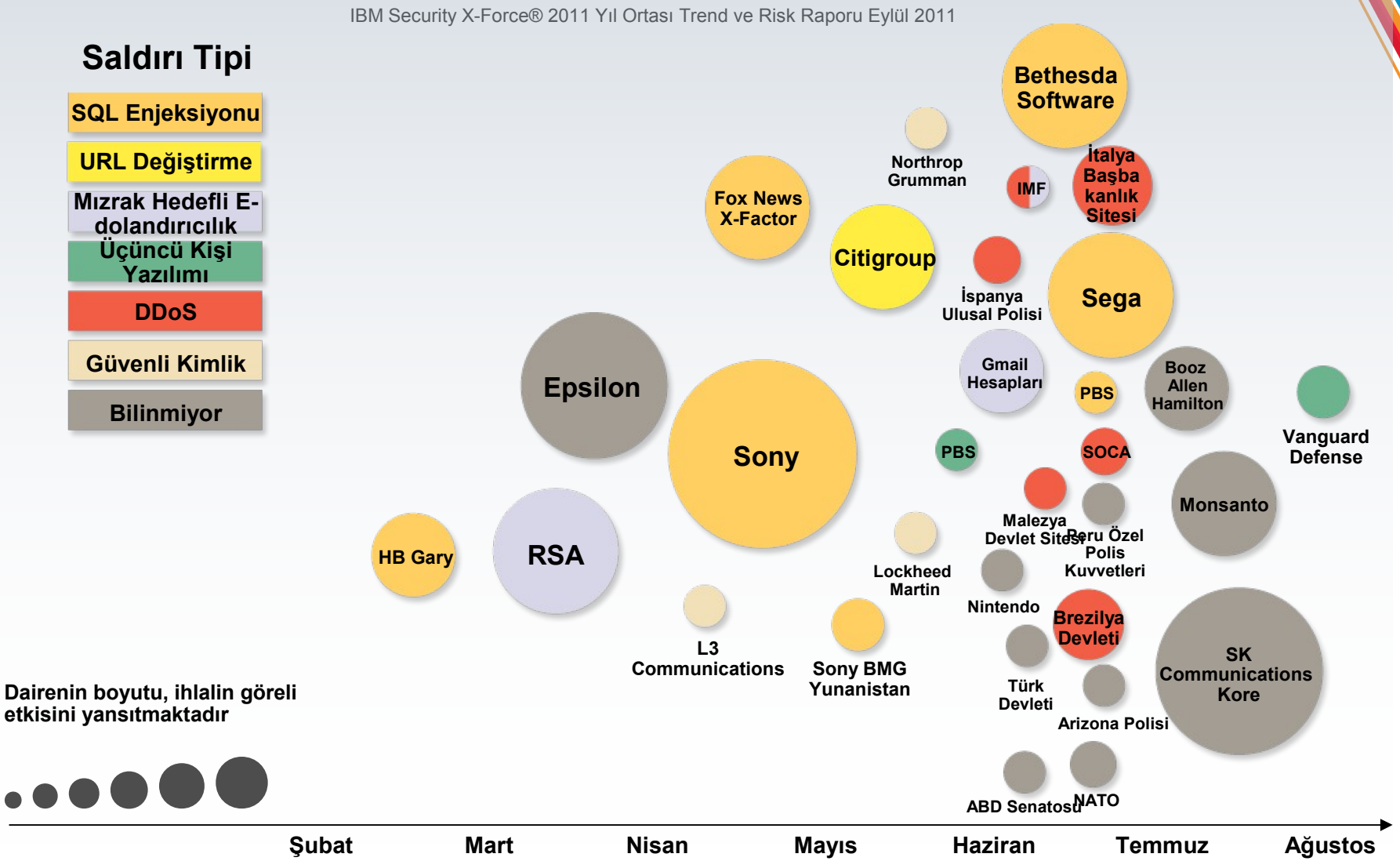
Bulut, sanallaştırma ve diğerleri dahil olmak üzere yeni yenilikçi platformlar, karmaşıklık ve maliyet açısından daha da büyük zorluklara neden olmaktadır.

SOFİSTİKE SALDIRILAR

Saldırılar artık BT altyapısını değil, işin kendisini hedef almaktadır.

...güvenliği **yönetim kurulu odasından** başlayarak en öncelikli konulardan biri haline getiriyor

Kanıt noktaları: Hedefli saldırılar işletmeleri ve devletleri sarsıyor



. . ve üst düzey yönetici önceliklerini etkiler

	Yönetim Kurulu Başkanı	Finans/Operasyon Yöneticisi	Bilgi Teknolojileri Yöneticisi	İK Yöneticisi	Pazarlama Yöneticisi
Yönetici önceliği	Rakiplerden farklılığın sürdürülmesi	Mevzuata uygunluk	Mobil aygıt kullanımının yaygınlaştırılması	Küresel çalışma esnekliğine olanak sağlanması	Markanın geliştirilmesi
Güvenlik riskleri	Fikri mülkiyetin suistimal edilmesi İş açısından hassas verilerin suistimal edilmesi	Yasal gereksinimlerin yerine getirilmemesi	Veri artışı Güvenli olmayan uç noktaları ve uygun olmayan erişim	Hassas verilerin açığa çıkması Çalışanların dikkatsizliği	Müşterilerin veya çalışanların kişisel bilgilerinin çalınması
Potansiyel etki	Pazar payı ve itibar kaybı Yasaların ihlali	Denetimlerin olumsuz sonuçlanması Para cezaları ve cezai kovuşturma Finansal zarar	Veri gizliliğinin, bütünlüğünün ve/veya kullanılabilirliğinin kaybı	Çalışan gizliliğinin ihlal edilmesi	Müşteri güveninin kaybı Marka itibarının kaybı

İşletmeler, giderek artan oranda Denetim Kuruluyla doğrudan bağlantılı Risk Yöneticileri ve Bilgi Güvenliği Yöneticileri atamaktadır

*Kaynak: IBM Üst Düzey Yönetici Araştırmaları Serisi kapsamında 13.000'den fazla üst düzey yönetici ile yapılan görüşmeler

Günümüzde her kurumsal yöneticinin bir güvenlik sorumluluğu vardır

Yönetim Kurulu Başkanı	Finans Yöneticisi	Operasyon Yöneticisi	Bilgi Teknolojileri Yöneticisi	İK Yöneticisi	Pazarlama Yöneticisi
Güvenlik risklerinin hissedar değerini ve güvenini etkilemesinin önlenmesi	Olumsuz güvenlik olaylarının finansal etkilerinin bilinmesi	BT sistemlerindeki kesintilerin sürekli operasyonlar üzerindeki etkisinin değerlendirilmesi	İşletme çapındaki bilgi güvenliği ihlallerinin zaman içinde ortaya çıkan etkilerinin anlaşılması	Çalışan verilerinin uygunsuz bir şekilde açığa çıkması ile bağlantılı risklerin belirlenmesi	Güvenlik ihlalleri ile bağlantılı marka sorunlarının çözülmesi

Tüm öngörülebilir tehditlere karşı koruma sağlanmaya çalışılması yerine, güvenlik riski yönetimi önceliklerinin iş etkisi doğrultusunda belirlenmesi

Siz hangi konumdasınız?

Mevzuata uygunluk

1. Güvenlik risklerinizi değerlendirdiniz mi?
2. Güvenlik etkinliğini ölçmek için bir endüstri standardından yararlanıyor musunuz?
3. Mevzuata uygunluk için ortak bir denetim kümeniz var mı?
4. Güvenlik kanıtlarının bulunması için kritik kayıtları ve günlükleri saklıyor musunuz?

Dahili ve Harici Tehditler

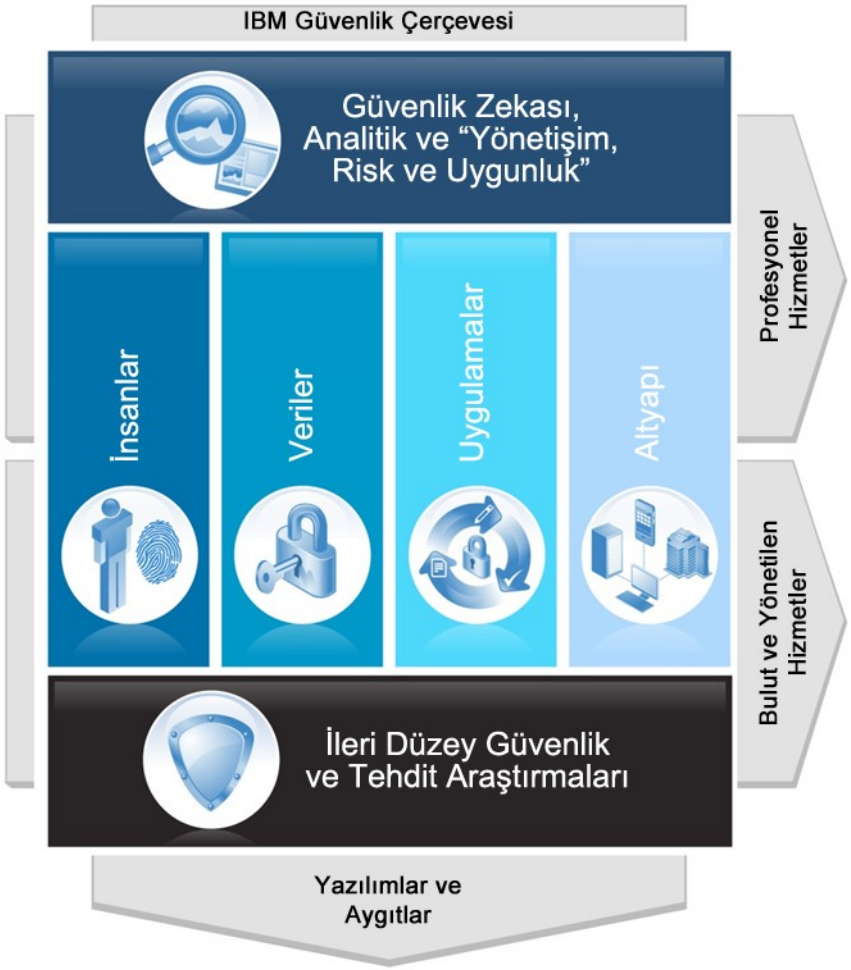
5. Tehditlere ilişkin en son araştırmalardan yararlanıyor musunuz?
6. Verilerinize, uygulamalarınıza ve sistemlerinize kimler erişiyor?
7. Olaylara verilen yanıtları ve olağanüstü durumdan kurtarmayı nasıl yönetiyorsunuz?
8. Hassas verileri gizli olarak sınıflandırıp şifrelediniz mi?
9. Yetkili kullanıcıların verilerinizle ne yaptıklarını biliyor musunuz?
10. Güvenlik, bulut bilgi işlem gibi yeni girişimlerde yerleşik hale getiriliyor mu?

IBM Yardımcı Olabilir - IBM Güvenlik Çerçevesi

IBM Security Systems

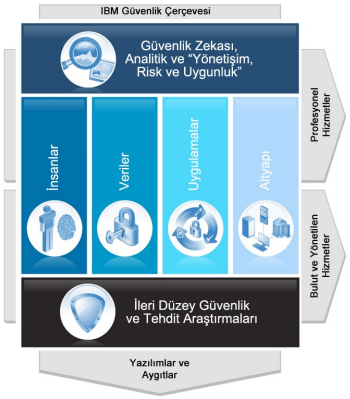
- Pazarda temel güvenliği uçtan uca kapsayan tek satıcı firma
- Yenilikçi teknolojilere 1,8 milyar ABD doları yatırım
- 6.000'den fazla güvenlik mühendisi ve danışmanı
- Ödüllü X-Force® araştırma birimi
- Endüstrideki en büyük güvenlik açığı veritabanı

Zeka • Bütünleştirme • Uzmanlık



IBM Güvenlik
Zeka, Bütünleştirme ve Uzmanlık Sağlıyor

= IBM'in hizmet verdiği alanlar



Güvenlik Yönetişimi, Risk ve Mevzuata Uygunluk

SIEM (Güvenlik Zekası, Kurumsal Olarak Mevzuata Uygunluk)

Kimlik ve Erişim Yönetimi

Kimlik Yönetimi

Erişim Yönetimi

Veri Güvenliği

Veri Kaybının Önlenmesi

Şifreleme ve Anahtar Yaşam Çevrimi Yönetimi

İleti Sistemi Güvenliği

E-posta Güvenliği

Veritabanı İzleme ve Koruma

Veri Gizleme

Uygulama Güvenliği

Uygulama Güvenlik Açığı Taraması

Uygulama Kaynak Kodu Taraması

Web Uygulaması Güvenlik Duvarı

Web / URL Adresi Süzme

Erişim ve Yetki Yönetimi

Hizmet Odaklı Mimari Güvenliği

Altyapı Güvenliği

Güvenlik Açığı Değerlendirmesi

Anabilgisayar Güvenliği

Tehdit Değerlendirmesi

Web / URL Adresi Süzme

İzinsiz Giriş Önleme Sistemi

Güvenlik duvarı, IDS/IPS, MFS, Uç Noktası Yönetimi

Güvenlik Olayı Yönetimi

Sanal Sistem Güvenliği

- ✓ X-Force Araştırma ve Geliştirme
- ✓ T.J. Watson ve diğer 8 güvenlik araştırmaları merkezi
- ✓ IBM Kassel içerik güvenliği ekibi
- ✓ Yönetilen Güvenlik Hizmetleri
- ✓ 11 merkezde 2.000'den fazla güvenlik mühendisi

Entegre Servis Y
Güvenlik Çözümleri

IBM, uçtan uca değerlendirildiğinde, rakiplerine göre güçlü bir güvenlik pozisyonuna sahiptir

Uzmanlık: Rakipsiz Küresel Kapsam ve Güvenlik Farkındalığı

Dünya Çapında Yönetilen Güvenlik Hizmetleri Kapsamı

- Sözleşme kapsamındaki 20.000'den fazla aygıt
- Tüm dünyada 3.700'den fazla yönetilen güvenlik hizmetleri müşterisi
- Her gün yönetilen 9 milyardan fazla olay
- 1.000'den fazla güvenlik patenti*
- 133 izlenen ülke (yönetilen güvenlik hizmetleri)

Güvenlik Operasyonları Merkezleri

Güvenlik Araştırmaları Merkezleri

Güvenlik Çözümü Geliştirme Merkezleri

İleri Güvenlik Dalları Enstitüsü

IBM Research

IBM İleri Güvenlik Enstitüsü

Siber güvenlik inovasyonuna ve işbirliğine olanak sağlıyor

Analiz edilen 10 milyar Web sayfası ve görüntü
Günde 150 milyon izinsiz giriş girişimi
40 milyon istenmeyen posta ve e-dolandırıcılık
46 bin belgelenmiş güvenlik açığı
Milyonlarca özgün kötü niyetli yazılım örneği

X FORCE

Entegre Servis Yönetimi ve Güvenlik Çözümleri

YRU: Yönetim, Risk, Uyum
(Governance, Risk, Compliance)

Güvenlik Zekası Nedir?

Güvenlik Zekası

--isim

- Kullanıcılar, uygulamalar ve altyapı tarafından üretilen ve bir kuruluşun BT güvenliğini ve risk pozisyonunu etkileyen verilerin gerçek zamanlı olarak toplanması, normalleştirilmesi ve bu verilere analitik uygulanması.

Güvenlik Zekası, risklerin ve tehditlerin, koruma ve belirlemeden iyileştirmeye kadar yönetilmesi için etkinliğe dönüştürülebilir ve kapsamlı iş kavrayışı sağlar

Tam Güvenlik Zekası ile Müşterilerin Zorluklarının Çözülmesi

Diğerlerinin gözden kaçırdığı tehditlerin belirlenmesi

- Tüm diğer güvenlik ürünlerinin gözden kaçırdığı "Here You Have" virüsünü içeren 500 ana sistem keşfetmiştir

Veri silolarının birleştirilmesi

- Günde 2 milyar günlük ve olay, 25 adet yüksek öncelikli ihlale indirgenmiştir

İçeriden dolandırıcılığın belirlenmesi

- Güvenilen çalışanların önemli verileri çalması ve silmesi

İşinizle ilgili risklerin öngörülmesi

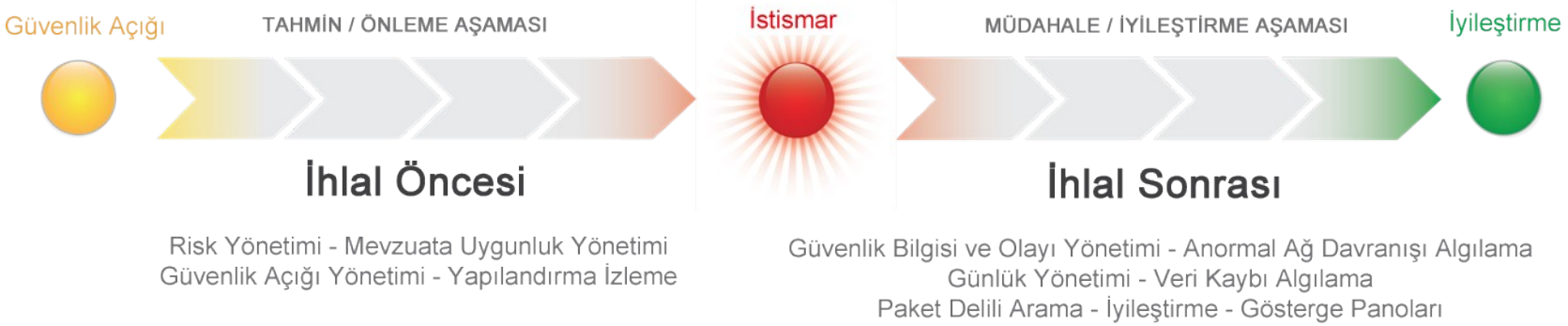
- Altyapıda yapılandırma değişikliği için ilke izleme ve değerlendirme sürecinin otomatikleştirilmesi

Yasal zorunlulukların aşılması

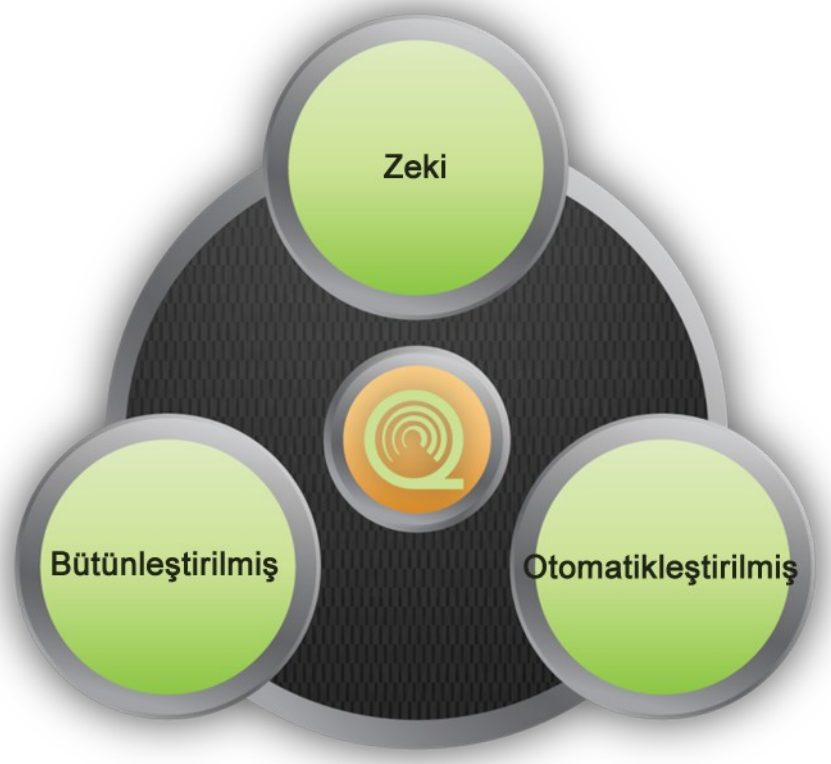
- PCI zorunluluklarına ek olarak tüm ağ etkinliğinin gerçek zamanlı olarak izlenmesi

Mevzuata Tam Uygunluk İçin Çözümler ve Güvenlik Zekası Zaman Çizelgesi

Harici / dahili tehditler nelerdir?	Yapılandırmamız bu tehditlere karşı koruma sağlıyor mu?	Şu anda neler oluyor?	Etkisi nedir?



QRadar: En Zeki, Bütünleştirilmiş, Otomatikleştirilmiş Güvenlik Zekası Platformu

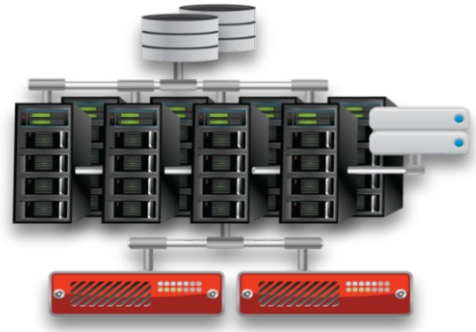


Zeki: Bağlam ve İlişkilendirme ile En Derinlemesine İş Kavrayışını Sağlar

Kaynaklar + Zeka = En Doğru ve Etkinliğe Dönüştürülebilir İş Kavrayışı

Bütünleştirilmiş: Ölçeklendirme ve Kullanım Kolaylığı için Bütünleştirilmiş Platform

Birleştirilmiş Çözüm



- Ölçeklendirme sorunları
- Bütünleştirilmemiş raporlama ve arama
- Yerel karar yok
- Çok sayıda ürün ile yönetim
- Birbirinin kopyası günlük havuzları
  - ➢ ***İşletim darboğazları***

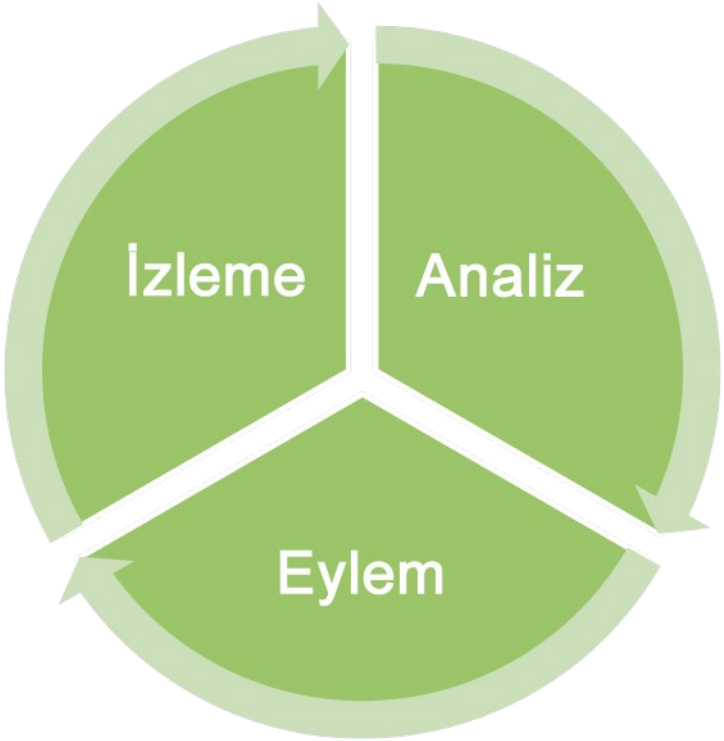
QRadar Bütünleştirilmiş Çözümü

- Yüksek düzeyde ölçeklenebilir
- Ortak raporlama ve arama
- Dağıtılmış ilişkilendirme
- Birleşik yönetim
- Tek kopya olarak saklanan günlükler
  - ➢ ***Tam görüş netliği***

Bolted together vs Integrated

Otomatikleştirilmiş: Ek personel gerektirmez

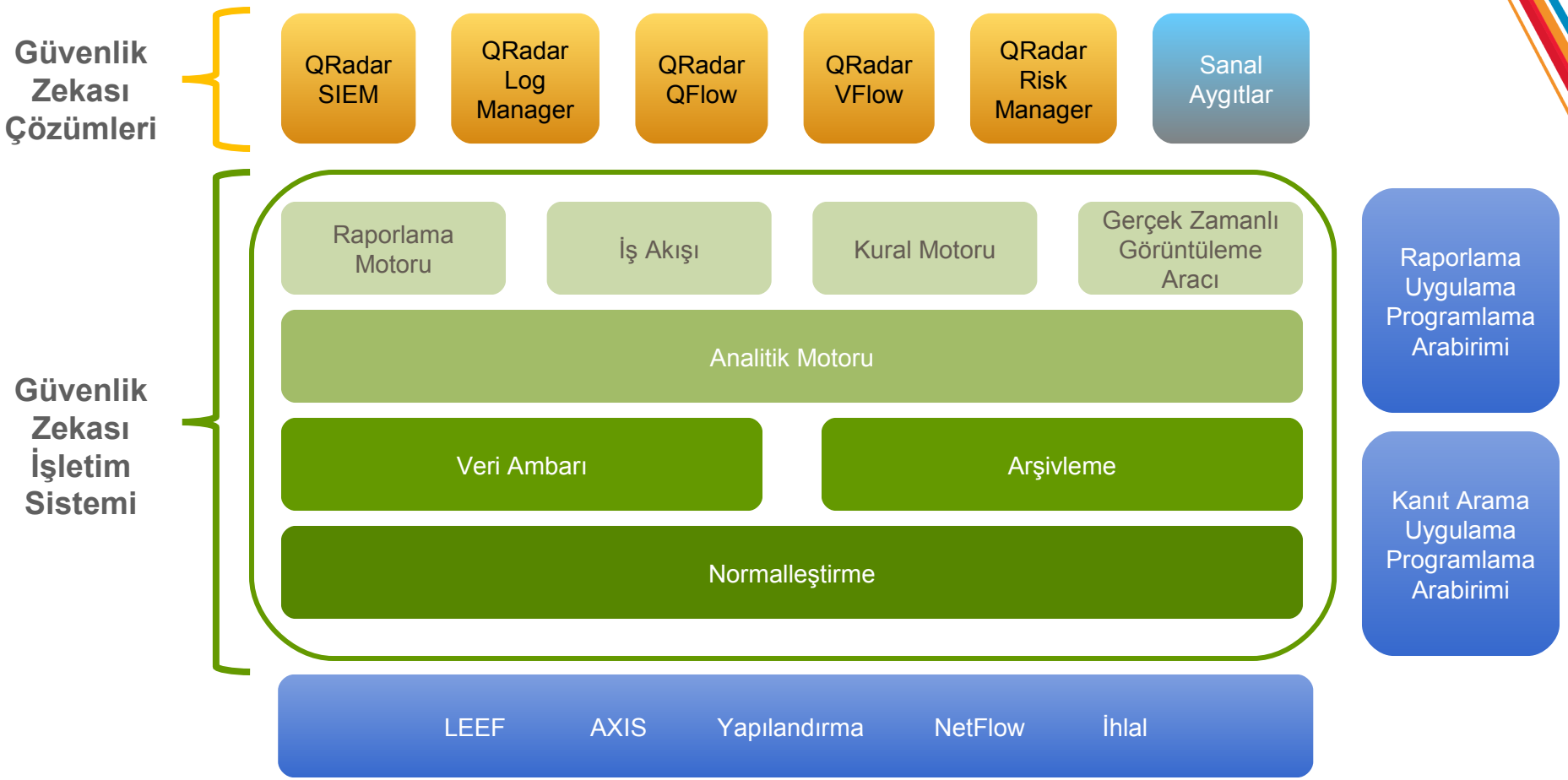
- Günlük kaynaklarının, uygulamaların ve varlıkların otomatik olarak keşfedilmesi
- Otomatik varlık gruplandırma
- Merkezileştirilmiş günlük yönetimi
- Otomatikleştirilmiş yapılandırma denetimleri



- Varlık tabanlı öncelik belirleme
- Otomatik tehdit güncelleme
- Otomatik müdahale
- Yönlendirilen iyileştirme

- Otomatik ayar
- Otomatik tehdit algılama
- Binlerce önceden tanımlanmış kural ve görev tabanlı rapor
- Kullanımı kolay olay süzme
- Gelişmiş güvenlik analitiği

QRadar Ürün Ailesi: Ortak Bir Temel Üzerine Kurulmuştur



Zeki, Bütünleştirilmiş, Otomatikleştirilmiş - Tek Konsolla Güvenlik

Tamamen Bütünleştirilmiş Güvenlik Zekası

Günlük Yönetimi	Radar Log Manager  Radar Log Manager Free Edition 	• Anahtar teslimi günlük yönetimi • KOBİ'lerden büyük kuruluşlara kadar • Kurumsal güvenlik bilgisi ve olayı yönetimine büyütülebilir
Güvenlik Bilgileri ve Olay Yönetimi	Radar SIEM 	• Bütünleştirilmiş günlük, tehdit, risk ve mevzuata uygunluk yönetimi • Gelişmiş olay analitiği • Varlık profili oluşturma ve akış analitiği • İhlal yönetimi ve iş akışı
Risk Yönetimi	Radar Risk Manager 	• Tahmine dayalı tehdit modeli oluşturma ve benzetim • Ölçeklenebilir yapılandırma izleme ve denetimi • Gelişmiş tehdit görselleştirme ve etki analizi
Ağ Etkinliği ve Anormallik Algılama	Radar SIEM  Radar QFlow 	• Ağ analitiği • Davranışa ve anormallik algılama • Güvenlik bilgisi ve olayı yönetimi ile tam bütünleştirilmiş
Ağ ve Uygulama Görünürlüğü	Radar QFlow  Radar VFlow 	• Katman 7 uygulama izleme • İçerik toplama • Fiziksel ve sanal ortamlar

Entegre Servis Yönetimi ve Güvenlik Çözümleri

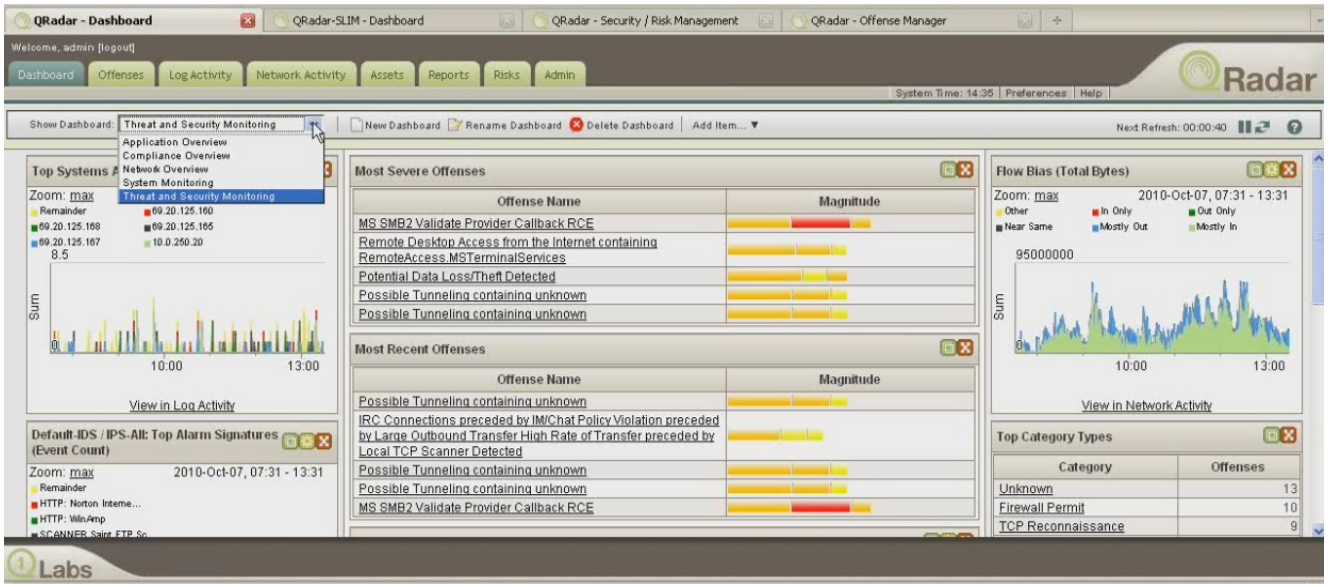
30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

Tamamen Bütünleştirilmiş Güvenlik Zekası

- Günlük Yönetimi
- Güvenlik Bilgileri ve Olay Yönetimi
- Risk Yönetimi
- Ağ Etkinliği ve Anormallik Algılama
- Ağ ve Uygulama Görünürlüğü

Tek Konsolla Güvenlik



Tek Veri Mimarisi Üzerine Kurulmuştur

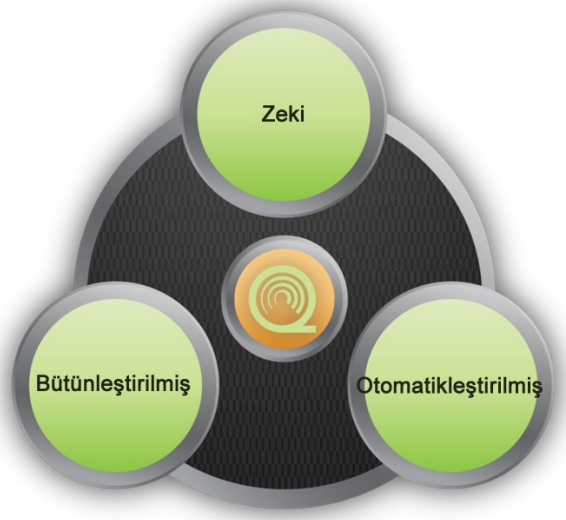
Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba
Grand Hyatt İstanbul

QRadar: En Zeki, Bütünleştirilmiş, Otomatikleştirilmiş Güvenlik Zekası Platformu

- Proaktif tehdit yönetimi
- En kritik anormallikleri tanımlar
- Hızlı, eksiksiz etki analizi

- Siloları ortadan kaldırır
- Yüksek düzeyde ölçeklenebilir
- Esnek, geleceğe hazır

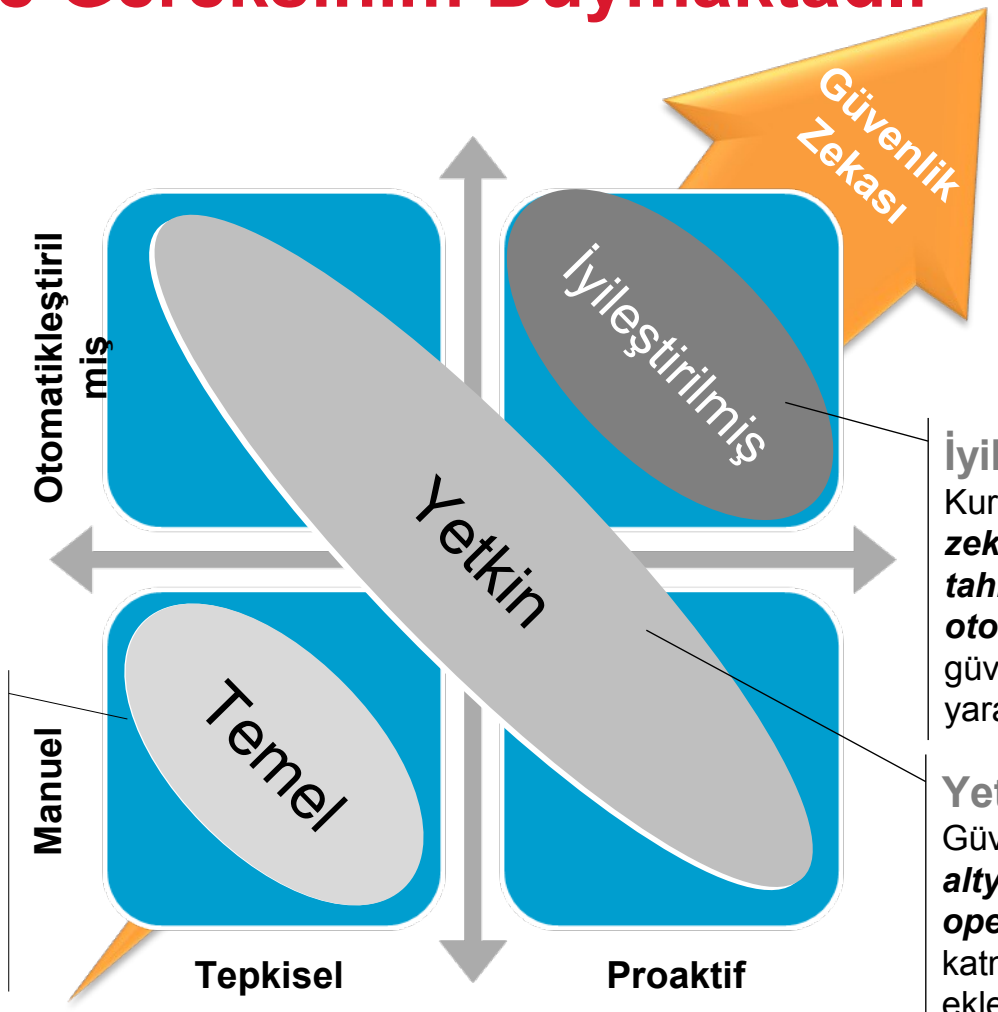


- Kolay devreye alma
- Kısa değer elde etme süresi.
- İşletim verimliliği

Müşterilerin Q1 Labs'ı Tercih Etmesinin En Önemli Nedenleri

1. En zeki, bütünleştirilmiş ve otomatikleştirilmiş çözüm
2. En gelişmiş tehdit analitiği ve mevzuata uygunluk otomasyonu
3. Az sayıda personel gereksinimi ile kısa değer elde etme süresi
4. Sistemler ve güvenlik verileri arttıkça kolaylıkla ölçeklenir
5. Köklü pazar liderliği ve mükemmel destek
6. En iyi kanal ilişkileriyle desteklenen birlikte iş yapma kolaylığı
7. IBM'in rakipsiz güvenlik uzmanlığı ve bütünleştirilmiş yeteneklerinin çeşitliliği

Kuruluşlar Güvenlik Pozisyonlarının Zekice Bir Görünümüne Gereksinim Duymaktadır

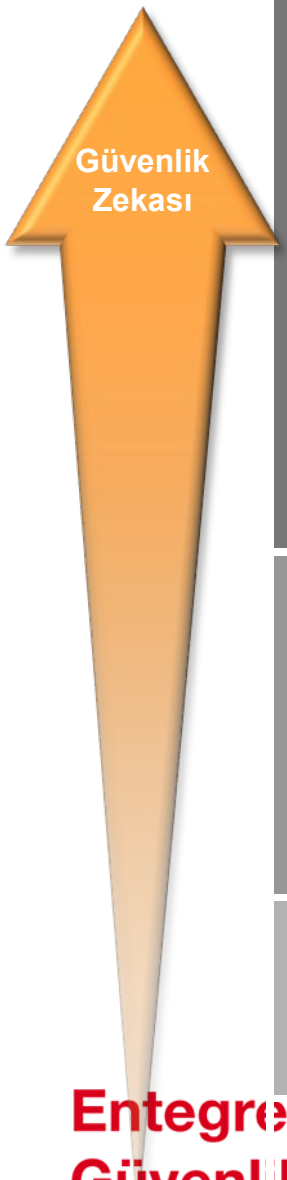


Temel
Kuruluşlar erişimi düzenleyen ve manuel raporlamaya veri sağlayan ***çevre korumasından*** yararlanmaktadır

İyileştirilmiş
Kuruluşlar, ***güvenlik zekasını*** oluşturmak için ***tahmine dayalı ve otomatikleştirilmiş*** güvenlik analitiğinden yararlanmaktadır

Yetkin
Güvenlik, ***BT altyapısına*** ve ***iş operasyonlarına*** katmanlar halinde eklenmiştir

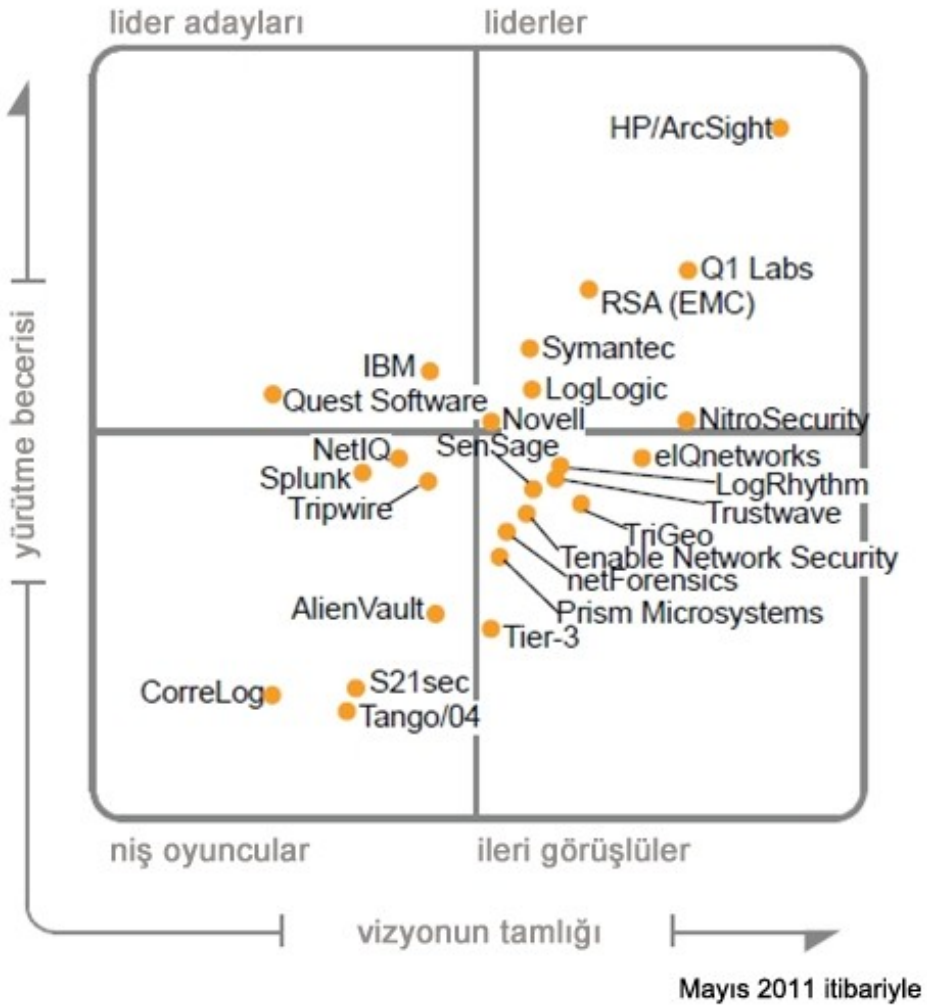
Güvenlik Zekası İyileştirilmiş Güvenliğe Doğru İlerlemeye Olanak Sağlar



	Güvenlik Zekası: Bilgi ve olay yönetimi: Gelişmiş ilişkilendirme ve ayrıntılı analitik Harici tehdit araştırmaları			
İyileştirilmiş	- Görev tabanlı analitik - Kimlik yönetişimi - Ayrıcalıklı kullanıcı denetimleri	- Veri akışı analitiği - Veri yönetişimi	- Güvenli uygulama mühendisliği süreçleri - Dolandırıcılığın belirlenmesi	- Gelişmiş ağ izleme - Kanıt arama / veri madenciliği - Güvenli sistemler
Yetkin	- Kullanıcı yetkilendirme - Erişim yönetimi - Güçlü kimlik doğrulaması	- Erişim izleme - Veri kaybı önleme	- Uygulama güvenlik duvarı - Kaynak kodu tarama	- Sanallaştırma güvenliği - Varlık yönetimi - Uç noktası / ağ güvenliği yönetimi
Temel	- Merkezileştirilmiş dizin	- Şifreleme - Erişim denetimi	- Uygulama tarama	- Çevre güvenliği - Virüs önleme
	İnsanlar	**Veriler**	**Uygulamalar**	**Altyapı**

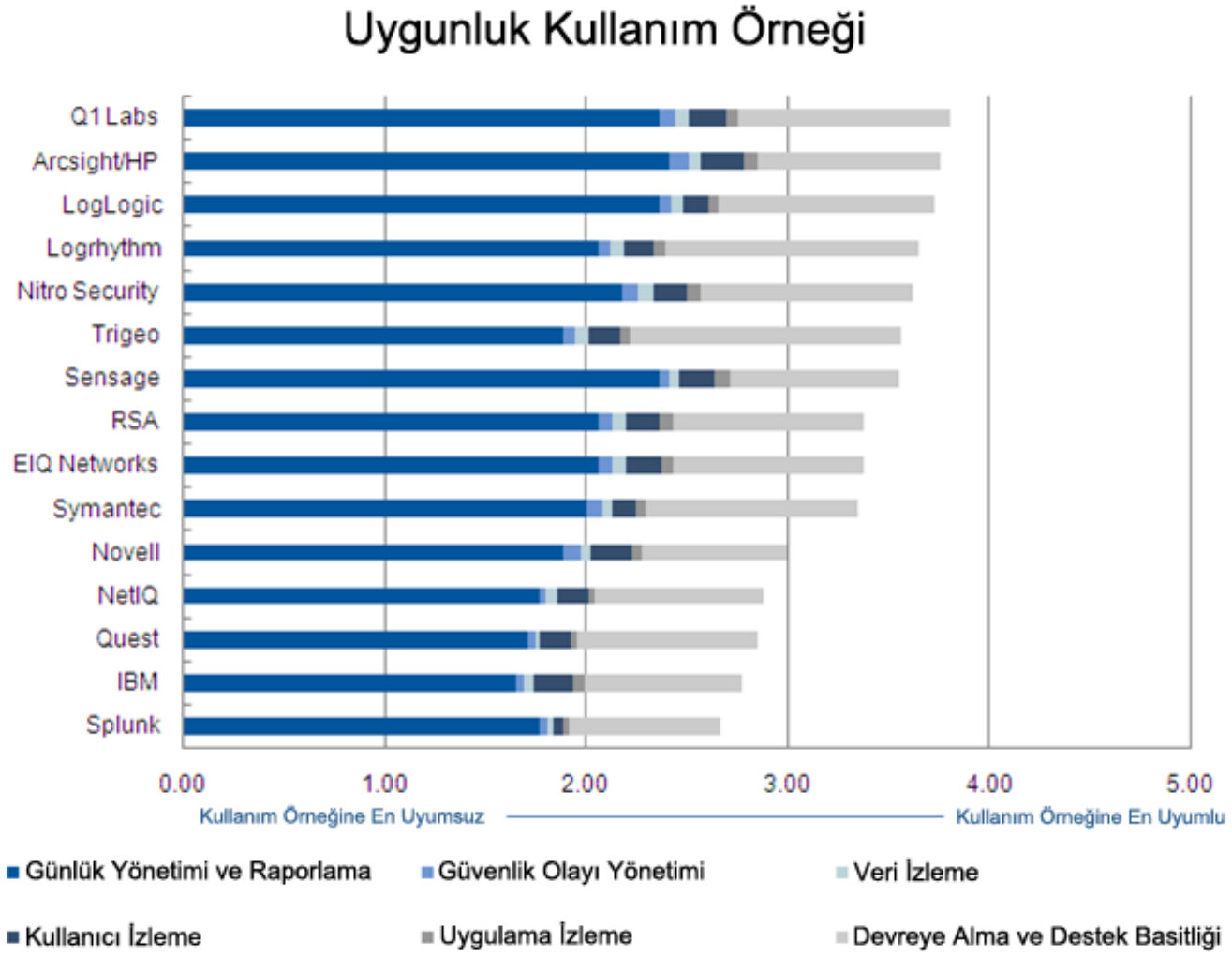
Entegre Servis Güvenlik Çözü

2011 Gartner Güvenlik Bilgileri ve Olay Yönetimi Magic Quadrant (MQ)



Kaynak: Gartner (Mayıs 2011)

Güvenlik Bilgileri ve Olayı Yönetiminin en önemli etkeni olan mevzuata uygunlukta 1 numara



Üç başlıca kullanım örneği:
1.) Mevzuata uygunluk
2.) Tehdit yönetimi
3.) Genel devreye alma (ikisinin karışımı)


Teşekkürler