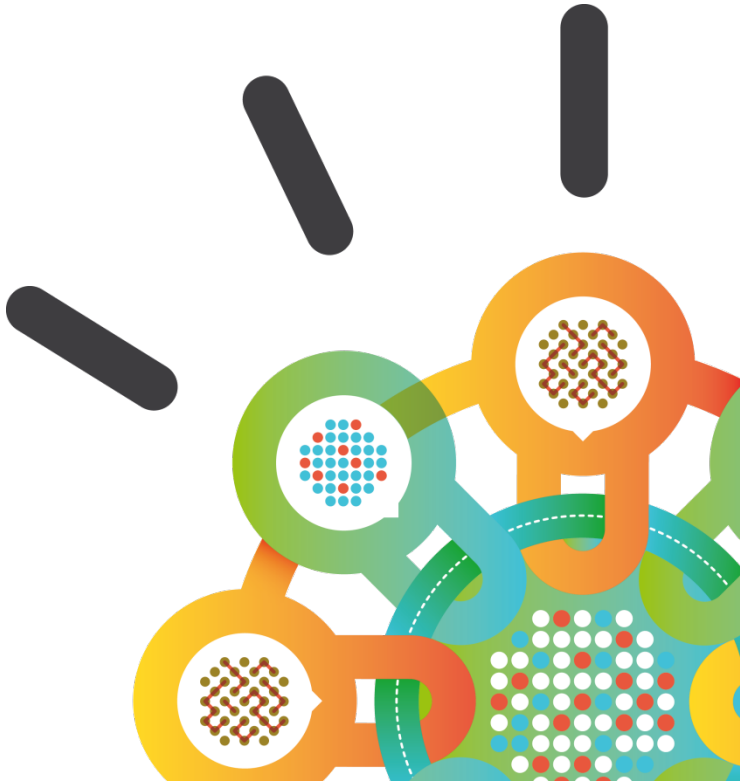
Security Intelligence.
Think Integrated.

# IBM Security Systems

*Yeni nesil Güvenlik Olay Yönetimi ve Atak Önleme Sistemleri*

*Hakan Turgut*
*Bölge Yöneticisi*
*Turkiye, Doğu Avrupa, Rusya ve CIS Ülkeleri*
IBM Security Systems
HAKANT@tr.ibm.com



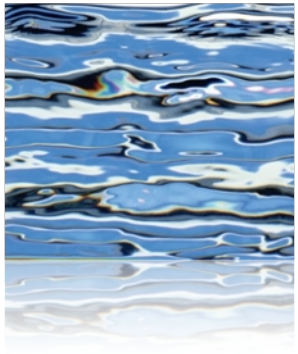
# Dünya giderek daha donanımlı, birbiriyle bağlantılı ve zeki hale geliyor

Akıllı Tedarik Zincirleri

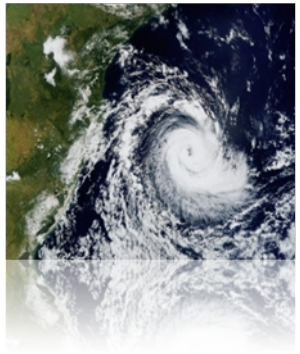
Akıllı Ülkeler

Akıllı Perakendecilik

Akıllı Su Yönetimi



Akıllı Hava



Akıllı Enerji Şebekeleri

DONANIMLI

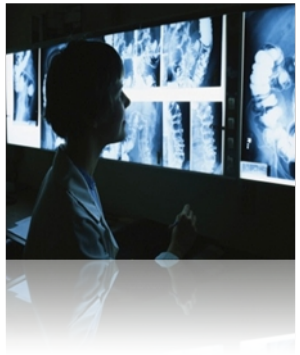
BİRBİRİYLE BAĞLANTILI

ZEKİ

Akıllı Petrol Sahası Teknolojileri

Akıllı Bölgeler

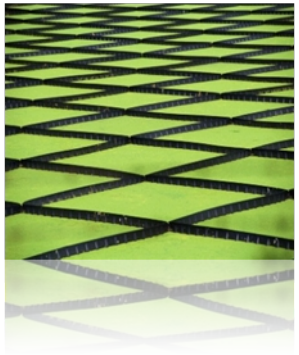
Akıllı Sağlık Hizmetleri



Akıllı Trafik Sistemleri

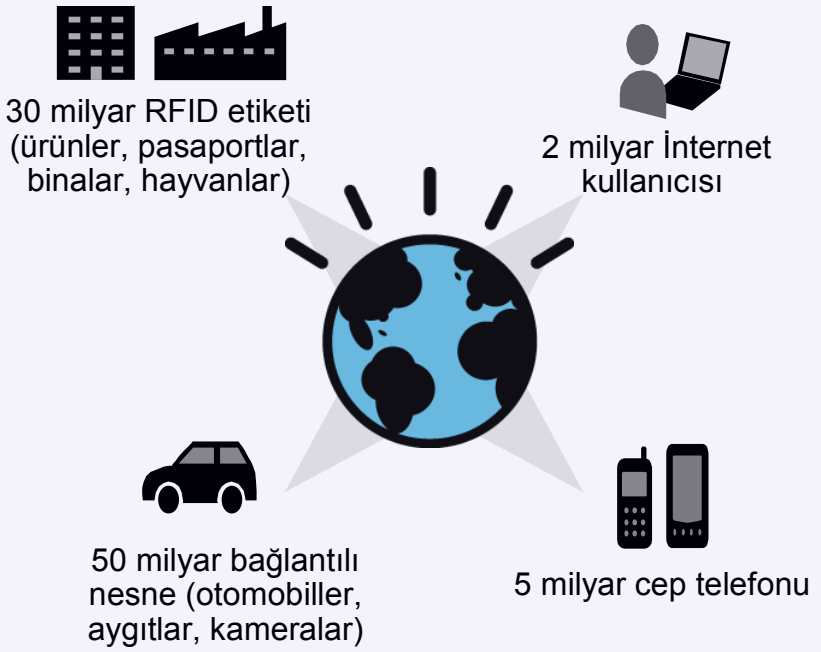
Akıllı Şehirler

Akıllı Gıda Sistemleri

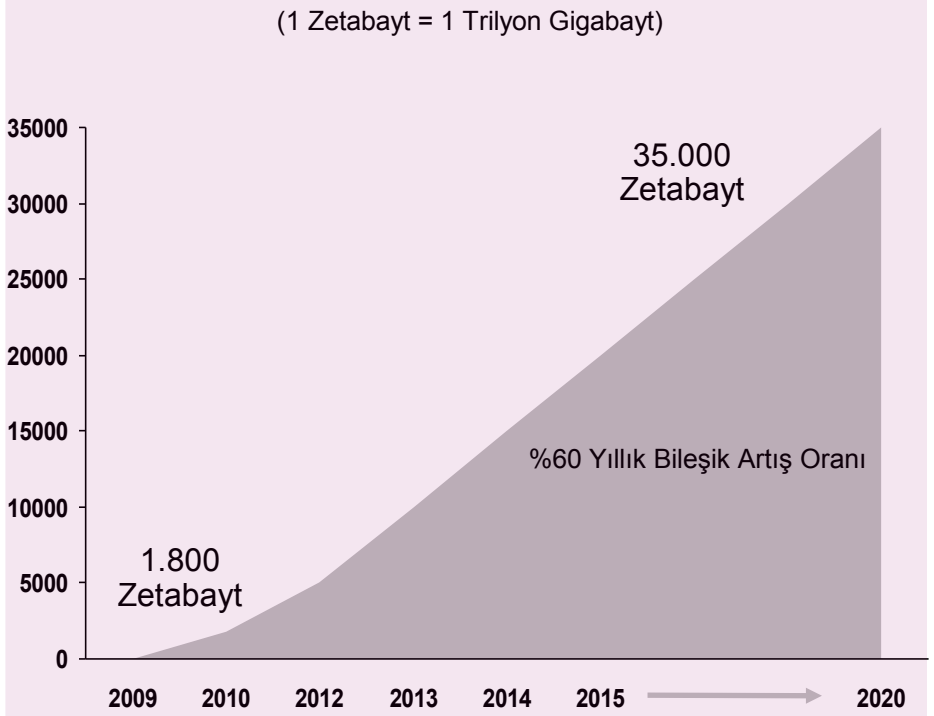


# Bununla birlikte daha fazla hedef ve güvenlik açığı ortaya çıkıyor

## 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

# Network Güvenliği

Stealth Bots • Targeted Attacks
Worms • Trojans • Designer Malware

**SOFİSTİKE ATAKLAR**

Çok sayıda atak vektörü kullanılan ve riskleri ortaya koyan daha sofistike ataklar


**ÇEVRİM İÇİ VİDEO SİTELERİ**

Çevrim içi sitelerinin çok büyük oranlarda bandwidth tüketmesi


**SOSYAL AĞLAR**

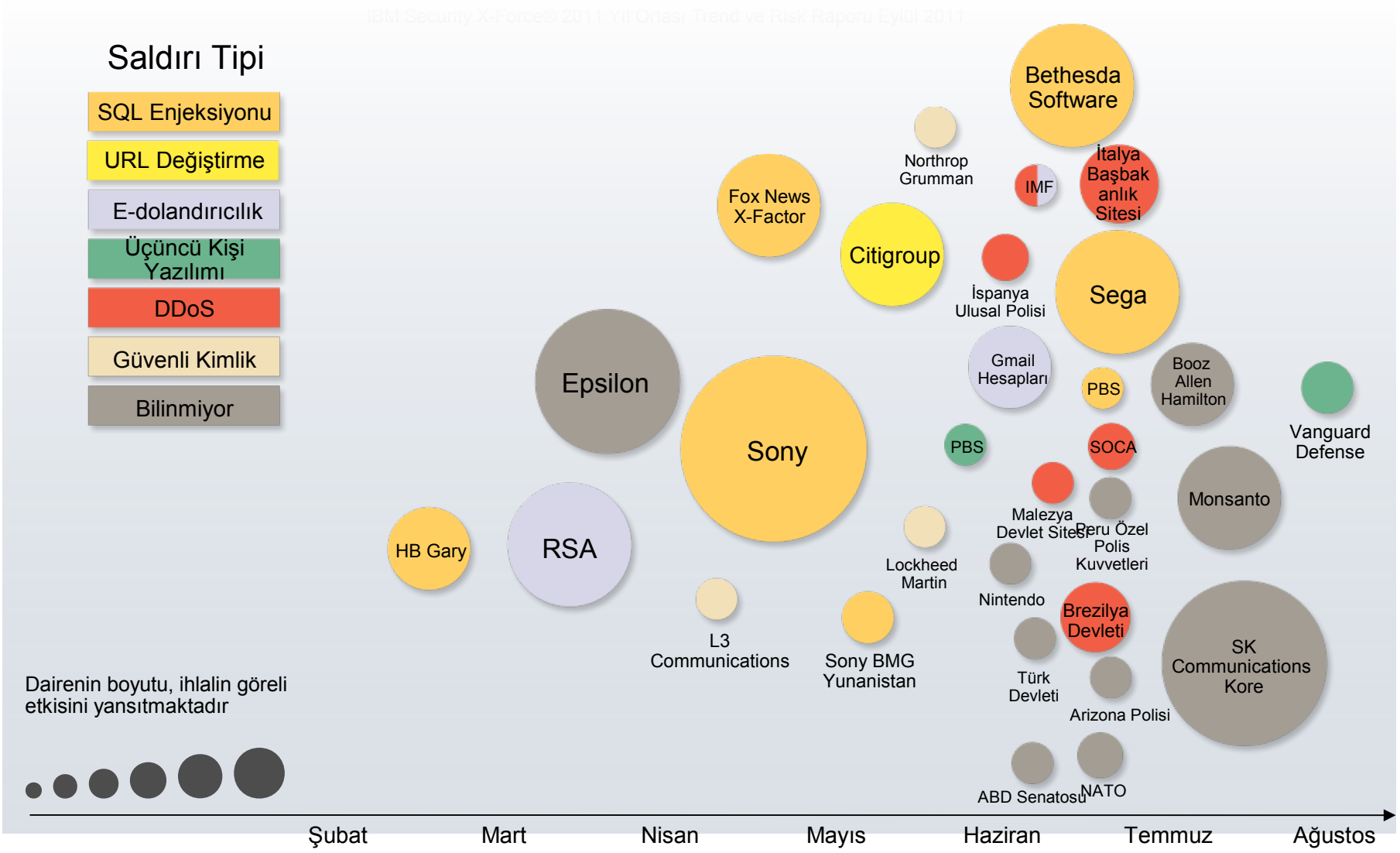
Yeni atak vektörleri için sosyal media sitelerinin üretkenlik, gizlilik ve güvenlik risklerini sunması

URL Filtering • IDS / IPS
IM / P2P • Web App Protection
Vulnerability Management

**NOKTASAL ÇÖZÜMLER**

Noktasal çözümlerin minimum entegrasyon ya da veri paylaşımı ile silolanabilmesi

# Kanıt noktaları: Hedefli saldırılar işletmeleri ve devletleri sarsıyor



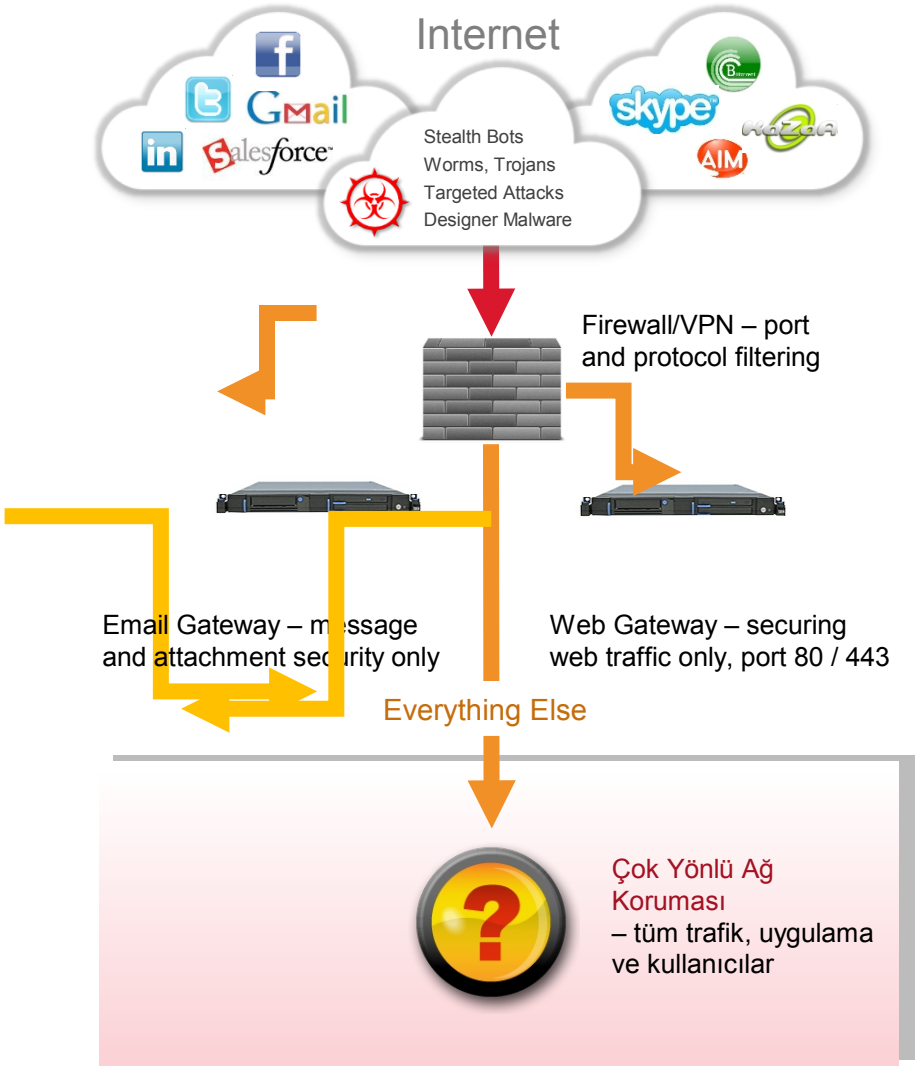
# Bugünkü değişimler ve geleneksel çözümler

## Limitler

- Standart tanımlama metodları yeterliliğini kaybediyor
- Çevrimiçi video siteleri ve gelişen web uygulamaları ile gelen yeni açıklıklar
- Temel “Block Only” modunun gereklilikleri de limitlemesi
- Entegre edilen uygulamaların karmaşıklık ve maliyeti artırması

## Gereklilik: Çok yönlü koruma

- 0-day threat protection gerekliliği ve diğer çözümlerle entegrasyonunun yeterince güçlü olmaması
- İş dışı uygulamaların maliyetini azaltabilme
- İş gereksinimi ve kullanıcı rolüne göre kısıtlı erişim kontrolleri uygulanması
- Toplam karmaşıklığın azaltılması



# KİM, NE ve NE ZAMAN SORULARININ GEREKLİLİĞİ

- Server
- Network
- Geography
- Reputation
- User or Group


- Web Category Protection
- Access Control
- Protocol Aware Intrusion Protection
- Client-Side Protection
- Botnet Protection
- Network Awareness
- Web Protection
- Reputation

- Pazarlama ve satış takımına erişime izin verilmesi
- Tüm dışarı doğru Mail veya chat trafiği İçin eklerin bloklanması
- Daha net trafik kurallarının iletişimde bulunulan ülkeler için uygulanması
- Web serverlara gelen uygulama trafiğinin daha iyi anliz edilebilmesi
- Bilinen botnet serverları ve phishing sitelerinin bloklanması
- Finansal ve medya sitelerine giden trafiğin izin verilemesi ama içeriğinin izlenmemesi

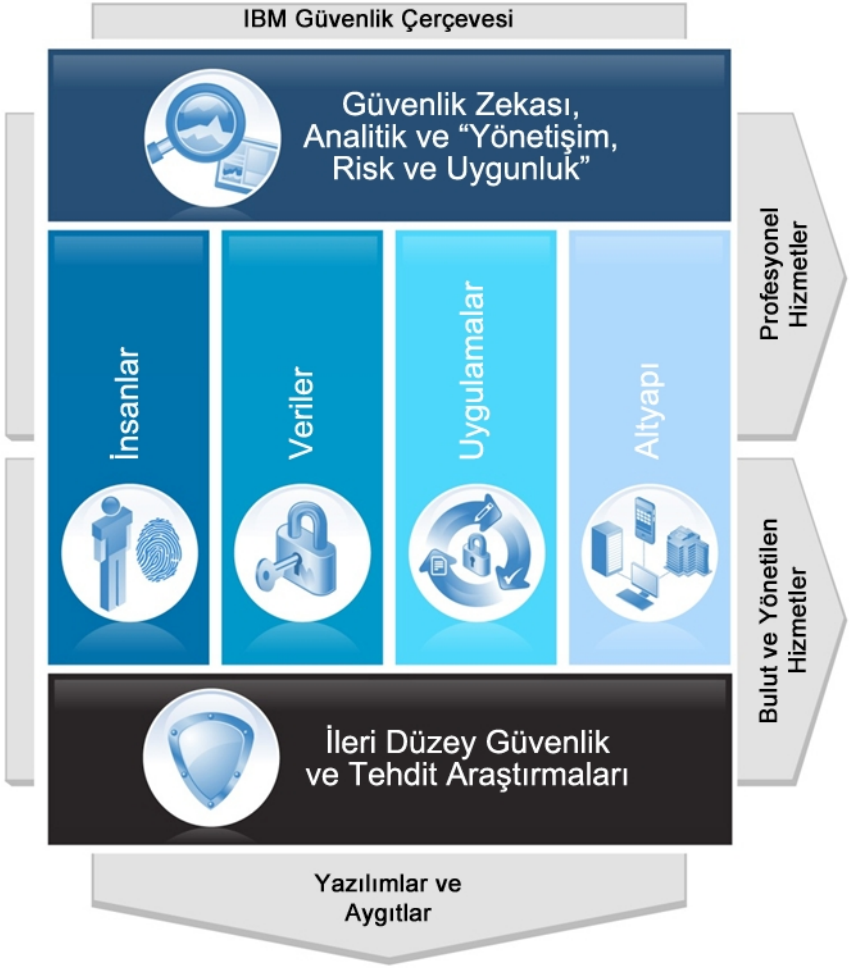
| KİM? | NE? | Kontrol? | Güvenlik |
|---|---|---|---|
| 172.29.230.15, 192.168.0.0 /16 | 80, 443,25, 21, 2048-65535 | ? | |

# IBM Güvenlik Çerçevesi

## IBM Security Systems

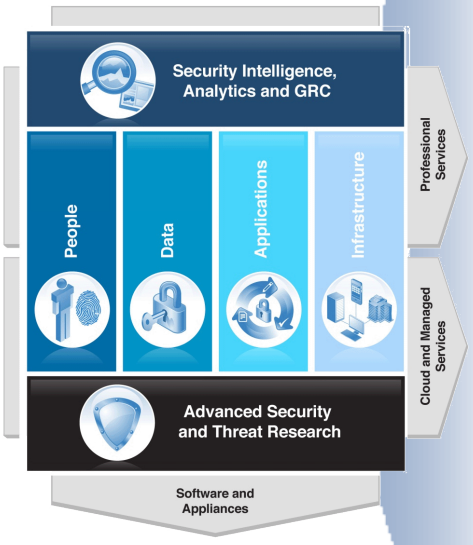
- Pazarda temel güvenliği uçtan uca kapsayan tek satıcı firma
- Yenilikçi teknolojilere 1,8 milyar ABD doları yatırım
- 6.000'den fazla güvenlik mühendisi ve danışmanı
- Ödüllü X-Force® araştırma birimi
- Endüstrideki en büyük güvenlik açığı veritabanı

Zeka • Bütünleştirme • Uzmanlık



# IBM Security – Delivering Intelligence, Integration and Expertise

= IBM addresses




Security Governance, Risk & Compliance

SIEM (Security Intelligence, Enterprise Compliance)

Identity and Access Management

Identity Management

Access Management

Data Security

Data Loss Prevention

Encryption and Key Lifecycle Management

Messaging Security

E-mail Security

Database Monitoring and Protection

Data Masking

Application Security

App Vulnerability Scanning

Web Application Firewall

App Source Code Scanning

Web / URL Filtering

Access and Entitlement Management

SOA Security

Infrastructure Security

Vulnerability Assessment

Mainframe Security

Threat Assessment

Web/URL Filtering

Intrusion Prevention System

Firewall, IDS/IPS, MFS, End Point Mgmt.

Security Event Management

Virtual System Security

- ✓ 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

# IBM X-Force İstihbarat Yaşam Çevrimi


**Yeni koruma rehberliği**

- Bilinen Kötü Niyetli Web Sitelerinin Derinlemesine Taranması
- Yeni İstismar Yöntemlerinin Analiz Edilmesi
- Yeni Koruma Rehberliği Sağlanması

**Yeni IPS güncellemeleri**

- Korumanın Geliştirilmesi
- Güncellemeler Sağlanması

**Yeni kötü niyetli Web siteleri**

- Yönetilen Güvenlik Hizmetleri Bağlantılarının Sınıflandırılması
- İlgili Web Sitelerinin Bulunması (Derin Tarama)
- Kötü Niyetli Yazılımların Aranması
- Yeni Kötü Niyetli Web Sitelerinin Bulunması
- Tüm Kötü Niyetli Etki Alanlarının Engellenmesi

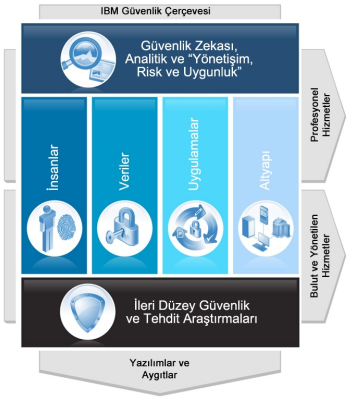
**Kötü niyetli URL adresleri**

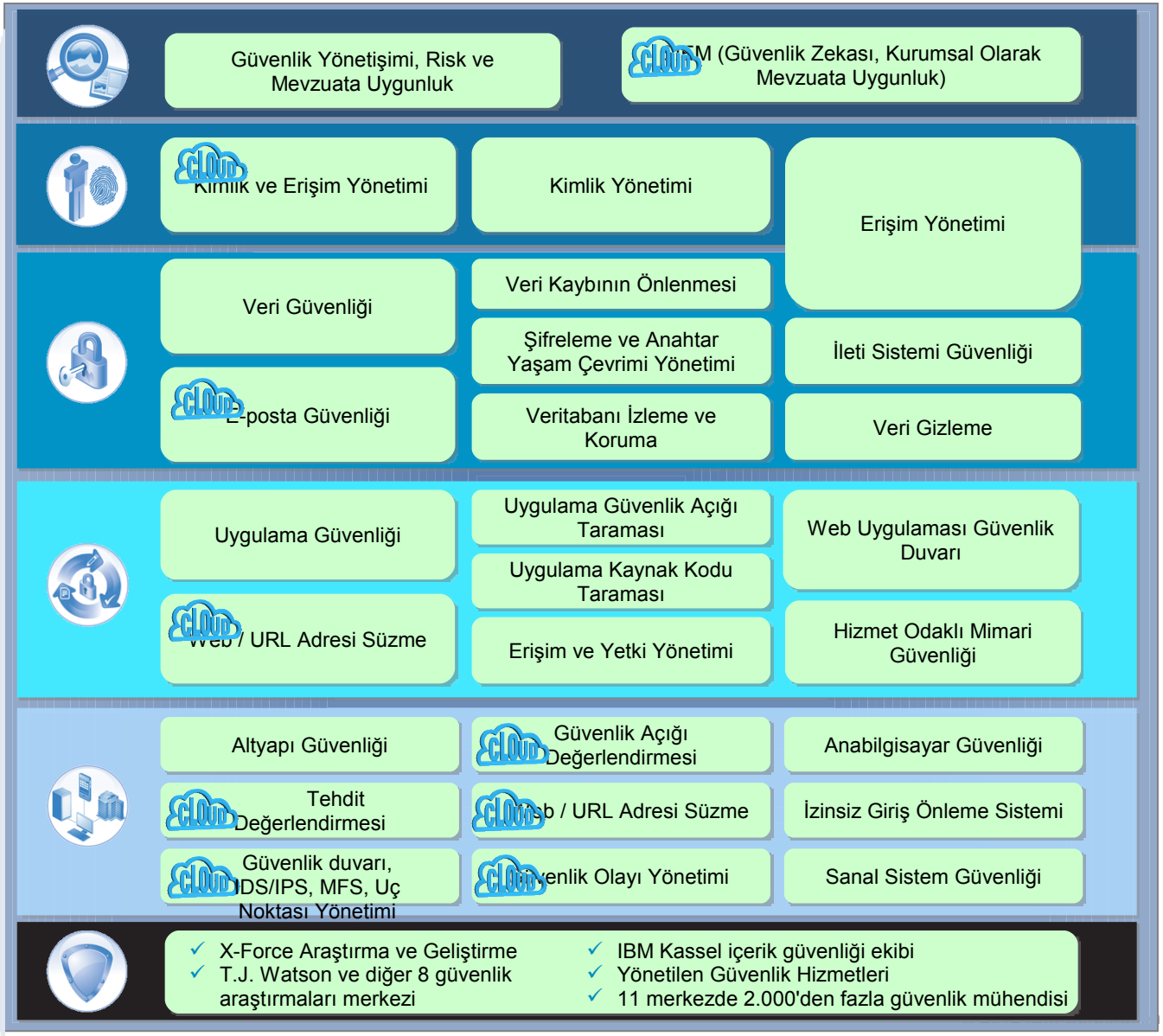
- Taramalarının İzlenmesi:
  - Milyonlarca Son Kullanıcı
  - Binlerce Müşteri
  - Yüzlerce Ülke
- Kötü Niyetli Bağlantıların Engellenmesi
- X-Force'a Bağlantılar Gönderilmesi

# IBM Güvenlik
## Zeka, Bütünleştirme ve Uzmanlık Sağlıyor

IBM Security Systems

= IBM'in hizmet verdiği alanlar



# Ağlarımıza kimler saldırıyor?

## Saldırgan Tipleri ve Yöntemleri 2011 Birinci Yarı

**Kullanıma Hazır** araçlar ve yöntemler

- Fark gözetmez
- Gelişmiş teknik becerilere sahip değildir
- İstismar araç takımı ve kötü niyetli yazılım seti kullanır
- Botnet geliştiricileri
- Finansal amaçlı kötü niyetli yazılım etkinliği
- İstenmeyen posta ve DoS

- Finansal amaçlı hedefli saldırılar
- DDoS saldırıları
- LulzSec ve Anonymous (aktivist bilgisayar korsanları)

**Gelişmiş**

- Siber Savaş

**Geniş Çaplı**

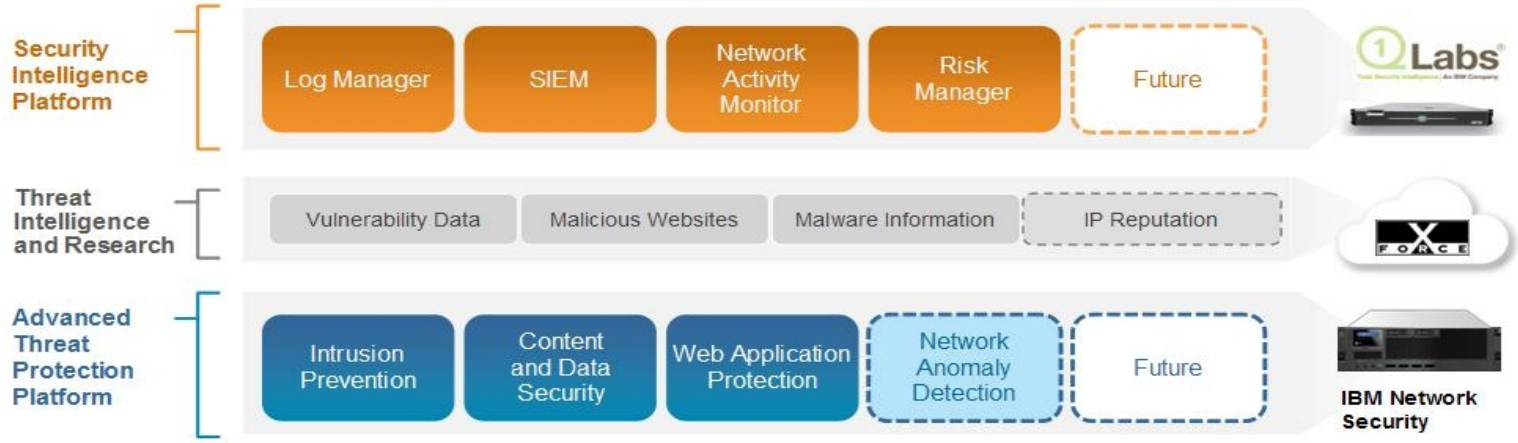
- Advanced Persistent Threat
- Organize, devlet destekli ekipler
- Yeni sıfır gün açıkları bulunması
- Benzeri görülmemiş saldırı yöntemleri

**Hedefli**

Kaynak: IBM X-Force® Araştırma ve Geliştirme

# IBM Security Network IPS ve “Hibrid Koruma”- IBM Gelişmiş Tehdit Koruma Platformu

- Web uygulaması güvenlik açıklarından Advanced Persistent Threat (APT) türü tehditlere kadar pek çok tehdide yanıt veren kapsamlı portföy




- Gerçek zamanlı tehdit bilgileri ve Güvenlik Zekasıyla birlikte geniş çeşitlilikteki ağ güvenliği yeteneklerinden yararlanarak olağandışı ağ davranışını saptamakta ve kapsamlı tehditlerden koruma sağlamaktadır.

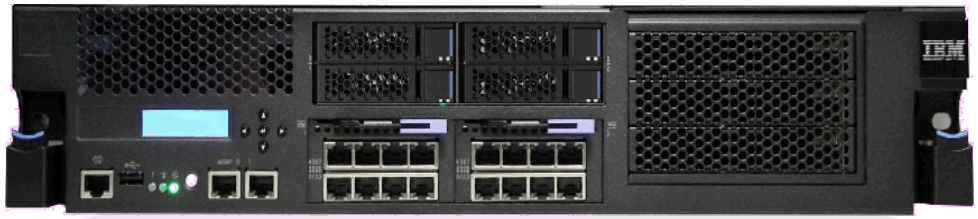
# IBM Security Network Protection XGS 5000

| KANITLANMIŞ GÜVENLİK | XGS İLE YENİLİKLER<br>MÜKEMMEL GÖRÜNEBİLİRLİK | XGS İLE YENİLİKLER<br>BÜTÜNLEŞİK KONTROL |
|---|---|---|
| 0-Day protection, X-Force® | Tüm network aktiviteleri için KİM, NE ve NE ZAMAN sorularının algılanması | Uygun uygulama ve network kontrolünden emin olunması |

IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements

# Kanıtlanmış Güvenlik: 0-Day Koruması Powered, X-Force®

- "Tehditin Önünde"
- Tam ve derinlemesine protokol ve uygulama incelemesi ile imzaların önüne geçme
- Şüpheli dosya ekleri ve web uygulama ataklarına karşı güvenlik



## IBM Security Network Protection XGS 5000

### IBM Security Threat Protection

- Vulnerability Modeling & Algorithms
- Stateful Packet Inspection
- Port Variability
- Port Assignment
- Port Following
- Protocol Tunneling
- Application Layer Pre-processing
- Shellcode Heuristics
- Context Field Analysis
- RFC Compliance
- Statistical Analysis
- TCP Reassembly & Flow Reassembly
- Host Response Analysis
- IPv6 Tunnel Analysis
- SIT Tunnel Analysis
- Port Probe Detection
- Pattern Matching
- Custom Signatures
- Injection Logic Engine

– X-Force®

– 15 yıldan fazla araştırma geliştirme

– Dünyanın en büyük hükümet ve ticari otoriteleri tarafında kabul görme

– Sadece imzalara bağlı kalmayan sistem

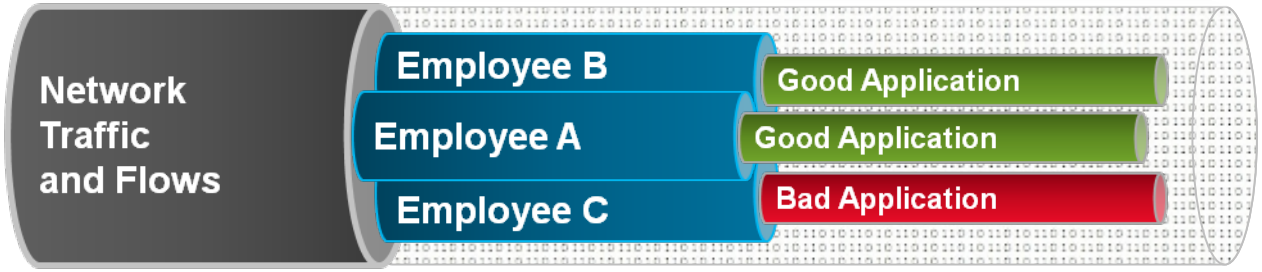
– Özelleştirilmiş Motorlar

- Exploit Payload Detection
- Web Application Protection
- Content and File Inspection

Bugünün ve yarının açıklarına karşı koruma yeteneği

# KİM, NE ve NE ZAMAN?

- Anlık hangi uygulamalara ve web sitelerine erişimin tespiti
- Hızlı bir şekilde uygulama, web sitesi, kullanıcı ve grupların amaç dışı kullanımının algılanması
- KİMİN NE KADAR band genişliğini kullandığının tespiti
- QRADAR ile entegrasyon




Network Flow Data (Ağ Akış verisi) ile gerçek zamanlı analiz ve korelasyon

Kullanıcı ve grupların ağ kullanımı, uygulama alışkanlıkları bilgilerinin gözlemlenmesi


Uygulama tanıma 1000+

Geliştirilmiş Güvenlik ● Düşük Maliyet ● Yenilikçiliği Destekler

# IBM Security Network IPS Yazılımının Yetenekleri

## Önemli Sorunlar

- Güvenlik ile iş açısından kritik uygulamaların performansının dengelenmesi
- Değişen tehditlerin sınırlı uzmanlık, kaynaklar ve bütçe ile çözülmesi
- Güvenlik altyapısı maliyetinin ve karmaşıklığının azaltılması
- Daha büyük kuruluşların, ağın merkezinde güvenliğe gereksinim duyması


## Temel Yetenekler

Geleneksel ağa izinsiz girişi önleme sisteminin ötesinde, aşağıdakiler dahil olmak üzere kapsamlı güvenlik sağlanması:

- Web uygulaması koruması
- İstemci tarafı saldırılarından koruma
- Veri Kaybının Önlenmesi
- Uygulama denetimi
- Virtual Patch Teknolojisi

Güvenliğin kalitesinden ve çeşitliliğinden taviz verilmeksizin 20 Gb/sn'nin üzerinde veri çıkışı ve 10 GbE bağlanırlık sağlayan rakipsiz performans

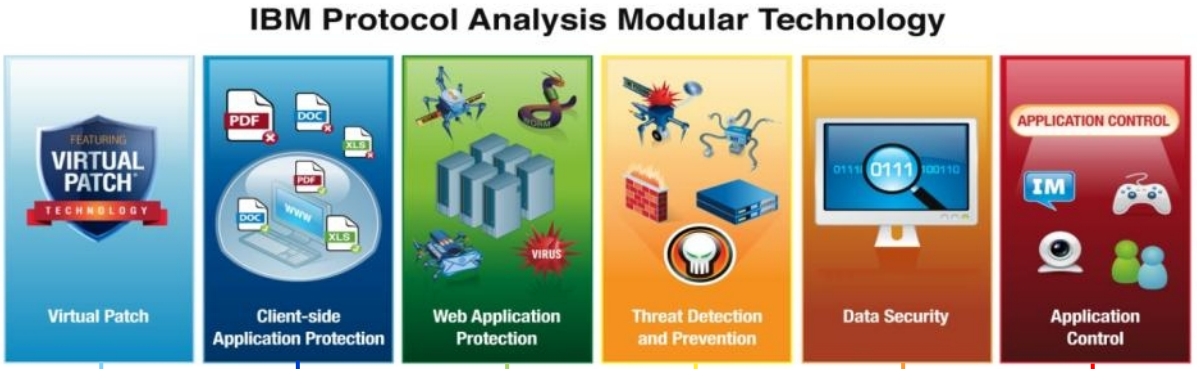
"Tehdidin ilerisinde" kalınması için gücünü dünyaca ünlü X-Force araştırmalarından alan sürekli gelişen koruma

Nokta çözümlerinin birleştirilmesi ve diğer güvenlik araçlarıyla bütünleştirme aracılığıyla daha düşük maliyet ve karmaşıklık

**IBM İletişim Kuralı Analizi Modüler Teknolojisi**

# Protokol Analiz Modulü ile Genişletilebilir koruma

X-Force veritabanın katkısı ile daha derin koruma




## Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2009, 52% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

## Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

## Web Application Protection

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

## Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

## Data Security

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy.

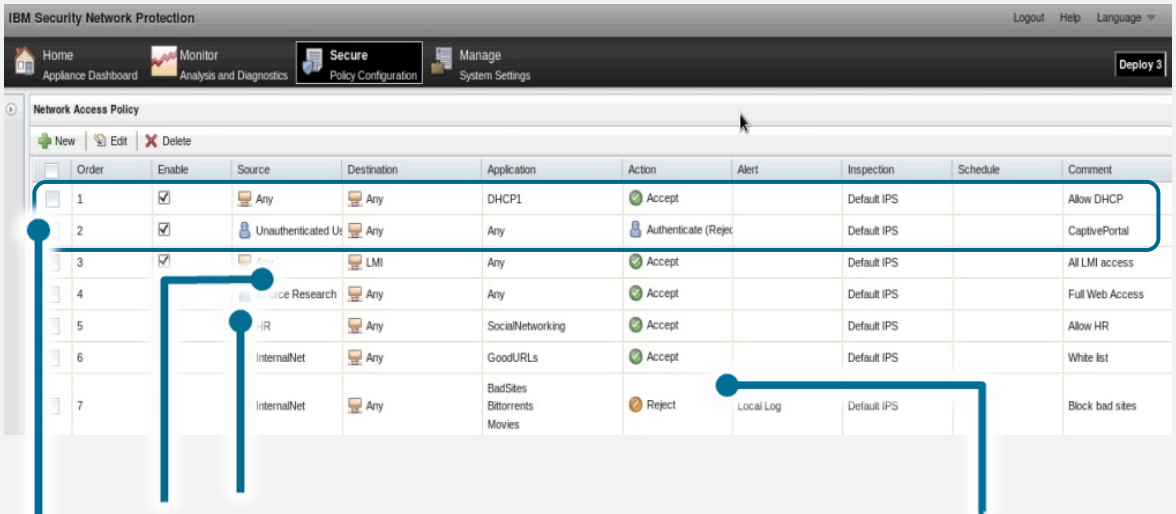
## Application Control

What It Does:
Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

# Tam Kontrol

- Ağ erişimi: Kullanıcı, grup, sistem, protokol ve uygulamaya göre
- Yüksek riskli sitelerin bloklanması ve Phishing, Malware gibi kategorilerin tanınması
- 16 Milyardan fazla URL
- 1000 den fazla uygulama ve onların faaliyetleri ile ilgili zengin destek



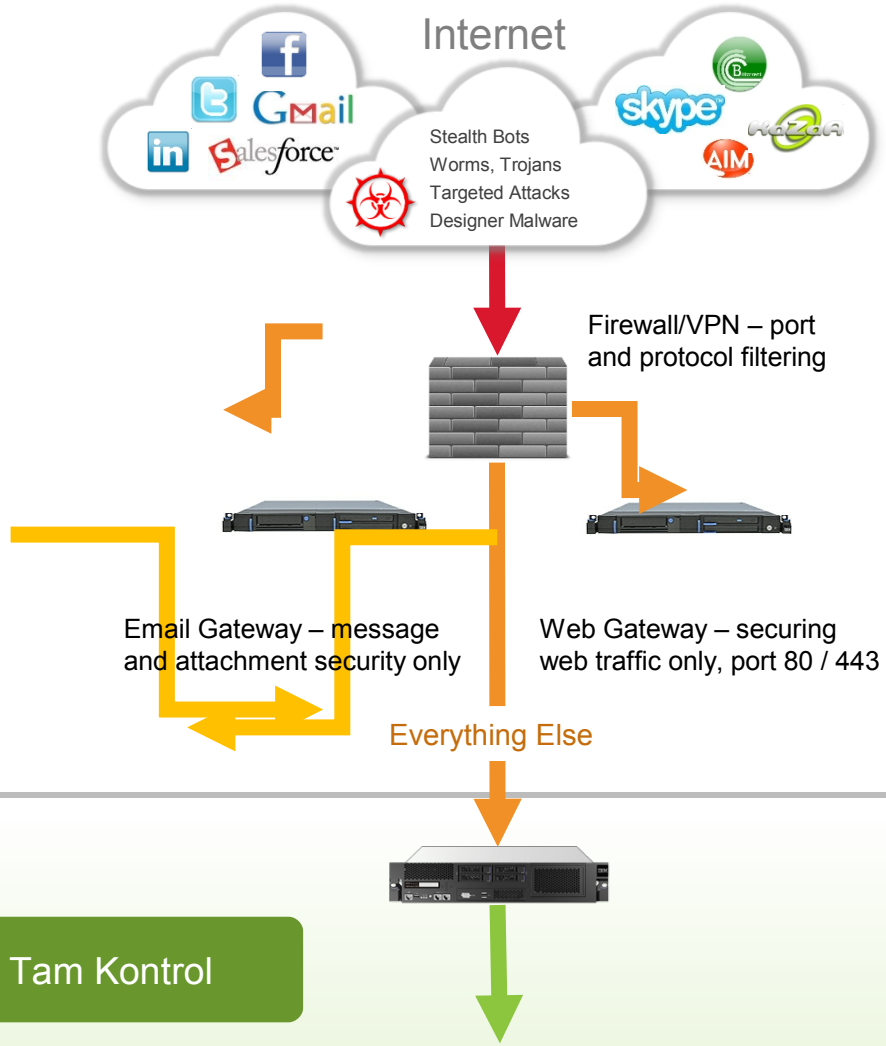
# The XGS 5000

## Daha iyi Network kontrolü

- Firewall ve VPN için tamamlayıcı destek
- Var olan sisteminizi etkilemeden herhangi birşeyi değiştirmeden entegrasyon
- Derinlemesine güvenlik ve kontrol

## Daha iyi Güvenlik Koruması

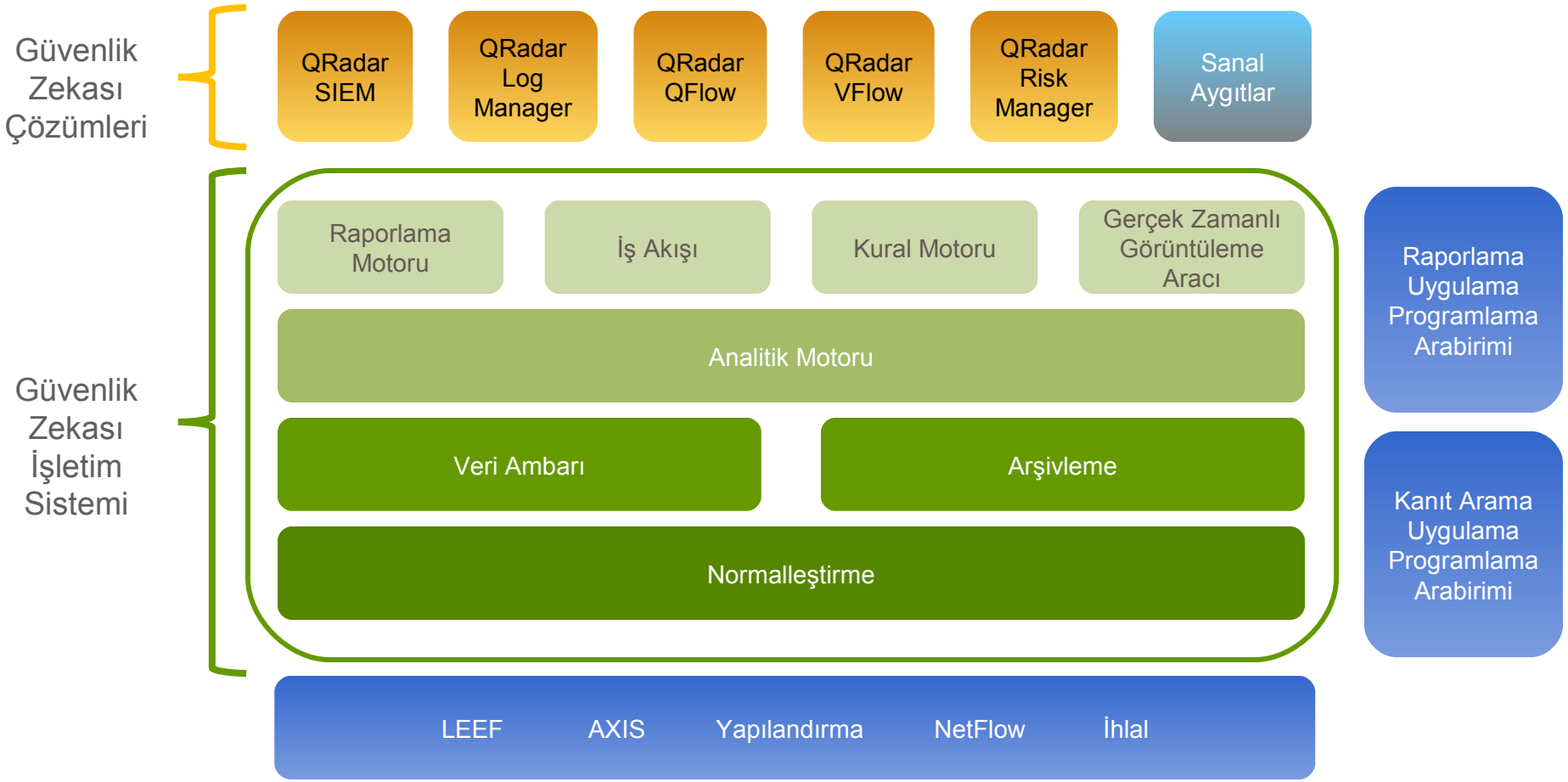
- Gerçek protokol tanımlaması ve farkındalığı
- Zero-day ataklarına karşı daha etkin koruma
- SNORT tabanlı özelleştirilmiş imza verisi




## IBM Security Network Protection XGS 5000

Kanıtlanmış Güvenlik | Gerçek Görünürlük | Tam Kontrol

# QRadar Ürün Ailesi: Ortak Bir Temel Üzerine Kurulmuştur




Zeki, Bütünleştirilmiş, Otomatikleştirilmiş - Tek Konsolla Güvenlik

# 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? |
|---|---|---|---|


Risk Yönetimi - Mevzuata Uygunluk Yönetimi
Güvenlik Açığı Yönetimi - Yapılandırma İzleme

Güvenlik Bilgisi ve Olayı Yönetimi - Anormal Ağ Davranışı Algılama
Günlük Yönetimi - Veri Kaybı Algılama
Paket Delili Arama - İyileştirme - Gösterge Panoları

# *Zeki:* Bağlam ve İlişkilendirme ile En Derinlemesine İş Kavrayışını Sağlar



Kaynaklar + Zeka = En Doğru ve Etkinliğe Dönüştürülebilir İş Kavrayışı

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation


Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

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

# *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

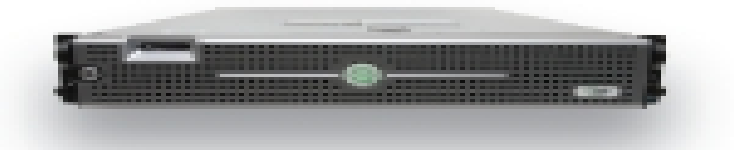
- Yüksek düzeyde ölçeklenebilir
- Ortak raporlama ve arama
- Dağıtılmış ilişkilendirme
- Birleşik yönetim
- Tek kopya olarak saklanan günlükler
  - ➢ *Tam görüş netliği*

Bolted together vs Integrated

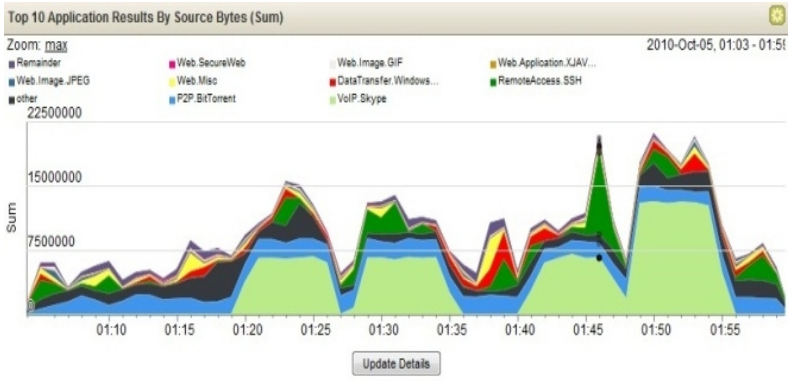
# QRadar Network Anomaly Detection

- QRadar Network Anomaly Detection IBM'in Atak Önleme portfolyosu için Qradar ürününün özel versiyonu

- Qradar'ın davranış analitiği ve gerçek zamanlı korelasyonu

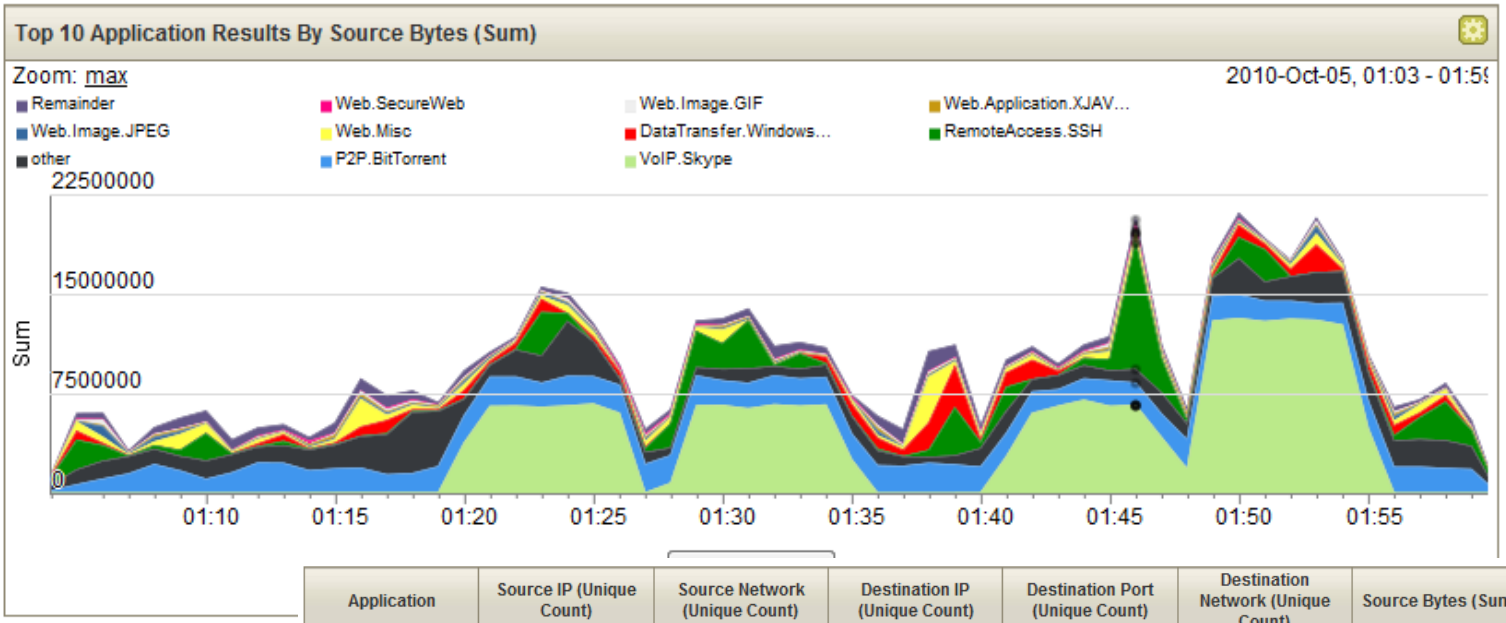


- IBM Security Network Protection ile entegrasyon



# Akış analitiği ve Anamoli Tespiti

- Ağ trafiği yalan söylemez!
- Atak yapan parmak izlerini silebilir fakat network akışını kesemez.
- Zero- day Ataklarının tayini için imzasız yapı
- Kesin kanıt sunabilmeTüm atak iletişimini gözlemleyebilme

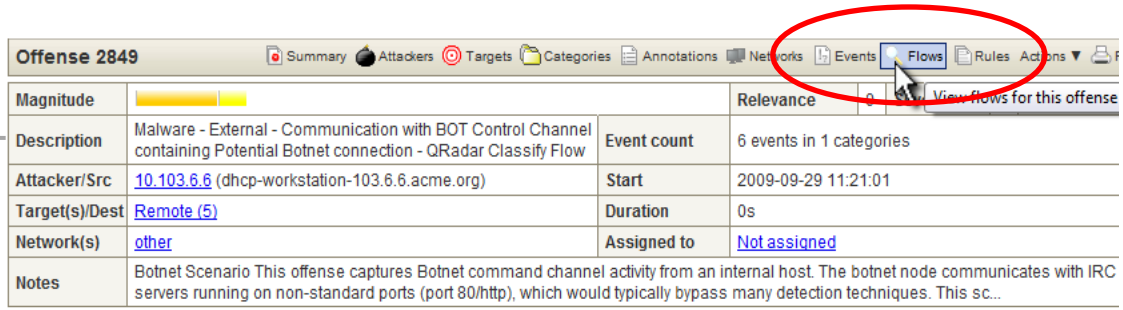



| Application | Source IP (Unique Count) | Source Network (Unique Count) | Destination IP (Unique Count) | Destination Port (Unique Count) | Destination Network (Unique Count) | Source Bytes (Sum) | Destination Bytes (Sum) |
|---|---|---|---|---|---|---|---|
| DataTransfer.Window | Multiple (24) | Multiple (7) | Multiple (13) | Multiple (2) | Multiple (7) | 16 319 315 | 531 531 708 |
| P2P.BitTorrent | Multiple (20) | Multiple (5) | Multiple (85) | Multiple (60) | Multiple (3) | 44 216 868 | 191 621 654 |
| other | Multiple (259) | Multiple (9) | Multiple (3 063) | Multiple (2 877) | Multiple (10) | 37 349 699 | 168 802 101 |
| VoIP.Skype | Multiple (5) | Multiple (4) | Multiple (40) | Multiple (40) | other | 131 172 458 | 46 819 290 |
| RemoteAccess.SSH | Multiple (10) | Multiple (5) | Multiple (7) | 22 | Multiple (4) | 37 885 116 | 111 228 020 |
| Web.Misc | Multiple (16) | Multiple (5) | Multiple (295) | 80 | other | 10 726 080 | 20 635 741 |
| Web.Application.Misc | Multiple (9) | Multiple (4) | Multiple (31) | 80 | other | 654 743 | 23 125 267 |
| Web.Image.JPEG | Multiple (13) | Multiple (4) | Multiple (60) | 80 | other | 2 418 857 | 18 538 204 |

# Hırsızlık Atak Tespiti

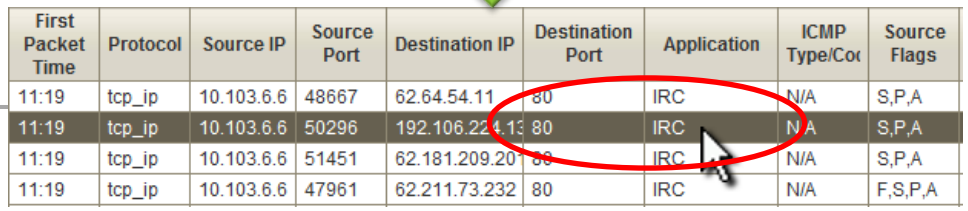
Potensiyel Botnet Tespiti?

Birçok çözümün gidebildiği son nokta!



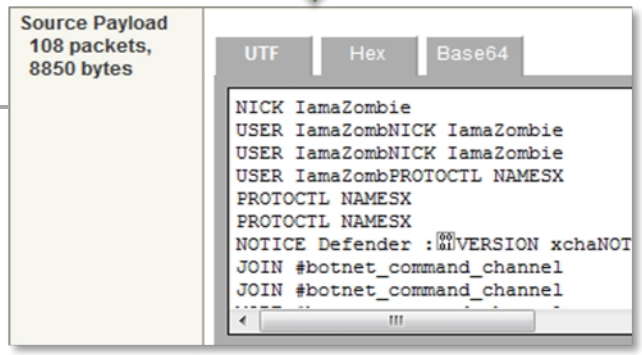

IRC --> port 80?

IBM Security QRadar QFlow Kanalın tespit edilmesi



| First Packet Time | Protocol | Source IP | Source Port | Destination IP | Destination Port | Application | ICMP Type/Co | Source Flags |
|---|---|---|---|---|---|---|---|---|
| 11:19 | tcp_ip | 10.103.6.6 | 48667 | 62.64.54.11 | 80 | IRC | N/A | S,P,A |
| 11:19 | tcp_ip | 10.103.6.6 | 50296 | 192.106.224.13 | 80 | IRC | N/A | S,P,A |
| 11:19 | tcp_ip | 10.103.6.6 | 51451 | 62.181.209.20 | 80 | IRC | N/A | S,P,A |
| 11:19 | tcp_ip | 10.103.6.6 | 47961 | 62.211.73.232 | 80 | IRC | N/A | F,S,P,A |

Layer 7 akış verisinin yardımı ile komut tespiti




Application layer (Uygulama Katmanı) akış analizi ile derinlemesine tespit

# Örnek: Atak Algılama

**Offense 3063** Summary | Attackers | Targets | Categories | Annotations | Networks | Events

| | | | |
|---|---|---|---|
| Magnitude | | Relevance | 3 |
| Description | Target Vulnerable to Detected Exploit<br>preceded by Exploit Attempt Proceeded by Recon<br>preceded by Exploit/Malware Events Across Multiple Targets<br>preceded by Recon - External - Potential Network Scan | Event count | 1428 events in 3 cate |
| Attacker/Src | 202.153.48.66 | Start | 2009-09-29 16:05:01 |
| Target(s)/Dest | Local (717) | Duration | 1m 32s |
| Network(s) | Multiple (3) | Assigned to | Not assigned |
| Notes | Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I<br>China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s | | |

## Sounds Nasty…

But how do we know this?

The evidence is a single click away.

## Network Scan

Detected by QFlow

## Buffer Overflow

Exploit attempt seen by Snort

| | Event Name | Source IP | Destination IP | Destination Port | Log Source | Low Level Category |
|---|---|---|---|---|---|---|
| | Network Sweep - QRadar Classify Flow | 202.153.48.66 | Multiple (716) | 445 | Flow Classification E | Network Sweep |
| | NETBIOS-DG SMB v4 srvsvc NetrpPathConon | 202.153.48.66 | Multiple (8) | 445 | Snort @ 10.1.1.5 | Buffer Overflow |

| Port | Service | OSVDB ID | Name | Description | Risk / Severity |
|---|---|---|---|---|---|
| 445 | unknown | 49243 | Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution | Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity. | 3 |

## Targeted Host Vulnerable

Detected by Nessus

**Total Security Intelligence:**
**Convergence of Network, Event and Vulnerability data**

# TEŞEKKÜRLER ...

IBM Security Systems

ibm.com/security