IBM Internet Security Systems

# Tehdit Önleme Sistemleri

## Tivoli Internet Security Systems

**Aytuğ Çelikbaş** – *IT Security Specialist, CEE*
*IBM Tivoli Internet Security Systems*

Tivoli IBM Internet Security Systems

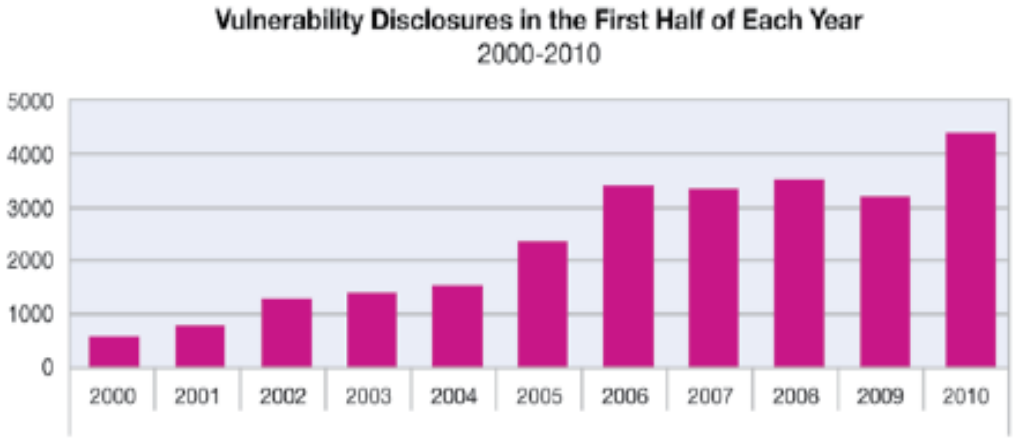
# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

# Üreticiler Öncesine Göre Çok Daha Fazla Güvenlik Açığı Raporluyorlar:

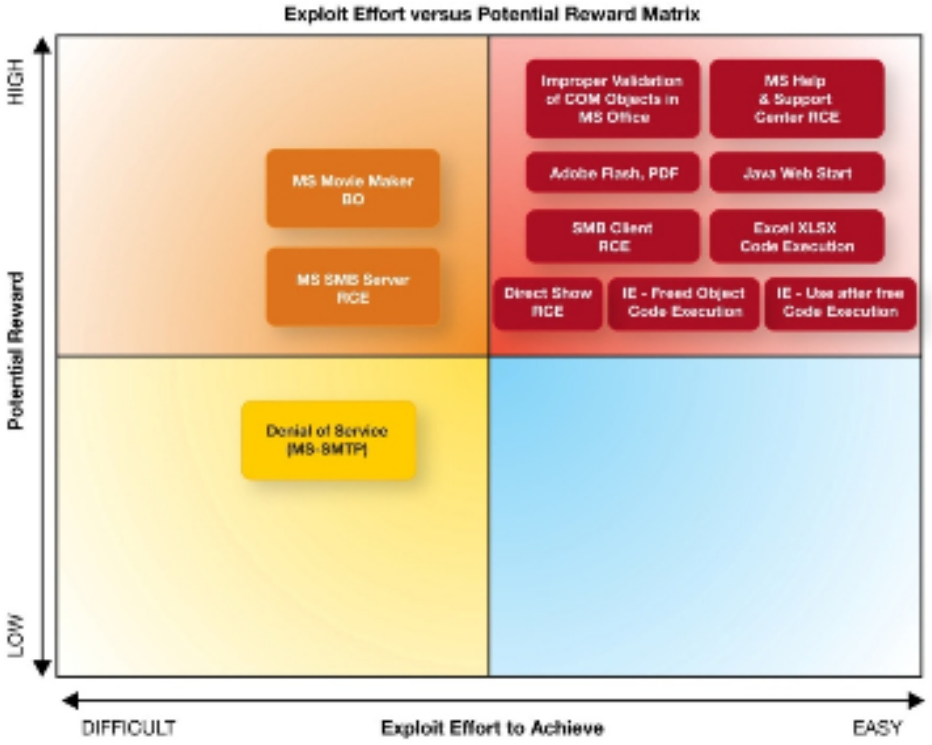
## *Tarihin En Yüksek Değerlerindeki Güvenlik Açık Sayısı*

- Güvenlik açıkları bir önceki yıla göre **36% artış göstermiş durumda.**
  - Web uygulamaları güvenlik açıklarındaki en yüksek kategoriyi oluşturmaya devam ediyor.
- Güvenlik açıklarından yararlanabilen zararlı kodların kamuyuna açık şekilde paylaşılması güvenlik açıklarının sayısının ciddi şekilde artış göstermesinde etkili.
- 2010 yılının ilk yarısında bulunan en kritik iki güvenlik açığı, ***Java Web Start*** ve ***Microsoft Windows Help and Support Center***'da bulunan uzaktan kod çalıştırılabilmesine olanak tanıyan açıklardı.
  - İki güvenlik açığı da üreticisi tarafından yamaları yayınlanmadan internet sitelerinde yayınlanmıştı.



# Açıktan Yararlanmak İçin Harcanan Efor vs. Potensiyel Kazanç

- Güvenlik açıklarından yararlanma denemelerinde ekonomik getiri hala en büyük paya sahip.
- Web Tarayıcıları, Doküman Okuyucular (PDF vb.) ve Ofis Dökümanlarında bulunan güvenlik açıkları, saldırganlar için kolay çalıştırılabilir ve geri kazanımları çok yüksek yazılımlar olarak karşımıza çıkıyor.




Source: IBM X-Force®

# Güvenlik Açıklarının Yarısı Hala Bir Yamaya Sahip Değil!

- 2010 yılının ilk yarısında duyurulan tüm güvenlik açıklarının yarısından fazlası (**55%**) hala üreticisi tarafından yayınlanmış bir yamaya sahip değil. Kritik ve yüksek önem derecesine sahip açıkların **71%'nin hala bir yaması yayınlanmamış durumda**.

| Operating System | Percentage of Critical and High | Percentage of all OS Vulnerabilities |
|---|---|---|
| Microsoft | 73% | 27% |
| Apple | 9% | 29% |
| Linux | 16% | 31% |
| HP-UX | 2% | 1% |
| Sun Solaris | 0% | 4% |
| BSD | 0% | 4% |
| IBM AIX | 0% | 2% |
| Others | 2% | 4% |

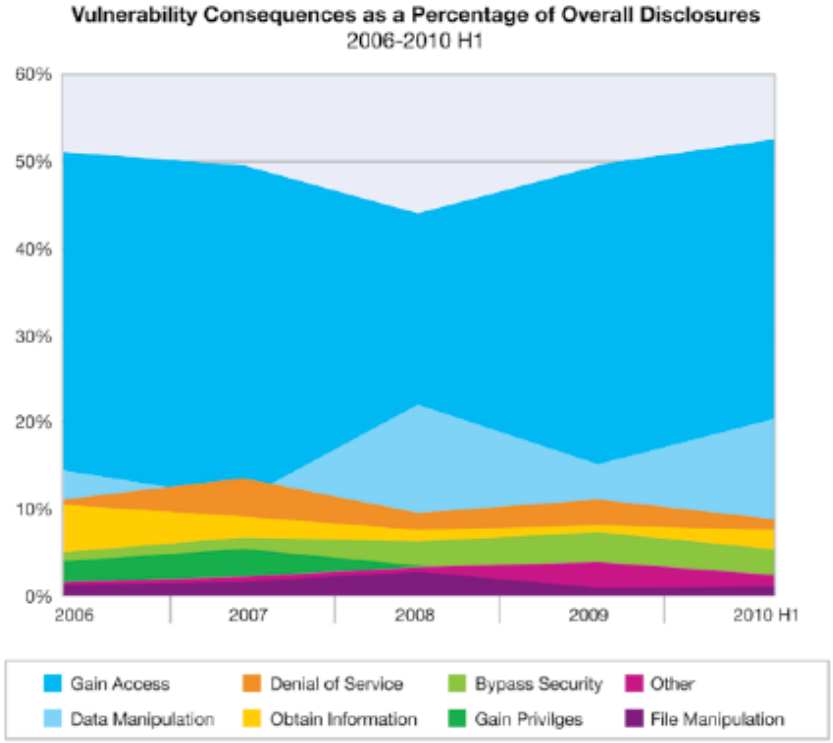
*Table 9:* Operating systems with the most critical and high vulnerability disclosures, 2010 H1.

- En popüler 5 işletim sistemi, tüm kritik ve yüksek önem derecesine sahip güvenlik açıklarının **98%**'ini oluşturuyor.
- En popüler 5 işletim sistemi tüm açıklarının **95%** kapsıyor.

| Vendor | Percent of 2010 H1 Disclosures with No Patch | Percent of Critical & High 2010 H1 Disclosures with No Patch |
|---|---|---|
| All Vendors - 2010 H1 Average | 55% | 71% |
| Microsoft | 23% | 7% |
| Mozilla | 17% | 4% |
| Apple | 12% | 0% |
| IBM | 9% | 29% |
| Sun | 8% | 0% |
| Oracle | 7% | 22% |
| Cisco | 6% | 2% |
| Novell | 5% | 10% |
| HP | 4% | 5% |
| Linux | 3% | 0% |
| Adobe | 3% | 2% |
| Google | 0% | 0% |

# Saldırganların Motivasyonu Erişim Elde Etmek ve Veriyi Manupile Etmek

- "*Erişim Elde Etmek*" güvenlik açığından yararlanmanın birinci sonucu olmaya devam ediyor.
  - Bu değer geçen yıl %50 iken bu yılın ilk yarısında **52%** değerine çıktığı görülüyor.
- "*Veriyi Manupile Etmek*" artış göstermekte.
  - Bu yılın ilk yarısında bu değer **21%** 'e çıkmış durumda.
- "*Güvenliği Bypass Etmek*" ve "*Servis Engelleme*" geçen yılın değerleri ile aynı.



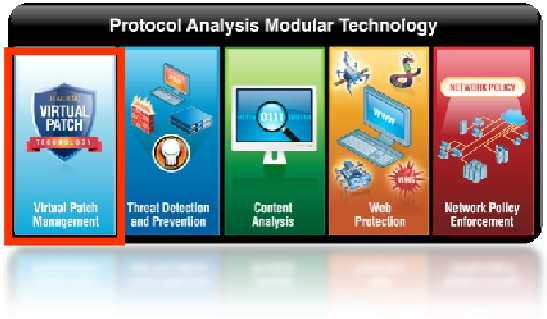

**Sorulması gereken sorular:**
- Bir saldırganın sistemlerinize erişmediğinden ne kadar eminsiniz?
- Kritik bilgileriniz yeterince güvende mi?

**IBM Güvenlik Çözümleri:**
- IBM Tivoli Identity & Access Management Products & Services
- IBM Security Network, Server and Endpoint Prevention products and services
- IBM Web Application Security Products & Services (Rational, IBM Security Network IPS, Data Power, MSS)
- IBM Data Security products and services (Guardium, Big Fix, MSS)

# Sanal Yama Teknolojisi

## *IBM Virtual Patch® Technology*

- Bir güvenlik açığından yararlanılmasını yazılım yamasından bağımsız olarak engeller.
- Yama yönetimi süreçlerinin, tehditlerden etkilenmeden sürdürülmesine yardımcı olur.
- IBM, Microsoft Aktif Koruma Programı (MAPP) iş ortağıdır.




# X-Force Araştırma ve Geliştirme Ekibi

## *Benzersiz Güvenlik Öncüsü*

**IBM X-Force® araştırma ve geliştirme ekibinin amacı:**

- Tehditlerin araştırılarak bulunması ve karşı koruma sistemlerinin geliştirlmesi
- Bugünün güvenlik problemlerine karşı güvenlik çözümleri üretmesi
- Yarının güvenlik tehditleri için yeni teknolojiler üretilmesi
- Medya ve kamuoyunun bilinçlendirlmesi

X-Force Araştıma

10 Milyar Web sayfası analizi

150 Milyon Günlük saldırı denemesi

40 Milyon Spam & Phishing saldırısı

51 Bin Dökümante edilmiş güvenlik açığı veritabanı

Milyonlarca zararlı kod örneği

# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

# Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları (GX-V2)
## Yeni Donanımlar - Mart 2010
## (Yenilenmiş Performans)

- **GX4004-V2**
- **GX5008-V2**
- **GX5108-V2**
- **GX5208-V2**
- **GX7000 (Bütünleşik 10GB+)**

- Çok çekirdekli işlemciler
- Yeni jenerasyon donanımlar
- İçerik analizi performans artışı
- Önemli fiyat/performans iyileştirmesi
- 64 Bit Protokol Analiz Modülü

# Ağ Tabanlı Saldırı Tespit/Önleme Cihazlarının Performansları

## Benzersiz ağ güvenliği sağlar

Ağ üzerinde transparan, trafiği üzerinden geçirecek şekilde çalışarak tehditlerin sistemlere ulaşmadan gerçek zamanlı engellenmesini sağlar.

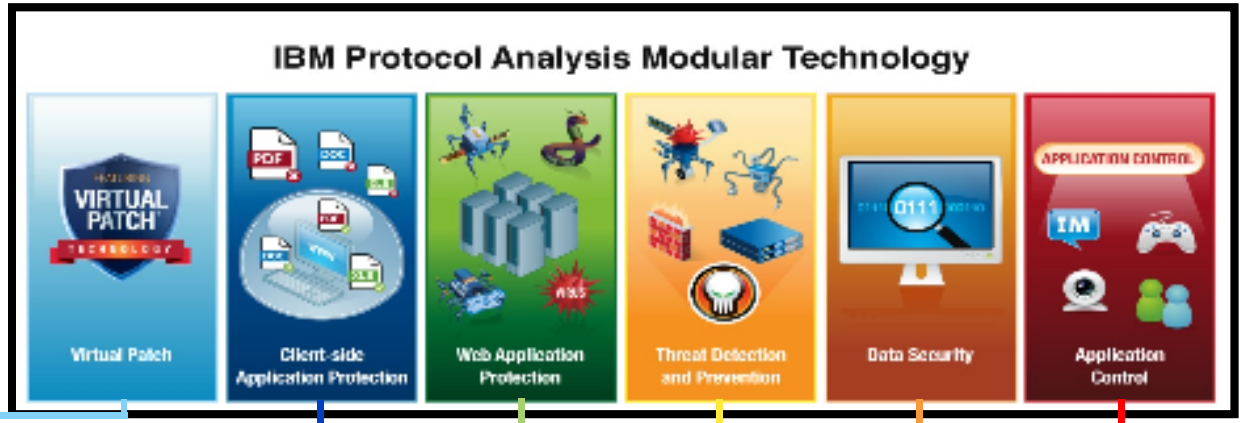
- Geniş ürün yelpazesine sahiptir:
  - 8 Gbps'e kadar analiz değerlerine sahip
  - Tek bir cihazda 8 ağ segmentine kadar koruma sağlar

- Yeni tanıtılan donanım artışı aşagıdaki özellikleri içermektedir.
  - İki kat performans & Güvenlik modülleri için ek performans – veri güvenliği, web uyulama koruması
  - 64 bit işlemciler
  - Arttırılmış bellek
  - Yenilenmiş daha hızlı anakart

| IBM Security Network IPS Hız Metrikleri | | | | | |
|---|---|---|---|---|---|
| | Çevresel | | | Merkez | |
| **Model** | **GX4004-V2** | **GX5008-V2** | **GX5108-V2** | **GX5208-V2** | **GX6116** |
| **Analiz Hız Değerleri** | **800 Mbps** | **1.5 Gbps** | **2.5 Gbps** | **4 Gbps** | **8 Gbps** |
| **Korunan Segment Sayısı** | **2** | **4** | **4** | **4** | **8** |

# Ürünlerimizin Arkasındaki Koruma Motoru “Protokol Analiz Modülü”

**IBM X-Force ekibi tarafından geliştirilen genişleyebilir koruma yapısı ile benzersiz saldırı önleme özellikleri sunar**




## Sanal Yama

**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.

## Kullanıcı Uygulama Güvenliği

**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 Uygulama Koruması

**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.

## Tehdit Tespiti ve Engellenmesi

**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.

## Veri Güvenliği

**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.

## Uygulama Kontrolü

**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.

# IBM Ağ Tabanlı Saldırı Tespit/Önleme Cihazlarının Analizi

| Nasıl Çalışır? |
| --- |
| Network trafiğinin derin analizi |
| 200'den fazla ağ ve uygulama protokolünü tanımlar ve analiz eder. |

| What it Prevents | |
| --- | --- |
| Worms | Spyware |
| P2P | DoS/DDoS |
| Cross-site Scripting | SQL Injection |
| Buffer Overflow | Web Directory Traversal |

| **Protokol Analiz Modülü** (PAM) | |
| --- | --- |
| Vulnerability Modeling & Algorithms | RFC Compliance |
| Stateful Packet Inspection | TCP Reassembly & Flow Reassembly |
| Protocol Anomaly Detection | Statistical Analysis |
| Port Variability | Host Response |
| Port Assignment | IPv6 Native Traffic Analysis |
| Port Following | IPv6 Tunnel Analysis |
| Protocol Tunneling | SIT Tunnel Analysis |
| Application-Layer Pre-Processing | Port Probe Detection |
| Shellcode Heuristics | Pattern Matching |
| Context Field Analysis | Custom Signatures |
| IBM Security Content Analyzer | Injection Logic Engine |

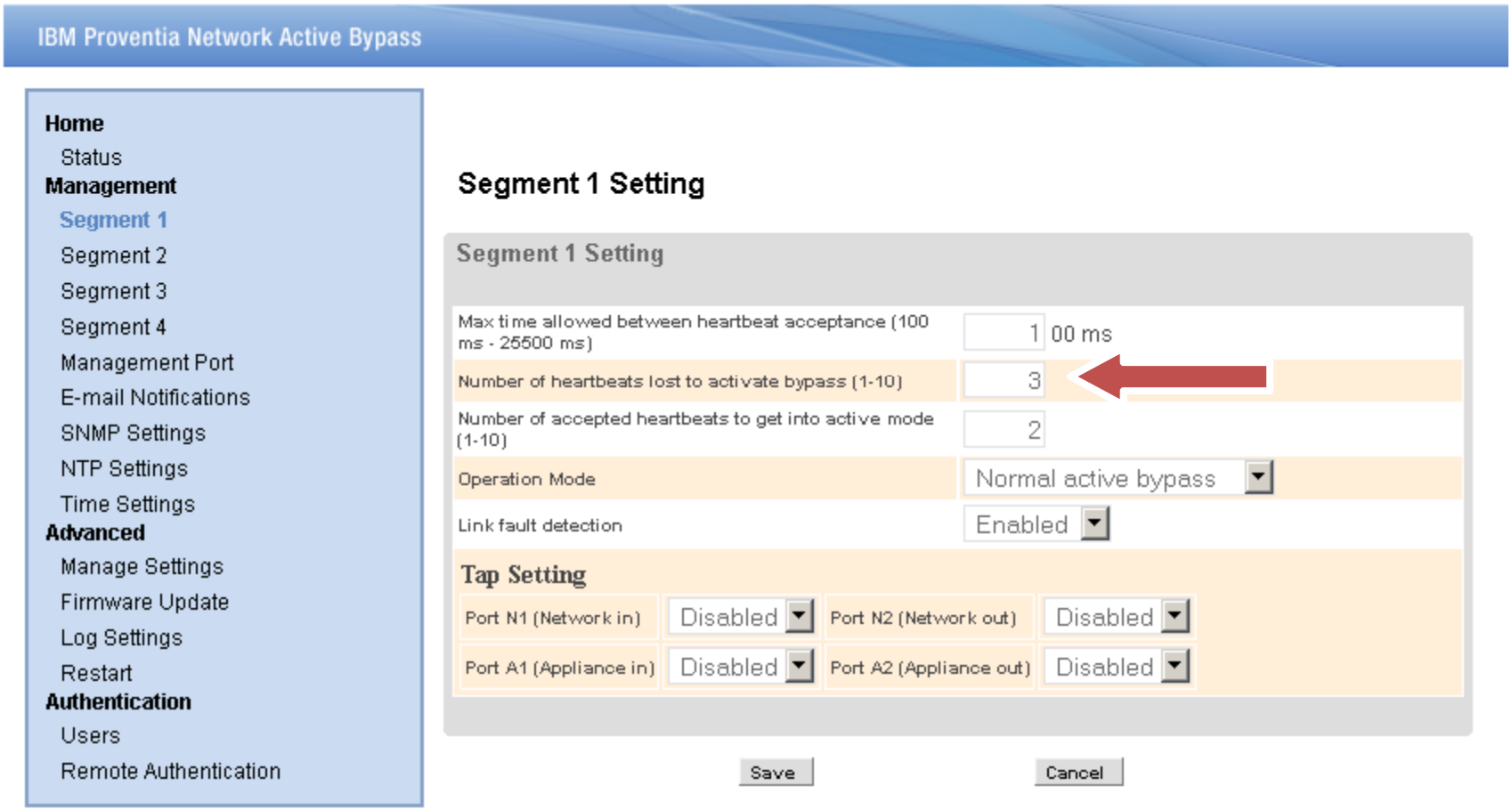
# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

# IBM Aktif Bypass Cihazları

- Kesintileri minimuma indirerek, ağ sürekliliğini maksimum seviyeye yükseltir.
- Hat durumunu bağlantı durum sinyalleri(*link state*) ile sağlar.
- Her segment için ayrı ayrı konfigüre edilebilir.
- SNMP ve E-mail desteği ile hata arama sürelerini kısaltır.
- Dört ağ segmentine kadar tüm kombinasyonları destekler: Bakır, Uzun Fiber ve Kısa Fiber.
- Basit konfigürasyon ile tak çalıştır özelliği
- Yedekli güç kaynağı – Güç kesintisi durumunda düz kablo görevi görme özelliği

# Konfigüre Edilebilir Kullanıcı Arabirimi



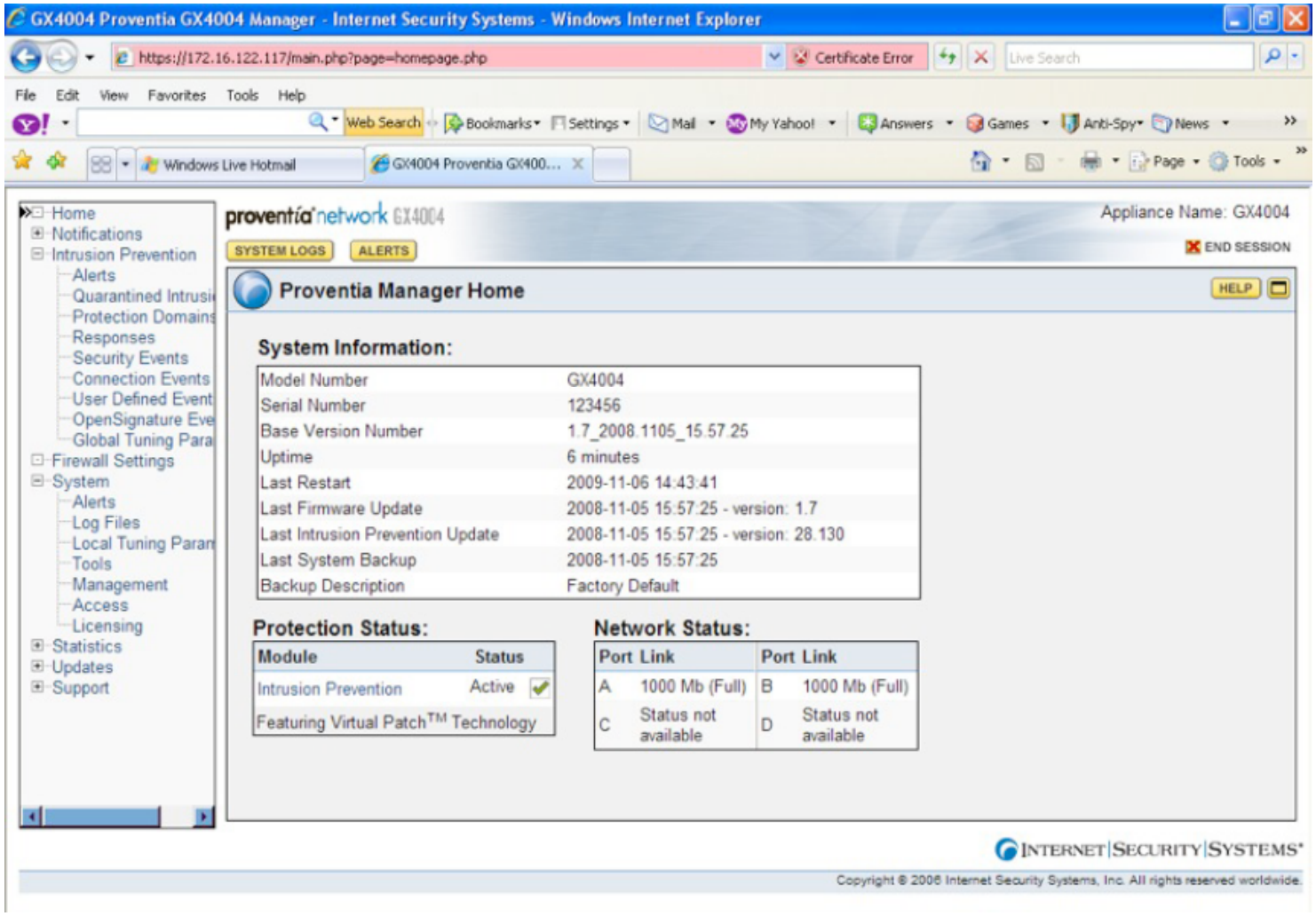
# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

- Kullanılabilirlik...
  - İçerik Analiz Politikaları (LMI)
  - Web Uygulamarı Politikaları (LMI)
  - Yama Yönetimi Politikaları (LMI)
  - Cihaz Durum İstatistikleri (LMI)
  - Koruma İstatistikleri (LMI)
  - Ağ Kullanım İstatistikleri(LMI)
  - Lokal Kullanım İstatistikleri(LMI)
  - Log Kanıt(LMI)
- Yeni Özellikler
  - Rational AppScan entegrasyonu
  - Gerçek zamanlı atak bloklama
  - Rol tabanlı erişim kontolü
  - Radius /LDAP/AD  Entegrasyonu
  - Tam IPv6 destekli IPS
  - Açık Kaynak Kodlu Atak İmzaları
- Performans:
  - Protokol Analiz Modülü 2.0

***10 Haziran 2010***

# Kullanılabilirlik: Eski Arabirim



# Kullanılabilirlik: Yeni Arabirim

# Yeni Web Tabanlı Konfigürasyon

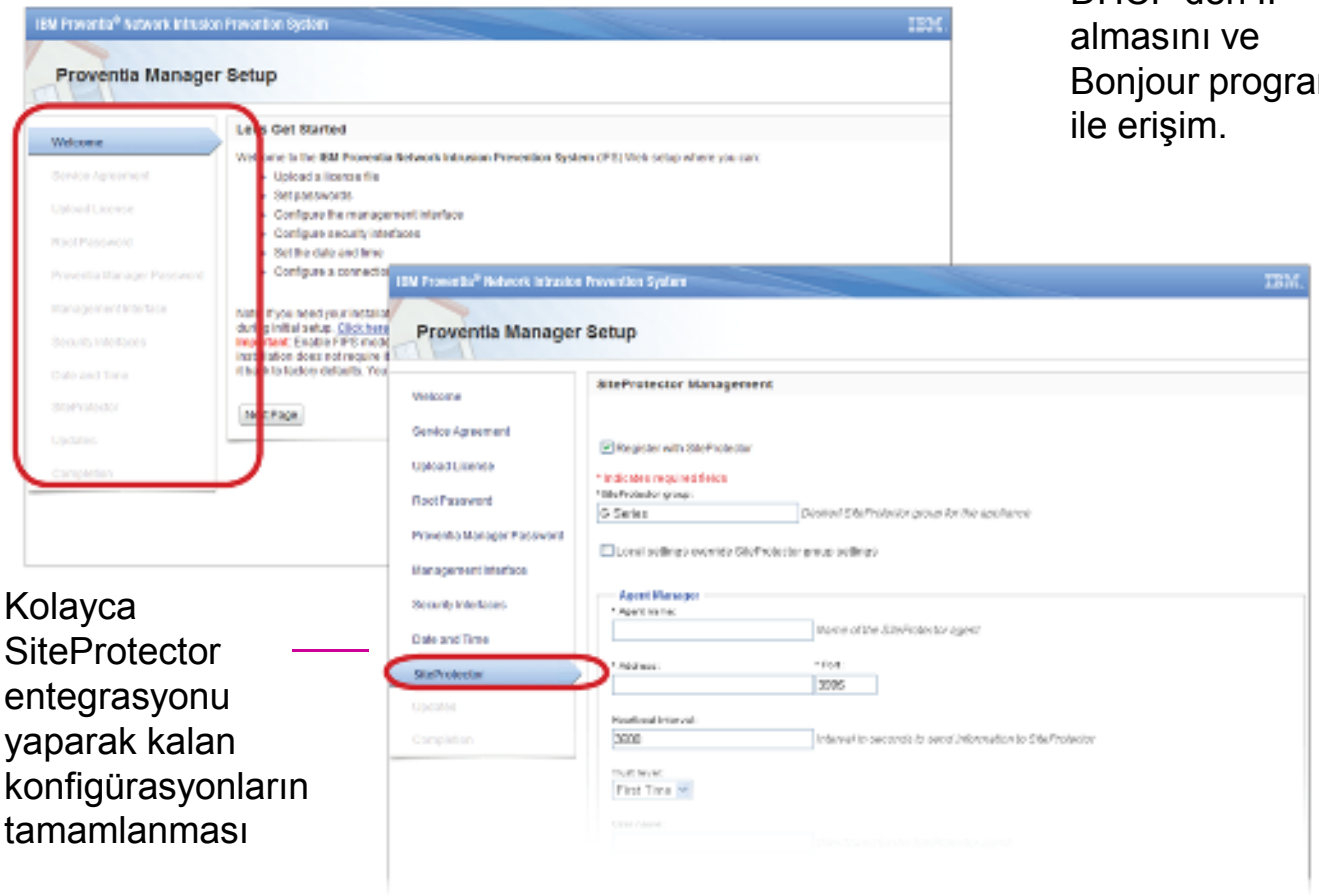
Streamlined Set Up

Cihazı ağa bağlayarak DHCP'den IP almasını ve Bonjour programı ile erişim.

Cihazın ilk konfigürasyonu komut satırı yerine web tarayıcısı kullanarak yapılabilir.

Başlangıç kurulum menüsünü kullanarak – Cihazın çalışması için gereken minimum ayarların konfigüre edilmesi

Konfigürasyon aşamasının adımlarında navigasyon imkanı




Kolayca SiteProtector entegrasyonu yaparak kalan konfigürasyonların tamamlanması

Updated Console Configuration

Güncellenmiş konsol tabanlı başlangıç kurulumu interaktiviteyi arttırarak kurulumu kolaylaştırmaktadır.

# Yeniden Tasarlanmış Proventia Manager Arayüzü

Aerodinamik organizasyon, geliştirilmiş görev akışları ve genişletilmiş uyumluluk

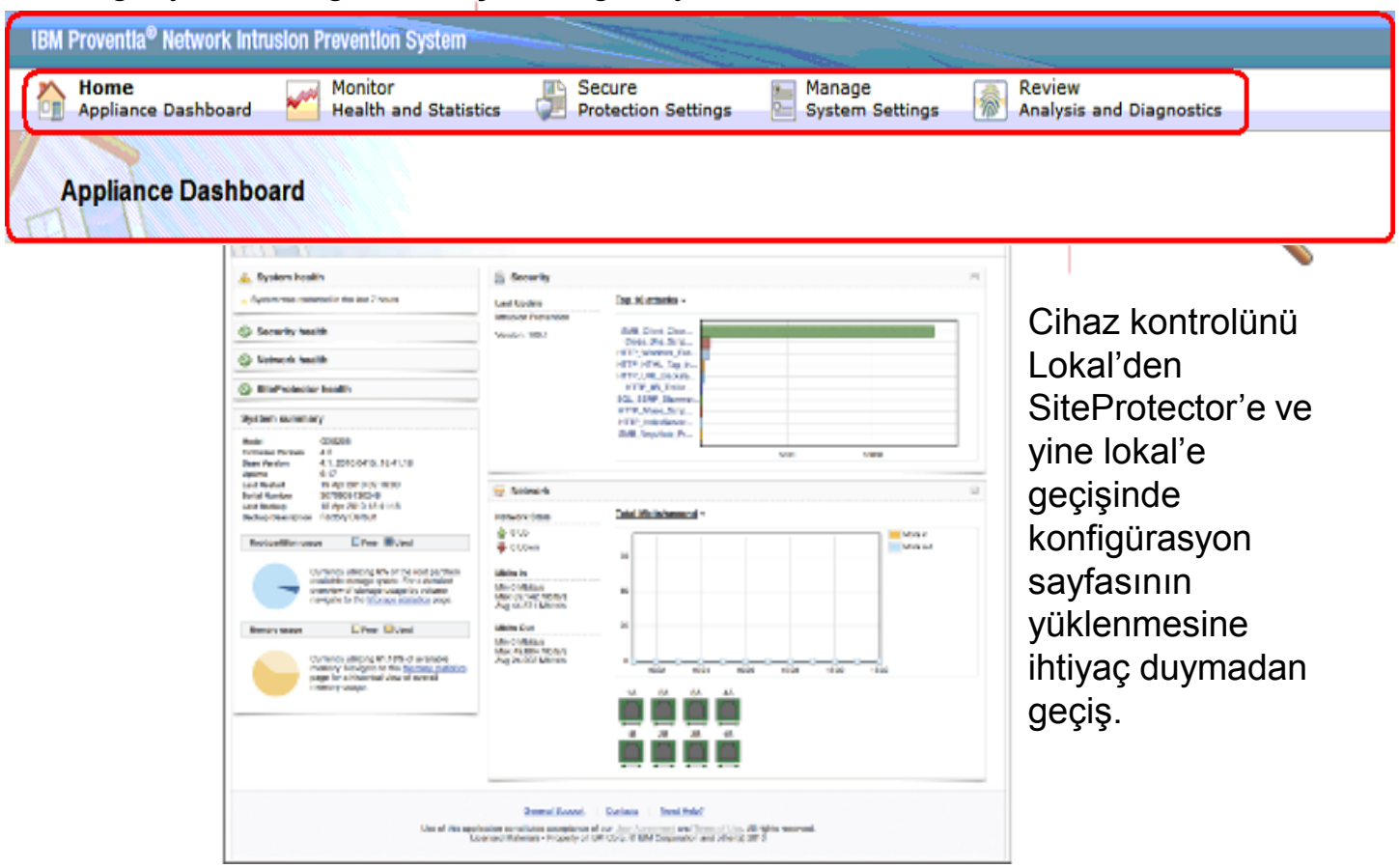
Navigasyon ortak görev akışlarına göre yeniden tasarlandı.

**Improved Navigation**

İleri, geri, yenileme gibi web tarayıcısı özelliklerinin kullanımı

**Additional Browser Compatability**

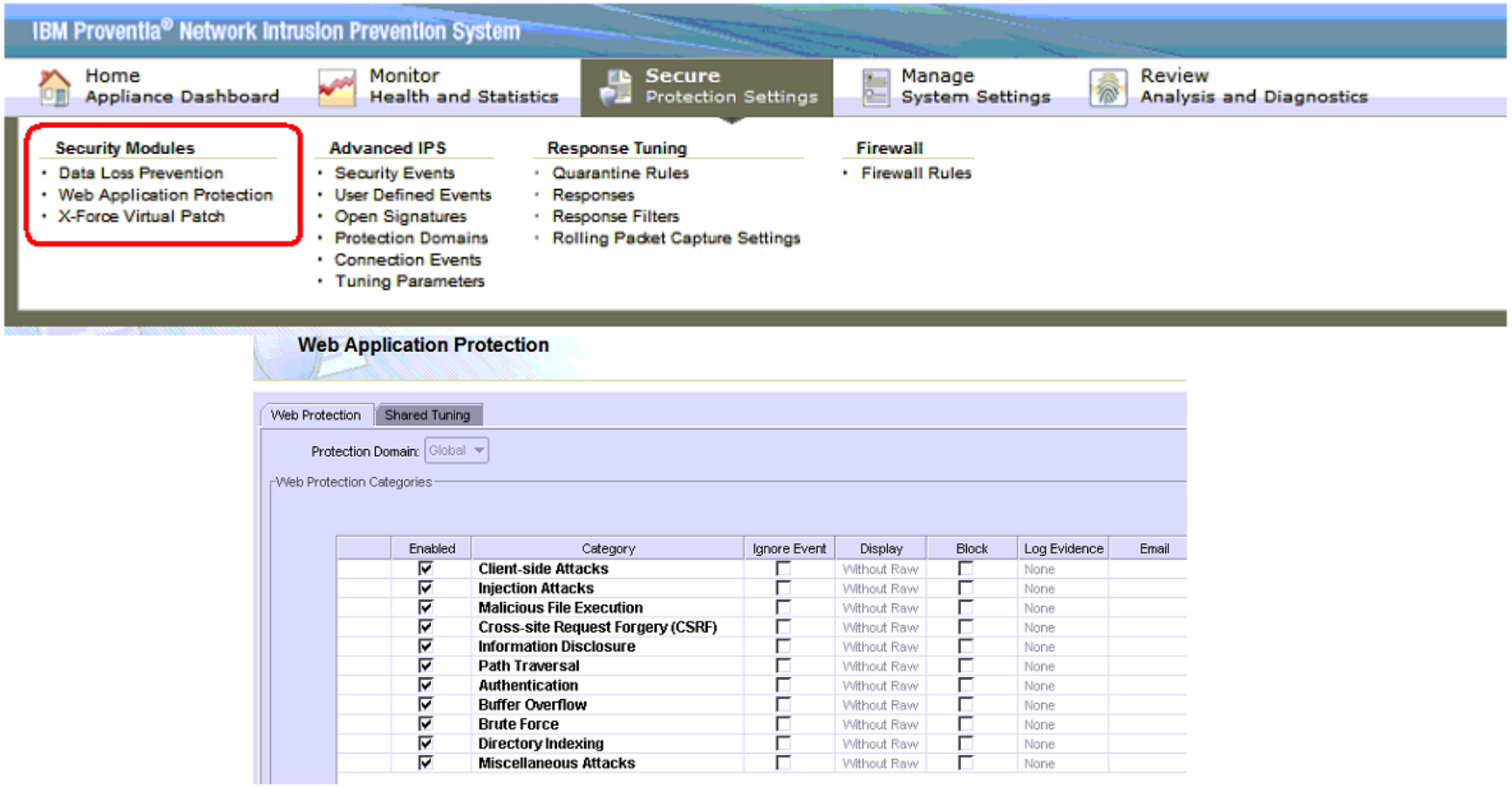
Internet Explorer'ın yanında Firefox gibi web tarayıcı desteği




Cihaz kontrolünü Lokal'den SiteProtector'e ve yine lokal'e geçişinde konfigürasyon sayfasının yüklenmesine ihtiyaç duymadan geçiş.

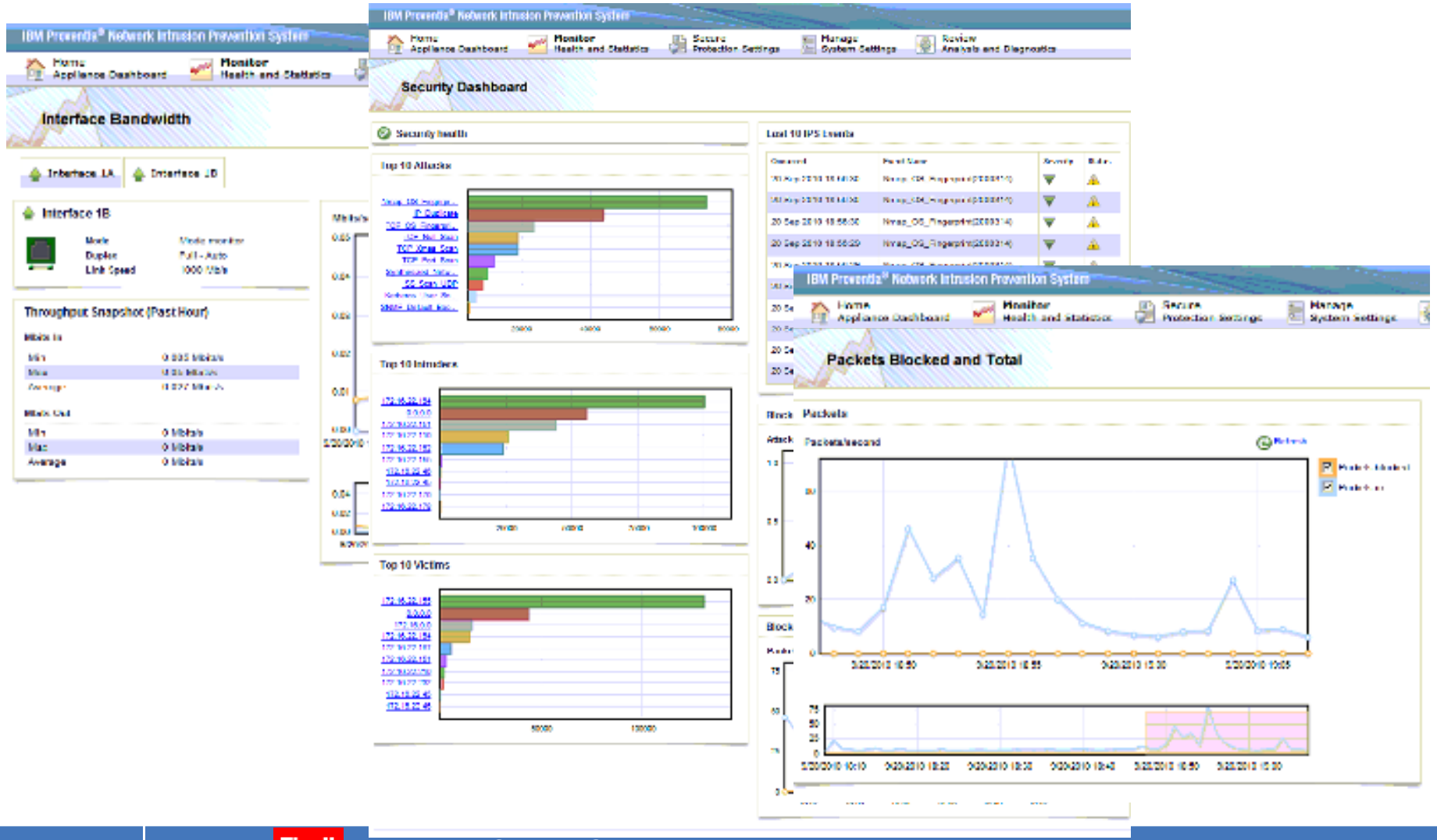
# Yeni Güvenlik Modülleri

Spesifik tipteki tehditler ve standartlara uyumluluk için gereken politikaların kolay konfigürasyonu



# Kontrol Panelleri

Performansı izleyerek sistem , güvenlik ve ağ hakkında detaylı bilgi edinme imkanı





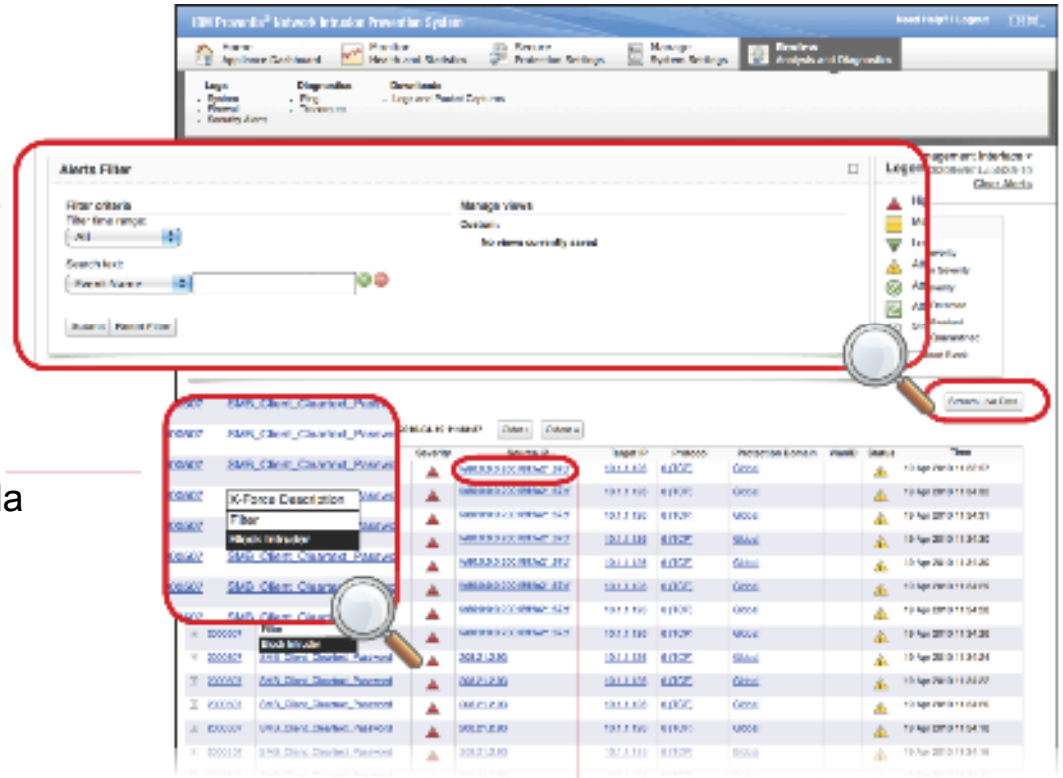

Tivoli. IBM Internet Security Systems

# Yeni Log Sayfaları

Web tabanlı arayüzü kullanarak sistem, firewall ve güvenlik olaylarına erişim ve analiz imkanı

Olay detayları için kompleks filtreler oluşturarak kaydetme ve daha sonra kullanma imkanı

Bir olayın üzerinden anında saldırganın ve atağın bloklaması özelliği




Gerçek zamanlı olay akışı

Yeni IPv6 desteği ile cihaza IPv6 adres verebilme ve IPv6 adreslerini raporlayabilme özelliği

# Yeni Özellik: Tam IPv6 Desteği

IPv6:

- Saldırı Tespit/Önleme cihazına IPv6 adres tanımlayabilme imkanı, tüm olayların IPv6 olarak raporlanma imkanı.

**Önce:**

| Rec.# | Risk Level | Alert Name | Source IP | Source Port | Target IP | Target Port | Protocol | Vuln Status | Alert Date & Time |
|---|---|---|---|---|---|---|---|---|---|
| 3 | ▲ | IPV6_Bad_Fragment_Chain | 0.0.0.1 | | 0.0.0.2 | | 0 | Blocked attack | 02/28/2005 23:00:22 |
| 2 | ▲ | IPV6_Bad_Fragment_Chain | 0.0.0.1 | | 0.0.0.2 | | 0 | Blocked attack | 02/28/2005 23:00:22 |
| 1 | ▲ | IPV6_Bad_Fragment_Chain | 0.0.0.1 | | 0.0.0.2 | | 0 | Blocked attack | 02/28/2005 23:00:22 |

**Sonra:**

| Rec.# | Risk Level | Alert Name | Source IP | Source Port | Target IP | Target Port | Protocol | Vuln Status | Alert Date & Time |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ▬ | Email_WIZ | 3ffe:b80:c84:ac07:260:8ff:fecb:b374 | 33036 | 3ffe:b80:c84:8200:280:c8ff:fecf:bf06 | 25(smtp) | 6(TCP) | Blocked attack | 06/02/2008 15:14:42 |

# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

# Sanallaştırma IT Organizasyonlarının Maliyetlerini Azaltırken, Yönetim Kolaylığı ve Artan Verimlilik Sağlamaktadır.

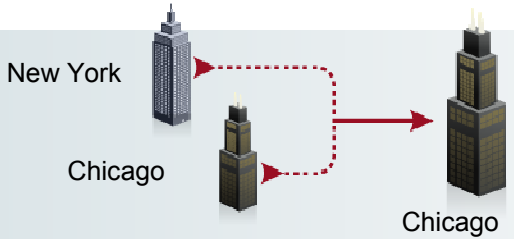
Fiziksel Konsolidayson

Bulut Bilişimine olanak tanır

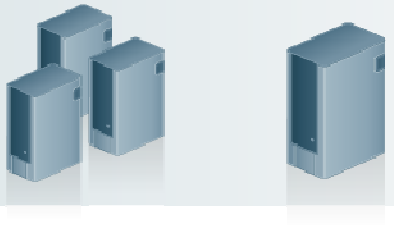
Yüksek Performanslar sağlar

Servis seviyelerini arttırır.

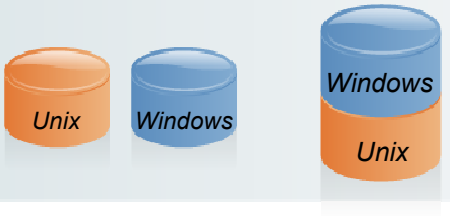
Bölge sayısını azaltır.



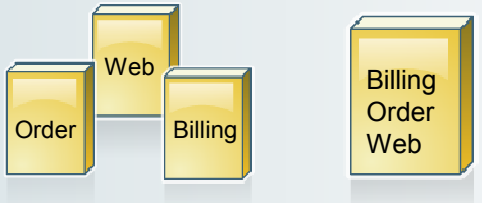

Sunucu sayısını azaltır



Farklı kaynaklardaki verilerin merkezi bir ortamda depolar

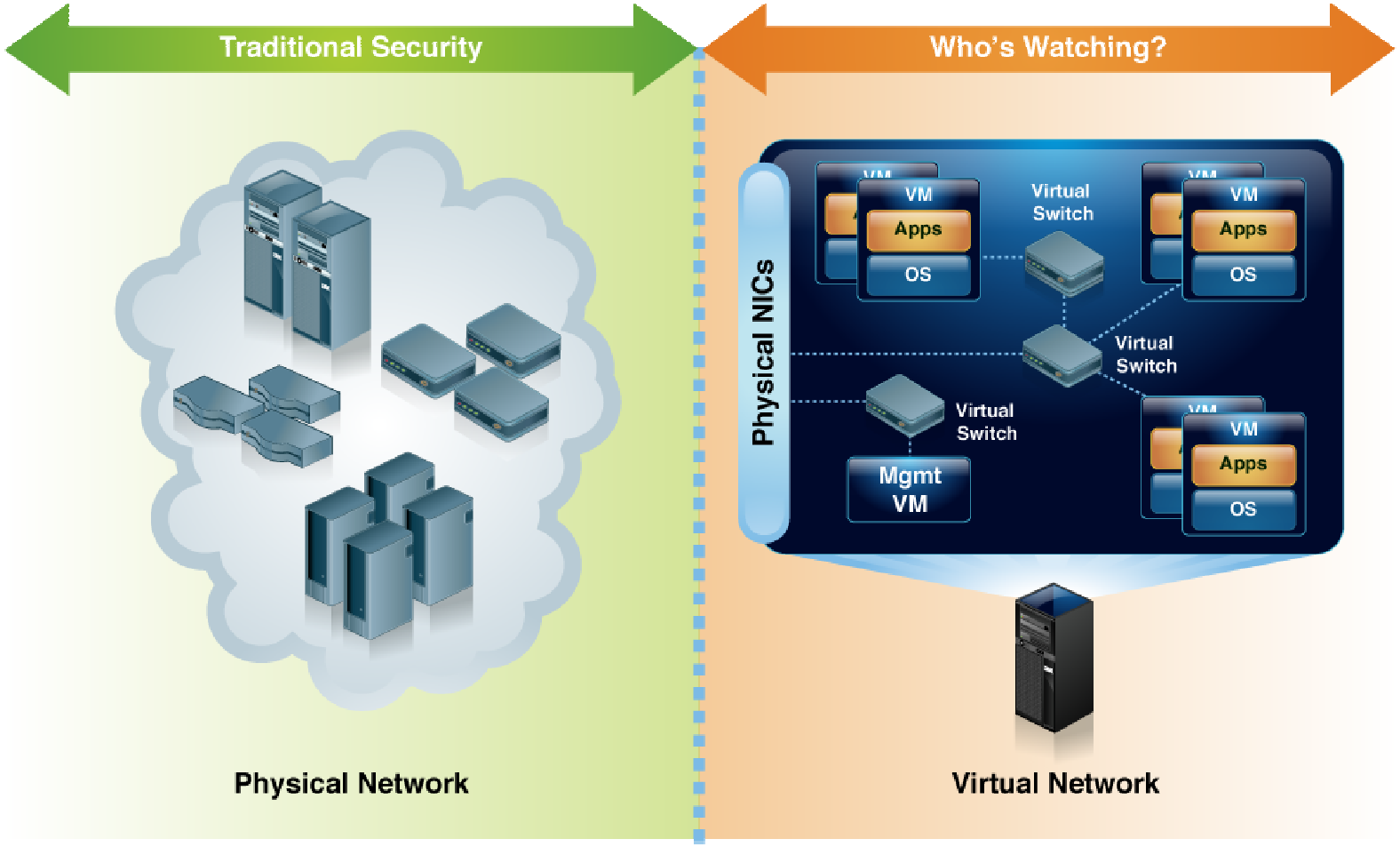



Uygulama verimliliğini arttırır.




Kaynak: Gartner, Inc.

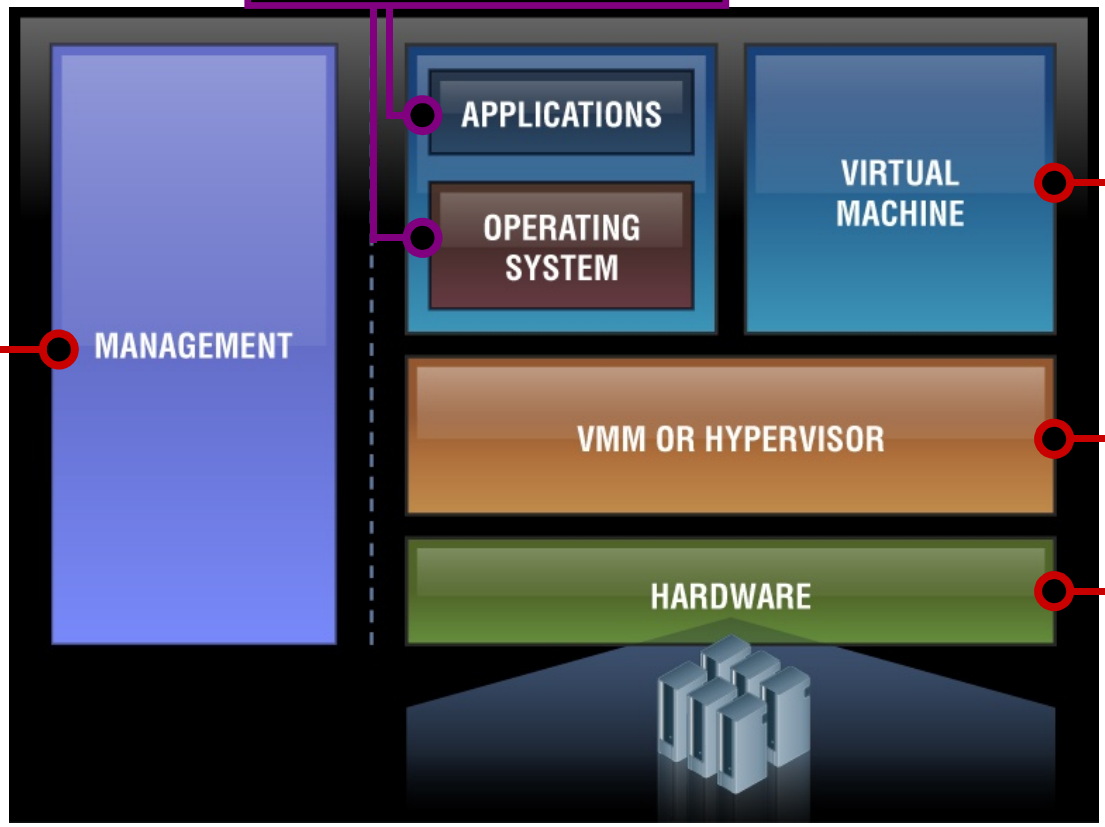
# Sunucu ve Ağların Birleşmesi



# Sanallaştırma ile Gelen Yeni Güvenlik Riskleri

- Geleneksel tehditler
- Sanal ortamların yeni tehditleri

Geleneksel tehditler sanal makinaları gerçek sistemler gibi etkileyebilir




Yönetim güvenlik açıkları

Sanal sistemlerin depolama güvenliği, yönetim verilerinin güvenliği

Yeni yetenekler/bilgi birikimi ihtiyacı

Sanal sistem koplalama

Dinamik yer değiştirme

Sanal sistem hırsızlığı

Kaynak paylaşımı

Kaynakların ortak kullanımı

Gizli rootkitler

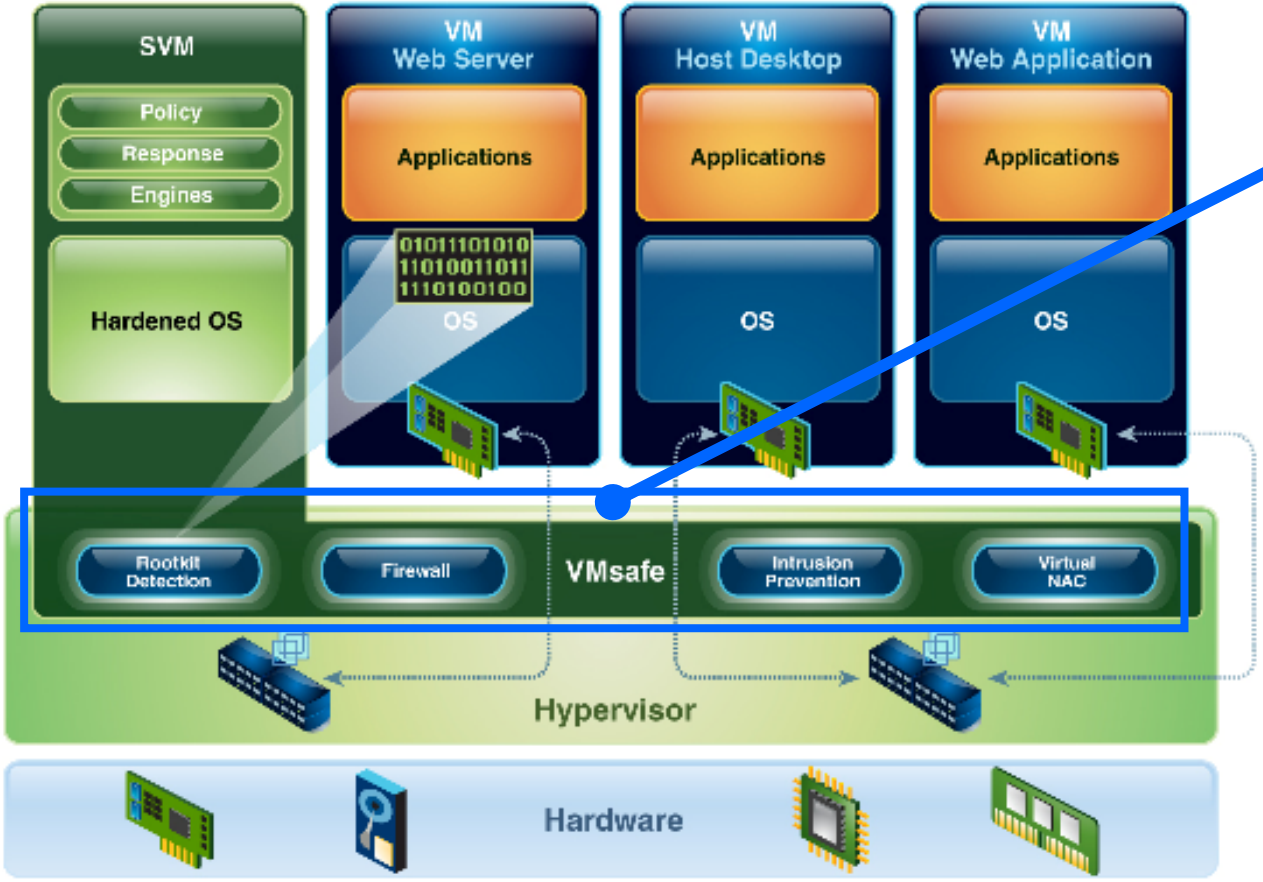
Sanal NIC ve Sanal donanım tehditlere açık

**DAHA FAZLA BİLEŞEN = DAHA ÇOK AÇIK**

# IBM Sanal Sunucu Güvenliği - VMware

## VMware vSphere 4 için tasarlanmış bütünleşik koruma

Sanal veri merkezlerinin daha güvenli, standartlara uyumlu ve verimli çalışmasını sağlamaktadır.




### IBM Sanal Sunucu

- VMsafe entegrasyonu
- Firewall ve Saldırı tespit/önleme
- Rootkit tespiti ve önleme
- Sanal makinalar arasındaki trafiğin analizi
- VMware vMotion desteği
- Sanal ağ segment koruması
- Sanal ağ seviyesi koruması
- Sanal altyapı denetimi (Yetkili Kullanıcı)
- Sanal Ağ Erişim Kontrolü
- Dosya ve Registry kayıt izlemesi sunucu tabanlı IPS (Real Secure ve Proventia Server kullanarak)

# Ajanda

1. Günümüzde Tehditler
2. Yeni Jenerasyon IBM Saldırı Tespit/Önleme Cihazları(GX-V2)
3. Yeni IBM Aktif Bypass Cihazları
4. Yeni IBM IPS Firmware (versiyon 4.1)
5. IBM Sanal Sunucu Güvenliği - VMware
6. IBM Sunucu Güvenliği

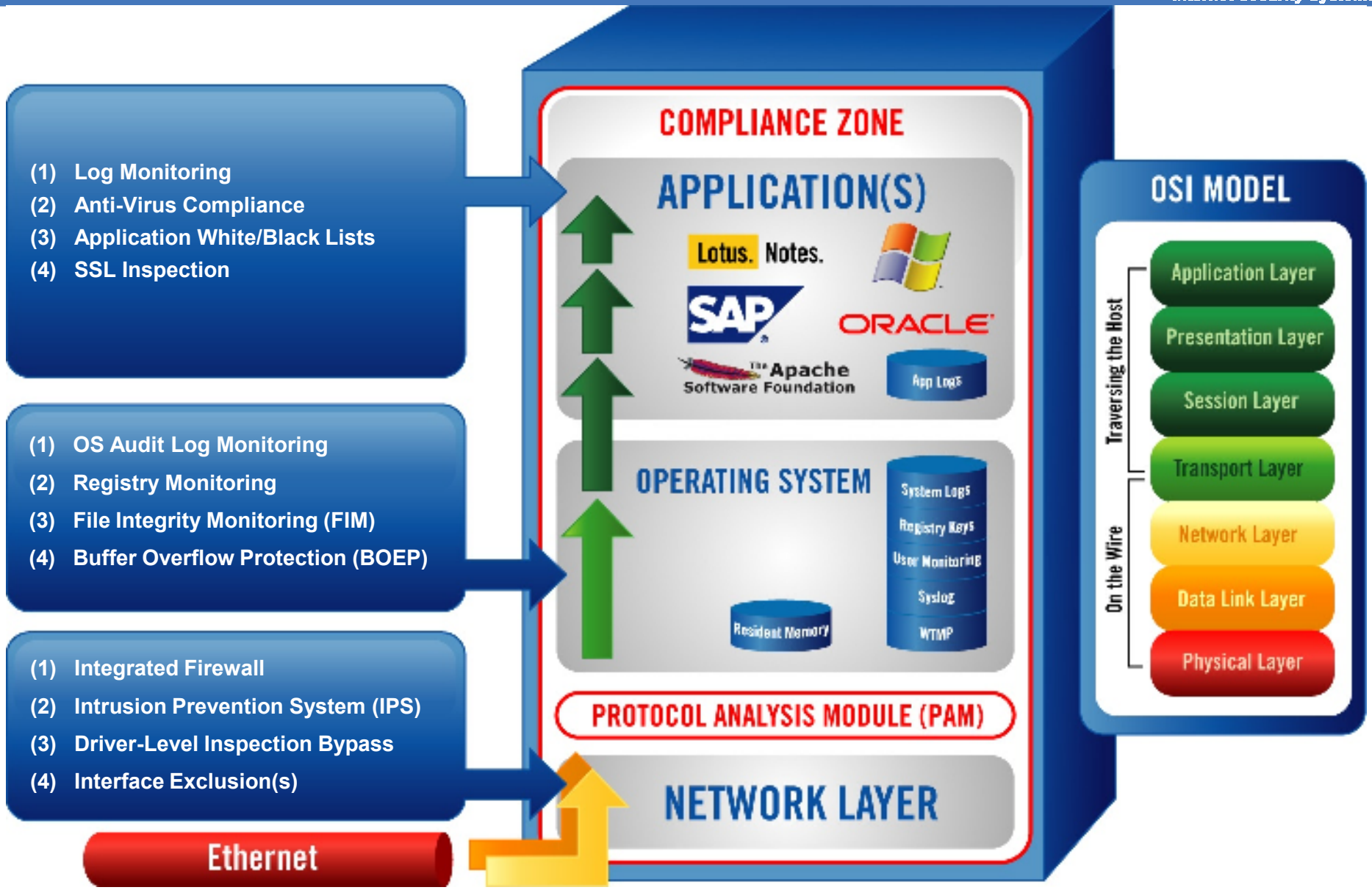
# IBM Sunucu Güvenliği

## **RealSecure Server Sensor** ve **Proventia Server**

- Tek bir ajan ile kapsamlı ve geniş koruma özellikleri
- Proventia SiteProtector ile merkezcil yönetim imkanı
- Sanal Yama Teknolojisi
- NSS Labs Sertifikasyonu
- Kim, Ne, Ne Zaman, Nerede gibi kullanıcı aktivitelerinin izlenmesi
- Standartlara Uyumluluk: Dosya İçerik İzlemesi (FIM), İşletim Sistemi Denetimi, Registry Bütünlük İzlemesi, Anti-Virus Standartlarına Uyumluluk, uygulama Kontrolü
- Geniş İşletim Sistemi desteği: **Windows, Linux, AIX, Solaris, HP-UX**



NSS Labs APPROVED



# Teşekkürler