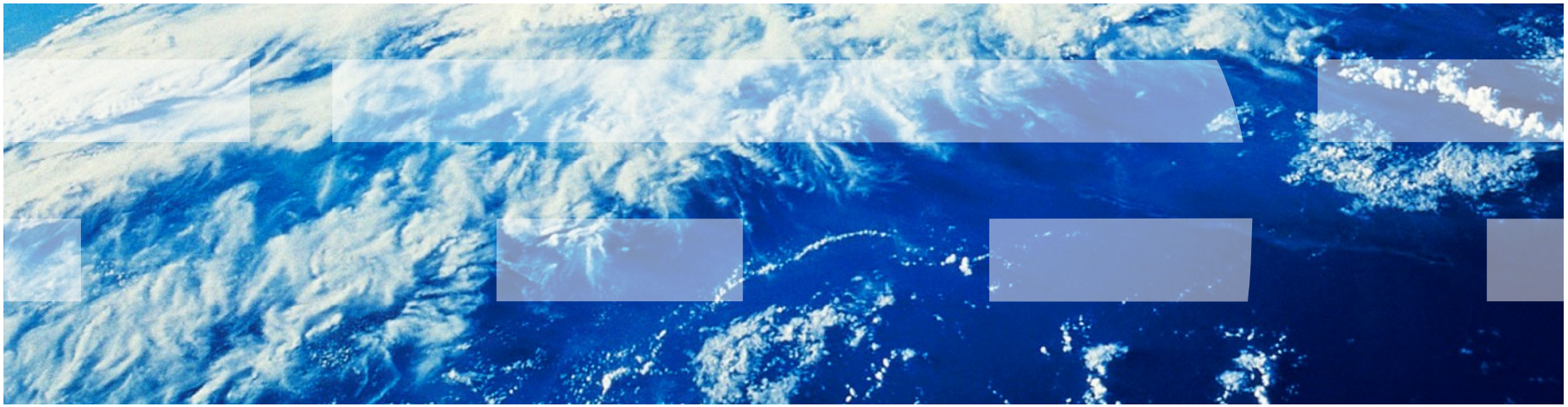
Tansel ZENGINLER – Tivoli Çözümleri Uzmanı

22/10/2009

IBM yazılım zirvesi '09

Dinamik Altyapı Radarında Güvenlik Çözümleri Yol Haritası



İçindekiler

- Mevcut iklim
- Akıllı Dünya/ Dinamik altyapı
- IBM Güvenlik çerçevesi
- IBM Güvenlik Stratejisi ve olanakları
  - Çalışanlar ve Kimlik
  - Veri ve Bilgi
  - Uygulama ve Süreç
  - Ağ, Sunucular ve Uç Noktaları

Küresel pazar kuvvetleri hepimizi etkilemektedir

- Küresel olarak bütünleşmiş bir dünyada yaşama gerçeği
  - Ekonomik krizin ve belirsizliğin yaygın etkisi
  - Enerji yetersizliği ve değişken mal fiyatları
  - Yeni müşteri talepleri ve iş modelleri
  - Bilgi patlaması ve risk/fırsat büyümesi
- İşletmeler aşağıdaki hususlar konusunda giderek artan baskı altındadır:
  - İşletim maliyetlerinin ve karmaşıklığın yönetilmesi
  - Sürekli ve yüksek kaliteli hizmet
  - İnovasyon, gelişen yeni teknolojiler, veri/bilgi patlaması vb. ile artan güvenlik risklerinin ele alınması

"We have seen more change in the last 10 years than in the previous 90."

Ad J. Scheepbouwer,
CEO, KPN Telecom

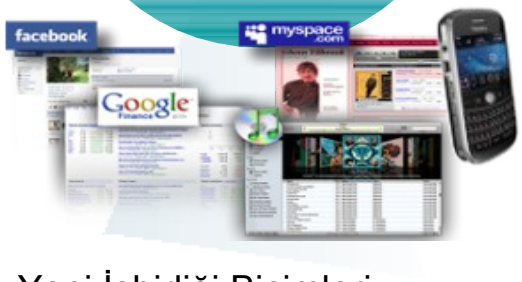
Dünyamız giderek daha
donanımlı, birbirine bağlı ve akıllı hale geliyor.

Akıllı dünyaya hoş geldiniz...

Küreselleşme ve Küresel Kaynaklar

Web'e erişen milyarlarca mobil aygıt

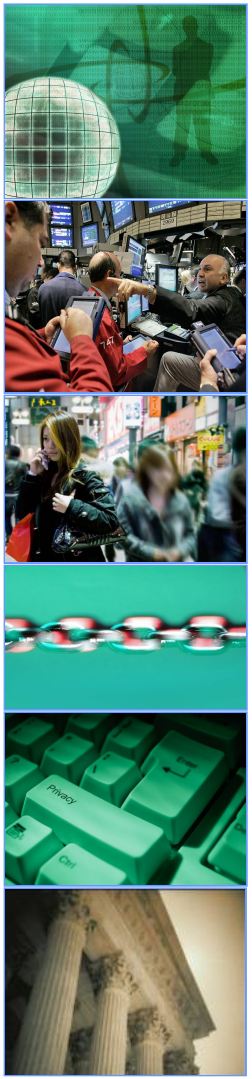
Bilgi akışlarına Gerçek Zamanlı erişim



Yeni İşbirliği Biçimleri

Yeni olasılıklar.
Yeni karmaşıklıklar.
Yeni riskler.

Yeni fırsatların yol açtığı risklerin yönetilmesi



Gelişmekte olan teknoloji

- Sanallaştırma ile cloud computing, altyapı karmaşıklığını artırır.
- Web 2.0 ile Hizmet Odaklı Mimari tarzı birleşik uygulamalar, güvenlik ihlallerine ve saldırılara karşı savunmasız uygulamalar nedeniyle yeni zorluklara yol açar.

Veri ve bilgi patlaması

- Veri hacimleri her 18 ayda iki katına çıkmaktadır.*
- Bilgi bağlamı çevresindeki depolama, güvenlik ve keşif giderek daha önemli hale gelmektedir.

Kablosuz Dünya

- Mobil platformlar yeni tanımlama yolları olarak gelişmektedir.
- Güvenlik teknolojisi, PC'lerin korunması için kullanılan güvenliğin yıllarca gerisindedir.

Tedarik zinciri

- Zincir sadece en zayıf halkası kadar güçlüdür...ortakların uygunluk ve başarısızlık sorumluluğunun getirdiği yükten üstlerine düşeni sırtlaması gerekir.

Müşteriler gizlilik bekler

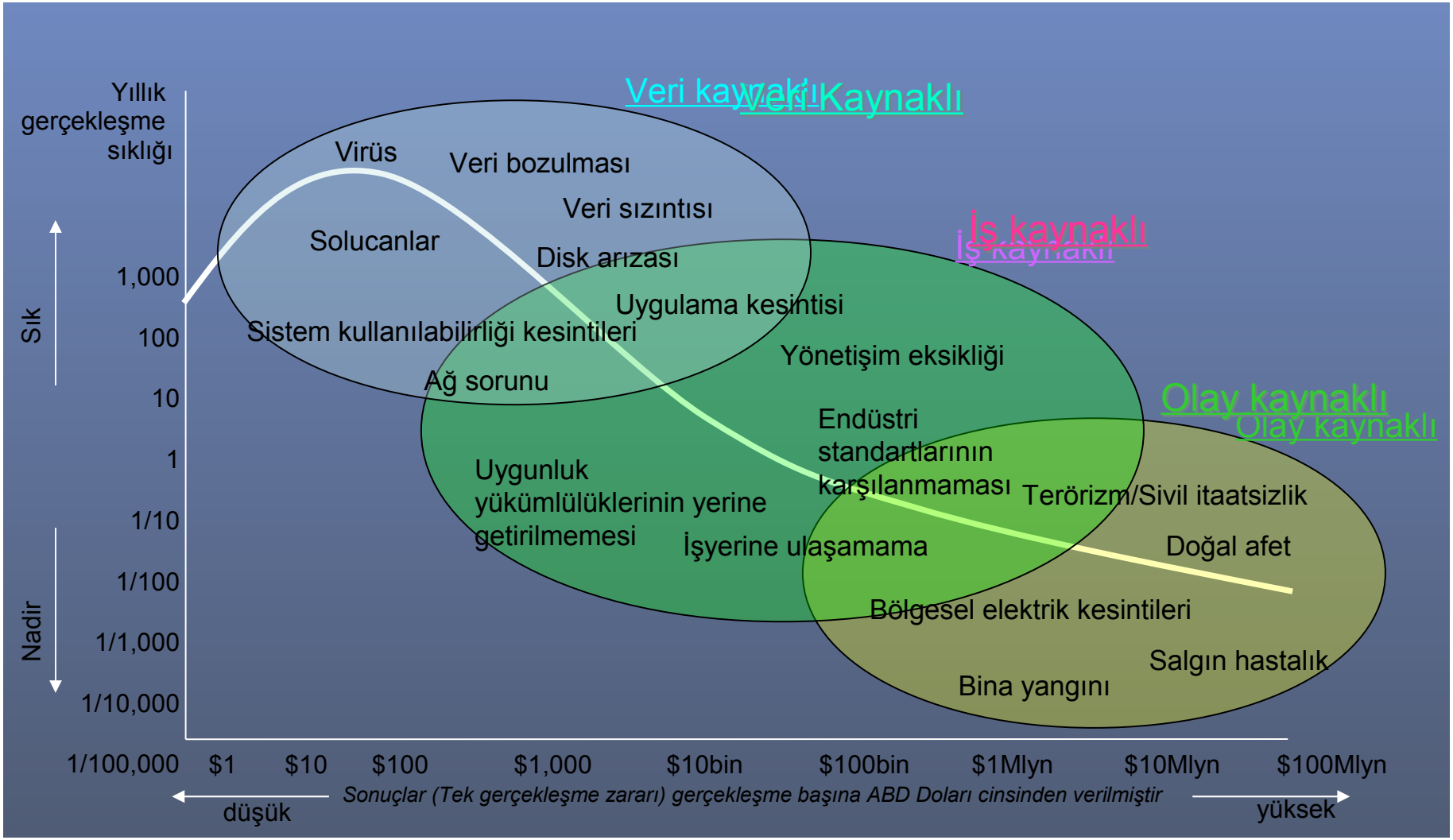
- Gizliliğin korunması için güvenliğin altyapıyla, süreçlerle ve uygulamalarla bütünleştirilmesine yönelik bir varsayım veya beklenti bulunmaktadır.

Uygunluk yükü

- Kuruluşlar güvenlik ve uygunluk yatırımları arasında denge sağlamaya çalışmaktadır.

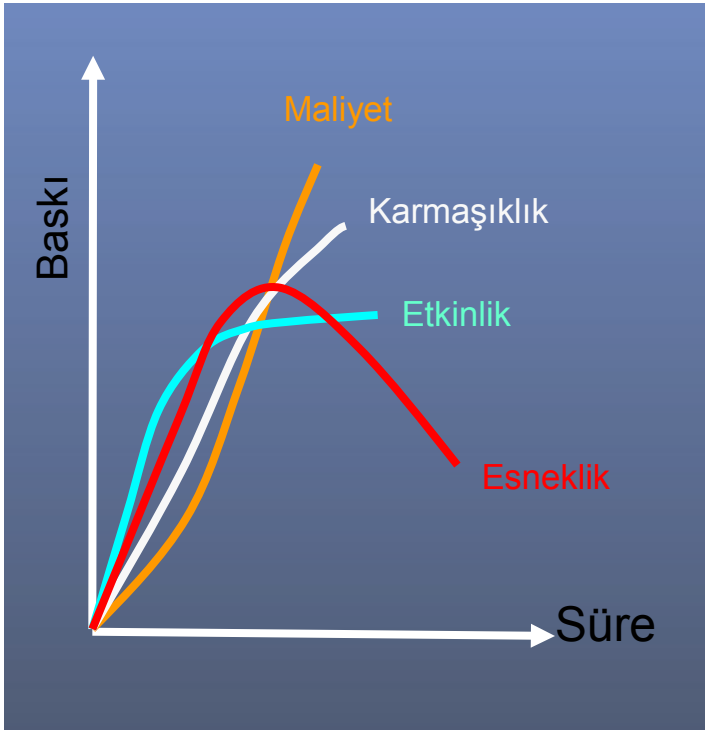
Kaynak: Pyramid Research, Ekim 2007

Her risk eşit değildir



Tıpkı bütün Güvenlik çözümlerinin eşit olmaması gibi...

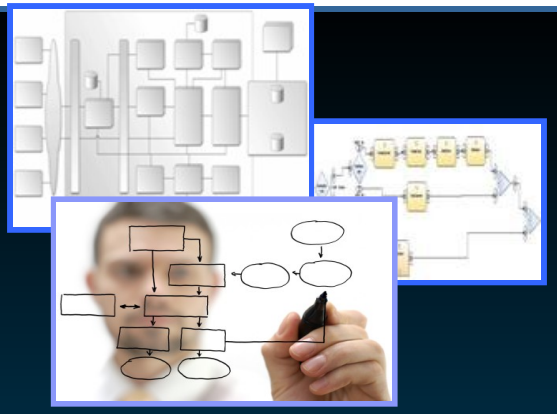
- Etkin güvenlik ile maliyet arasında bir denge kurun
  - Kural...asla 10 Dolarlık atı korumak için çite 100 Dolar harcama
- Araştırmalar, Pareto İlkesinin (80-20 kuralı) BT güvenliği için geçerli olduğunu göstermektedir*
  - İhlallerin %87'sinin makul denetimlerle önlenebileceği kabul edilir
- Küçük bir güvenlik denetimleri grubu, fazlasıyla geniş bir kapsam sağlar
  - Kritik denetimler, işletmenin her katmanında riski denetler
  - Güvenlik denetimleri kullanan işletmeler çok daha yüksek performansa sahiptir*



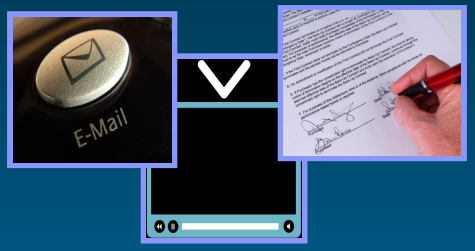
**Kaynaklar: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, Haziran 2008*
ITPI: IT Process Institute, EMA Aralık 2008

Riskler nerededir?

Çalışanlar



Süreç

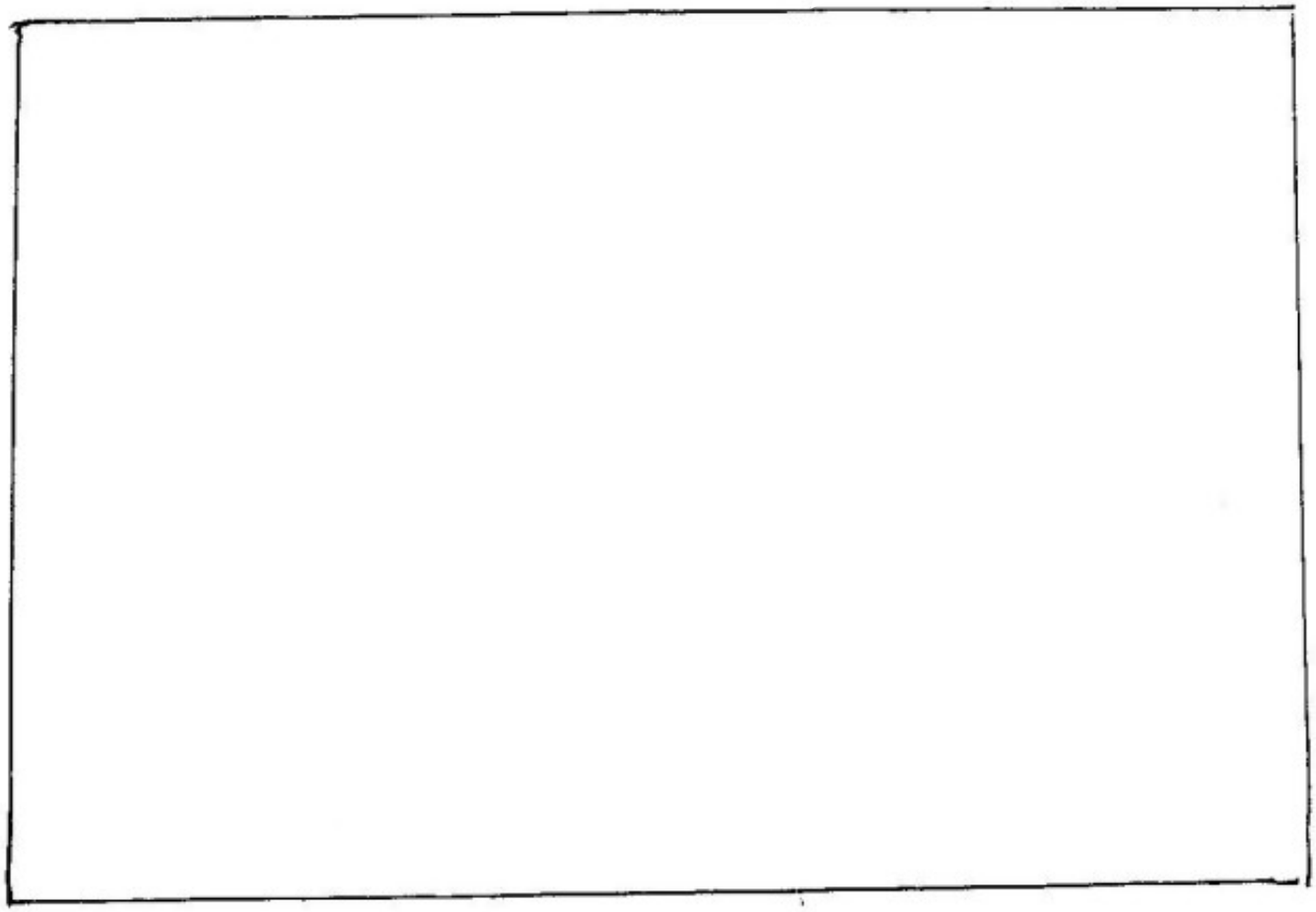


Bilgi

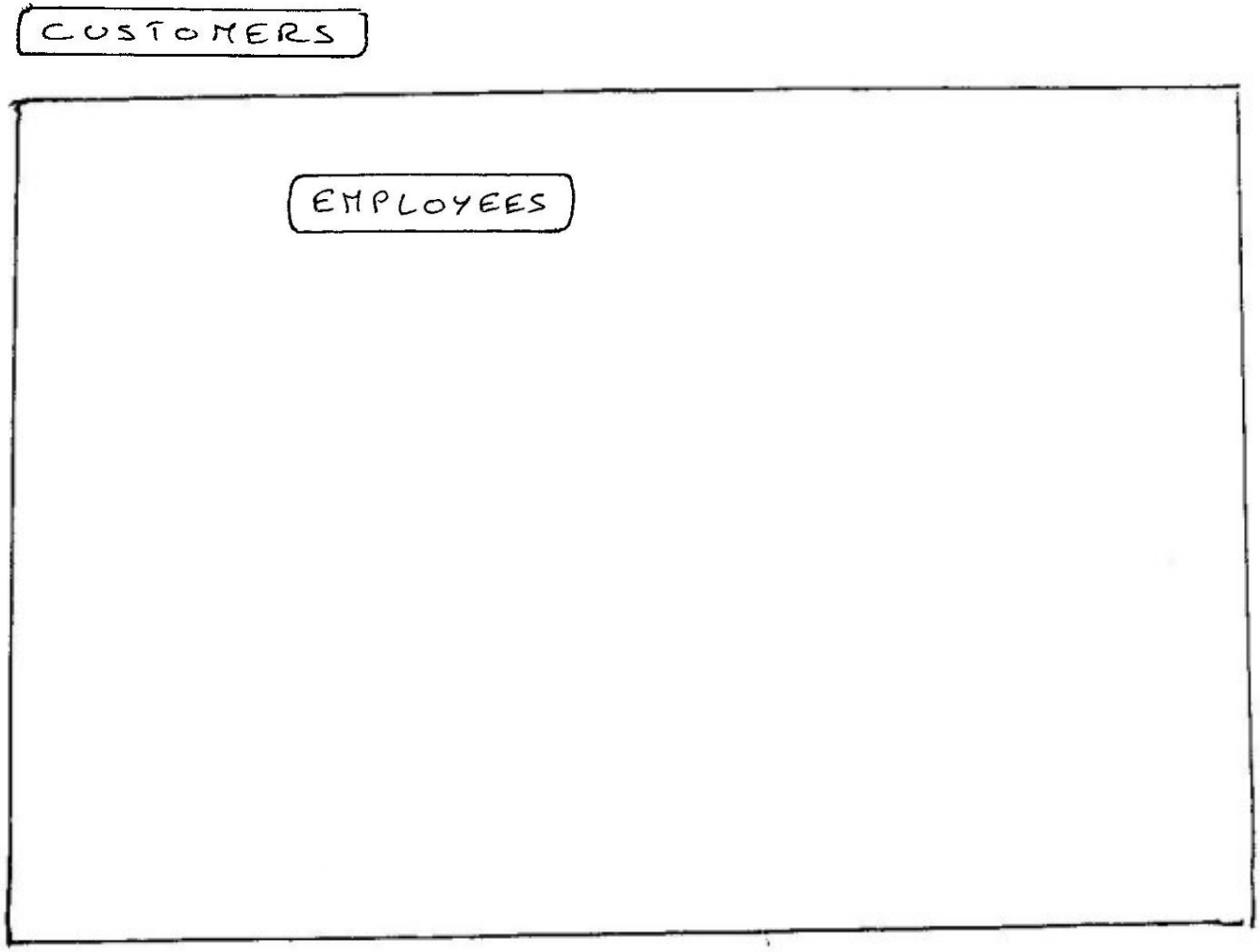
Teknoloji

İşimiz kuruluşları korumak...

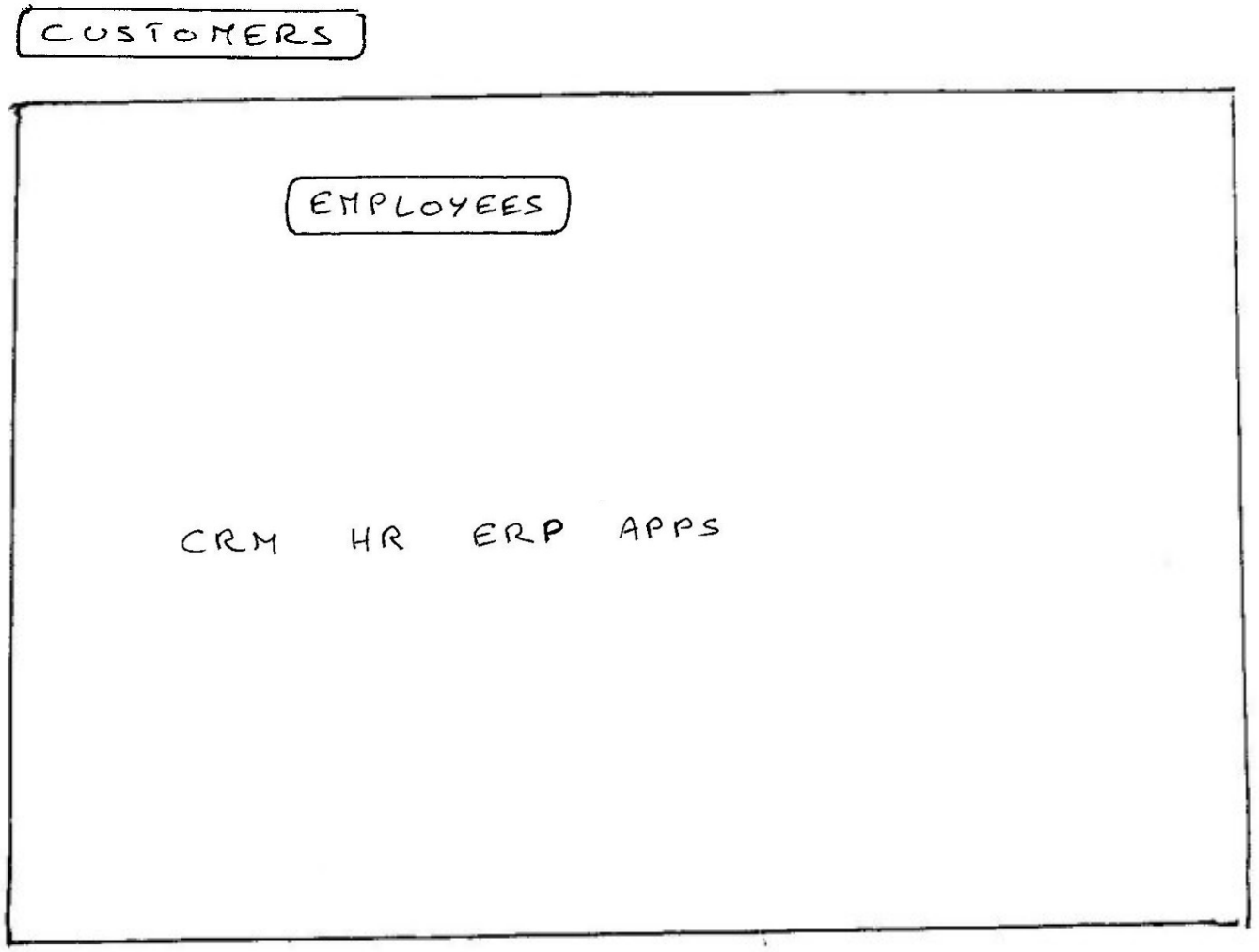
ORGANIZATION



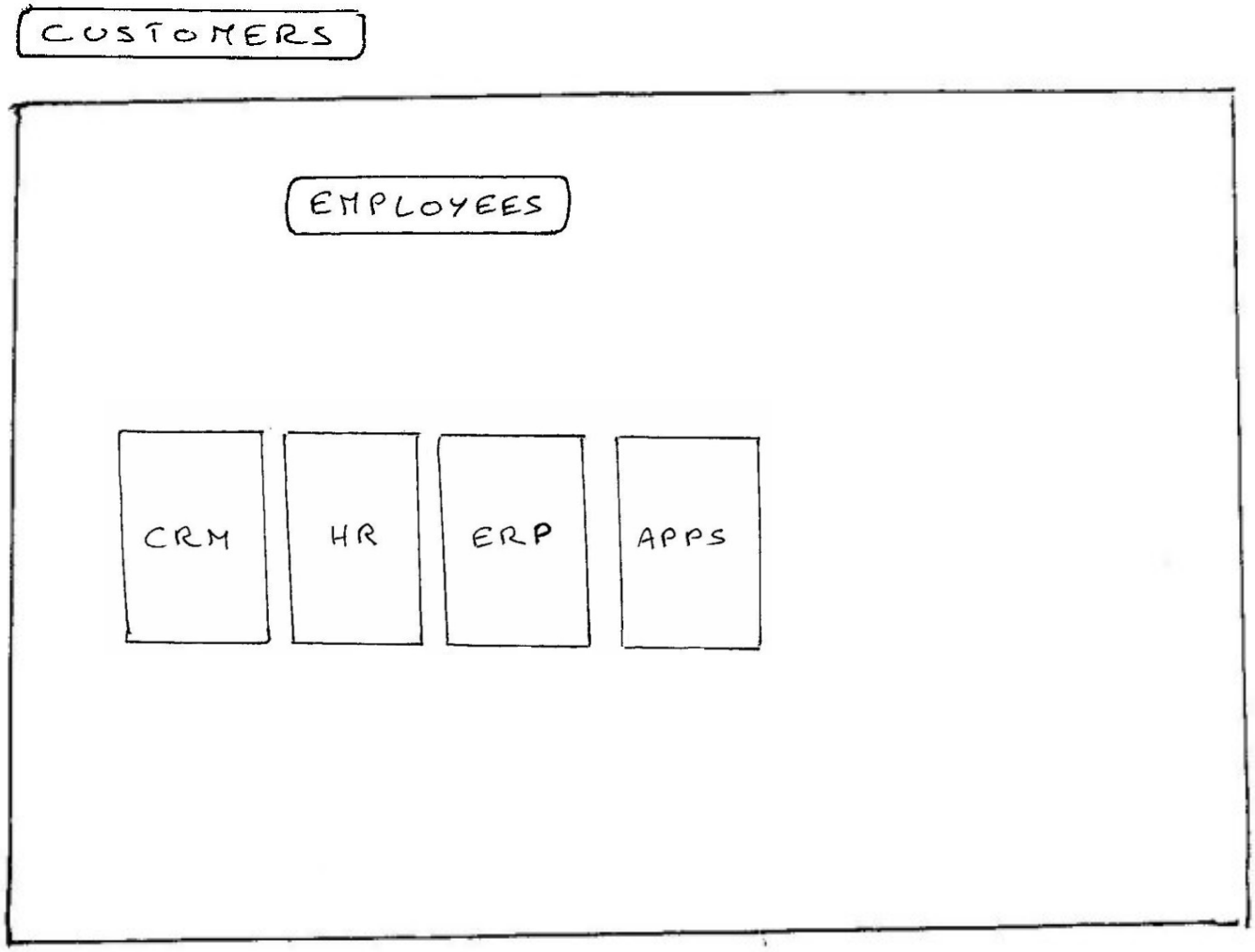
... müşterileri ve çalışanlarıyla...



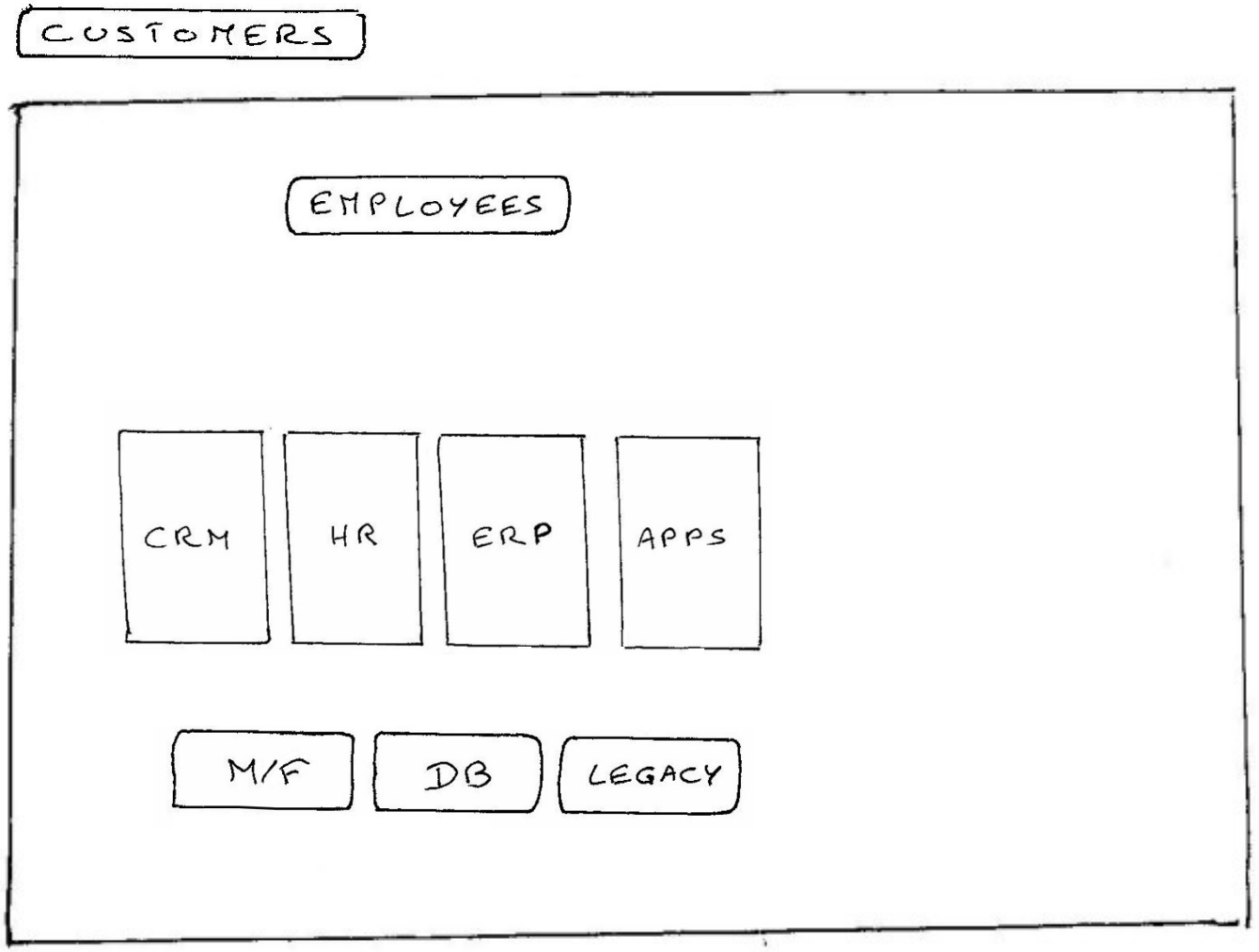
... uygulamalara erişen ...



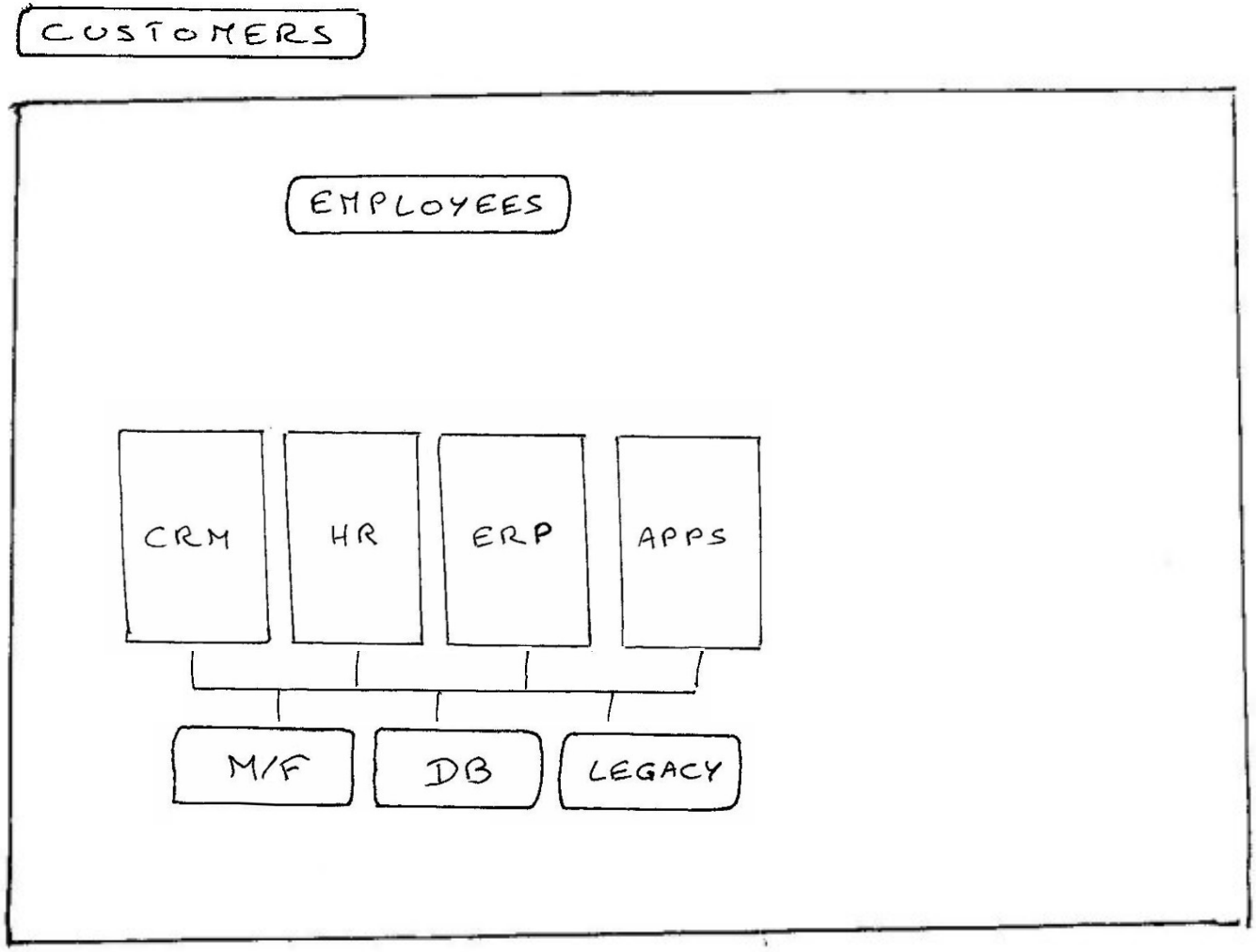
... kritik sistemlerde barındırılan ...



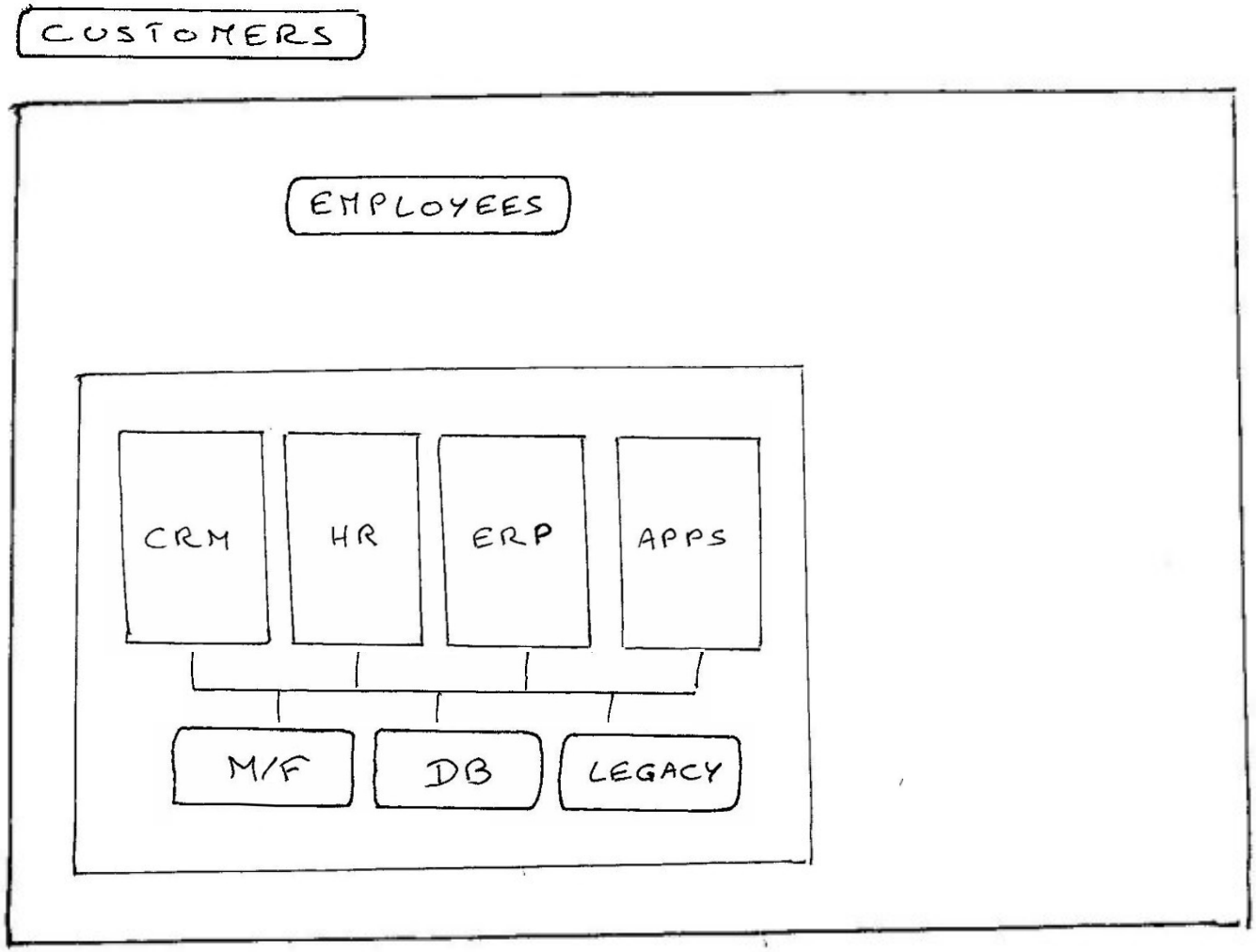
... kurumsal bilgi varlıklarını kullanan ...



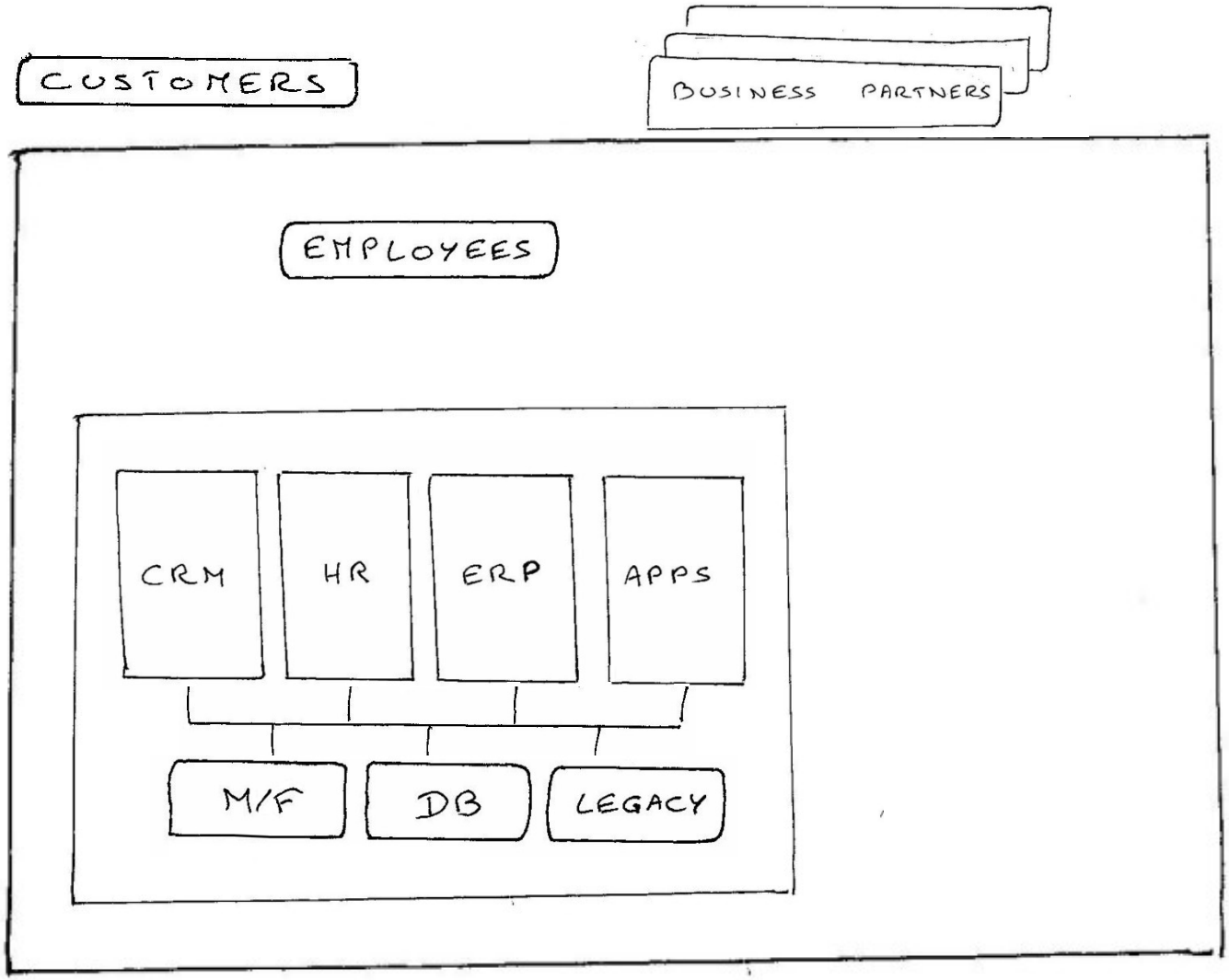
... bir ağ veya kurumsal hizmet veriyolu üzerinden ...



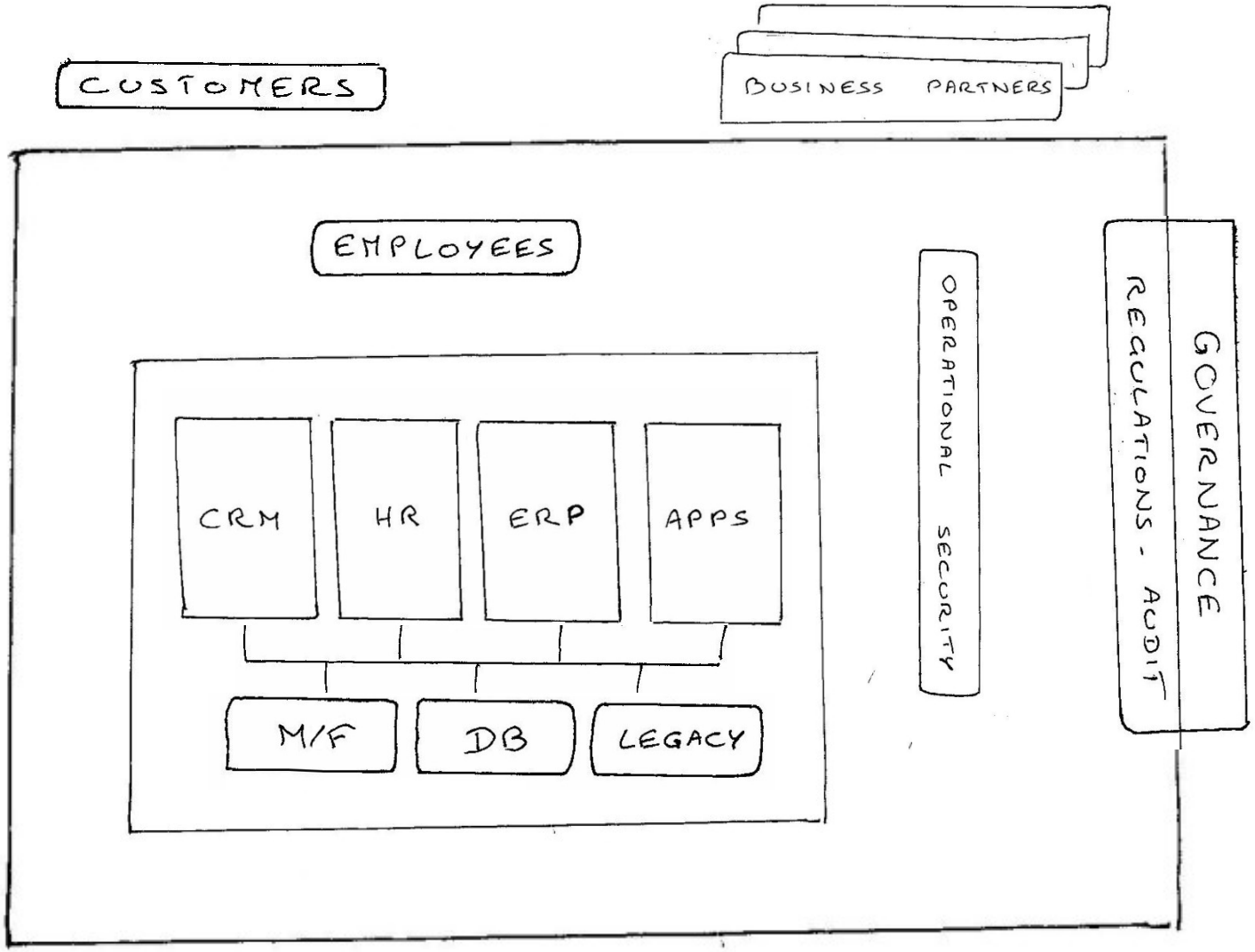
... bir bilgisayar merkezinde ...



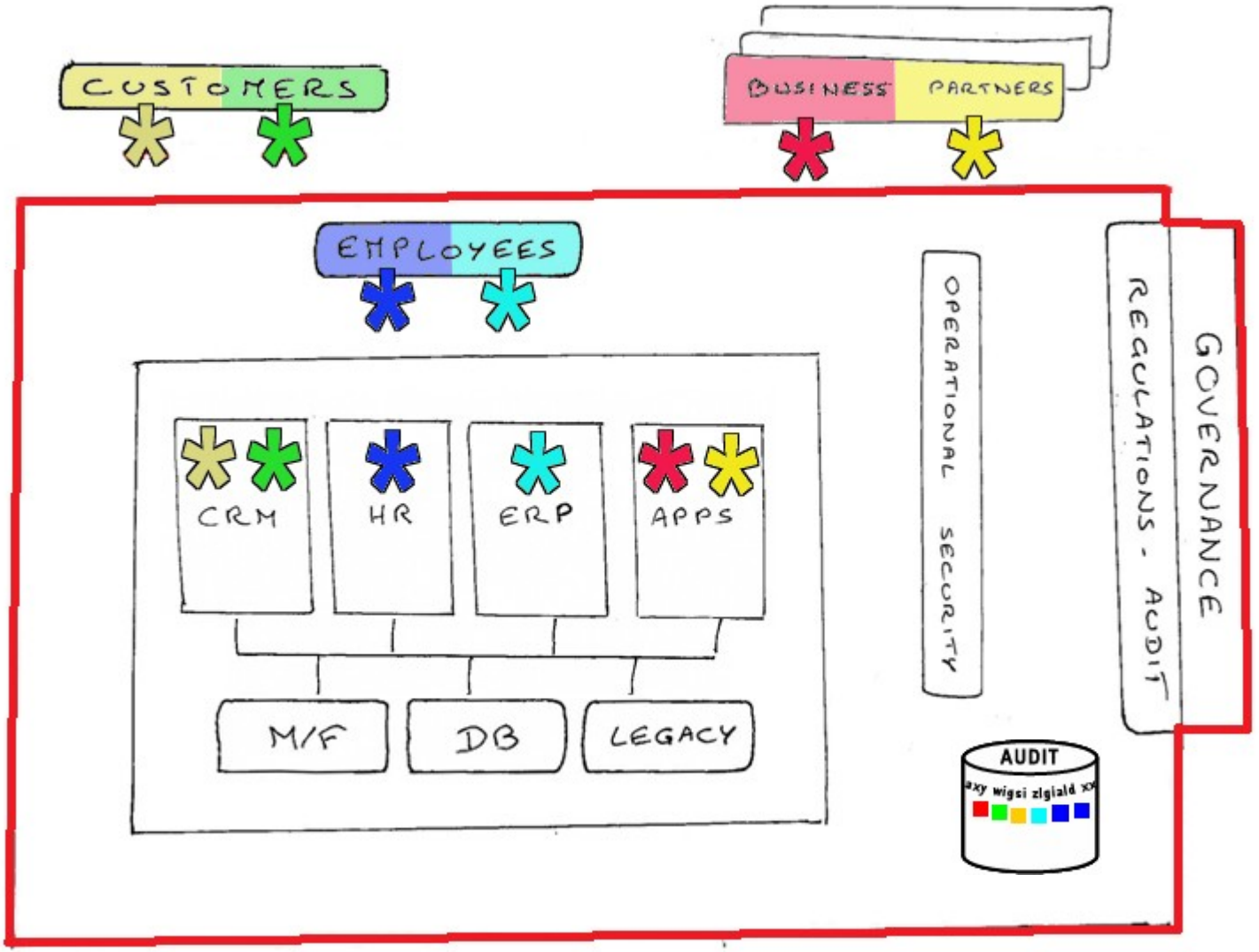
... iş ortakları ile etkileşim içinde ...



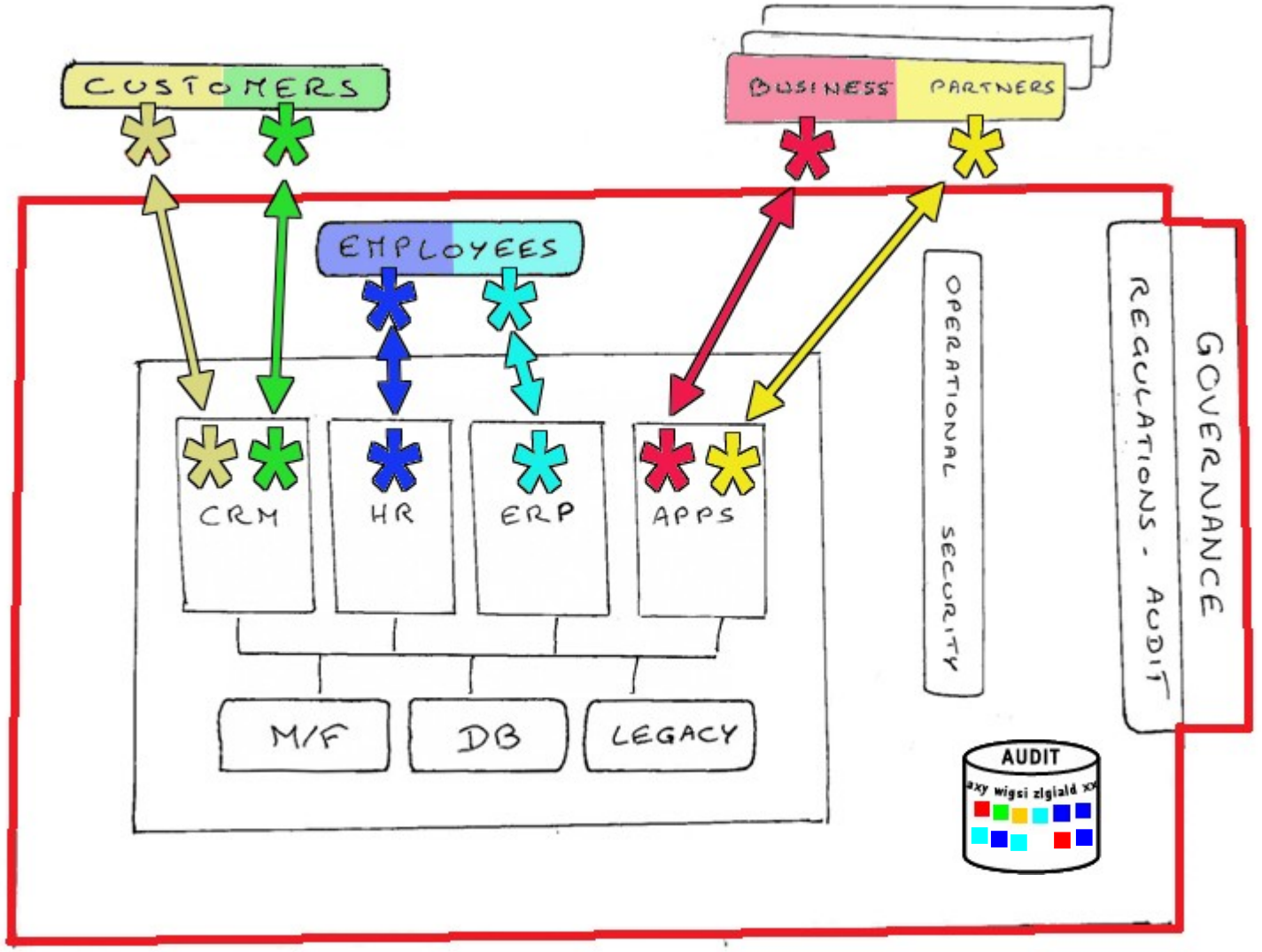
... denetimlere ve yönetişime tabi olarak ...



... kullanıcıların uygulamaları ve verileri kullanmasını sağlayarak



... erişimi yöneterek ...



Tivoli Identity Manager

"İş" kralsa...

- En yüksek merci
- Kuralları tanımlar
- Biraz paranoyaktır
- Sükuneti korumak... dertten uzak olmak ister

... TIM de çok cepheli bir kimlik ambarıdır

Otomasyon

- Kimlikler oluşturur
- Çalışanlar ve görevler
- Kendi kendine hizmet seçenekleri

Yönetişim

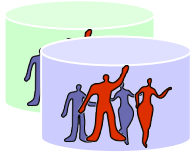
- Veri toplar
- Sertifikalandırır
- Yeniden sertifikalandırır
- Uygunluk raporları
- Kralı dertten uzak tutar

Tivoli Identity Manager - Kısa, Pratik bir Örnek

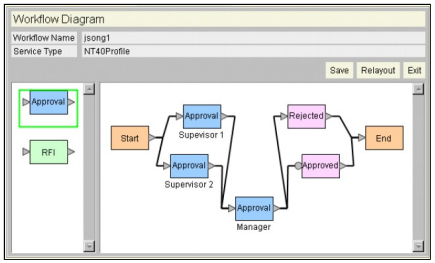
Evrensel kullanıcı yetkilendirme süreci:

Kimlik değişikliği (ekle/sil/düzenle) → Erişim ilkesi değerlendirilir → Onaylar toplanır → Hesaplar güncellenir

TDI ve TIM (yerleşik) iş akışı otomasyonu ile gerçekleştirilir



TDI



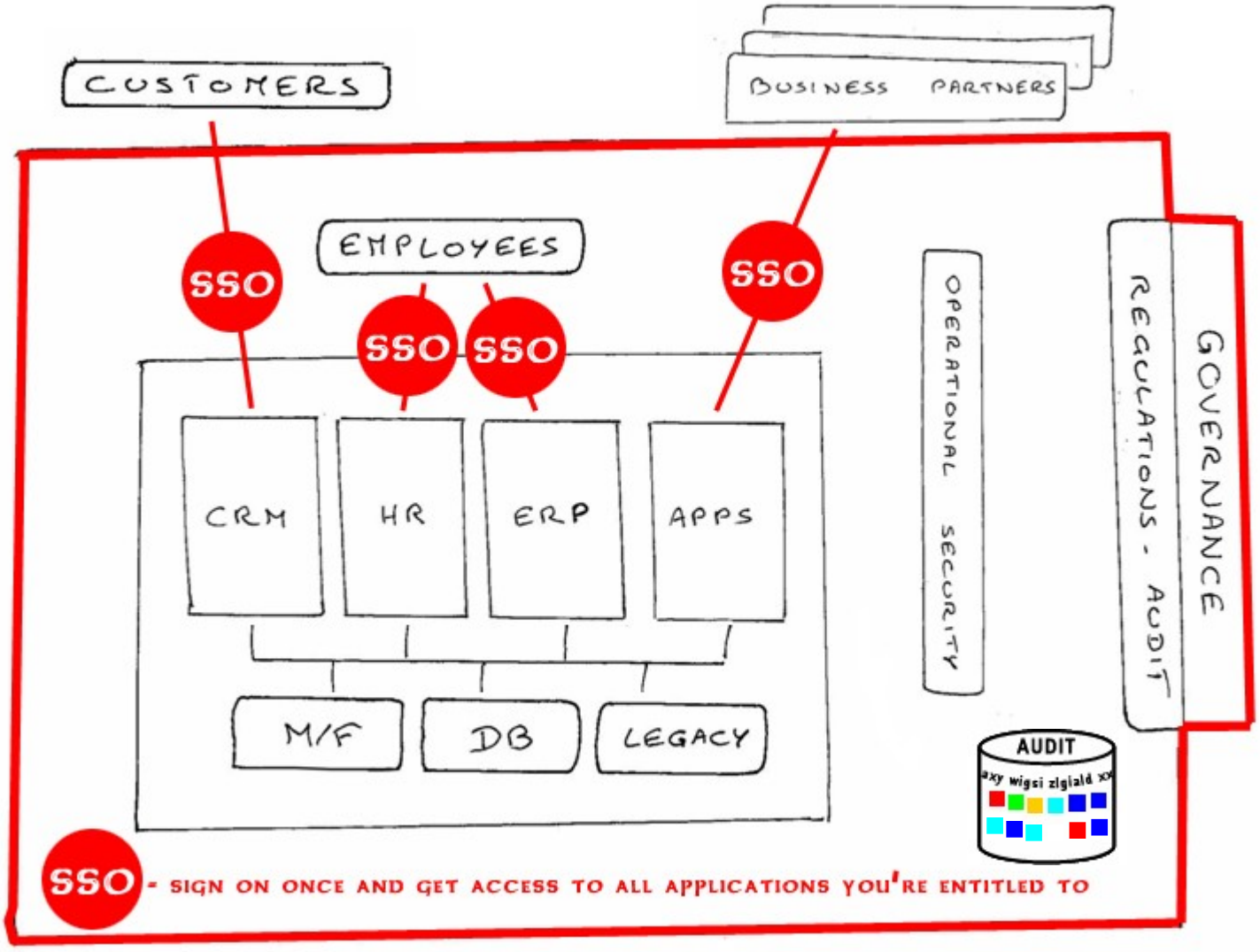
TDI

Uzlaştırma

Kapalı devre yetkilendirme paradan tasarruf sağlar ve uygunluk sağlanmasına yardımcı olur

1. Yeni kullanıcı / kullanıcı değişikliği
2. İş akışı tetiklenir
3. Onaylar/hesaplar güncellenir
4. Uzlaşma - ilke içerisinde?

... oturum açmanın basitleştirilmesi ...



TAMeb / TAM E-SSO / TFIM

Eksiksiz Tek Oturum Açma - TAMeb + TAM E-SSO + TFIM

Internet

Extranet

Intranet/Kiosk

Unified SSO

TFIM

TAMeb

TAM E-SSO
Web Workplace

Web Hizmetleri

- Birleşik
- Hizmet Odaklı Mimari

Web SSO Hedefleri

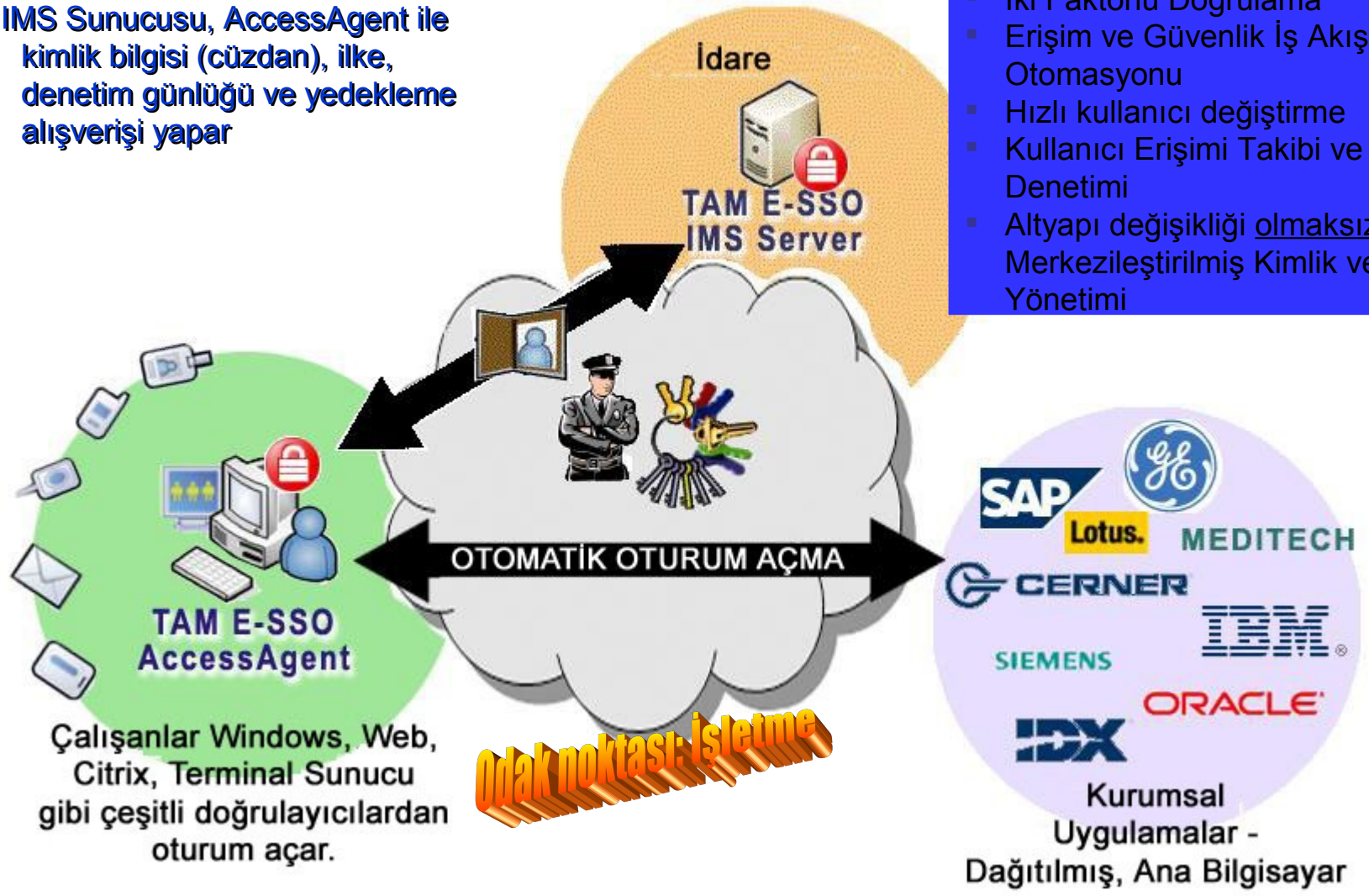
- Web Sunucuları
- Web Uygulamaları
- Portallar,örneğin WPS

Web Dışı Hedefler

- Windows
- URL
- Java
- Citrix/ Terminal Hizmetleri
- Ana Bilgisayar

TAM E-SSO Çözümüne Genel Bakış

IMS Sunucusu, AccessAgent ile kimlik bilgisi (cüzdan), ilke, denetim günlüğü ve yedekleme alışverişi yapar

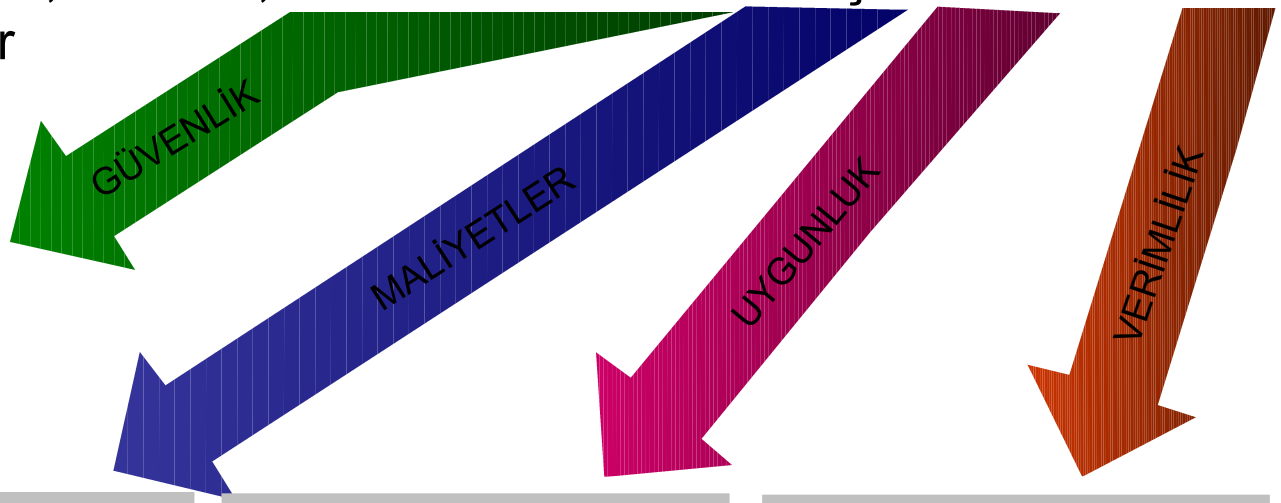


TAM ESSO aşağıdakileri sağlar:

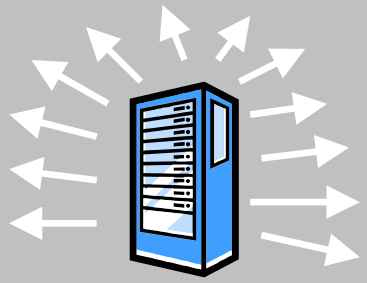
- ESSO
- İki Faktörlü Doğrulama
- Erişim ve Güvenlik İş Akışı Otomasyonu
- Hızlı kullanıcı değiştirme
- Kullanıcı Erişimi Takibi ve Denetimi
- Altyapı değişikliği olmaksızın Merkezileştirilmiş Kimlik ve İlke Yönetimi

TAM E-SSO Hangi İş Sorunlarını Çözebilir?

Güvenlik Yöneticileri, CFO'lar, CCO'lar ve kullanıcılar için en önemli sorunları ele alır

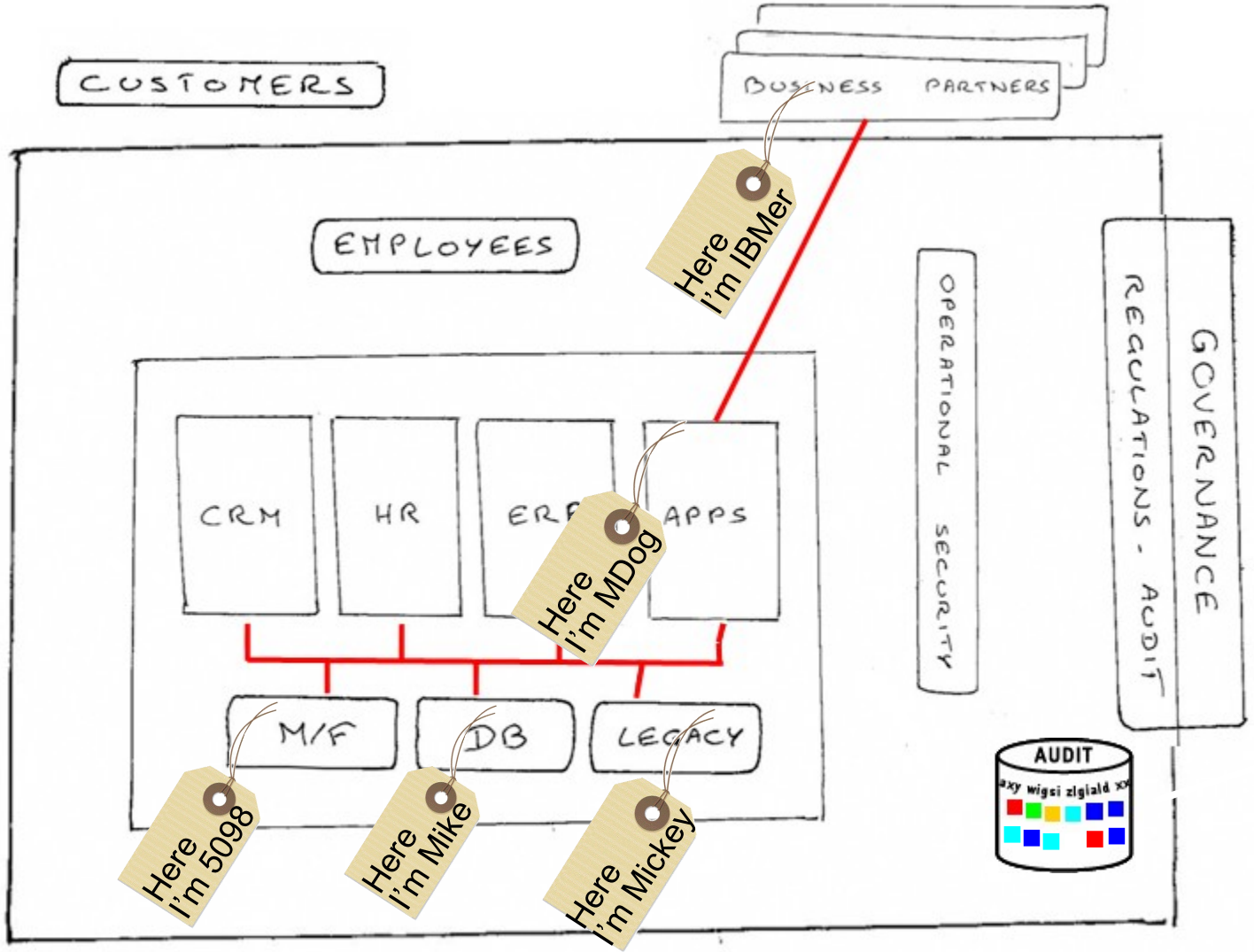


ARAMA BAŞINA 20 - 25 ABD DOLARI!



GERÇEKTEN KİMİN NEYE ERİŞTİĞİNİ BİLİYOR MUYUZ?

... Web hizmeti (SOA) yapılandırmalarının ele alınması ...



BT personeli, ne kadar kimlik değiştirirsem değiştireyim ne yaptığımı bilmek zorundadır

TFIM

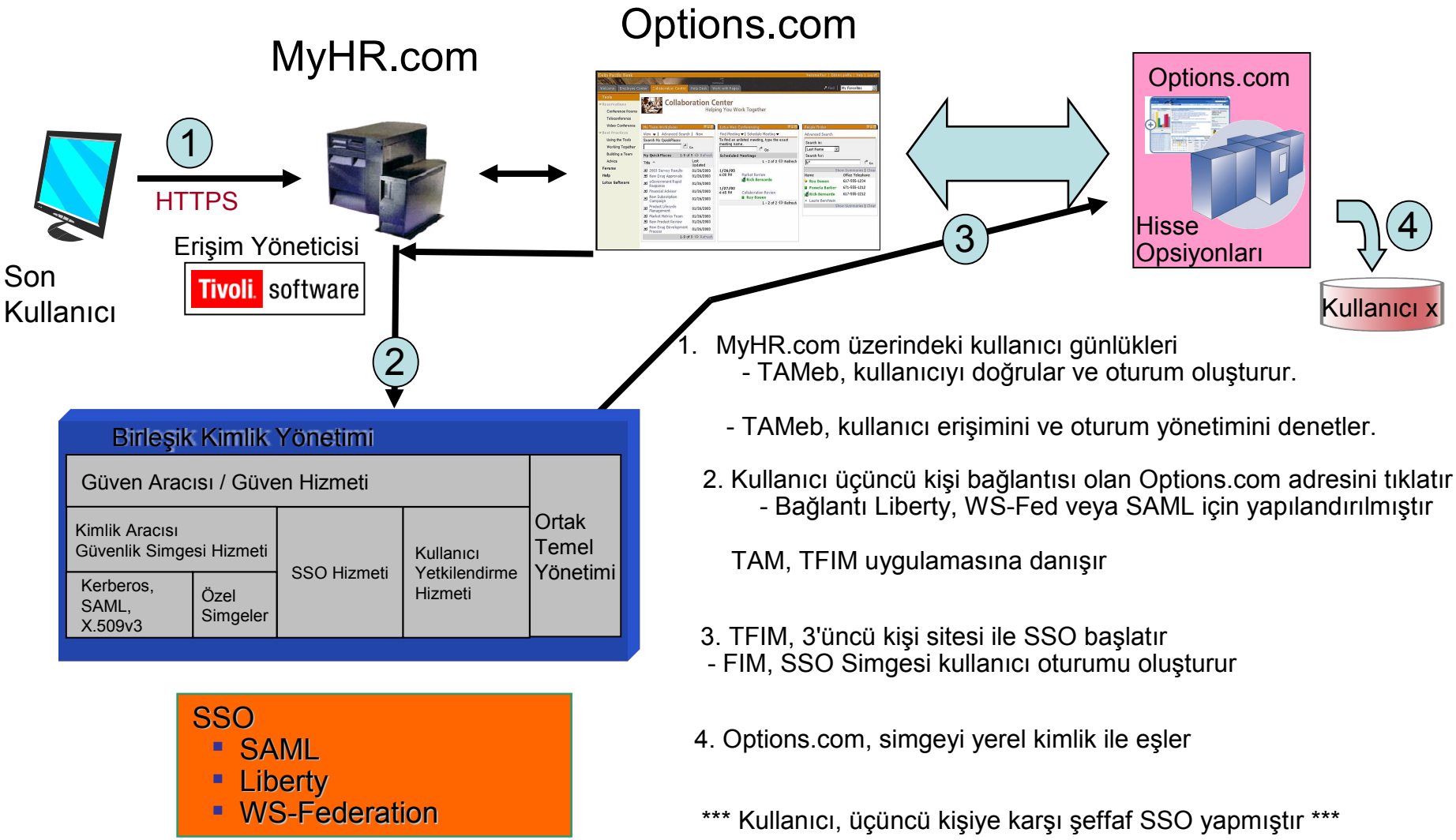
Tivoli Federated Identity Manager

Hesap numaranıza bakması için bir banka veznedarına ehliyetinizi vermek gibi

Gündelik yaşamda, bir ortamdan diğerine geçerken kim olduğunuzu kanıtlar.

TFIM bu kuralı, bir kimliğin bir etki alanından diğerine (veya bir Web hizmetinden diğerine) geçmesi şeklinde kullanır

Birleşik SSO nedir?



1. MyHR.com üzerindeki kullanıcı günlükleri
   - TAMeb, kullanıcıyı doğrular ve oturum oluşturur.

   - TAMeb, kullanıcı erişimini ve oturum yönetimini denetler.

2. Kullanıcı üçüncü kişi bağlantısı olan Options.com adresini tıklatır
   - Bağlantı Liberty, WS-Fed veya SAML için yapılandırılmıştır

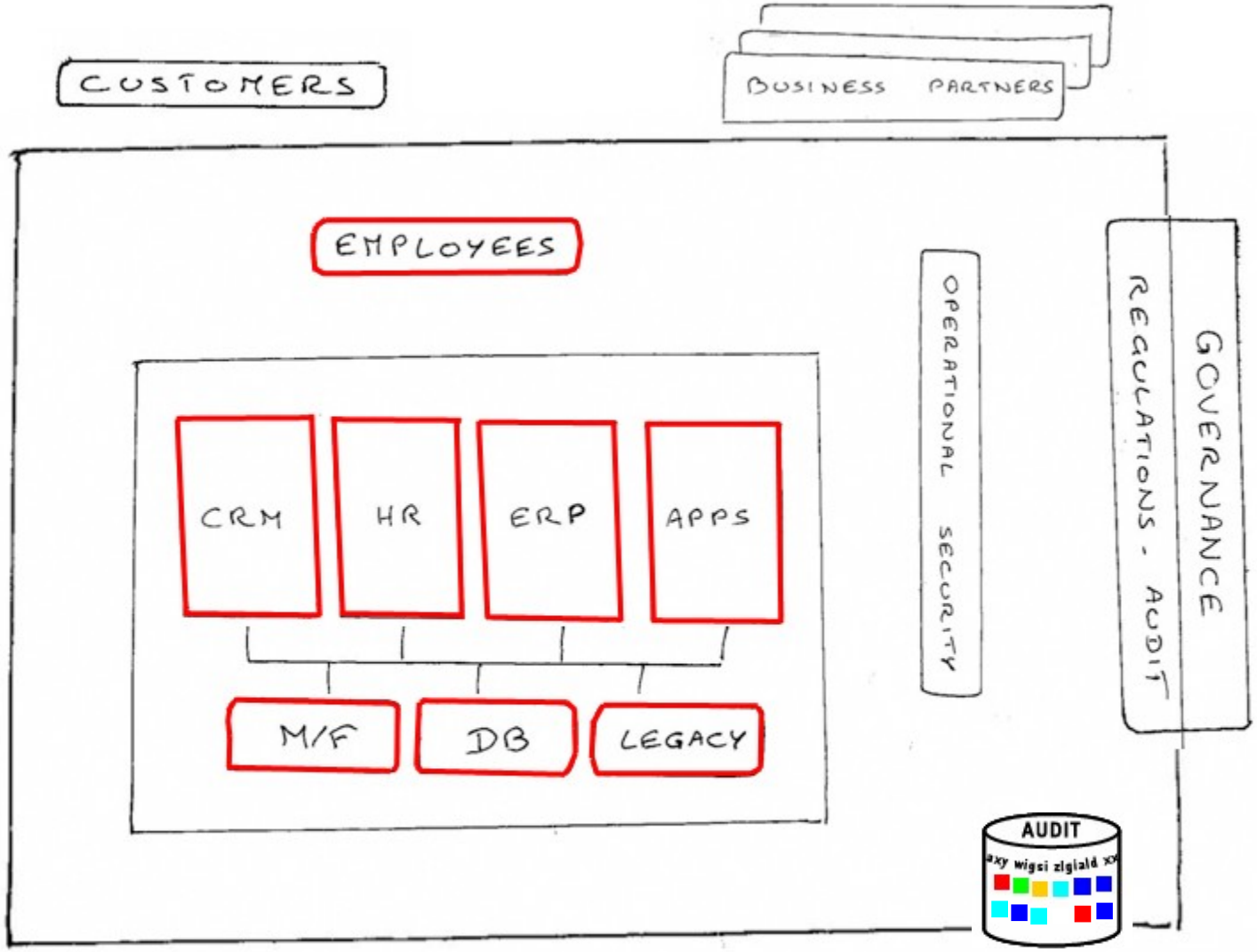
   TAM, TFIM uygulamasına danışır

3. TFIM, 3'üncü kişi sitesi ile SSO başlatır
   - FIM, SSO Simgesi kullanıcı oturumu oluşturur

4. Options.com, simgeyi yerel kimlik ile eşler

*** Kullanıcı, üçüncü kişiye karşı şeffaf SSO yapmıştır ***

... sunucuları ve masaüstlerini korur ...

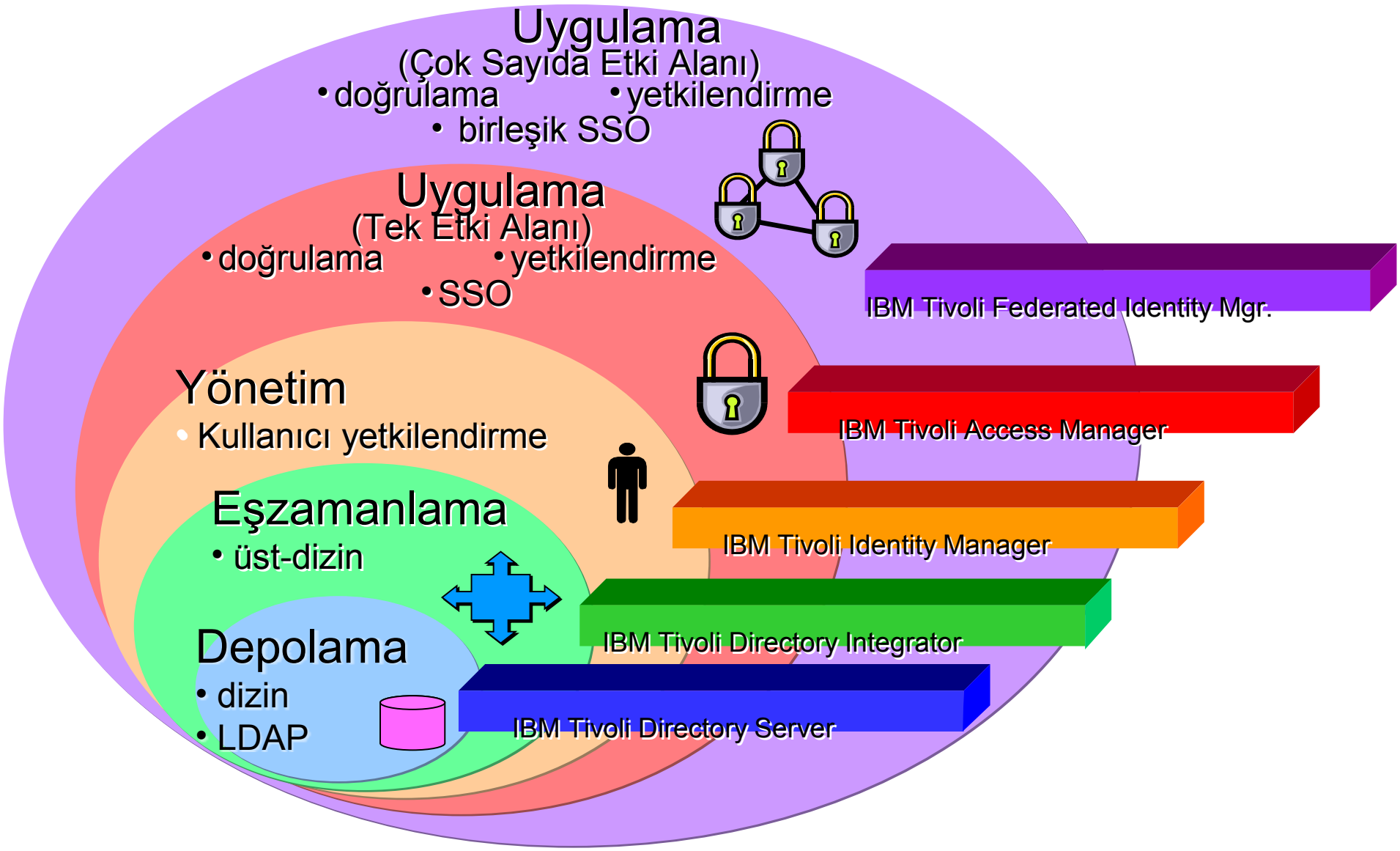


TAMOS / TSCM

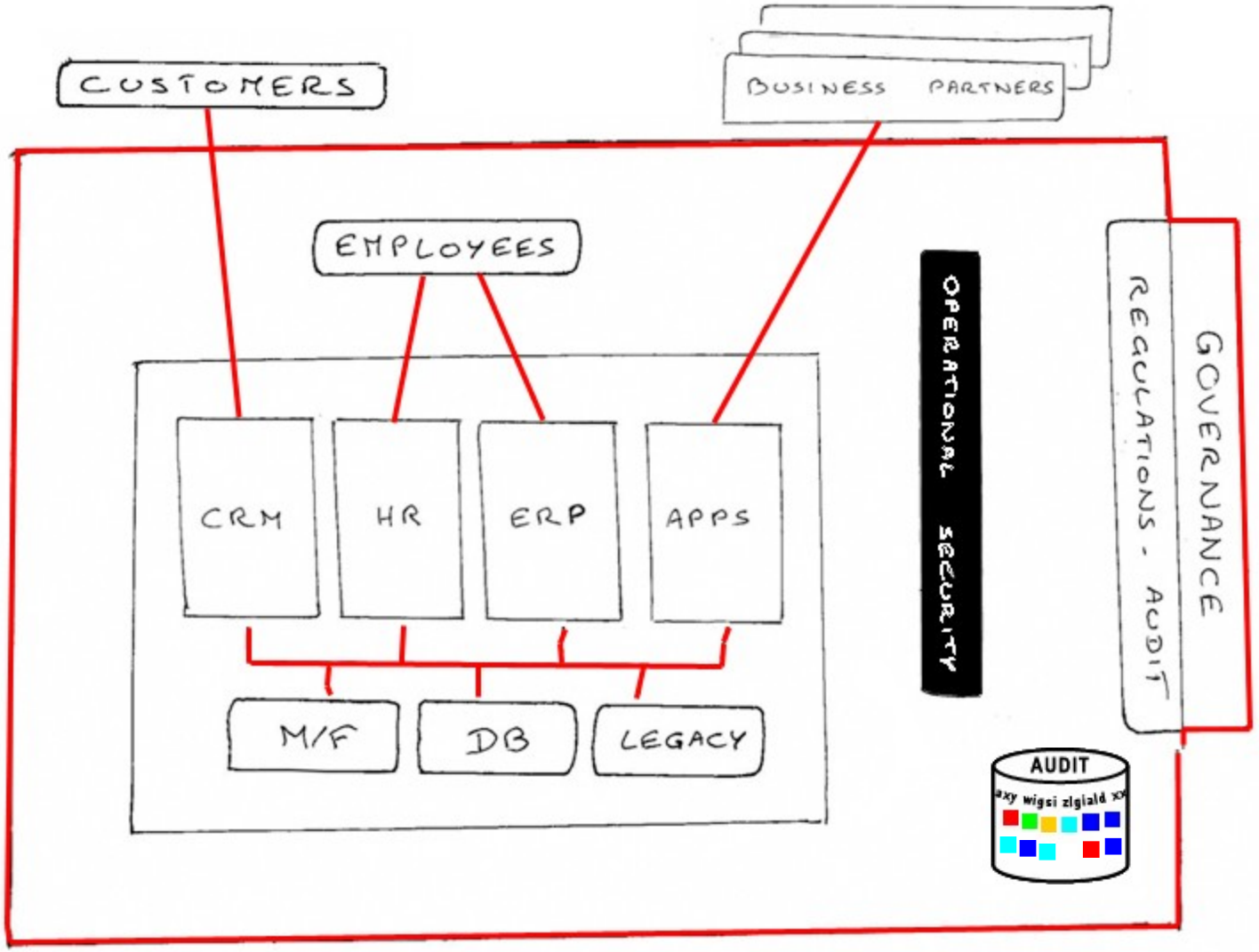
İşletim Sistemleri için Tivoli Access Manager

TAMOS, bir "gaz kolu" işlevi görür ve kullanıcıların (özellikle kök kullanıcıların) arzu edilmeyen veya hatalı/zararlı işlemler gerçekleştirmelerini önler.

Kimlik Yönetimi - Yüksek Düzeyde Teknoloji Yeniden Kullanımı

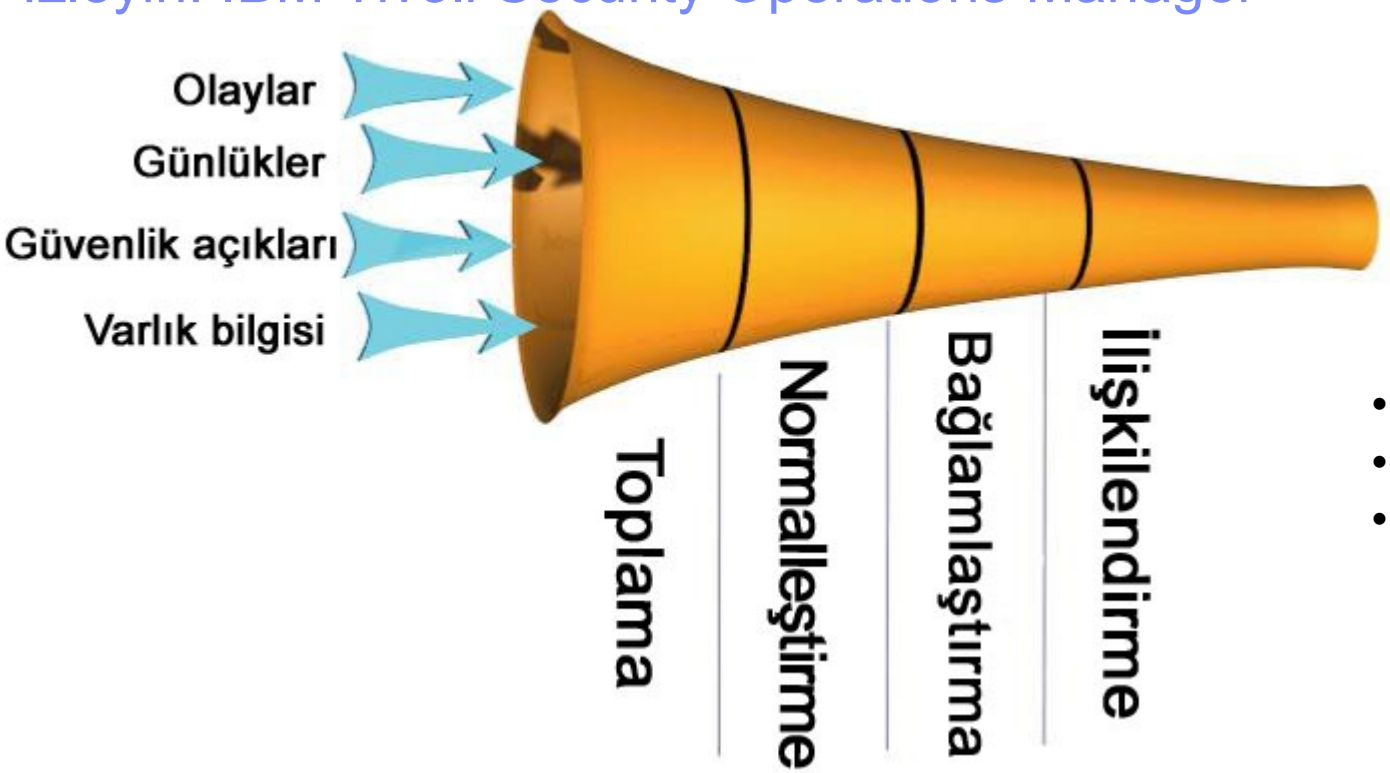


... ağın korunması ...



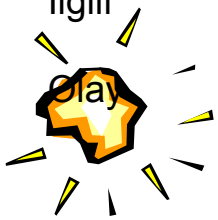
TSO M

İzleyin: IBM Tivoli Security Operations Manager



İşle

İlgili



- Etkinlikler
- Gösterge tabloları
- Raporlar

"TSOM, birleştirme ve ilişkilendirme sürecini otomatikleştirir. Hatalı tehdit algılamalarını azaltır ve ekibimi gerçek tehditlere karşı zamanında uyarır. Ürün, dört yıl ve bir geliştirici havuzu ile kendi tasarlayabileceğim ve üreteceğim ürünle yaklaşık olarak aynıdır."

~ NETCOOL/TSOM İletişim Kullanıcısı

TSOM, 200'den Fazla Olay/Günlük Kaynağını Destekler

Güvenlik Duvarları
Check Point Firewall-1
Cisco PIX
CyberGuard
Fortinet FortiGate
GNATBox
Juniper (Netscreen)
Linux IP Tables
Lucent Brick
Microsoft ISA Server
Nortel Switched Firewall
Stonesoft's StoneGate
Secure Computing's Sidewinder
Symantec's Raptor
SonicWALL
Sun SunScreen

Güvenlik Açığı Değerlendirmesi
Nessus
Vigilante
ISS Internet Scanner
QualysGuard
Foundstone
eEye Retina, REM
SPI Dynamics WebInspect
nCircle IP360
Harris STAT
Tenable Lightning

Yönlendiriciler/Anahtarlar
Cisco Routers
Cisco Catalyst Switches
Cisco RCMD
Foundry Switches
F5 Big IP, 3-DNS
Juniper JunOS
TACACS / TACACS+
Nortel Ethernet Routing Switch 5500, 8300, 8600, 400 series
Extreme Networks

İlke Uygunluğu
Vericept

Ağa İzinsiz Giriş Algılama/Önleme
McAfee Intrushield
Sourcefire Network Sensor
Sourcefire RNA
Juniper IDP
ISS RealSecure
ISS Proventia G, M
ISS BlackICE Sentry
Cisco Secure IDS
SNORT IDS
Enterasys Dragon
Nortel Threat Protection System (TPS)
Intrusion's SecureNetPro
Mirage Networks
NFR NID
Symantec ManHunt
ForeScout ActiveScout
QRadar
Top Layer Attack Mitigator
Labrea TarPit
IP Angel
Lancope StealthWatch
Tipping Point UnityOne NDS
Arbor Networks PeakflowX
Mazu Networks

Ana Sistem Tabanlı İzinsiz Giriş Algılama/Önleme
Type80 SMA_RT (z/OS-Mainframe RACF)
PowerTech (iSeries-AS/400)
Cisco CSA
NFR HID
IBM Netcool SSMs
Sana
Snare
Symantec Intruder Alert (ITA)
Sygate Secure Enterprise
Tripwire
ISS BlackICE Defender
ISS Server Sensor
McAfee Entercept

VPN
Juniper SSL VPN
Nortel VPN Router (Contivity)
Check Point
Cisco IOS VPN
Cisco VPN 3000
Juniper VPN
Nortel VPN Gateway (SSL VPN)

Ek olarak masaüstü güvenlik duvarları, eposta güvenliği, ağ altyapısı . . .

Uygulamalar
Apache
BEA
Linux/UNIX (FTPD, SENDMAIL, …)
Microsoft IIS
IBM WebSphere
Lotus Domino
Oracle
Peoplesoft
SAP R3
Sun iPlanet
VMWare ESX
IBM DB2 (yakında sunulacak)

İşletim Sistemi Günlükleri, Günlük Platformları
AIX (IBM)
Apple
RedHat Linux
SuSE Linux
HP/UX
Microsoft Windows Event Log (W2K3 DHCP, W2K DHCP, IIS)
Microsoft SNMP Trap Sender
Nokia IPSO
Novell NetWare
OpenBSD
Solaris (Sun) *
Tru64
Tripplight UPS
Monitorware SYSLOG
KiwiSyslog
zOS-Mainframe IDS

Virüse Karşı Koruma
CipherTrust IronMail
McAfee Virus Scan
Norton AntiVirus (Symantec)
McAfee ePO
Trend Micro InterScan

Uygulama Güvenliği
Blue Coat Proxy
Nortel ITM (Intelligent Traffic Mgmt)
Teros APS
Sentryware Hive
IBM DataPower(yakında sunulacak)

Erişim ve Kimlik Yönetimi
IBM Tivoli Access Manager
IBM Tivoli Identity Manager
CA eTrust Access
CA eTrust Secure Proxy Server
CA eTrust Siteminder (Netegrity)
Microsoft Active Directory
Netscape Directory Server
RSA SecurID RADIUS (ACE)
Oracle Identity Management (Oblix)
Sun Java System Directory Server
Cisco ACS_

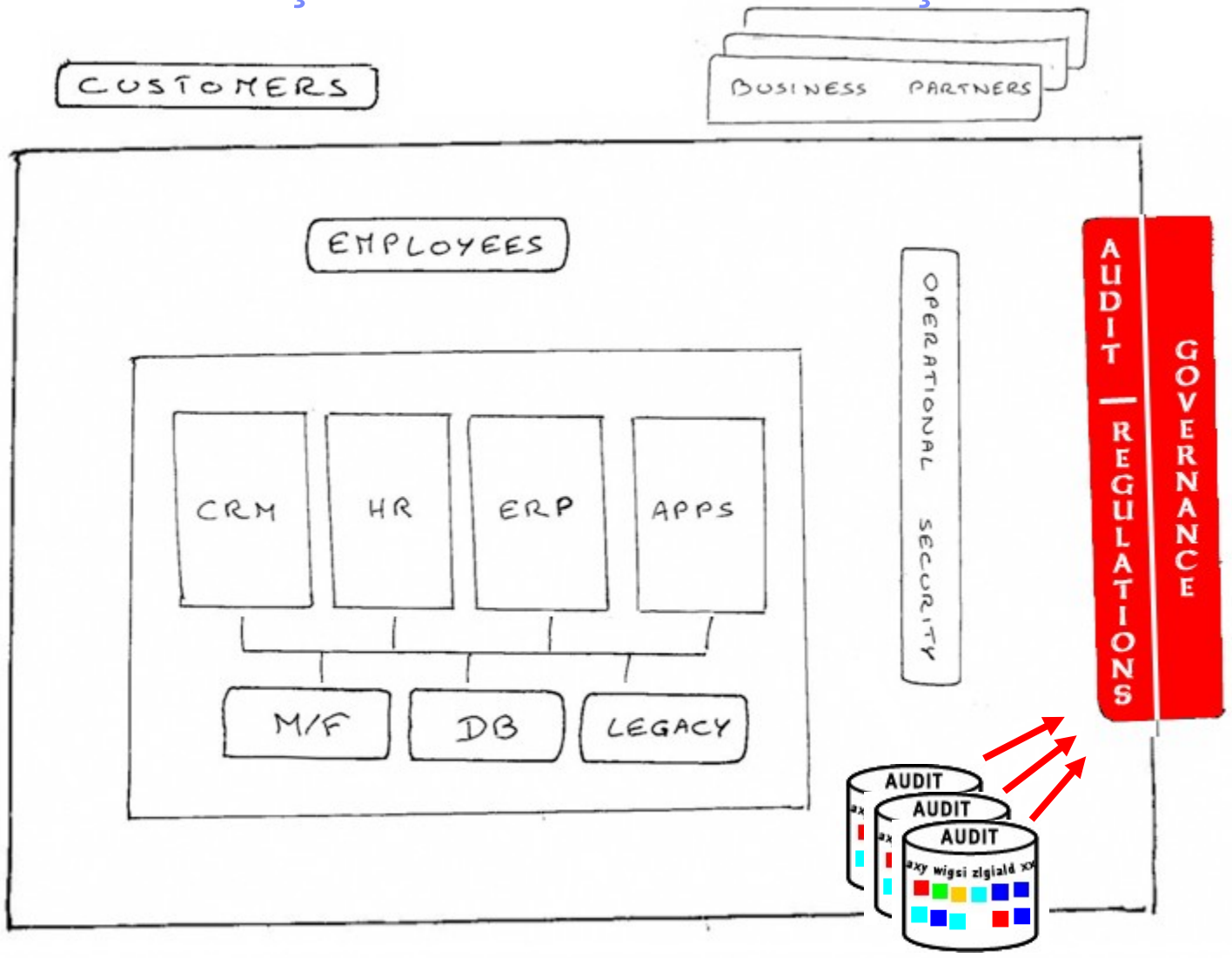
Kablosuz Bağlantı Güvenliği
AirMagnet
AirDefense

Yönetim Sistemleri
TSOM, şu sistemlere yükseltir:
IBM Netcool (Micromuse)
IBM/Tivoli Enterprise Console
Cisco Information Center
Remedy ARS
HP OpenView
CA Unicenter

Yönetim Sistemleri
TSOM'ye olay kaynağı:
Check Point Provider-1
CiscoWorks
IBM Netcool (Micromuse)
ISS SiteProtector
Juniper Global Pro (Netscreen)
Juniper NSM (Netscreen)
Tripwire Manager
Intrusion, Inc. SecureNet Manager
McAfee ePO
Nortel Defense Center
Sourcefire Defense Center
Q1 QRadar Mgmt Server

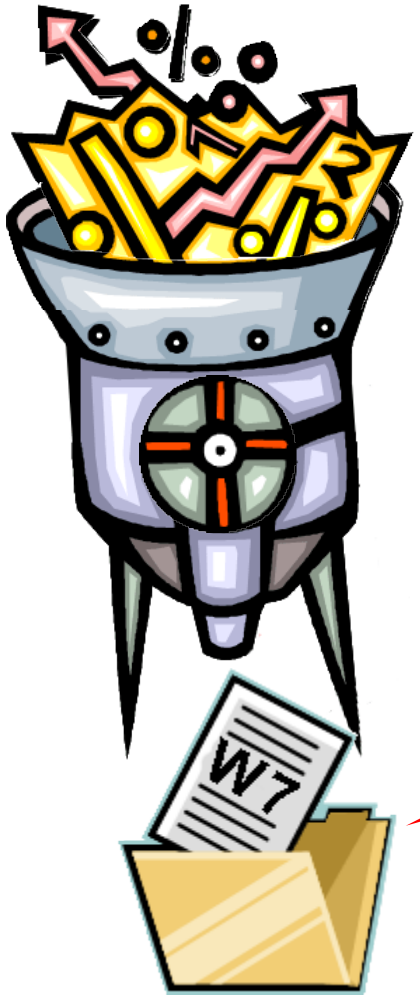
Keşif Araçları
Lumeta IPSonar
NMAP
Sourcefire RNA

Kurumsal Yönetişim Tarafından İzlenir ve Ölçülür



TSIEM / TCIM

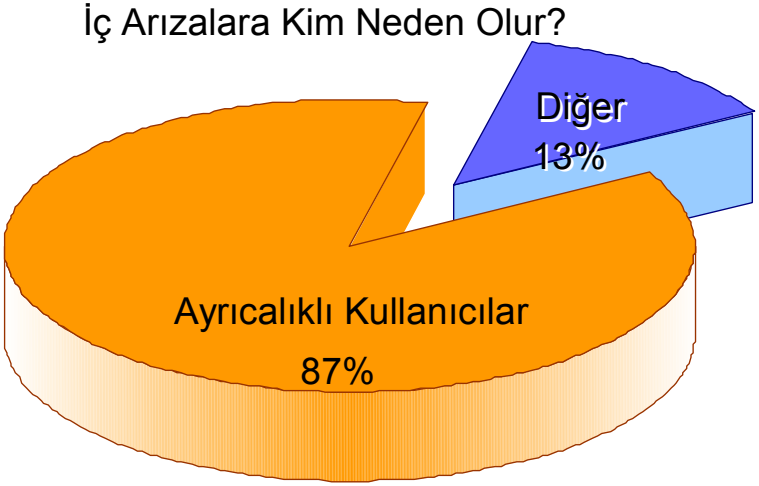
Tivoli Compliance Insight Manager



Pek çok farklı kaynaktan çok miktarda denetim bilgisi

Açık, net, normalleştirilmiş denetim bilgisi

Güvenilen kullanıcıların izlenmesi artık bir seçenek değil



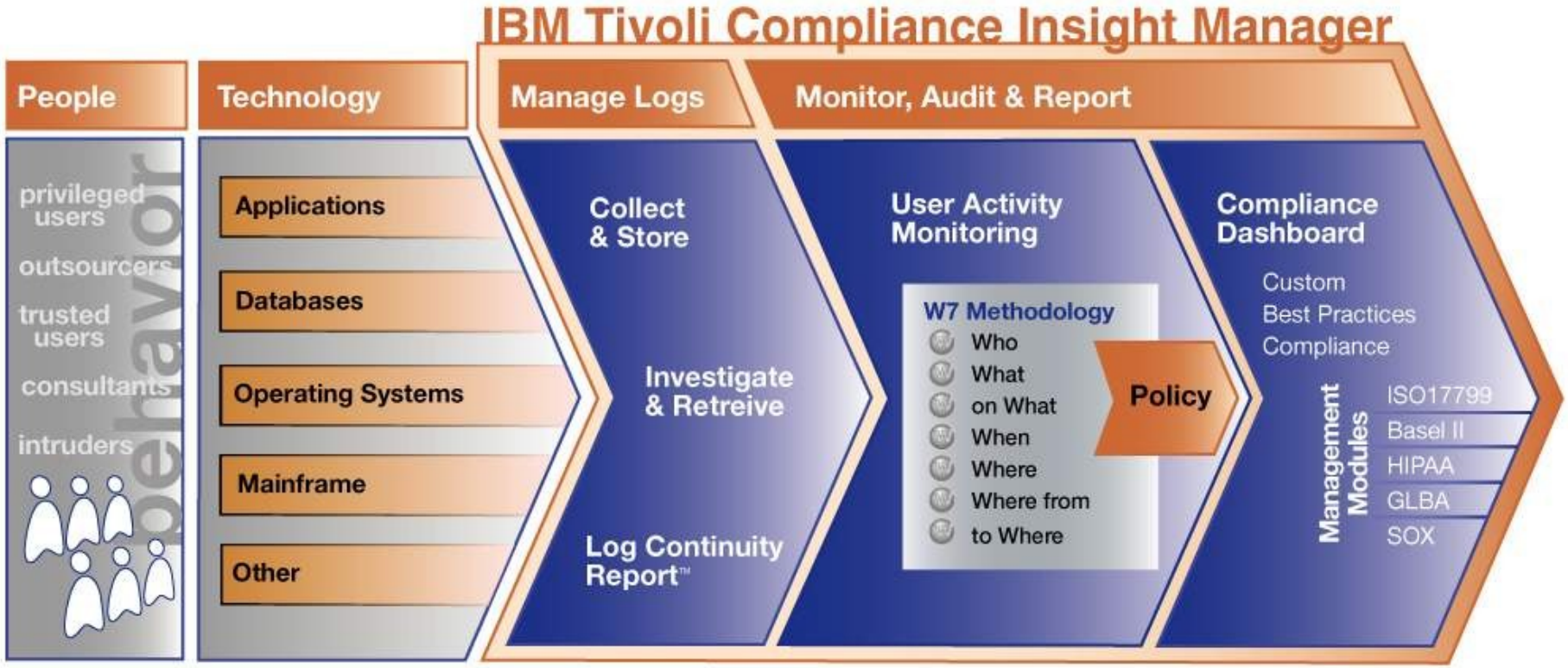
Kaynak: USSS/CET Insider Threat Survey 2005

Bu arızalar göz ardı edilemeyecek kadar yüksek maliyetlidir:

- İç saldırılar, brüt yıllık gelirin %6'sına mal olur
- Sadece ABD'de 400 milyar ABD Dolarına mal olur

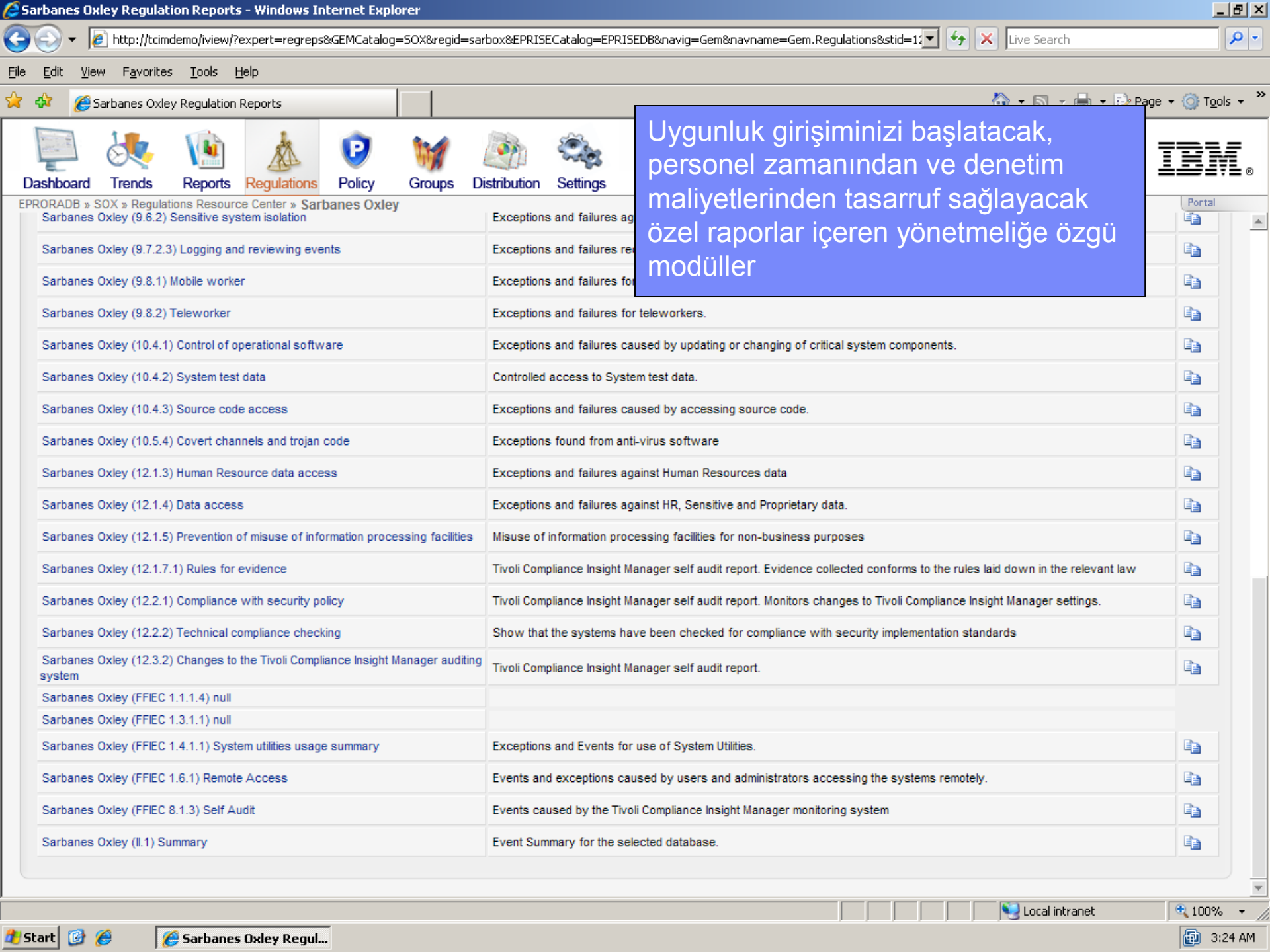
TCIM, Arzu Edilen Davranışı Gerçek Davranışla Karşılaştırır

Tivoli Compliance Insight Manager



3 Temel Nokta:

1. Kaynak tipleri arasında
2. W7 Teknolojisi
3. Uygunluk Yönetmeliğine Göre Raporlar


Sarbanes Oxley Regulation Reports - Windows Internet Explorer
http://tcimdemo/iview/?expert=regreps&GEMCatalog=SOX&regid=sarbox&EPRISECatalog=EPRISEDB&navig=Gem&navname=Gem.Regulations&stid=1
Live Search
File Edit View Favorites Tools Help
Sarbanes Oxley Regulation Reports
Page Tools
Dashboard Trends Reports Regulations Policy Groups Distribution Settings
IBM
EPRORADB » SOX » Regulations Resource Center » Sarbanes Oxley
Portal
Uygunluk girişiminizi başlatacak, personel zamanından ve denetim maliyetlerinden tasarruf sağlayacak özel raporlar içeren yönetmeliğe özgü modüller
Sarbanes Oxley (9.6.2) Sensitive system isolation
Exceptions and failures ag
Sarbanes Oxley (9.7.2.3) Logging and reviewing events
Exceptions and failures re
Sarbanes Oxley (9.8.1) Mobile worker
Exceptions and failures fo
Sarbanes Oxley (9.8.2) Teleworker
Exceptions and failures for teleworkers.
Sarbanes Oxley (10.4.1) Control of operational software
Exceptions and failures caused by updating or changing of critical system components.
Sarbanes Oxley (10.4.2) System test data
Controlled access to System test data.
Sarbanes Oxley (10.4.3) Source code access
Exceptions and failures caused by accessing source code.
Sarbanes Oxley (10.5.4) Covert channels and trojan code
Exceptions found from anti-virus software
Sarbanes Oxley (12.1.3) Human Resource data access
Exceptions and failures against Human Resources data
Sarbanes Oxley (12.1.4) Data access
Exceptions and failures against HR, Sensitive and Proprietary data.
Sarbanes Oxley (12.1.5) Prevention of misuse of information processing facilities
Misuse of information processing facilities for non-business purposes
Sarbanes Oxley (12.1.7.1) Rules for evidence
Tivoli Compliance Insight Manager self audit report. Evidence collected conforms to the rules laid down in the relevant law
Sarbanes Oxley (12.2.1) Compliance with security policy
Tivoli Compliance Insight Manager self audit report. Monitors changes to Tivoli Compliance Insight Manager settings.
Sarbanes Oxley (12.2.2) Technical compliance checking
Show that the systems have been checked for compliance with security implementation standards
Sarbanes Oxley (12.3.2) Changes to the Tivoli Compliance Insight Manager auditing system
Tivoli Compliance Insight Manager self audit report.
Sarbanes Oxley (FFIEC 1.1.1.4) null
Sarbanes Oxley (FFIEC 1.3.1.1) null
Sarbanes Oxley (FFIEC 1.4.1.1) System utilities usage summary
Exceptions and Events for use of System Utilities.
Sarbanes Oxley (FFIEC 1.6.1) Remote Access
Events and exceptions caused by users and administrators accessing the systems remotely.
Sarbanes Oxley (FFIEC 8.1.3) Self Audit
Events caused by the Tivoli Compliance Insight Manager monitoring system
Sarbanes Oxley (II.1) Summary
Event Summary for the selected database.
Local intranet
100%
Start
Sarbanes Oxley Regul...
3:24 AM

Tivoli Key Lifecycle Manager

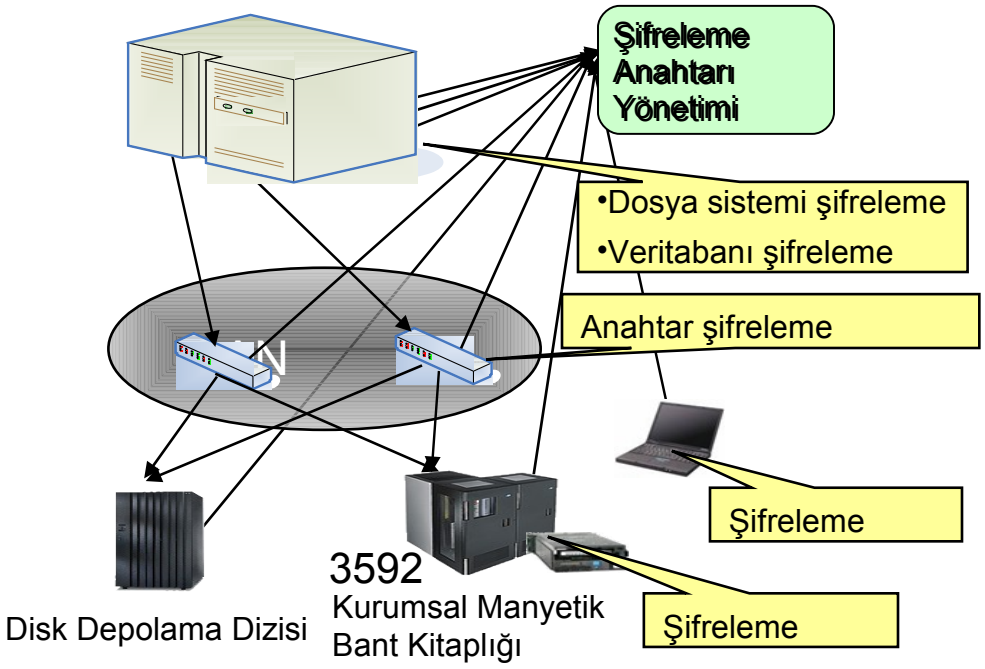
Şifreleme, güvenlik altyapınızın kalbiyse

TKLM, bu kalbin sağlığını takip eden bir gözlemcidir

Tivoli Key Lifecycle Manager (TKLM)

Sektörde benzersiz!

- Anahtar Yaşam Döngüsü Yönetimi güvenliği güçlendirir
  - Anahtar yönetimi (simetrik, asimetrik)
  - Kurallar ve kısıtlamalar yoluyla yönetim
  - Uygunluk raporlaması için denetim yolları
  - Safe-harbor durumları için kanıt
- Standart tabanlı
  - Genel anahtarlar
  - Akıllı kartlar, PCMCIA kartları
  - Depolanan verilerin şifrelenmesi
  - Sertifika yönetimi protokolü
  - Sertifika durumu denetimi
- Birden Çok Kanaldan sunulur
  - Yazılım lisansı
  - IBM Depolama ürünlerinin özelliğidir
  - OEM olarak teslim edilebilir



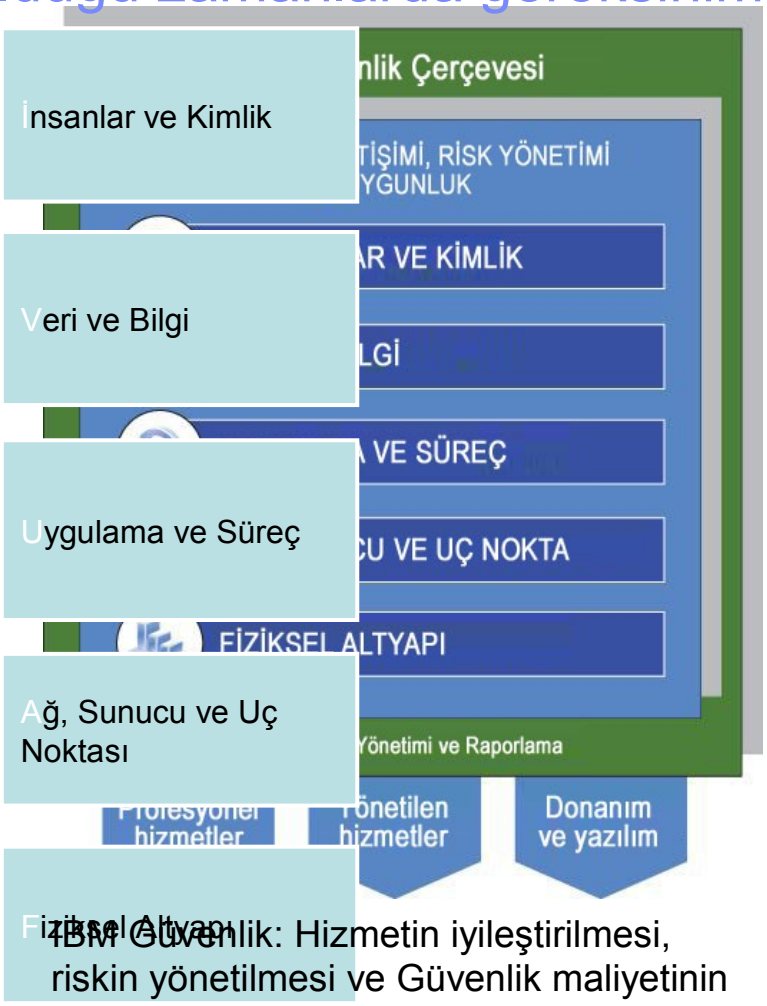
TKLM ve Yatırım Getirisi

TKLM, müşteriler için önemli ölçüde yatırım getirisi sağlayabilir

- Yasal keşfe maruz kalmayı sınırlar - olay başına ortalama 150 - 250 bin ABD Doları
- Gizliliğin ihlaline karşı korur - Kayıt başına 200 ABD Doları, olay başına milyonlar
- Kurulumu, yapılandırılması kolaydır
- Sınırlı operasyon maliyetleri

Küresel Güvenlik Erişimi ve Uzmanlığı

IBM, tüm BT etki alanları için sunduğu çözümlerle belirsizliğin hakim olduğu zamanlarda gereksinim duyduğunuz iş yanıtlarını sağlar

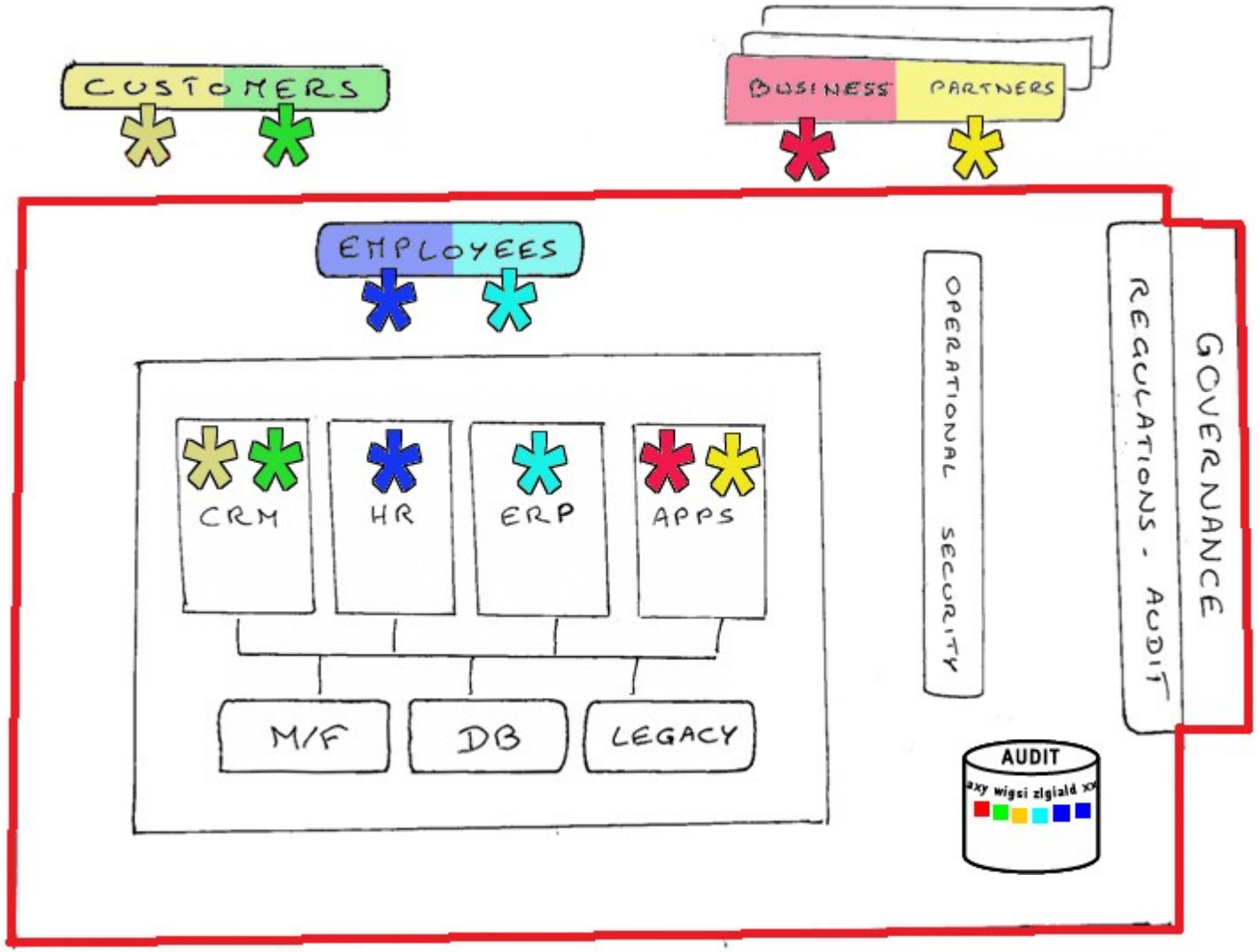


- IBM Güvenlik: Hizmetin iyileştirilmesi, riskin yönetilmesi ve Güvenlik maliyetinin ödün vermeden düşürülmesi

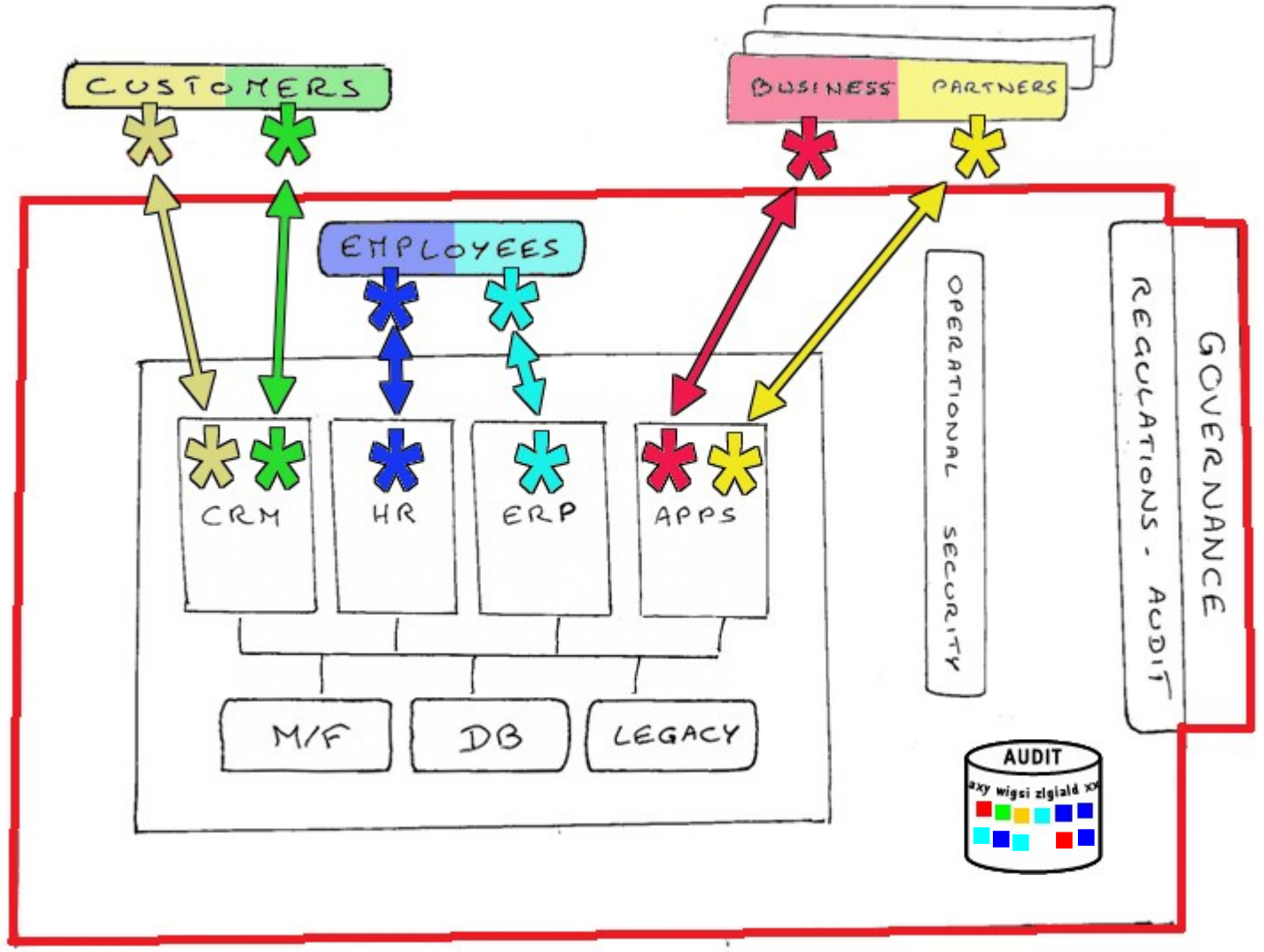
- IBM, bugün pazarda *kritik denetimleri uçtan uca kapsayan tek güvenlik satıcı firmasıdır.*

- IBM Kanıt Noktaları
  - Güvenlik girişimlerinde çalışan 15.000 araştırmacı, geliştirici ve konu uzmanı
  - 3.000'in üzerinde güvenlik ve risk yönetimi patenti
  - 200'ün üzerinde güvenlik müşterisi referansı ve 50'nin üzerinde örnek olay incelemesi
  - System z ortamının güvenliğinin sağlanmasında 40 yılı aşkın kanıtlanmış başarı
  - 2008 yılında 1,5 milyar Dolar güvenlik harcaması

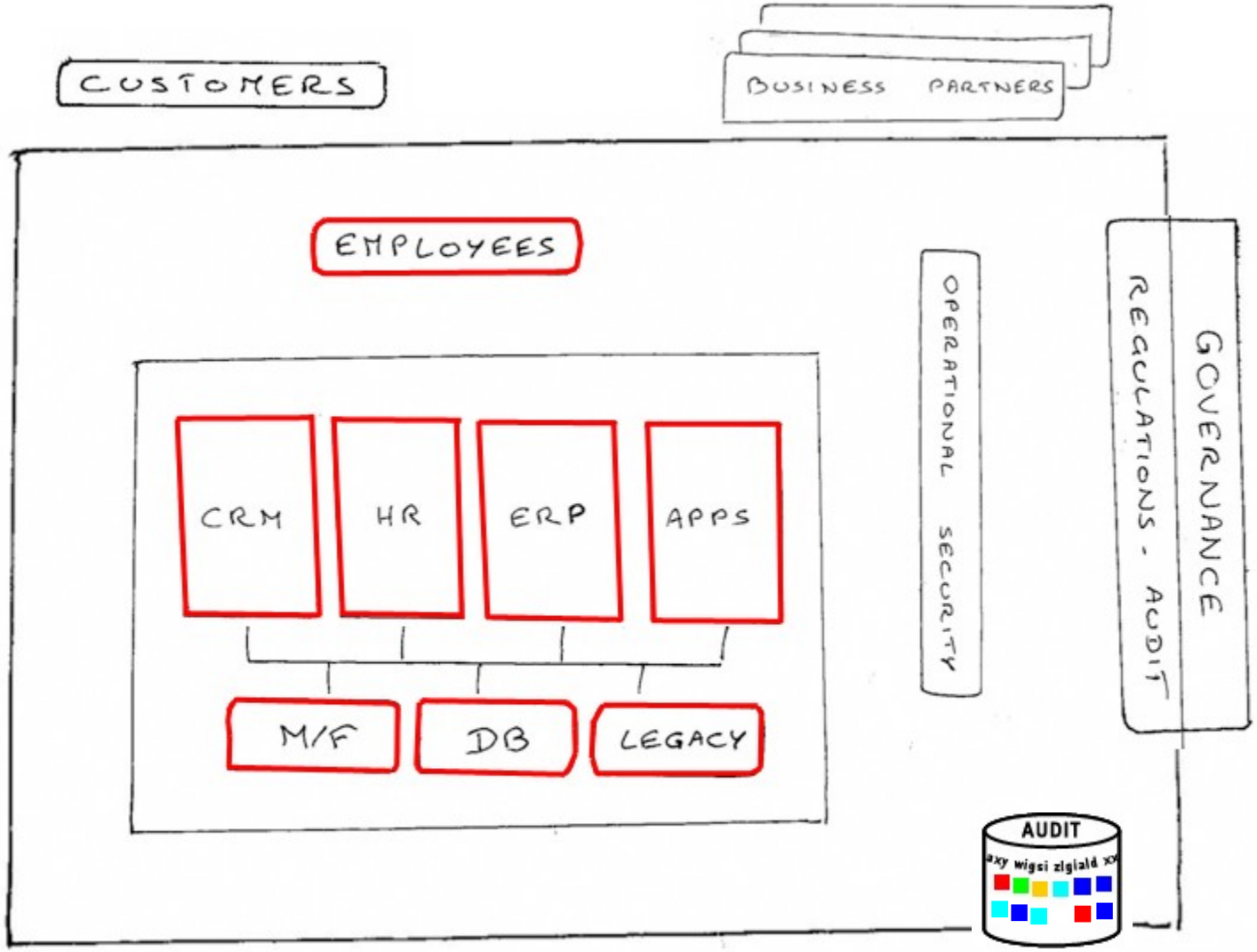
Kimlik Yönetimi...



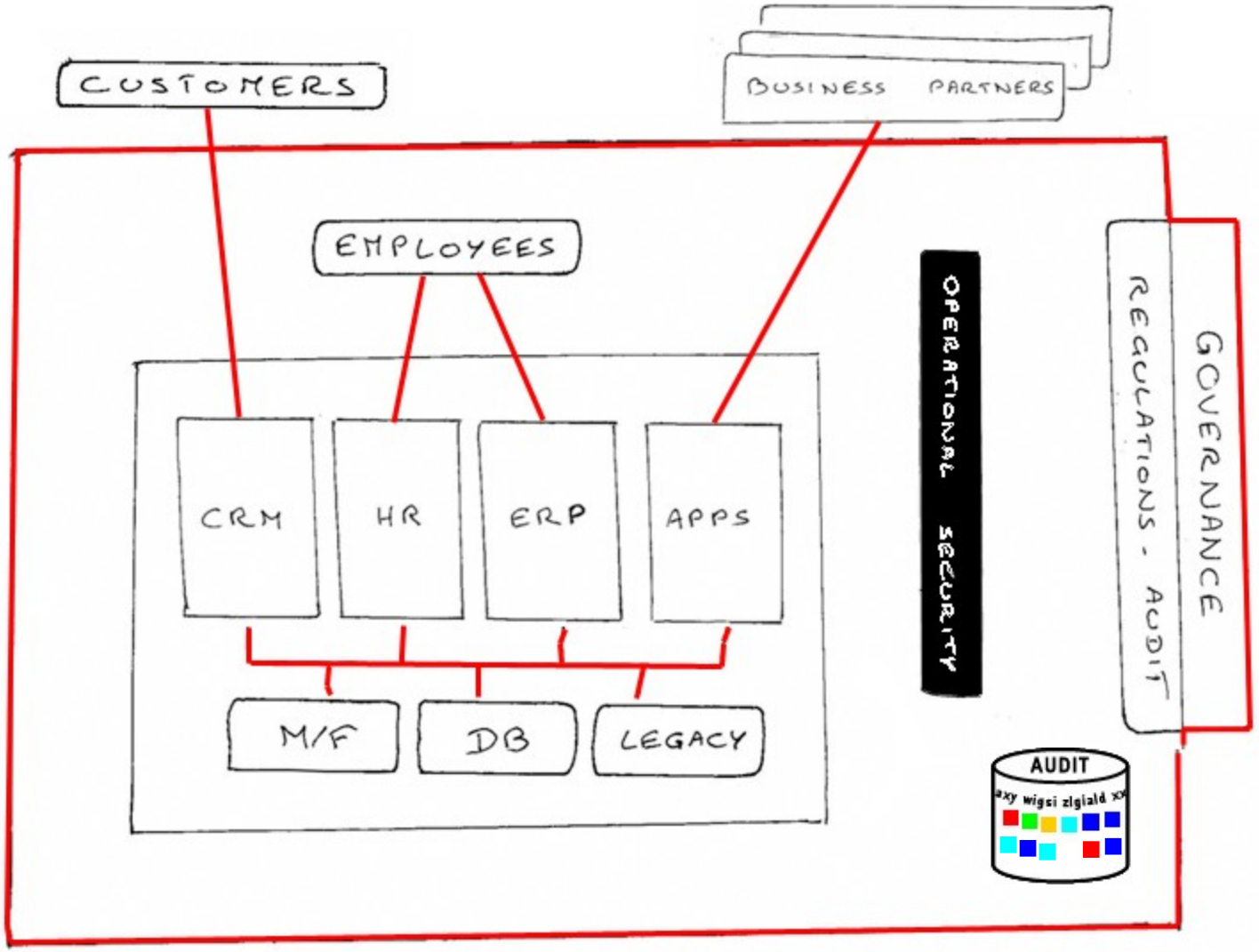
Erişim Yönetimi...



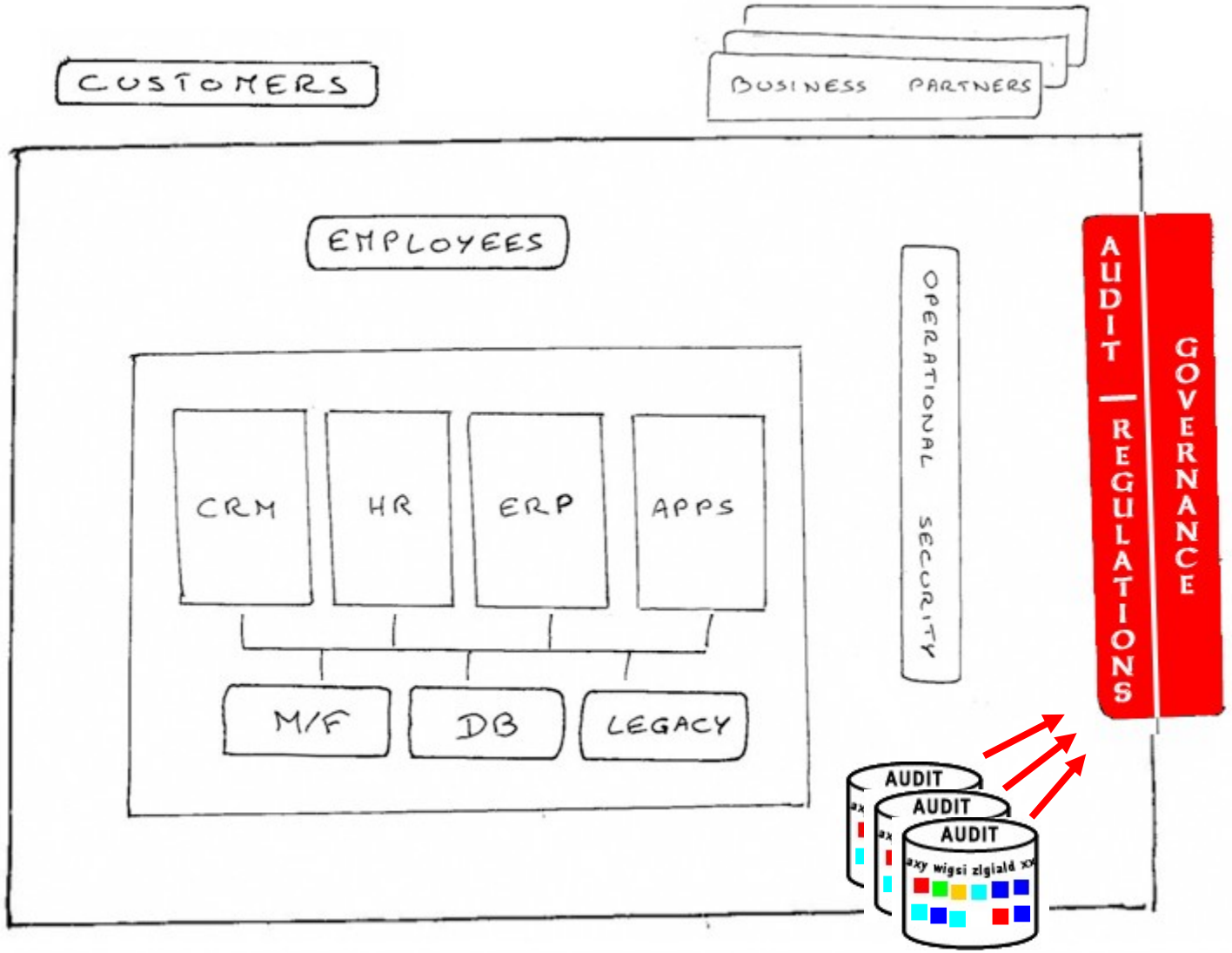
Sunucuları ve Masaüstlerini korunması...



Ağın Korunması...



Raporlanma...



TEŞEKKÜRLER...

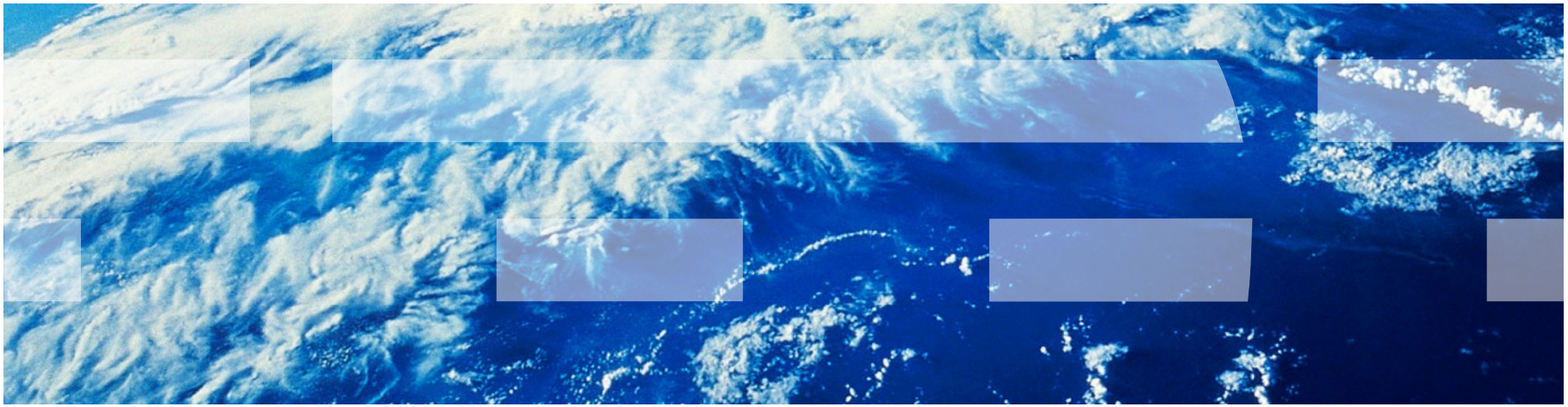
IBM yazılım zirvesi '09

Tansel ZENGİNLER

Tel : 0530 317 1675
e-Mail : tansel@tr.ibm.com

Certified for IBM. Tivoli. software

ITIL®



Bu sunum 22 Ekim 2009 tarihinde İstanbul Swissotel the Bosphorus'da yapılan Yazılım Zirvesi 2009 için hazırlanmıştır.

http://www.ibm.com/software/tr