Bulut Bilişim ve Bilgi Güvenliği

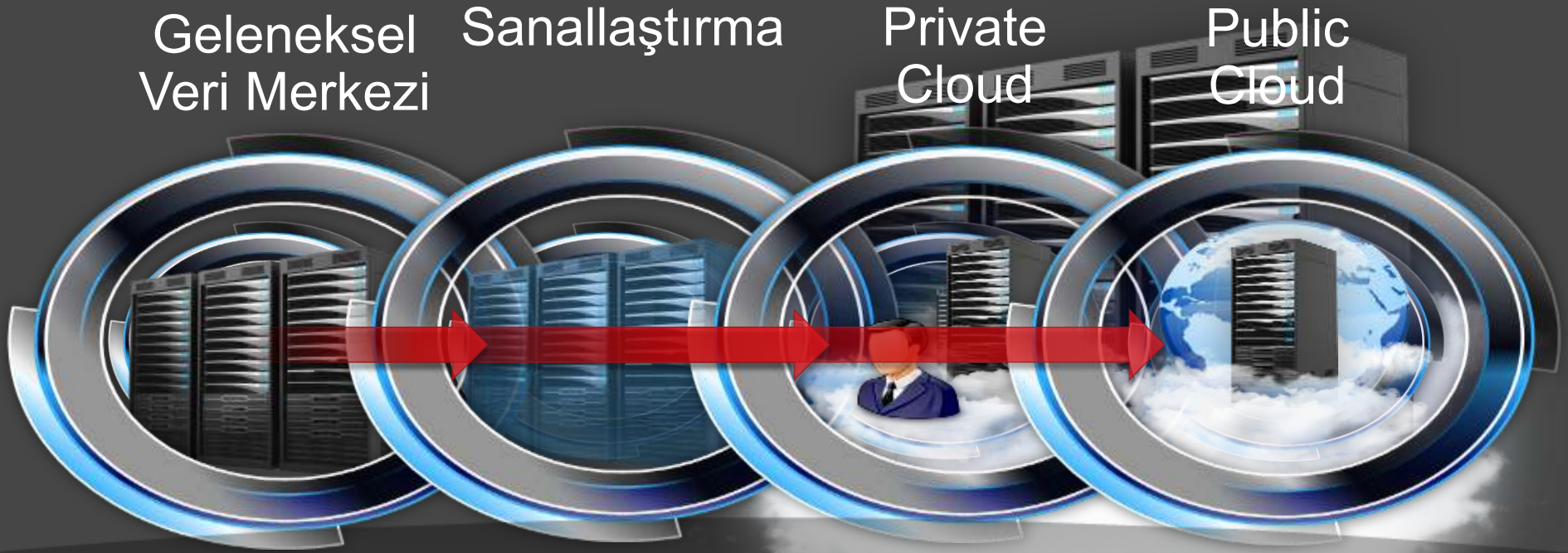
Buğra Karabey (CISM)
National Technology Officer
Microsoft Türkiye

Gelecek…

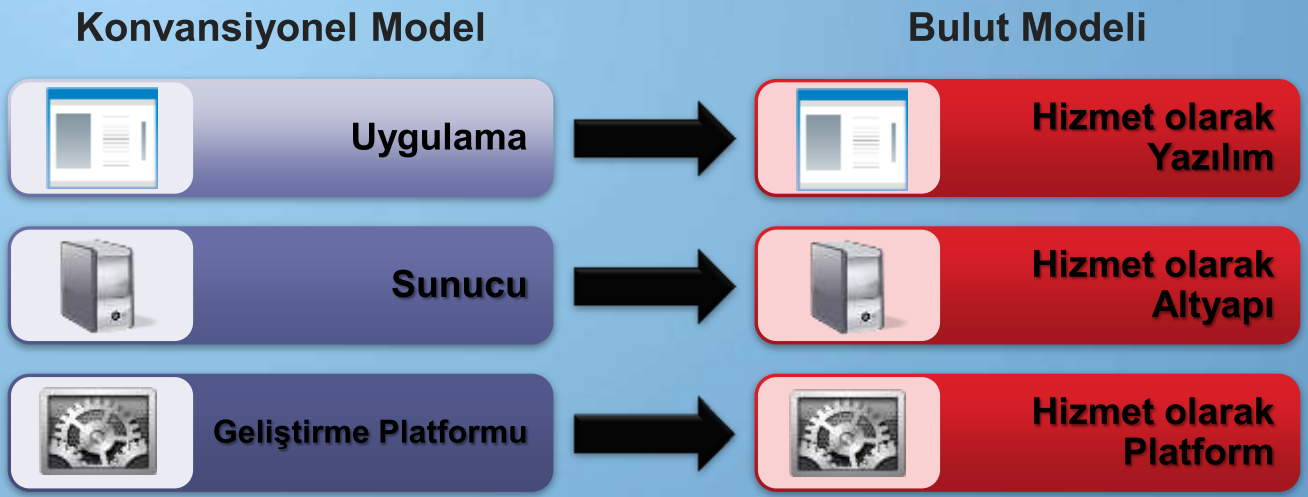
Bulut Bilişim- Bizim tanımımız

“Internet teknolojileri kullanarak, kullandığın-kadar-öde bazında ve de self servis olarak sunulan, **standart hale getirilmiş**, **y**azılım, uygulama **p**latformu, **a**ltyapı tarzındaki BT yetenekleri.”

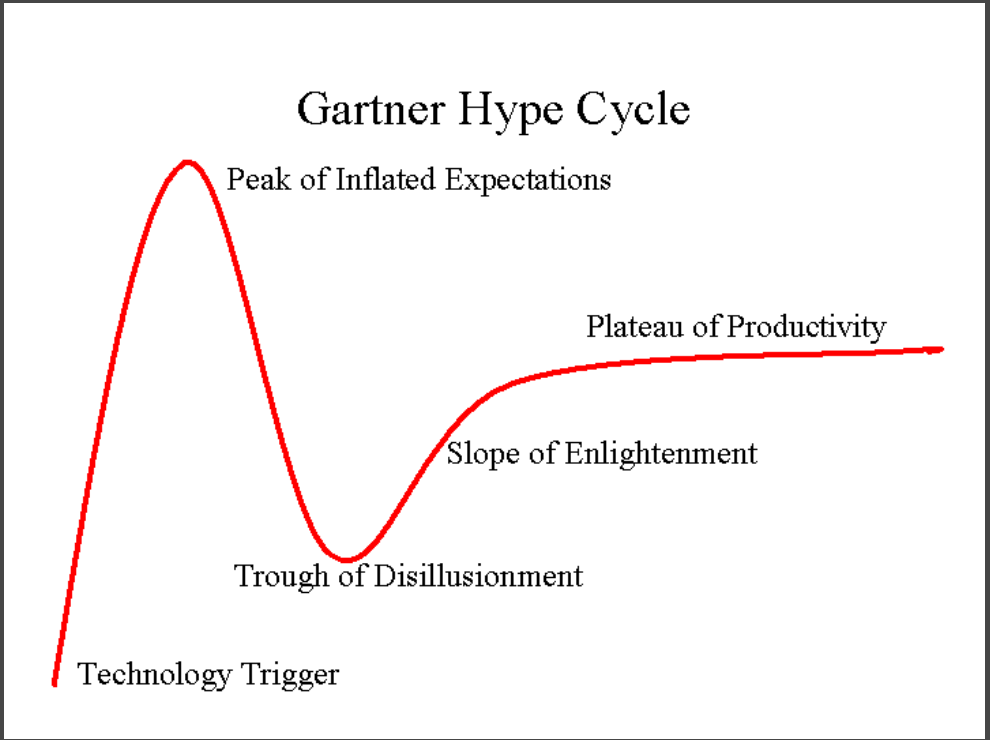
Veri Merkezi'nin değişimi



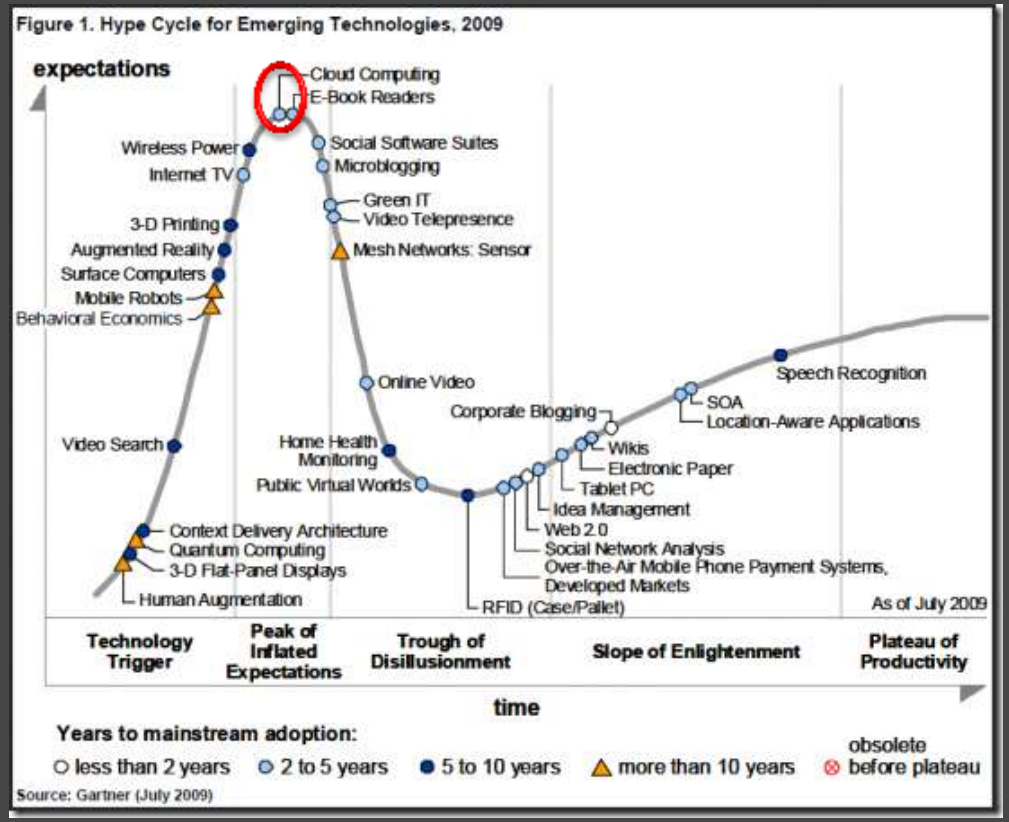
Bulut çeşitleri



Teknoloji heyecan (hype) eğrisi



Teknoloji heyecan (hype) eğrisi



IT Profile and Forecast: Turkey

	2008	2009	2010	2011	2012	2013	08-13 CAGR
Spending (Million LOCAL)							
IT Hardware	7,547	7,509	8,150	9,255	10,320	11,261	8.3%
Software	848	830	911	1,042	1,179	1,338	9.6%
IT Services	1,126	1,146	1,238	1,369	1,524	1,688	8.4%
Total IT	9,520	9,486	10,299	11,667	13,022	14,287	8.5%
IT Contribution							
IT/GDP (%)	1.0%	1.0%	1.1%	1.2%	1.3%	1.4%	
IT Tax Revenues (Million LOCAL)	2,534	2,322	2,662	2,968	3,291	3,627	7.4%
Total Number of IT Companies	7,868	7,862	8,067	8,380	8,680	8,966	2.6%
IT Employment							
Total Number of Employees	155,731	155,687	165,764	181,564	197,680	213,769	6.5%
Total Software-Related Employees	44,339	45,878	51,647	57,979	63,905	71,544	10.0%
Cloud plus Clients							
Net New Business Revenues (Million LOCAL)	-	-	904	2,220	4,021	6,490	

Source: IDC Economic Impact Study, 2009

Microsoft'un Bulut Bilişim Güvenliği Deneyimi

Bulut Güvenliği

- Cloud Security Alliance
  - Top Threats to Cloud Computing V1.0
  - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
- ENISA (European Network and Information Security Agency)
  - Cloud Computing: Benefits, Risks and Recommendations for Information Security

CSA- Bulut Bilişimde Kritik Odak Alanlarında Güvenlik Rehberi

- 13 Alanda (Domain) Best Practice'ler ve tavsiyeler;
  - D1: Bulut Bilişim Mimari Çerçevesi
  - Yönetişim Alanları (Governance Domains)
    - D2: Yönetişim ve Kurumsal Risk Yönetimi
    - D3: Adli Bilişim
    - D4: Uyum ve denetim (Compliance and Audit)
    - D5: Bilgi Hayat Çevrimi Yönetimi
    - D6: Taşınabilirlik ve birlikte çalışabilirlik
  - Operasyonel Alanlar
    - D7: Güvenlik, İş sürekliliği ve Disaster Recovery
    - D8: Veri Merkezi İşlemleri
    - D9: Olay müdüdahale, bildirim ve çözüm (Incident response, notification and remediation)
    - D10: Uygulama güvenliği
    - D11: Kriptolama ve anahtar yönetimi
    - D12: Kimlik ve ereişim yönetimi
    - D13: Sanallaştırma

Bulutta Güvenliğin karşısındaki ana tehditler (CSA)

- Bulut Bilişimin kötü amaçlı kullanımı
- Güvenli olmayan Uygulama-Program Arayüzleri (API)
- Kötü niyetli personel
- Ortak teknoloji zaafiyetleri
- Veri kaybı ve sızıntısı
- Hesap, hizmet ve trafik çalınması
- Bilinmeyen risk profili

Bulut Bilişimin kötü amaçlı kullanımı (Domain 8&9)

Iaas	PaaS	SaaS

- Kötü amaçlı kod yazarları, spam'ciler, Bulut ortamını kendi işlemleri için kullanmakta. Nispeten anonim bir ortam ve de bedelsiz deneme kullanımlar mümkün.
- Şifre kırma, DDOS, botnet komuta-kontrol, ve de CAPTCH çözme amaçlı kullanım mümkün.
- Şu ana kadar Zeus botnet, InfoStealer trojan'ı ve de Office ve Adobe PDF exploit'leri Bulut ortamlarında host edilmiştir.

Güvenli olmayan programlama arayüzleri (Domain 10)

Iaas	PaaS	SaaS

- Bulut Bilişim sunucuları müşterilerin kullanabileceği arayüzler ve API'ler sunmakta. Bu arayüzlerdeki zaafiyet tüm Bulut ortamına riske atmakta.
- İzinsiz erişim ve şifre/token ele geçirme, içeriğin veya erişim bilgilerini açık taşınması, erişim kontrollarından veya kimlik yönetiminden doğan zaafiyetler, izleme ve loglama işlemlerinin karmaşıklığı, API zaafiyetleri buna sebep olmakta.

Kötü niyetli personel (Domain 2&7)

Iaas	PaaS	SaaS

- Kötü amaçlı personelin verebileceği zarar, birçok kurum/kuruluşun hizmet almakta olduğu ve ortak kullandığı Bulut ortamında güçlenmektedir.

Altyapı paylaşımından doğan zaafiyetler (Domain 8&13)

Iaas	PaaS	SaaS

- IaaS sunucuları ellerindeki altyapıyı paylaştırarak hizmet vermektedirler. Çoğu zaman paylaştırılan bu kaynaklar çoklu kullanım mimarisine (multi tenant) göre tasarlanmamış olup bu işlev altaypı üzerine kurulan hypervisor ‘lar tarafından sağlanmaya çalışmaktadır.
- Hypervisor’ların altta yatan kaynaklar ile kesin bir ayrım sağlamadığı durumlar görülmüştür.
- Güçlü bir ayrım (Compartmentalization), bir kullanıcının diğer müşteri/kullanıcıları etkilememesi için tesis edilmelidir

Veri kaybı ve sızıntısı (Domain 5&11&12)

Iaas	PaaS	SaaS

- Veri kaybı ve sızıntı ihtimali Bulut bilişimin mimari ve operasyonel özellikleri sebebi ile artmaktadır.
- AAA kontrolları, idari sorunlar, veri merkezi güvenilirliği ve felaketten kurtarma yetenekleri.

Hesap, hizmet ve trafik çalınması (Domain 2&9&12)

Iaas	PaaS	SaaS

- Bu tehditler yeni olmasa da Bulut ortamı bunların etkilerini güçlendirmekte ve de icrasını komplike yapısı ile kolaylaştırmakta, tespitini de güçleştirmektedir.

Bilinmeyen risk profili (Domain 2&3&8&9)

Iaas	PaaS	SaaS

- Halihazırda Bulut Bilişim hizmetlerinin sunulduğu yapıların mimarisi ve iç detayları standartlara dayanmamakte ve de açık olarak paylaşılmamaktadır.
- Gizlilik ile güvenlik (Security by obscurity)??

Bulut bilişim için idari/regulasyon/yasal düzenlemeler

Bulut Bilişim (yasal/regülasyon)

- Kişisel bilgilerin gizliliği (privacy)
- Adli bilişim (forensics)
- Ülkeler arası dayanışma
- Hizmet seviyesi anlaşmaları (SLA’s)

Microsoft'un Bulut Bilişim Güvenliği Deneyimi

BTYD 2010

www.btyd.org