MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(13. Hafta)

İçerik

- 3.Yazılım Güvenliği ve Güvenilir sistemler
  - 3.1.Arabellek Taşması
  - 3.2.Yazılım Güvenliği
  - 3.3.İşletim Sistemi Güvenliği
  - 3.4.Bulut Güvenliği
  - 3.5.IoT Güvenliği

3.4.Bulut Güvenliği

3.4.İçerik

- Bulut bilişim
- Bulut Güvenliği Kavramları
- Bulut Güvenliği Yaklaşımları

Bulut bilişim:

- NIST, NIST SP-800-145'te (*Bulut Bilişimin NIST Tanımı*, Eylül 2011) bulut bilşşim şu şekilde tanımlanır:

"**Bulut bilişim:**Minimum yönetim çabası veya hizmet sağlayıcı etkileşimi ile hızlı bir şekilde sağlanabilen ve serbest bırakılabilen, yapılandırılabilir bilgi işlem kaynaklarının (ör. ağlar, sunucular, depolama, uygulamalar ve hizmetler) paylaşılan bir havuzuna her yerde hazır, kullanışlı, isteğe bağlı ağ erişimi sağlamak için bir modeldir. Bu bulut modeli kullanılabilirliği destekler ve beş temel karakteristik üç hizmet modeli ve dört dağıtım (hizmete alma) modeli içerir."

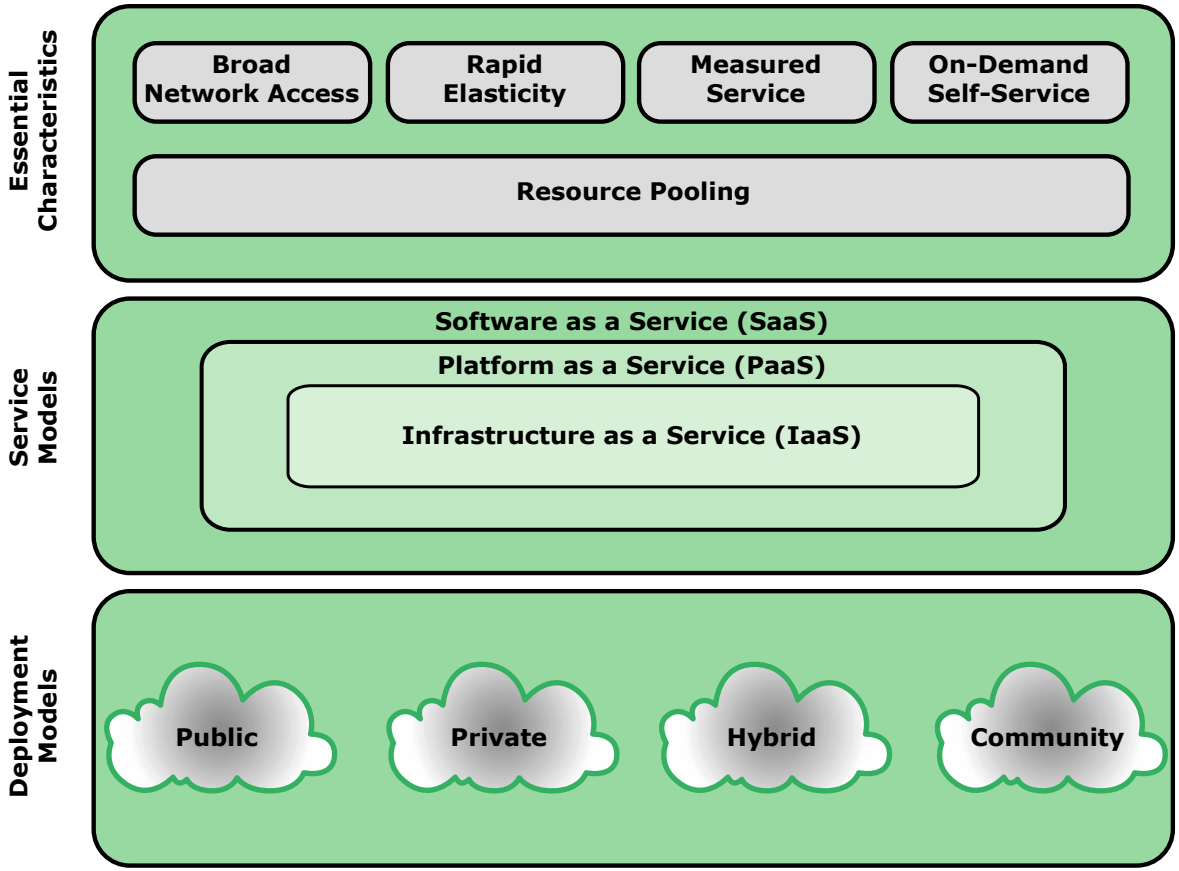


Figure 13.1 Cloud Computing Elements

Temel Karakteristikleri

• **Geniş ağ erişimi**: Araçlara ağ üzerinden ve heterojen platformlarının (ör. cep telefonları, dizüstü bilgisayarlar ve tabletler) yanı sıra diğer geleneksel veya bulut tabanlı mekanizmalar aracılığıyla erişilebilir.

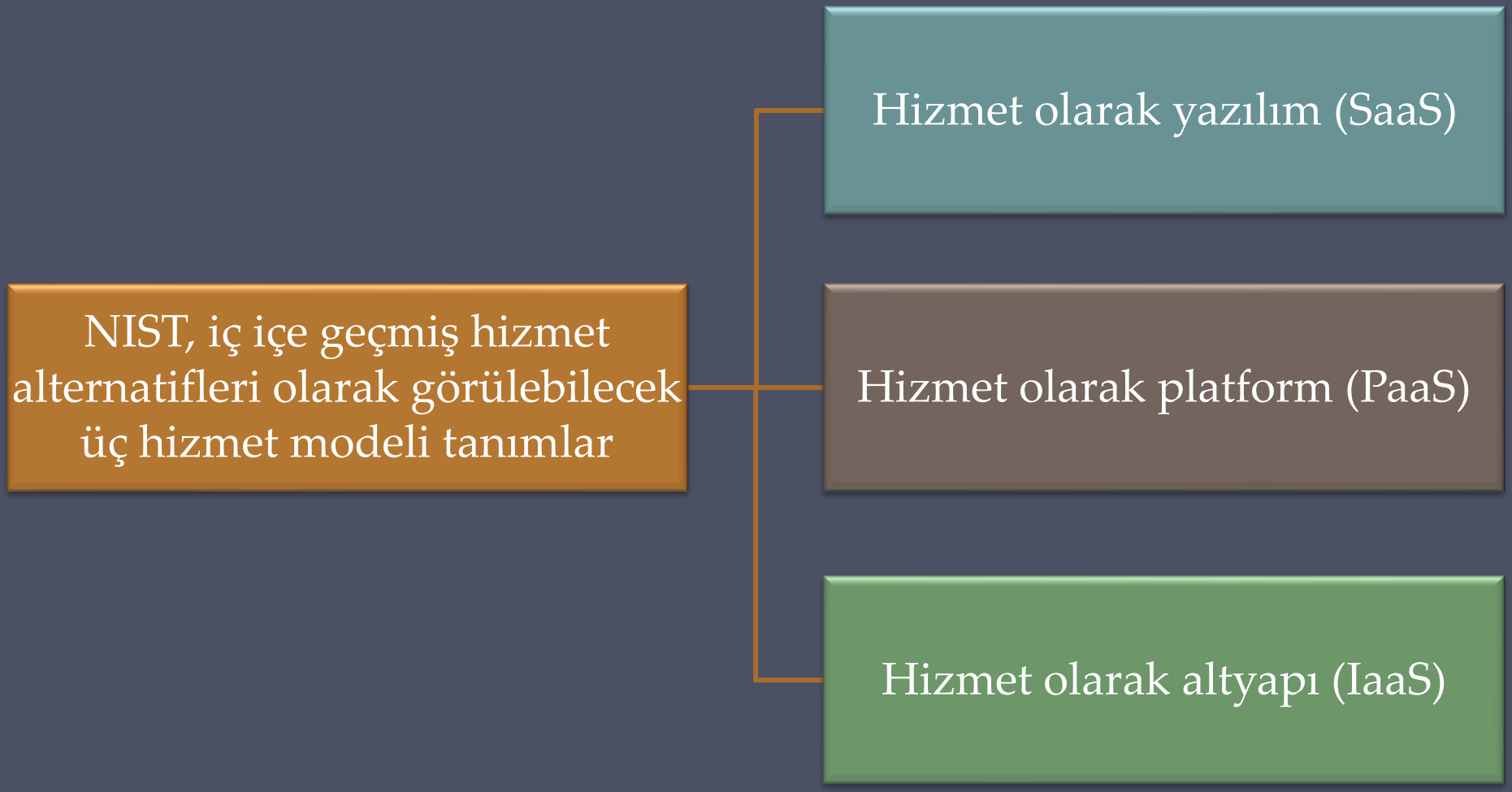
Hızlı esneklik: Bulut bilgi işlem özel hizmet gereksinimlerinize göre kaynakları genişletme ve azaltma yeteneği sunar.

Ölçülen hizmet: Kullanılan hizmetin hem sağlayıcısı hem de tüketicisi için şeffaflık sağlayarak kaynak kullanımı izlenebilir, kontrol edilebilir ve raporlanabilir.

İsteğe bağlı self servis: Tüketici(CSC), hizmet sağlayıcıyla insan etkileşimi gerektirmeden gerektiğinde otomatik olarak sunucu süresi ve ağ depolama gibi bilgi işlem yeteneklerini tek taraflı olarak alabilir.

Kaynak havuzu oluşturma: Sağlayıcının bilgi işlem kaynakları, tüketici talebine göre dinamik olarak atanan ve yeniden atanan farklı fiziksel ve sanal kaynaklarla çok kiracılı bir model kullanılarak birden çok CSC'ye hizmet verecek şekilde havuzlanır.

Bulut Hizmet Modelleri



Hizmet olarak Yazılım (SaaS)

SaaS, müşterilere bulut üzerinde çalışan ve erişilebilen yazılım, özellikle uygulama yazılımı şeklinde hizmet sağlar

Müşterinin, sağlayıcının bulut altyapısı üzerinde çalışan bulut sağlayıcı uygulamalarını kullanmasını sağlar.

- Uygulamalara, Web tarayıcısı gibi basit bir arabirim aracılığıyla çeşitli istemci aygıtlarından erişilebilir.
- Bir işletme, kullandığı yazılım ürünleri için masaüstü ve sunucu lisansları almak yerine, aynı işlevleri bulut hizmetinden alır.

SaaS kullanımı, yazılım yükleme, bakım, yükseltme ve yamaların karmaşıklığını ortadan kaldırır

Bu hizmete örnek olarak Google Gmail, Microsoft 365, Salesforce, Citrix GoToMeeting ve Cisco WebEx verilebilir.

Hizmet olarak Platform (PaaS)

Bir PaaS bulutu, müşterilere, müşterinin uygulamalarının üzerinde çalışabileceği bir platform biçiminde hizmet sağlar

PaaS, müşterinin, müşteri tarafından oluşturulan veya edinilen uygulamaları bulut altyapısına dağıtmasını sağlar

Bir PaaS bulutu, kullanışlı yazılım yapı taşlarının yanı sıra programlama dili araçları, koşturma ortamları ve yeni uygulamaların devreye alınmasına yardımcı olan araçlar sağlar.

Aslında, PaaS buluttaki bir işletim sistemidir

İhtiyaç duyulan bilgi işlem kaynaklarına yalnızca gerektiği kadar ve yalnızca ihtiyaç duyulduğu sürece ödeme yaparken yeni veya özel uygulamalar geliştirmek isteyen bir kuruluş için yararlıdır.

PaaS örnekleri arasında AppEngine, Engine Yard, Heroku, Microsoft Azure, Force.com ve Apache Stratos yer alır

Hizmet olarak altyapı (IaaS)

IaaS ile müşteri, temeldeki bulut altyapısının kaynaklarına erişebilir

Bulut hizmeti kullanıcısı, altta yatan bulut altyapısının kaynaklarını yönetmez veya kontrol etmez, ancak işletim sistemleri, bazı uygulamalar üzerinde kontrole ve muhtemelen belirli ağ bileşenleri üzerinde sınırlı kontrole sahiptir.

IaaS, sanal makineler ve diğer sanallaştırılmış donanım ve işletim sistemleri sağlar

IaaS müşteriye işleme, depolama, ağlar ve diğer temel bilgi işlem kaynakları sunar, böylece müşteri işletim sistemlerini ve uygulamaları içerebilen isteğe bağlı yazılımları kurabilir ve çalıştırabilir

IaaS, müşterilerin üst düzeyde uyarlanabilir bilgisayar sistemleri oluşturmak için hesaplama ve veri depolama gibi temel bilgi işlem hizmetlerini birleştirmelerini sağlar

IaaS örnekleri, Amazon Elastic Compute Cloud, Microsoft Windows Azure, Google Compute Engine ve Rackspace'dir

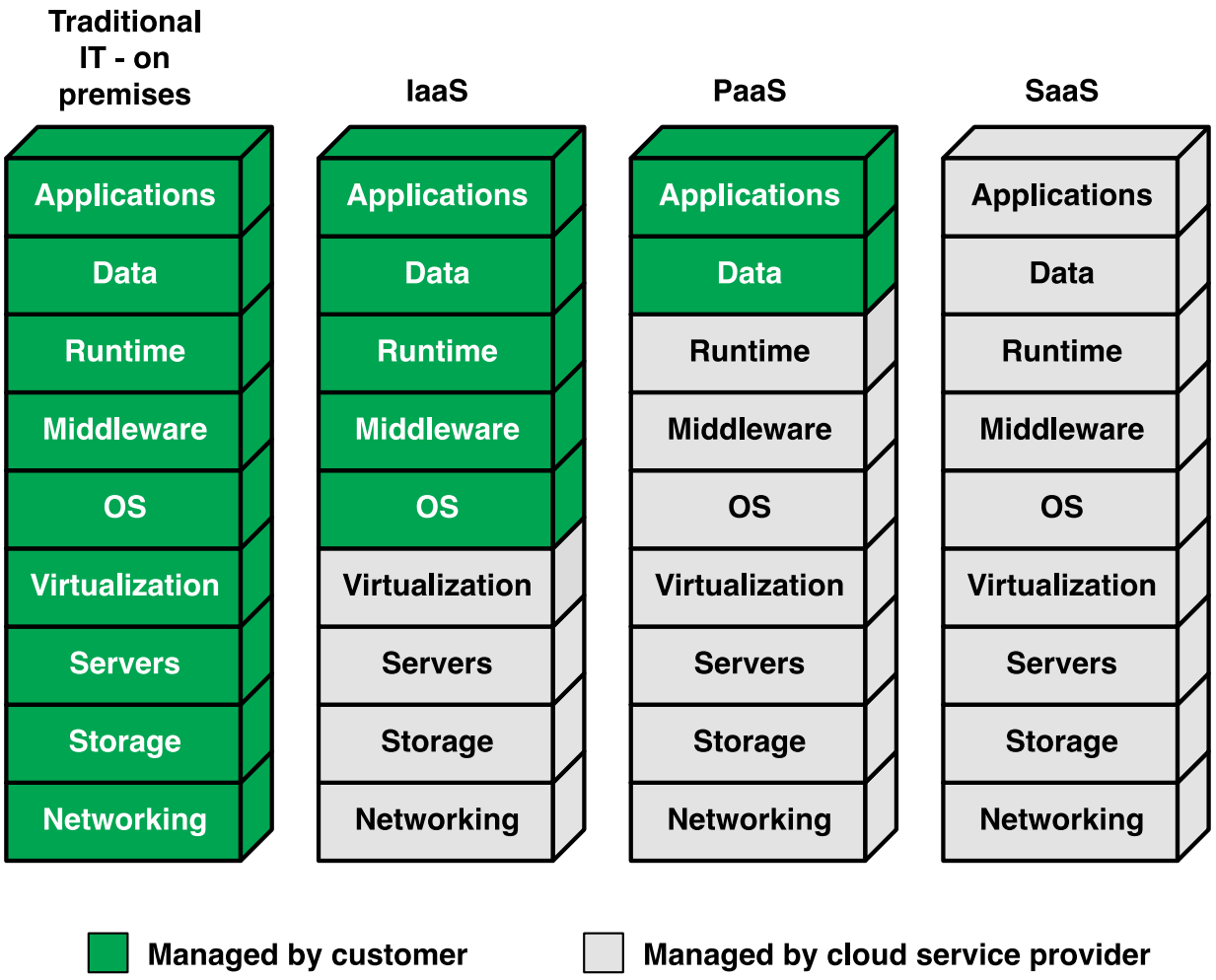


Figure 13.2 Separation of Responsibilities in Cloud Service Models

Bulut Hizmete Alma Modelleri

Genel/Açık Bulut

Topluluk bulutu

Bulut bilgi işlem için en öne çıkan dört kurulum modeli şunlardır:

Özel bulut

Hibrit bulut

Genel/Açık Bulut

- Genel bir bulut altyapısı, herkesin veya büyük bir endüstri grubunun kullanımına sunulur ve bulut hizmetleri satan bir kuruluşa aittir.
  - Bulut hizmet sağlayıcı, hem bulut altyapısından hem de bulut içindeki veri ve işlemlerin kontrolünden sorumludur.
- Bir genel bulut, bir iş, akademik veya devlet kuruluşu veya bunların bir kombinasyonu tarafından sahiplenilebilir, yönetilebilir ve işletilebilir.
  - Tüm ana bileşenler, çok kiracılı bir altyapıda bulunan kurumsal güvenlik duvarının dışındadır
  - Uygulamalar ve depolama, güvenli IP aracılığıyla İnternet üzerinden sağlanır ve ücretsiz veya kullanım başına ödeme ücreti karşılığında sunulabilir.
- Genel bulutun en büyük avantajı maliyettir
- Asıl endişe güvenliktir

Özel bulut

- Özel bulut kuruluşun dahili BT ortamı içinde kuruludur ve hizmet verir
- Kuruluş, bulutu kendi bünyesinde yönetmeyi veya yönetim işlevini üçüncü bir tarafla sözleşme yoluyla devretmeyi seçebilir
- Bulut sunucuları ve depolama cihazları şirket içi veya şirket dışı olabilir
- Özel bulutlar, IaaS'yi bir sanal özel ağ (VPN) aracılığıyla bir intranet veya İnternet aracılığıyla çalışanlara veya iş birimlerine ve ayrıca şube ofislerine hizmet olarak sunulabilir
- Özel bulut yoluyla sunulan hizmetlere örnek olarak talep üzerine veritabanı, talep üzerine e-posta ve talep üzerine depolama dahildir
- Özel bir bulutu seçmenin temel motivasyonlarından biri güvenliktir
- Diğer avantajlar arasında kolay kaynak paylaşımı ve kurumsal varlıklara hızlı erişim sayılabilir

Topluluk Bulutu

Bir topluluk bulutu, özel ve genel bulutların özelliklerini içerir	• Özel bir bulut gibi kısıtlı erişime sahiptir • Bulut kaynakları, bir genel bulut gibi bir dizi bağımsız kuruluş arasında paylaşılır
Topluluk bulutunu paylaşan kuruluşların benzer gereksinimleri vardır ve genellikle birbirleriyle veri alışverişi yaparlar	• Sağlık sektörü örnek verilebilir
Bulut altyapısı, katılımcı kuruluşlar veya üçüncü bir tarafça yönetilebilir ve yerinde veya şirket dışında bulunabilir	• Bu hizmet modelinde, maliyetler genel bir buluttan daha az kullanıcıya dağıtılır, bu nedenle bulut bilgi işlemin maliyet tasarrufu potansiyelinin yalnızca bir kısmı gerçekleştirilir.

Hibrit Bulut

- Hibrit bulut altyapısı, benzersiz varlıklar olarak kalan ancak veri ve uygulama taşınabilirliğini sağlayan standartlaştırılmış veya tescilli teknoloji ile birbirine bağlanan iki veya daha fazla bulutun (özel, topluluk veya genel) bir bileşimidir.
- Hibrit bulut çözümü ile hassas bilgiler bulutun özel bir alanına yerleştirilebilir ve daha az hassas veriler genel bulutun avantajlarından yararlanabilir.
- Hibrit bir genel/özel bulut çözümü, özellikle küçük işletmeler için çekici olabilir
- Güvenlik endişelerinin daha az olduğu birçok uygulama, kuruluşun daha hassas verileri ve uygulamaları genel buluta taşımasına gerek kalmadan önemli ölçüde maliyet tasarrufuyla giderebiliriz.

Bulut Hizmete Alma Modellerinin Karşılaştırılması

	Özel	Topluluk	Genel/Açık	Hibrit
Ölçeklenebilirlik	Sınırlı	Sınırlı	Çok yüksek	Çok yüksek
Güvenlik	En güvenli seçenek	Çok güvenli	Orta derecede güvenli	Çok güvenli
Verim	Çok iyi	Çok iyi	Düşük ila orta	İyi
Güvenilirlik	Çok yüksek	Çok yüksek	Orta	Ortadan yükseğe
Maliyet	Yüksek	Orta	Düşük	Orta

Bulut bilişim:

- NIST SP-500-292 (*NIST Bulut Bilişim Referans Mimarisi)* aşağıda açıklanan referans mimarisini oluşturur:

"NIST bulut bilgi işlem referans mimarisi, çözüm ve uygulama tasarımı "nasıl" değil, bulut hizmetlerinin "ne" sağladığı gereksinimlerine odaklanır. Referans mimarisi, bulut bilgi işlemdeki operasyonel inceliklerin anlaşılmasını kolaylaştırmak için tasarlanmıştır. Belirli bir bulut bilgi işlem sisteminin sistem mimarisini temsil etmez; bunun yerine, ortak bir referans çerçevesi kullanarak sisteme özgü bir mimariyi tanımlamaya, tartışmaya ve geliştirmeye yönelik bir araçtır."

Hedef

NIST, aşağıdaki hedefleri göz önünde bulundurarak referans mimarisini geliştirmiştir:

- Genel bir bulut bilgi işlem kavramsal modeli bağlamında çeşitli bulut hizmetlerini göstermek ve anlatmak
- CSC'lerin bulut hizmetlerini anlaması, tartışması, kategorize etmesi ve karşılaştırması için teknik bir referans sağlamak
- Güvenlik, birlikte çalışabilirlik ve taşınabilirlik için aday standartların ve referans uygulamalarının analizini kolaylaştırmak

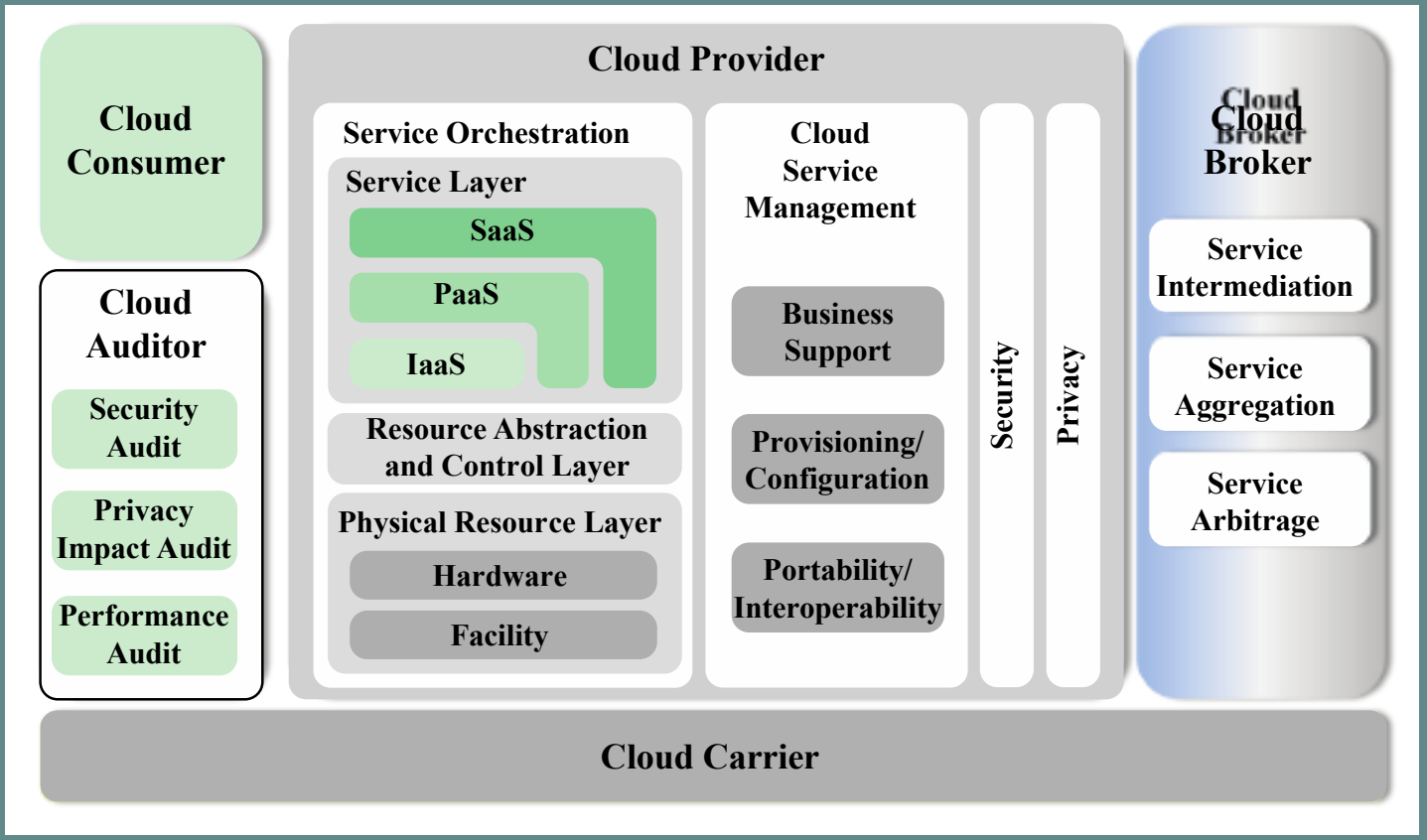


Figure 13.3 NIST Cloud Computing Reference Architecture

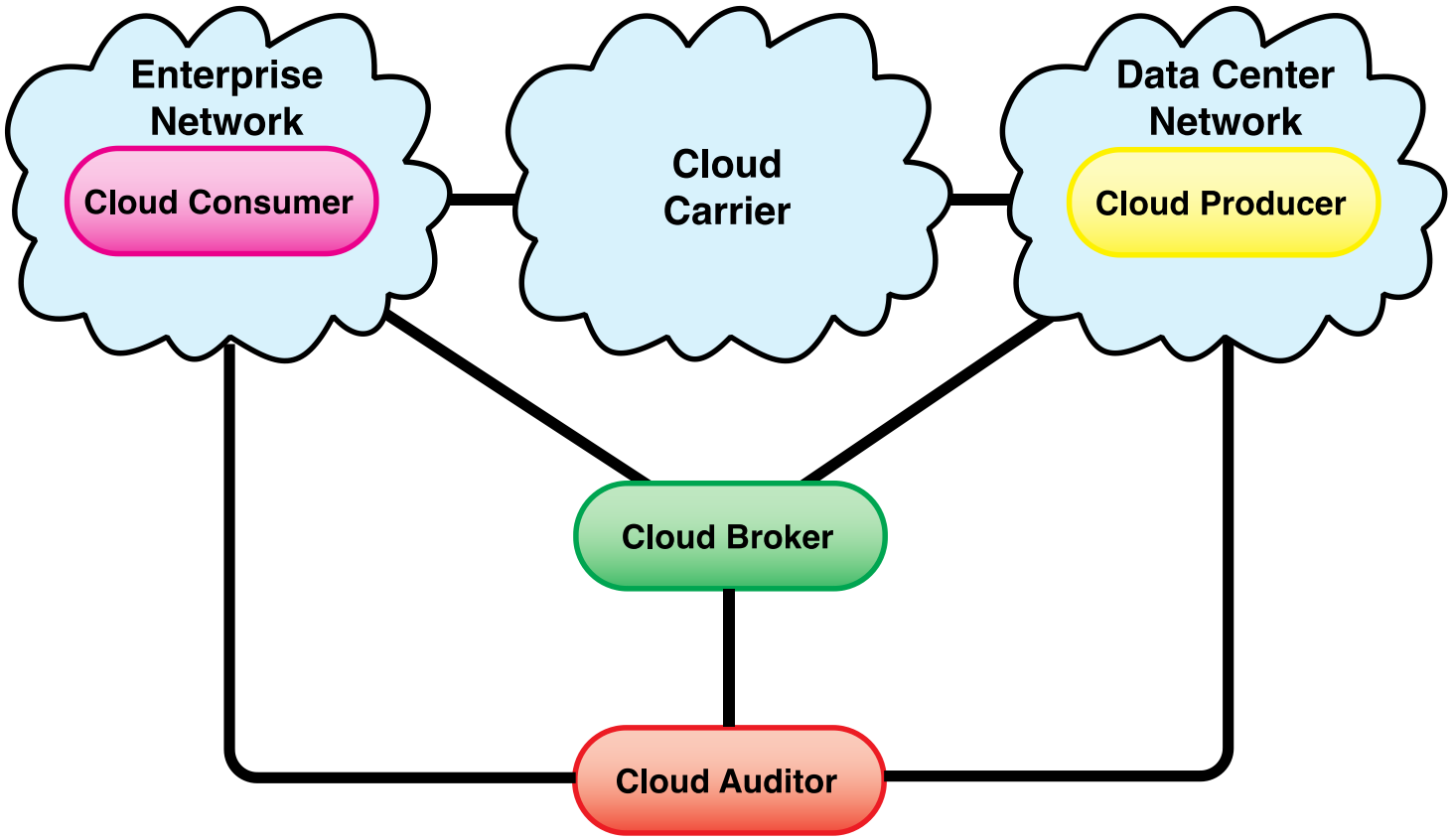


Figure 13.4 Interactions Between Actors in Cloud Computing

Bulut Güvenliği ve Gizlilik Sorunları ve Önerilerine İlişkin NIST Yönergeleri 1/3

Yönetim

Bulutta uygulama geliştirme ve hizmet sağlama için kullanılan politikalar, prosedürler ve standartların yanı sıra dağıtılan veya devreye alınan hizmetlerin tasarımı, uygulanması, test edilmesi, kullanımı ve izlenmesi ile ilgili kurumsal uygulamaları genişletin.

Kurumsal uygulamaların sistem yaşam döngüsü boyunca takip edilmesini sağlamak için denetim mekanizmalarını ve araçlarını devreye sokun.

Uyma

Kuruluşa güvenlik ve gizlilik yükümlülükleri getiren ve özellikle veri konumu, gizlilik ve güvenlik kontrolleri, kayıt yönetimi ve elektronik keşif gerekliliklerini içerenler olmak üzere bulut bilgi işlem girişimlerini potansiyel olarak etkileyen çeşitli yasa ve düzenlemeleri anlayın.

Karşılanması gereken kurumsal gereksinimler açısından bulut sağlayıcının tekliflerini gözden geçirin ve değerlendirin ve sözleşme hükümlerinin gereksinimleri yeterince karşıladığından emin olun. Bulut sağlayıcının elektronik keşif yeteneklerinin ve süreçlerinin, veri ve uygulamaların gizliliğini veya güvenliğini tehlikeye atmadığından emin olun.

Bulut Güvenliği ve Gizlilik Sorunları ve Önerilerine İlişkin NIST Yönergeleri 2/3

Güven

Hizmet düzenlemelerinin, bulut sağlayıcısı tarafından kullanılan güvenlik ve gizlilik kontrolleri ve süreçleri ile bunların zaman içindeki performanslarına ilişkin görünürlük sağlamak için yeterli araçlara sahip olduğundan emin olun.

Veriler üzerinde açık, münhasır mülkiyet hakları oluşturun.

Sistemin yaşam döngüsü boyunca sürekli gelişen ve değişen risk ortamına uyum sağlayacak kadar esnek bir risk yönetimi programı oluşturun.

Devam eden risk yönetimi kararlarını desteklemek için bilgi sisteminin güvenlik durumunu sürekli olarak izleyin.

Mimari

İlgili teknik kontrollerin tüm sistem yaşam döngüsü boyunca ve tüm sistem bileşenlerinde sistemin güvenliği ve gizliliği üzerindeki etkileri de dahil olmak üzere, bulut sağlayıcısının hizmetleri sağlamak için kullandığı temel teknolojileri anlayın.

Kimlik ve erişim yönetimi

Kimlik doğrulama, yetkilendirme ve diğer kimlik ve erişim yönetimi işlevlerini güvence altına almak için yeterli önlemlerin alındığından ve kuruluş için uygun olduğundan emin olun.

Bulut Güvenliği ve Gizlilik Sorunları ve Önerilerine İlişkin NIST Yönergeleri 3/3

Yazılım izolasyonu

Bulut sağlayıcının çok kiracılı yazılım mimarisinde kullandığı sanallaştırma ve diğer mantıksal yalıtım tekniklerini anlayın ve kuruluş için söz konusu olan riskleri değerlendirin.

Veri koruması

Bulut sağlayıcısının veri yönetimi çözümlerinin ilgili kurumsal veriler için uygunluğunu ve verilere erişimi kontrol etme, beklemede, aktarım halinde ve kullanımdayken verileri güvenli hale getirme ve verileri sterilize etme becerisini değerlendirin.

Tehdit profilleri yüksek olan veya verileri toplu olarak önemli ölçüde yoğunlaşmış değeri temsil eden diğer kuruluşların verileriyle kurumsal verileri karşılaştırma riskini göz önünde bulundurun.

Bulut ortamında bulunan tesisler ve bulut sağlayıcısı tarafından oluşturulan süreçlerle kriptografik anahtar yönetiminin içerdiği riskleri tam olarak anlayın ve tartın.

Kullanılabilirlik

Kullanılabilirlik, veri yedekleme ve kurtarma ve olağanüstü durum kurtarma için sözleşme hükümlerini ve prosedürlerini anlayın ve bunların kuruluşun süreklilik ve beklenmedik durum planlama gereksinimlerini karşıladığından emin olun.

Ara veya uzun süreli bir kesinti veya ciddi bir felaket sırasında, kritik operasyonların hemen devam ettirilebilmesini ve tüm operasyonların zamanında ve organize bir şekilde yeniden başlatılabilmesini sağlayın.

Olay yanıtı

Olay müdahalesi için sözleşme hükümlerini ve prosedürlerini anlayın ve bunların kuruluşun gereksinimlerini karşıladığından emin olun.

Bulut sağlayıcının şeffaf bir yanıt sürecine ve bir olay sırasında ve sonrasında bilgi paylaşmak için yeterli mekanizmaya sahip olduğundan emin olun.

Kuruluşun, bilgi işlem ortamı için ilgili rollerine ve sorumluluklarına uygun olarak bulut sağlayıcıyla koordineli bir şekilde olaylara yanıt verebilmesini sağlayın.

Bulut Bilişim için Güvenlik Sorunları

- Şirket içi sistemleri bulut hizmetleriyle büyütürken veya değiştirirken güvenlik önemli bir husustur
- Güvenlik endişelerini gidermek, genellikle bir kuruluşun bilgi işlem mimarisinin bir kısmını veya tamamını buluta taşımayla ilgili daha fazla tartışma için bir ön koşuldur.
- Kullanılabilirlik başka bir önemli endişe kaynağıdır
- Verilerin denetlenebilirliği sağlanmalıdır
- İşletmeler, hem bulutun dışından hem de içinden gelen güvenlik tehditlerine ilişkin durum tespiti yapmalıdır.
    - Bulut kullanıcıları, uygulama düzeyinde güvenlikten sorumludur
    - Bulut satıcıları, fiziksel güvenlikten ve bazı yazılım güvenliğinden sorumludur.
    - Yazılım yığınının ara katmanları için güvenlik, kullanıcılar ve satıcılar arasında paylaşılır
- Bulut sağlayıcıları, kullanıcılarının hırsızlık veya hizmet reddi saldırılarına karşı önlem almalı ve kullanıcıların birbirlerinden korunmaları gerekir
- İşletmeler, özellikle yanlışlıkla veri kaybı alanında, abonelerin sağlayıcıya karşı ne ölçüde korunduğunu dikkate almalıdır.

Kontrol Fonksiyonları ve Sınıfları

Teknik	Operasyonel	Yönetim
Giriş kontrolu Denetim ve Hesap Verebilirlik Tanımlama ve Kimlik Doğrulama Sistem ve İletişim Koruması	Farkındalık ve Eğitim Yapılandırma ve Yönetim Acil Durum Planlaması Olay Müdahalesi Bakım Medya Koruması Fiziksel ve Çevresel Koruma Personel Güvenlik Sistemi ve Bilgi Bütünlüğü	Sertifikasyon, Akreditasyon ve Güvenlik Değerlendirmesi Planlama Risk Değerlendirmesi Sistem ve Hizmet Edinimi

Riskler ve karşı önlemler

Cloud Security Alliance, buluta özgü en önemli güvenlik tehditleri olarak aşağıdakileri listelemiştir:

- Bulut bilişimin kötüye kullanımı ve kötü niyetli kullanımı
  - Karşı önlemler şunları içerir:
    - Daha sıkı ilk kayıt ve doğrulama süreçleri
    - Gelişmiş kredi kartı dolandırıcılığı izleme ve koordinasyonu
    - Müşteri ağ trafiğinin kapsamlı denetimi
    - Kişinin kendi ağ blokları için genel kara listeleri izleme
- Güvenli olmayan arayüzler ve API'ler
  - Karşı önlemler şunları içerir:
    - CSP arayüzlerinin güvenlik modelini analiz etme
    - Güçlü kimlik doğrulama ve erişim kontrollerinin şifreli iletimle birlikte uygulanmasını sağlama
    - API ile ilişkili bağımlılık zincirini anlama

- Kötü niyetli dahili kullanıcılar
  - Karşı önlemler şunları içerir:
    - Sıkı tedarik zinciri yönetimi uygulayın ve kapsamlı bir tedarikçi değerlendirmesi yapın
    - Yasal sözleşmenin bir parçası olarak insan kaynağı gereksinimlerini belirtin
    - Genel bilgi güvenliği ve yönetim uygulamalarının yanı sıra uyumluluk raporlamasında şeffaflık gerektir
    - Güvenlik ihlali bildirim süreçlerini belirleyin

- Paylaşılan teknoloji sorunları
  - Karşı önlemler şunları içerir:
    - Kurulum/yapılandırma için en iyi güvenlik uygulamalarını uygulayın
    - Yetkisiz değişiklikler/aktivite için ortamı izleyin
    - Yönetimsel erişim ve işlemler için güçlü kimlik doğrulama ve erişim kontrolünü teşvik edin
    - Yama uygulama ve güvenlik açığı düzeltme için SLA'ları zorunlu kılın
    - Güvenlik açığı taraması ve yapılandırma denetimleri gerçekleştirin

- Veri kaybı veya sızıntısı
  - Karşı önlemler şunları içerir:
    - Güçlü API erişim denetimi uygulayın
    - Aktarılan ve atıl durumdaki verilerin bütünlüğünü şifreleyin ve koruyun
    - Veri korumasını hem tasarım hem de çalışma zamanında analiz edin
    - Güçlü anahtar oluşturma, depolama ve yönetim ve imha uygulamalarını uygulayın
- Hesap veya hizmet ele geçirme
  - Karşı önlemler şunları içerir:
    - Hesap kimlik bilgilerinin kullanıcılar ve hizmetler arasında paylaşılmasını yasaklayın
    - Mümkün olduğunda güçlü iki faktörlü kimlik doğrulama tekniklerinden yararlanın
    - Yetkisiz etkinliği tespit etmek için proaktif izleme kullanın
    - CSP güvenlik politikalarını ve SLA'ları anlama
- Bilinmeyen risk profili
  - Karşı önlemler şunları içerir:
    - Uygulanabilir logların ve verilerin ifşası
    - Altyapı detaylarının kısmen/tam ifşası
    - Gerekli bilgilerin izlenmesi ve uyarılması

Bulutta Veri Koruması

Buluta özgü veya bulut ortamının mimari veya operasyonel özelliklerinden dolayı daha tehlikeli olan risklerin ve zorlukların sayısı ve bunlar arasındaki etkileşimler nedeniyle bulutta veri gizliliği tehdidi artar

Bu önlemlere rağmen, yolsuzluk ve diğer hizmet reddi saldırıları risk olmaya devam etmektedir

Veriler dururken, aktarılırken ve kullanılırken güvenlik altına alınmalı ve verilere erişim kontrol edilmelidir

Bekleyen veriler için ideal güvenlik önlemi, istemcinin veritabanını şifrelemesi ve yalnızca şifrelenmiş verileri bulutta depolaması ve CSP'nin şifreleme anahtarına erişimi olmamasıdır

İstemci, aktarılan verileri korumak için şifreleme kullanabilir, ancak bu, CSP için temel yönetim sorumluluklarını içerir

İstemci, erişim kontrol tekniklerini uygulayabilir, ancak kullanılan hizmet modeline bağlı olarak CSP bir dereceye kadar dahil olur

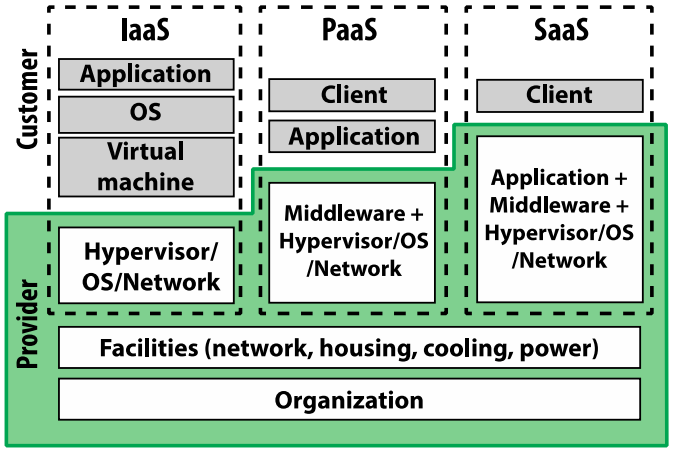
Bulutta Veri Koruması

Çoklu Örnek Modeli

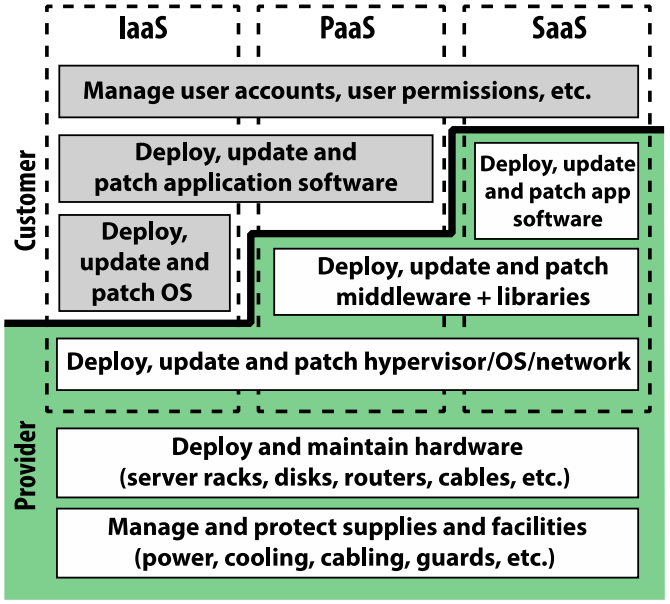
- Her bulut abonesi için bir sanal makine üzerinde çalışan benzersiz bir DBMS sunulur
- Bu, aboneye rol tanımı, kullanıcı yetkilendirmesi ve güvenlikle ilgili diğer idari görevler üzerinde tam kontrol sağlar.

Çoklu Kiracı Modeli

- Bulut kullanıcısı için diğer kiracılarla paylaşılan, genellikle verileri bir kullanıcı tanımlayıcısıyla etiketleme yoluyla önceden tanımlanmış bir ortam sağlar
- Etiketleme, örneğin özel olarak kullanıldığı izlenimini verir, ancak sağlam bir güvenli veritabanı ortamı oluşturmak ve sürdürmek için bulut sağlayıcısına güvenir



(a) Cloud computing assets



(b) Cloud computing management tasks

Figure 13.5 Security Considerations for Cloud Computing Assets

Hizmet olarak Bulut Güvenliği (SecaaS)

- Bulut bilgi işlem bağlamında, SecaaS olarak adlandırılan bir hizmet olarak bulut güvenliği, bir CSP'nin SaaS teklifinin bir bölümüdür
- CSA, SecaaS'ı güvenlik uygulamalarının ve hizmetlerinin bulut aracılığıyla bulut tabanlı altyapı ve yazılıma veya buluttan müşterilerin şirket içi sistemlerine sağlanması olarak tanımlar
- CSA aşağıdaki SecaaS hizmet kategorilerini tanımlamıştır:
    - Kimlik ve erişim yönetimi
    - Veri kaybı önleme
    - web güvenliği
    - E-posta güvenliği
    - Güvenlik değerlendirmeleri
    - izinsiz giriş yönetimi
    - Güvenlik bilgileri ve olay yönetimi
    - şifreleme
    - İş sürekliliği ve felaket kurtarma
    - Ağ güvenliği

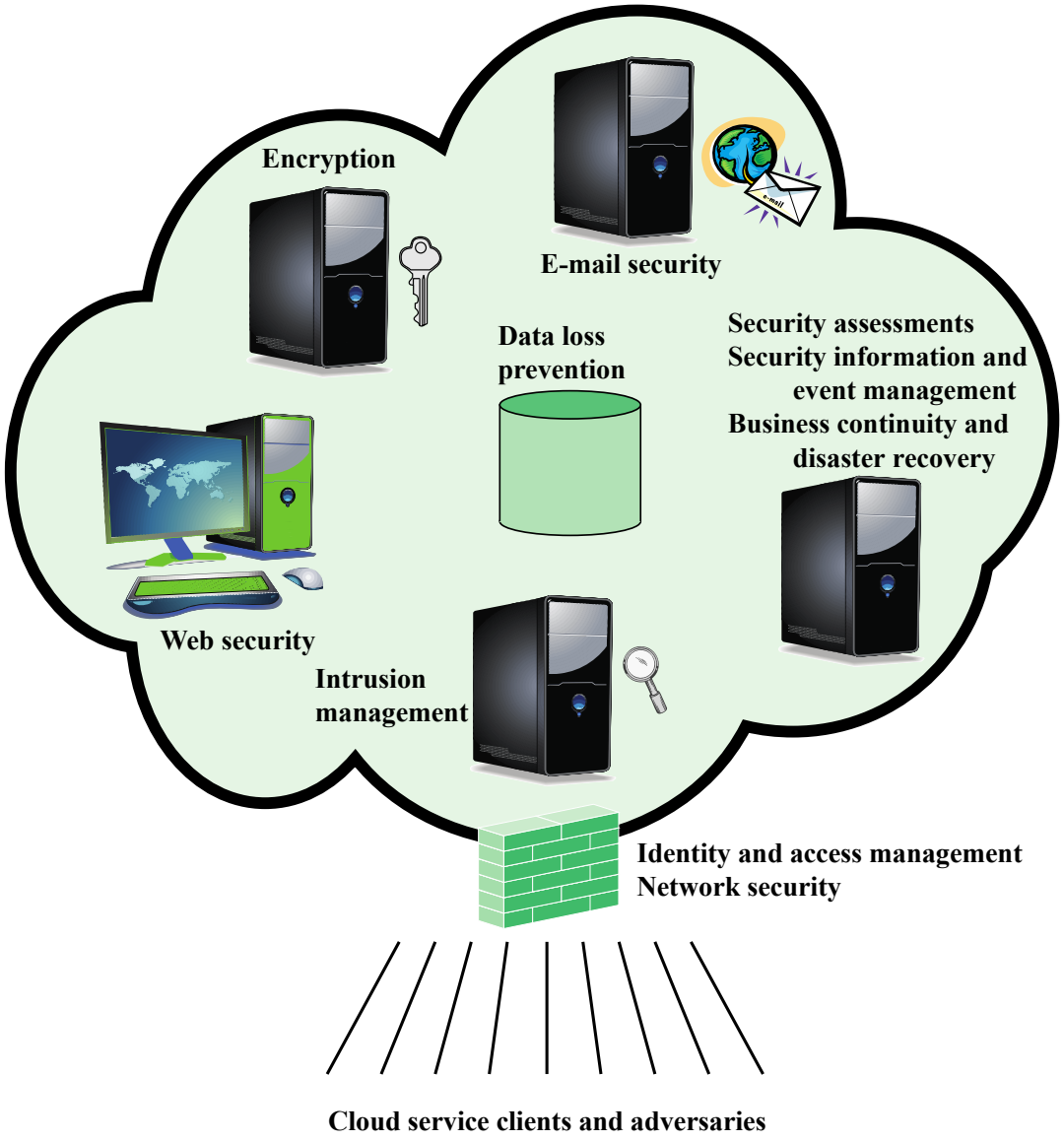


Figure 13.6 Elements of Cloud Security as a Service

OpenStack

Açık kaynaklı bir bulut işletim sistemi üretmeyi amaçlayan OpenStack Kurumunun açık kaynaklı yazılım projesidir

Temel amaç, bir bulut bilgi işlem ortamında devasa sanal özel sunucu gruplarının oluşturulmasını ve yönetilmesini sağlamaktır

OpenStack, bir dereceye kadar veri merkezi altyapısına ve bulut bilgi işlem ürünlerine yerleştirilmiştir

Çok kiracılı IaaS sağlar ve boyutu ne olursa olsun, uygulanması basit ve büyük ölçüde ölçeklenebilir olmasıyla genel ve özel bulutların ihtiyaçlarını karşılamayı amaçlar

OpenStack

- OpenStack İşletim Sistemi, her biri bir proje adı ve işlevsel bir adı olan bir dizi bağımsız modülden oluşur.
- OpenStack için güvenlik modülü Keystone'dur
- Keystone, işleyen bir bulut bilgi işlem altyapısı için gerekli olan paylaşılan güvenlik hizmetlerini sunar
  - Aşağıdaki ana hizmetleri verir:
    - Kimlik
    - Jeton/belirteç/token
    - Hizmet kataloğu
    - Politikalar

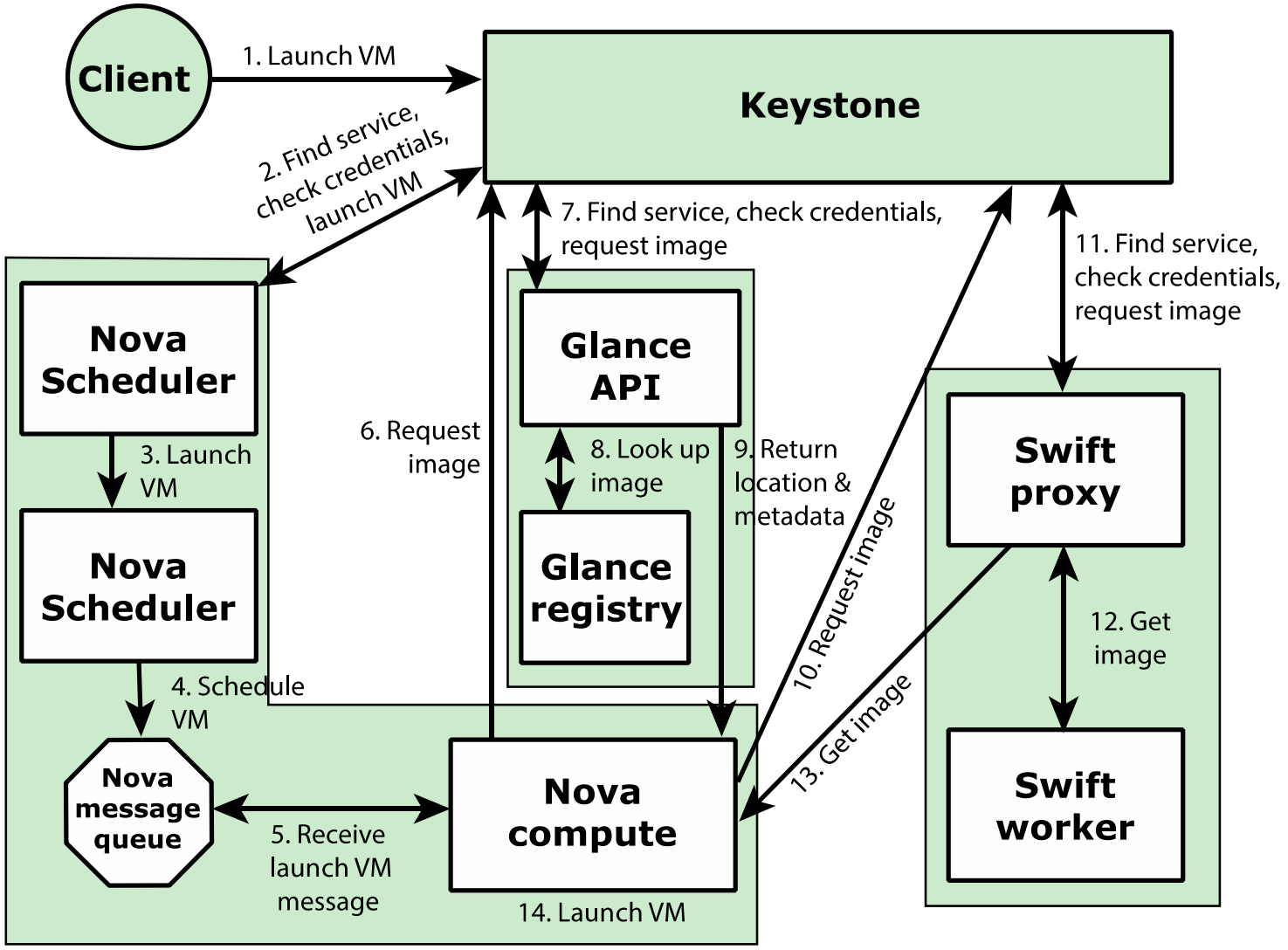


Figure 13.7 Launching a Virtual Machine in OpenStack