Zijn we niet teveel afhankelijk van de Cloud geworden?

12 april 2022

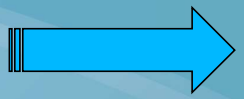
15 PvIB reconnect in cyber security

HUISHOUDELIJKE MEDEDELINGEN

Telefoon op stil

De badge graag inleveren bij vertrek

De evaluatie graag inleveren via de QR-code



Registratie bij binnenkomst en na afloop voor toekennen PE punten
Deze dien je zelf op te voeren (voor o.a. (C)PE punten)

Volgende bijeenkomst 12 mei 2022: Ontwikkeling van maatregelen tegen Ransomware

PvIB Platform voor InformatieBeveiliging

Programma

18:30	Uitreiking Artikel van het Jaar
18:45	Cloud intro - Max Webber & Daisy de Joode
18:55	Internet Beschikbaarheid - Iljitsch van Beijnum, inet6 consult
19:40	Can we still learn from the past? - Paul Oor, Sharedexperiences.nl
20:00	Pauze
20:15	Secure Connection Requirements of Hybrid Cloud, Peter van Eijk
21:15	Sluiting en borrel

PvIB Platform voor InformatieBeveiliging

ONEDAIS

Daisy de Joode

- Zelfstandig cybersecurity consultant (OneDais.nl) met focus op security compliancy, riskmanagement en gdpr

Securioso
Cyber Secure Together

Max Webber

- Cyber Privacy Security Consultant
- 20+ jaar Ervaring (C)ISO rollen

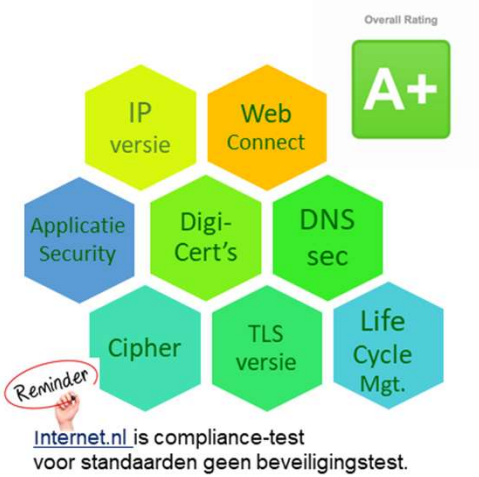
TLS+

Hoe veilig zijn uw beveiligde verbindingen

Securioso
Cyber Secure Together

Secure https: //

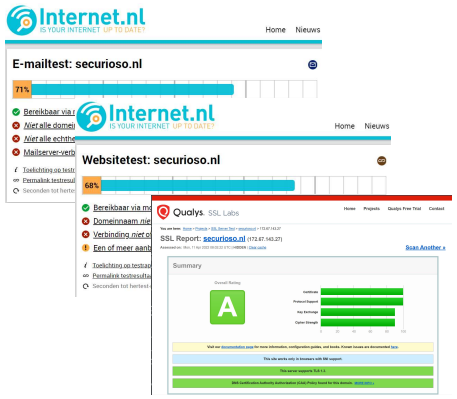
100% Website test Internet.nl



Internet.nl is compliance-test
voor standaarden geen beveiligingstest.

Wake Up Call

4 % Web
33 % Verbindingen

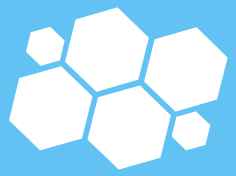


TLS+

- Top kwaliteit beveiligde verbinding TLS+
- Migratie support
- Onderhoud op de security standaard
- Monitoring op implementatie

PvIB Platform voor InformatieBeveiliging

92% A+



inet6 consult

Internetbeschikbaarheid

Hoe verhoog je die?

PvIB, Utrecht, 12 april 2022

Iljitsch van Beijnum

Internet beschikbaarheid

Hoe verhoog je die?

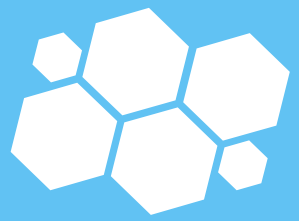
PvIB, Utrecht, 12 april 2022

inet6 consult

Iljitsch van Beijnum

PvIB Platform voor InformatieBeveiliging

Beveiliging: BIV

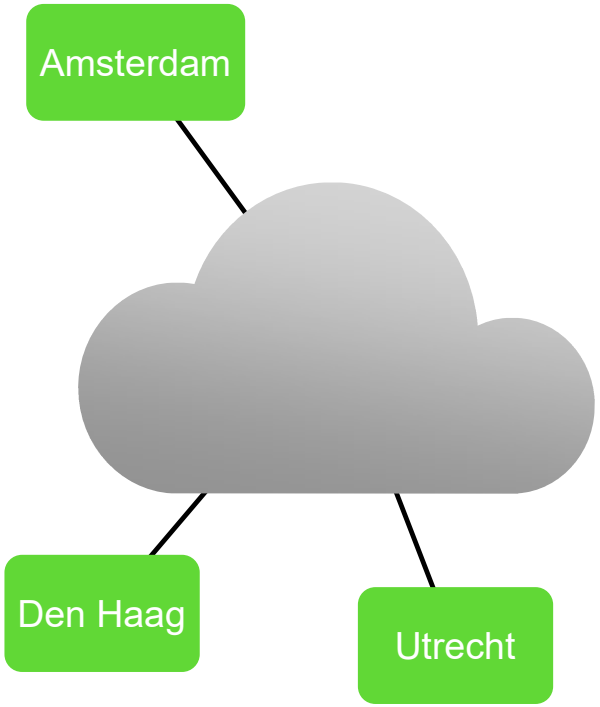


- BIV:
  - beschikbaarheid
  - integriteit
  - vertrouwelijkheid

Onderwerpen

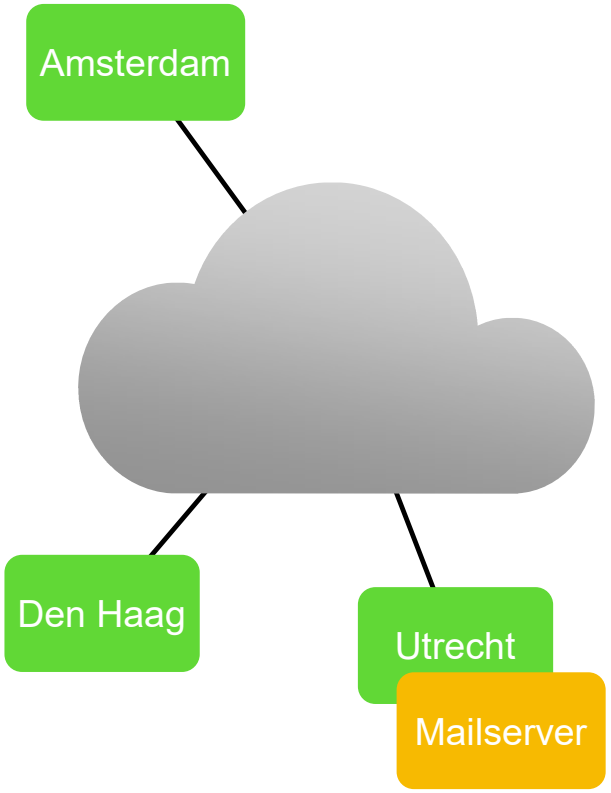
1. Hoe ziet de „cloud” eruit, gezien van uit het netwerk?
2. Afhankelijkheden
   - Inrichting eigen (kantoor-) locatie
   - ISP/internet-risico's
   - overige afhankelijkheden/risico's
3. Om het internet heen?
4. Conclusies

Hoezo "cloud"?



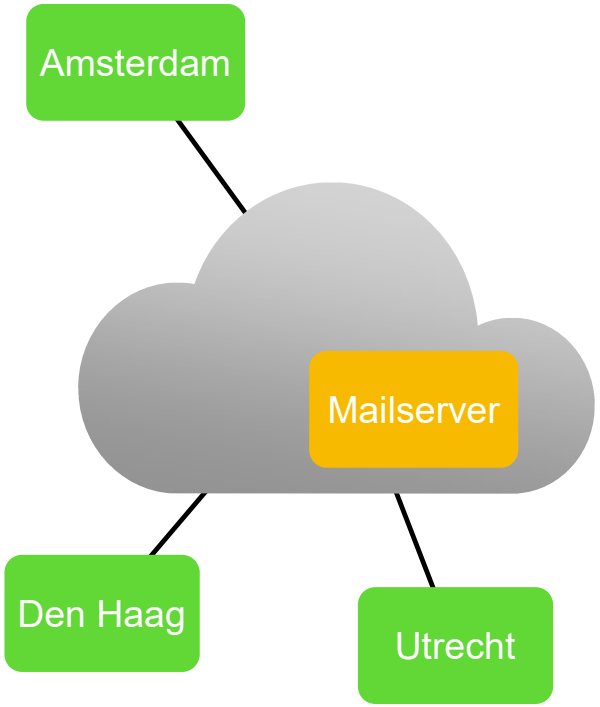
- Engels voor wolk!
- Voordat we het internet hadden...
- ...wisten we niet wat er met onze data gebeurde in het netwerk van de telecombedrijven
- Die netwerken tekenden we dus als een wolk:
  - er gaat wat in...
  - ...het wordt op één of andere manier getransporteerd...
  - ...en het komt er elders weer uit

Hoezo "cloud"? (2)



- Conceptueel:
  - in de wolk = *in* het netwerk
  - je communiceert met een DNS-naam
  - maakt niet uit waar
- Praktisch:
  - *aangesloten* op het netwerk
  - je communiceert met een IP-adres
  - dat leidt tot een specifieke server in een specifiek dataceter
- Kleinschalige uiterste:
  - DNS-naam → 1 IP-adres → 1 fysieke server

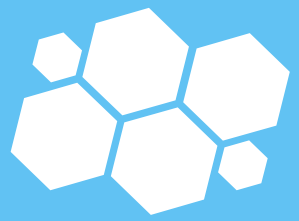
Hoezo "cloud"? (3)



- Grootschalige Saas/PaaS/IaaS-diensten:
  - DNS-naam ☁
  - → tussenliggende DNS-namen ☁
  - → 1 of meer publieke IP-adressen 🤔 / 😅 / 💶
  - → op 1 of meer locaties 🤔 / 😅 / 💶
  - → meerdere private IP-adressen ☁
  - → virtuele server ☁
  - → gedeelde fysieke servers ☁

☁ = aan clouddienstaanbieder 🤔 = nadenken
💶 = betalen voor kwaliteit 😅 = zelf doen

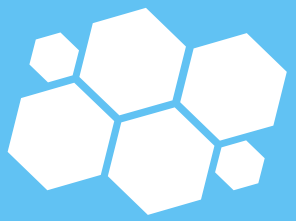
Afhankelijkheden



1. Apparatuur op je eigen (kantoor-) locatie
2. Verbinding naar ISP (de daadwerkelijke kabel)
3. Infrastructuur van je internet service provider
4. DNS
5. Routering tussen ISPs
6. Lokatie-infrastructuur clouddienstaanbieder
7. Dienstaanbieder in z'n geheel

   – (weet je nog waar je was 4-10-2021?)

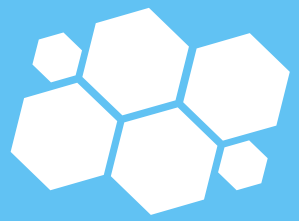
Hoe ben je on-afhankelijk?



- Simpel gezegd: van alles twee:
  - Apparatuur op je eigen (kantoor-) locatie 🤔 / 😅 / 💶
  - Verbinding naar ISP (de daadwerkelijke kabel) 🤔 / 💶
  - Infrastructuur van je internet service provider 💶 / 🤔
  - DNS 🤔
  - Routering tussen ISPs 🤔
  - Lokatie-infrastructuur clouddienstaanbieder ☁ (🤔 / 💶)
  - Dienstaanbieder in z'n geheel ☁ / 😳

☁ = aan dienstaanbieder 🤔 = over nadenken
💶 = betalen voor kwaliteit 😅 = zelf 😳 = lastig!

Je eigen (kantoor-) locatie

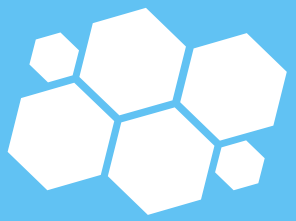


- Heel klein:
  - gewone vaste internetverbinding
  - 4G/5G als backup
- Middelgroot:
  - twee aparte ISPs
  - handmatig wisselen (b.v. tussen 2 Wi-Fi SSIDs)
- Groot:
  - eigen glasvezels naar meerdere ISPs
  - eigen BGP-routering om automatisch te herrouteren

BGP?

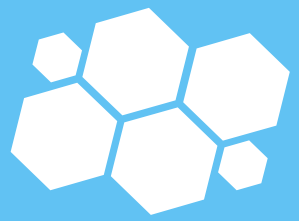
- Border Gateway Protocol (BGP) is de lijm die het internet bij elkaar houdt
- BGP berekent de routes naar alle IP-adressen op het internet
- Betekent wel:
  - eigen blok IP-adressen
  - "AS"-nummer
  - twee stevige routers
  - complexe instellingen
- Optimale robuustheid connectiviteit!

Tussenopties



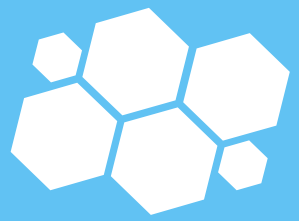
- Twee apart gerouteerde glasvezels naar *dezelfde* ISP
  - geen BGP: simpelere routers / routerinstellingen
  - maar nog wel maatwerk van ISP nodig
- Eén ISP voor IPv4, een andere ISP voor IPv6
  - kan al met consumenten-internetverbindingen
  - wel een iets geavanceerdere router nodig, maar hoeft niet duur, bijvoorbeeld Mikrotik
  - webbrowsers en veel applicaties zien vaak supersnel of IPv4 wel werkt en IPv6 niet of omgekeerd
  - maar niet alles beschikbaar via IPv6

Infrastructuur van je ISP



- Kan goed zijn of minder goed, zelden echt slecht
- Maar *als* het mis gaat... daar zit je dan
- Goed onderzoek vantevoren kan helpen:
  - grote storingen in het verleden? oplossnelheid?
  - andere incidenten? ("de-peering")
  - eigenstandig in Nederland, of bijkantoor buitenlandse partij?
- SLAs beschermen niet tegen storingen, maar in elk geval duidelijk aanspreekpunt en je krijgt geld terug

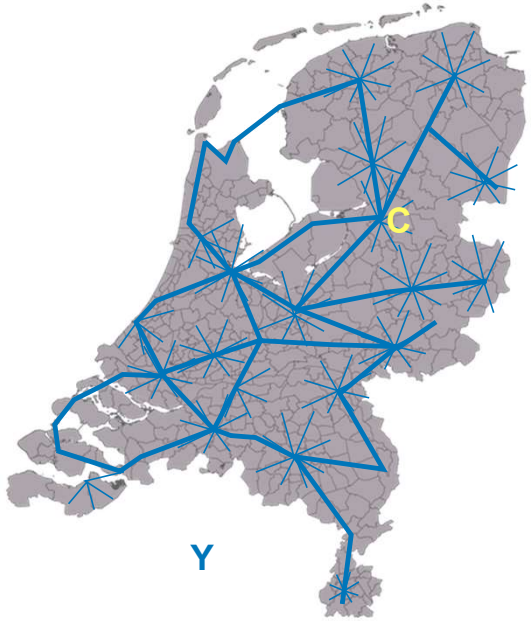
Interconnectie tussen ISPs



- Het internet is een "netwerk van netwerken"
- Veel van de netwerken overlappen. In Nederland:
  - KPN, Vodafone/Ziggo, T-Mobile, Telfort, Tele2, Eurofiber, Surfnet, Caiway, Delta, Dataweb, ...
- En toch kunnen klanten van elke ISP communiceren met klanten van elke andere ISP!
- Er zijn dus altijd koppelingen, rechtstreeks of via één of meer tussenliggende ISPs

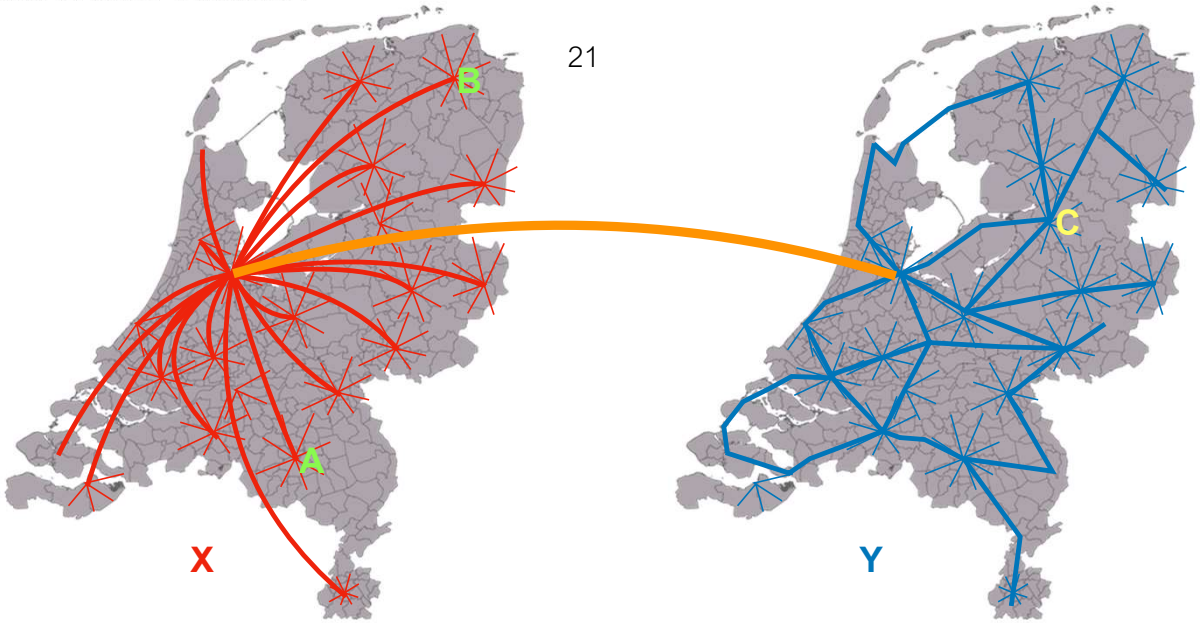
Interconnectie tussen ISPs (2)

- Iedere ISP heeft z'n eigen netwerk: A naar B: makkelijk
- Maar wat als A, klant van ISP X, wil communiceren met C, klant van ISP Y?

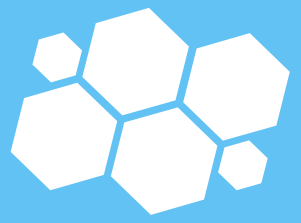


Interconnectie tussen ISPs (3)

- "Peering" tussen ISPs
- Via internet exchanges zoals AMS-IX
- of directe kabel

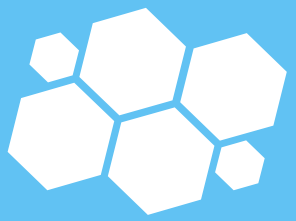


Interconnectie tussen ISPs (4)



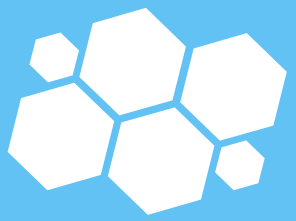
- BGP dus
- Er zijn een stuk of 12 "tier-1" netwerken
  - de rest van het internet is direct of indirect klant van één (of meer) van die grote netwerken
  - deze grote netwerken zijn allemaal onderling gekoppeld (op meerdere locaties): "peering"
- Kleinere netwerken doen ook aan peering
  - maar de groten willen meestal niet met de kleintjes

De-peering



- Soms krijgen grote(re) netwerken ruzie over peering-voorwaarden
- Dan kan één van beide partijen besluiten te "de-peeren"
- Dan is er geen rechtstreeks verkeer meer tussen netwerk A en netwerk B meer mogelijk
  - en dus ook niet tussen de klanten van A en de klanten van B
- Pas dus op met netwerken met een de-peeringgeschiedenis, en/of
  - Neem zelf meerdere ISPs, of
  - Neem een ISP die klant is van meerdere van de tier-1s

BGP-problemen



- BGP werkt tussen zo'n 100.000 netwerken
  - als één iets doet zien alle anderen dat binnen 30 tot 120 seconden
    - fouten hebben onmiddelijk effect!
    - maar de oplossingen meestal ook 😅
- Belangrijk type fout: "route leak"
  - klein(er) netwerk zegt bijvoorbeeld "Twitter is nu bereikbaar via ons!"
  - maar dat gaat natuurlijk niet goed
  - verkeer loopt dood

BGP-problemen (2)

- 28 maart nog:

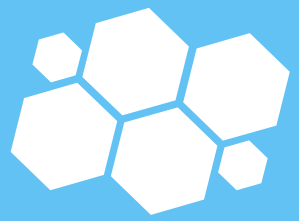
BGP —

Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap

Despite the timing, the 45-minute hijacking was most likely an error, not an attack.

- Maar bekendste: Youtube/Pakistan
  - gerelateerd aan:
- BGP-beveilingssysteem RPKI helpt vaak, maar niet altijd

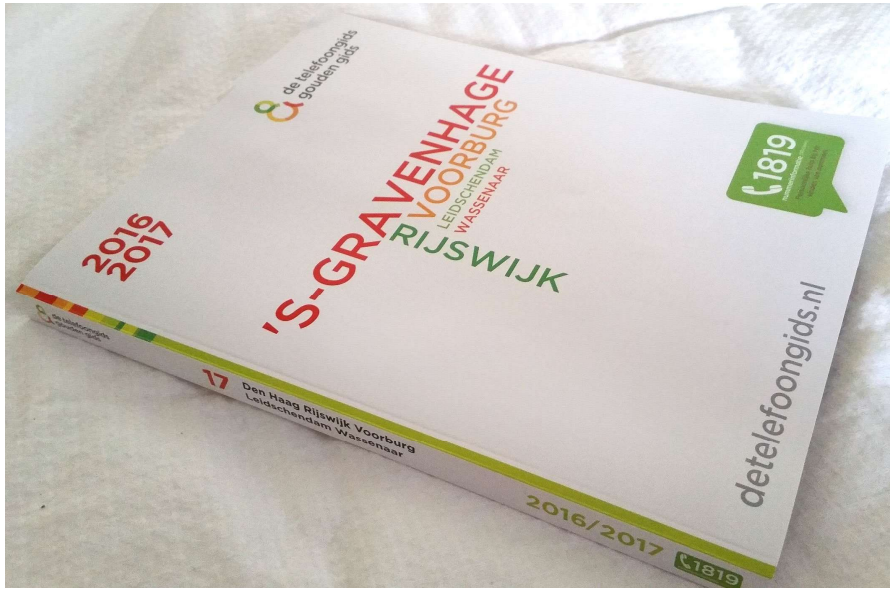
Infrastructuur dienstaanbieder



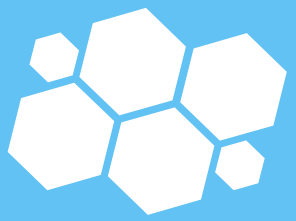
- Grote SaaS/PaaS/IaaS-dienstaanbieders hebben alles zeer meervoudig uitgevoerd:
  - zo goed als geen risico's door simpel uitvallen van apparatuur, verbindingen of stroom
  - desnoods word je naar een ander continent geherrouteerd!
- Overblijvende risico's:
  - falen complexe monitoring/herrouteringssystemen
  - "laag 8"-problemen

DNS

- "Telefoonboek" van het internet
- Kan veel mee mis gaan
- Maar gebeurt gelukkig zelden
- Wel handig om echt verschillende DNS-servers te gebruiken, niet twee van dezelfde ISP
- Bonuspunten: DNSSEC
- En let goed op de hosting van je eigen domeinen, als een aanvaller dat wachtwoord te pakken krijgt...

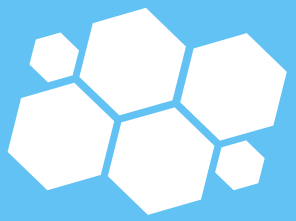


Om het internet heen?



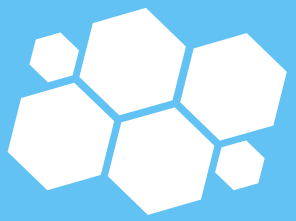
- Ondanks dat ze in de wolk getekend worden is de manier waarop deze diensten aan het internet gekoppeld worden vrij standaard
  - tenzij je een "cloud connect"-dienst afneemt:
    - telecomaanbieder brengt jouw data dan bij de voordeur van de dienstaanbieder
    - maar ja, je moet nog wel door de firewall en anti-DDoS, dus niet immuun voor alle internet-problemen

Om het internet heen? (2)



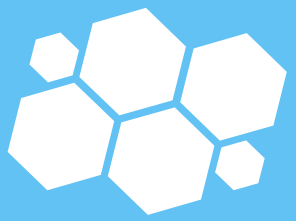
- Als je eigen apparatuur in een aantal datacenters hebt staan kan je glasvezels daar naartoe huren, geen internetrisico's!
  - met name nuttig als je ook nog kritische apparatuur op eigen (kantoor-) locaties hebt staan
- Rechtstreeks naar clouddiensten: "cloudconnect"
  - wel flinke beperkingen:
  - geen rechtstreekse glasvezel, er zit nog een telecombedrijf tussen
  - je kom vlak voor de "voordeur" uit:
    - dus samen met internetverkeer door firewalls en anti-DDoS
    - blijft afhankelijk van publieke DNS
    - blijft afhankelijk van publieke IP-adressen van de clouddienst
    - niet volledig immuun voor internet-routeringsproblemen

Conclusies



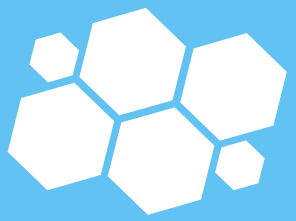
- Alles gaat ooit een keer kapot!
- Dus voorkom "single point of failure"
  - neem twee ISPs
    - al is het maar 4G/5G via je telefoon als backup
  - gebruik twee IP versies: IPv4 *en* IPv6
  - indien van toepassing: DNSSEC en RPKI
    - "publiceer" in elk geval, dat is relatief simpel
    - waar mogelijk: ook controles toepassen

Te afhankelijk ☁ ?



- De vraag van de avond...
- *Het hangt er vanaf:*
  - hoeveel miljoen kost elk uur dat bol.com onbereikbaar is?
  - hoeveel scheelt het als een medewerker een halve dag niet kan mailen en Googlen, maar wel verder kan met Word en Powerpoint op haar eigen PC?
  - voordelen van *zero footprint*-systemen voor medewerkers, maar dan wel het nadeel dat zonder netwerk medewerkers helemaal niks meer kunnen?
- Ofwel: als je er maar over nagedacht hebt

Vragen?



Bedankt voor het luisteren!

inet6consult.com

Shared Experiences

CAN WE STILL LEARN FROM THE PAST… ?

Have we become too dependant on The Cloud?

Paul Oor

PvIB Utrecht, 12 April 2022

15 PvIB reconnect in cyber security

Shared Experiences

CAN WE STILL LEARN FROM THE PAST… ?

Have we become too dependant on The Cloud?

PvIB Utrecht, 12 April 2022

PvIB reconnect in cyber security

INTRODUCTION

PAUL W.M. OOR CISSP, CCSP, CISM

THREAT ACTORS, a bit of History…

HISTORY

- PIRATES
- SUPPLY CHAINS, the Seven Seas…
- COLONIES, harbours, goods and people

TODAY

- HACKERS
- SUPPLY CHAINS, ICT/network infrastructure
- DATA COLONIES, information on goods and people

THE GLOBAL CLOUD, YOUR BUSINESS & PRIVATE ENVIRONMENT…

YEAR 2000 ***YOUR OWN*** **BIG COMPUTER**
DATA CENTRE CONCERNS & CONSIDERATIONS

- **NATURAL DISASTERS, HAZARDS**
- **PROXIMITY ENDUSERS**
- **AVAILABILITY SKILLED STAFF NEARBY**
- **PHYSICAL CONNECTIONS**
- **LOCAL REAL ESTATE SITUATION**
- **SAFE LOCATION & SURROUNDINGS**
- **NETWORK CONNECTION**
- **BUSINESS CASE, TAX CLIMATE**
- **PROCESSING CAPACITY/PERFORMANCE**
- **POWER SUPPLY**
- …


Interview
Ank Bijleveld: 'Mijn wereldbeeld is er niet vrolijker op geworden'

YEAR 2022 ***SOMEONE ELSES*** **BIG COMPUTER**
DATA COLONY , ***CLOUD*** CONCERNS & CONSIDERATIONS

- NATURAL DISASTERS, HAZARDS
- PROXIMITY ENDUSERS
- AVAILABILITY SKILLED STAFF NEARBY
- PHYSICAL CONNECTIONS
- LOCAL REAL ESTATE SITUATION
- **SAFE LOCATION AND SURROUNDINGS**
- **NETWORK CONNECTION**
- **BUSINESS CASE, TAX CLIMATE**
- **PROCESSING CAPACITY/PERFORMANCE**
- **POWER SUPPLY**
- **ENVIRONMENT, SUSTAINABILITY**
- **REGULATION, LEGISLATION**
- **ETHICS, SOCIAL CONCERNS**
- **GEO POLITICAL SITUATION**
- **NATIONAL SECURITY**
- **PRIVACY CONCERNS**
- **ECONOMIC DEPENDENCIES**
- **TRUST, CONFIDENTIALITY**
- **CONCENTRATION RISK**

THREATS and threat ACTORS…
learn from the past… actionable advice

- PIRATES, HACKERS
  are here to stay…deal with it…
- Protect (NETWORK) SUPPLY CHAINS
  Deal with it… OODA
  train as you fight, fight as you train…
- DATA (CENTER) CLOUD COLONIES

<u>Strategy</u> based on *evil scenarios*

1. Lessons from the past
= **Future success**

2. Cloud Deployment
= **Boardroom Strategy**

3. Focus
= **Digital Sovereignty!**

4. EMBRACE TOMORROW WITH
OPTIMISM, INTEREST AND **VIGILANCE**!

Hybrid Cloud and Its Associated Risks

Secure Connection Requirements of Hybrid Cloud

Peter van Eijk

Hybrid Cloud and Its Associated Risks

Secure Connection Requirements of Hybrid Cloud

PvIB, Utrecht, 12 april 2022

cloud security alliance®

Peter van Eijk

PvIB Platform voor InformatieBeveiliging

Hybrid Cloud and Its Associated Risks

Mitigation Measures for Risks, Threats, and Vulnerabilities in Hybrid Cloud Environment

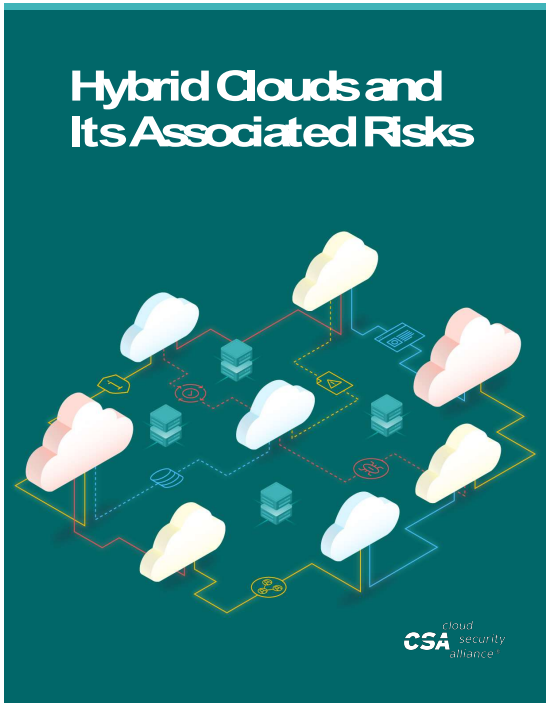
cloud security alliance®

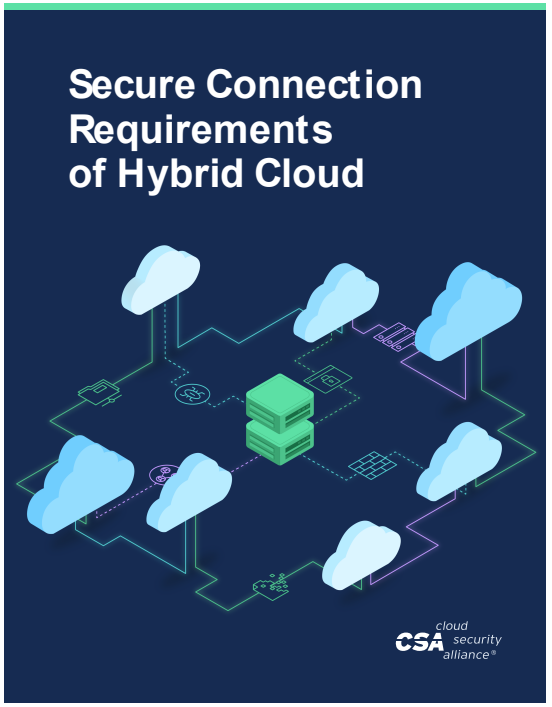
Hybrid Cloud Security Working Group

- This initiative aims to
  - Identify hybrid cloud security risks and countermeasures
  - Provide suggestions on hybrid cloud governance, hybrid cloud threat profiles and hybrid cloud security evaluation
  - Provide guiding both users and cloud service providers to choose and provide secure hybrid cloud solutions and promoting security planning and implementation.
- Current papers
  - Hybrid Clouds and Its Associated Risks
  - Mitigating Hybrid Cloud Risks
  - Secure Connection Requirements of Hybrid Cloud
- Co-Chair
  - Zou Feng, Director of Cloud Security Planning and Compliance, Huawei
  - Narudom Roongsiriwong, SVP and Head of IT Security, Kiatnakin Phatra Bank

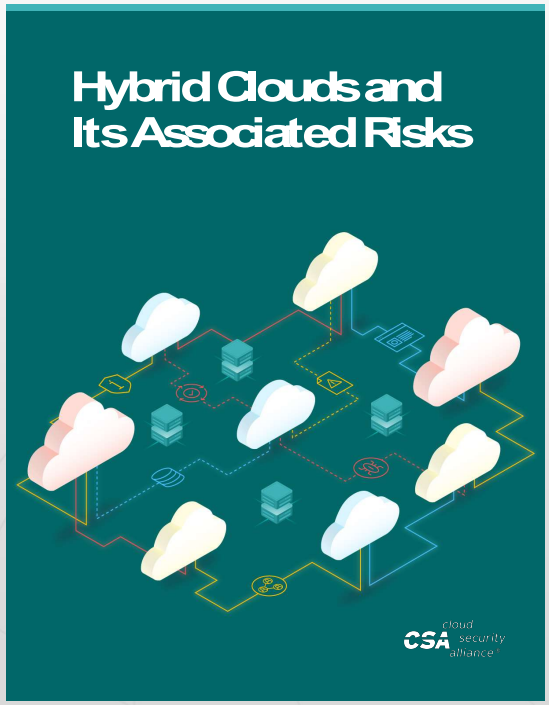
https://cloudsecurityalliance.org/research/working-groups/hybrid-cloud-security

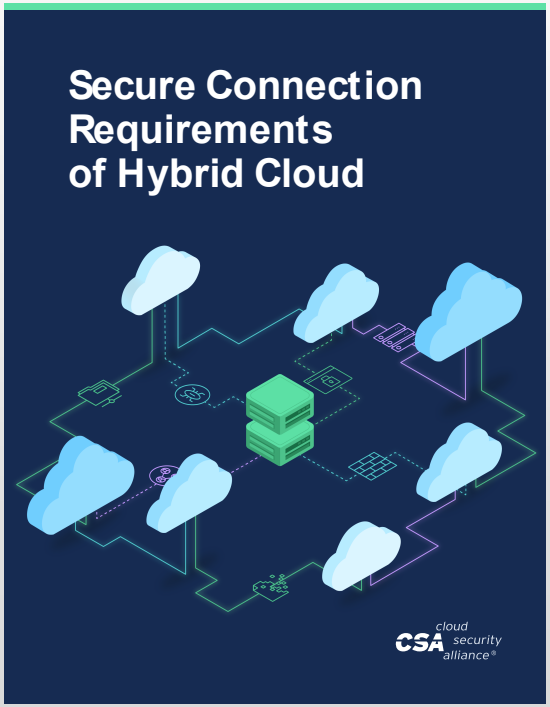
Research papers





Research papers





Introduction

- International Data Corporations (IDC) IaaSView report in 2019 indicates that 52% of IaaS enterprise Customers already have a hybrid cloud infrastructure in place.
- Gartner predicts that by 2020, 90% of organizations (who use Data Center Outsourcing or Infrastructure Utility Services) will adopt hybrid cloud infrastructure management capabilities and services

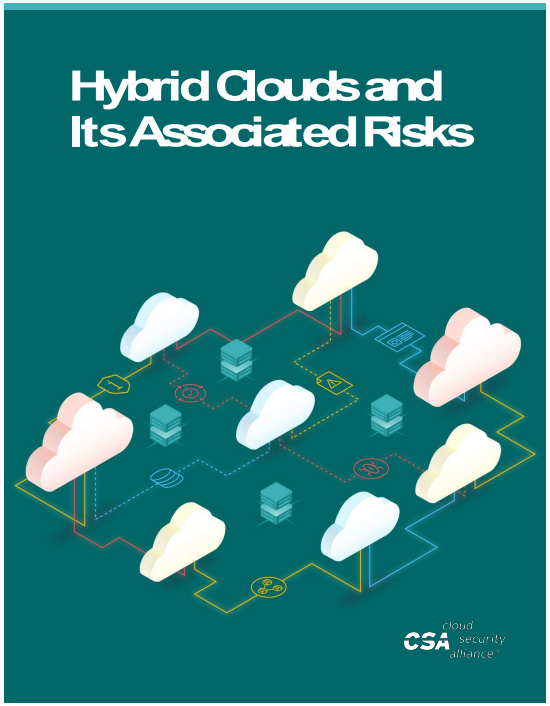
https://www.idc.com/getdoc.jsp?containerId=prUS45625619
https://www.gartner.com/en/newsroom/press-releases/2017-04-05-gartner-says-a-massive-shift-to-hybrid-infrastructure-services-is-underway

Introduction

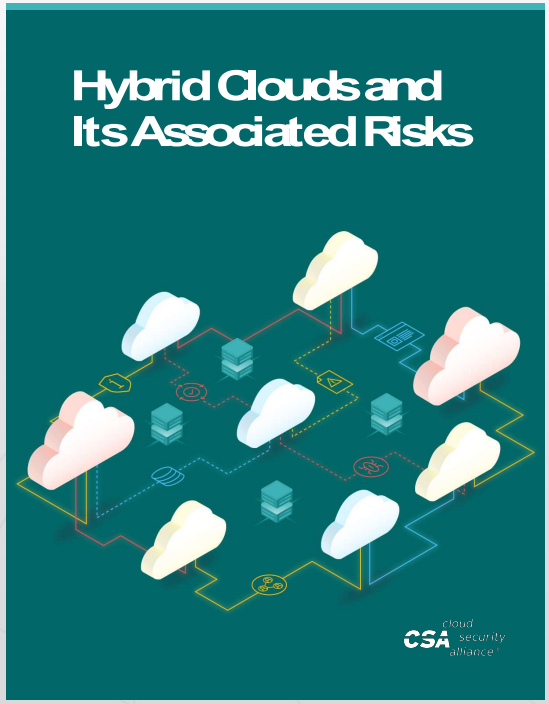
- International Data Corporations (IDC) IaaSView report in 2019 indicates that 52% of IaaS enterprise Customers already have a hybrid cloud infrastructure in place.
- NTT Ltd., in its 2021 Hybrid Cloud Report indicates 60.9% of organizations globally already using, or piloting hybrid cloud and a further 32.7% of respondents plan to implement a hybrid solution within 12-24 months

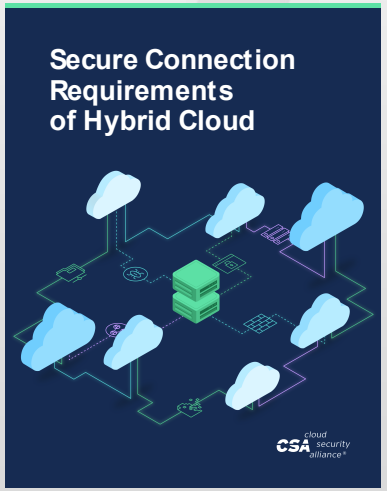
https://services.global.ntt/en-us/newsroom/global-businesses-see-hybrid-cloud-as-critical-to-meeting-business-needs
https://www.idc.com/getdoc.jsp?containerId=prUS45625619

Research papers



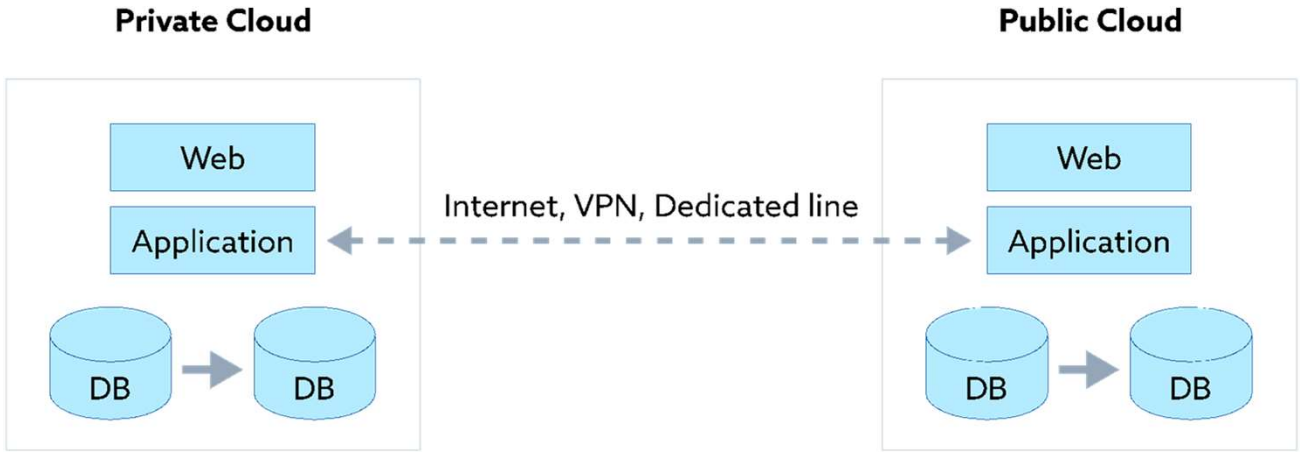
Research papers





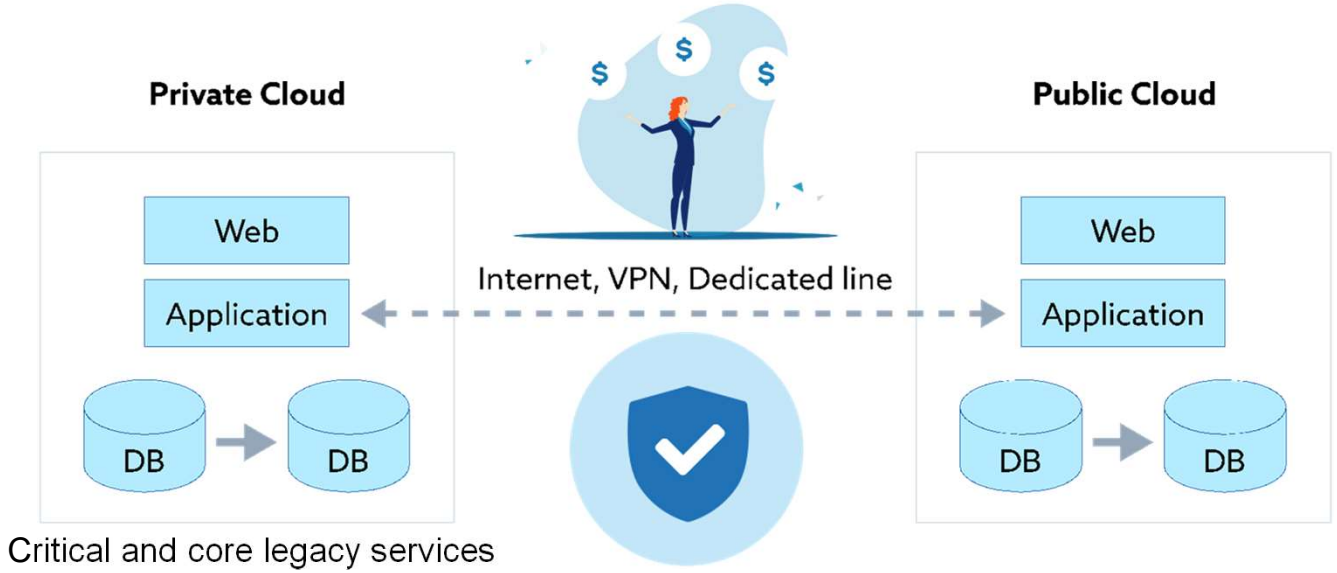
What is Hybrid Cloud?

- ISO/IEC 17788-2014, hybrid cloud is defined as a cloud deployment model that uses at least two different cloud deployment models (private, community, public)
- NIST Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).



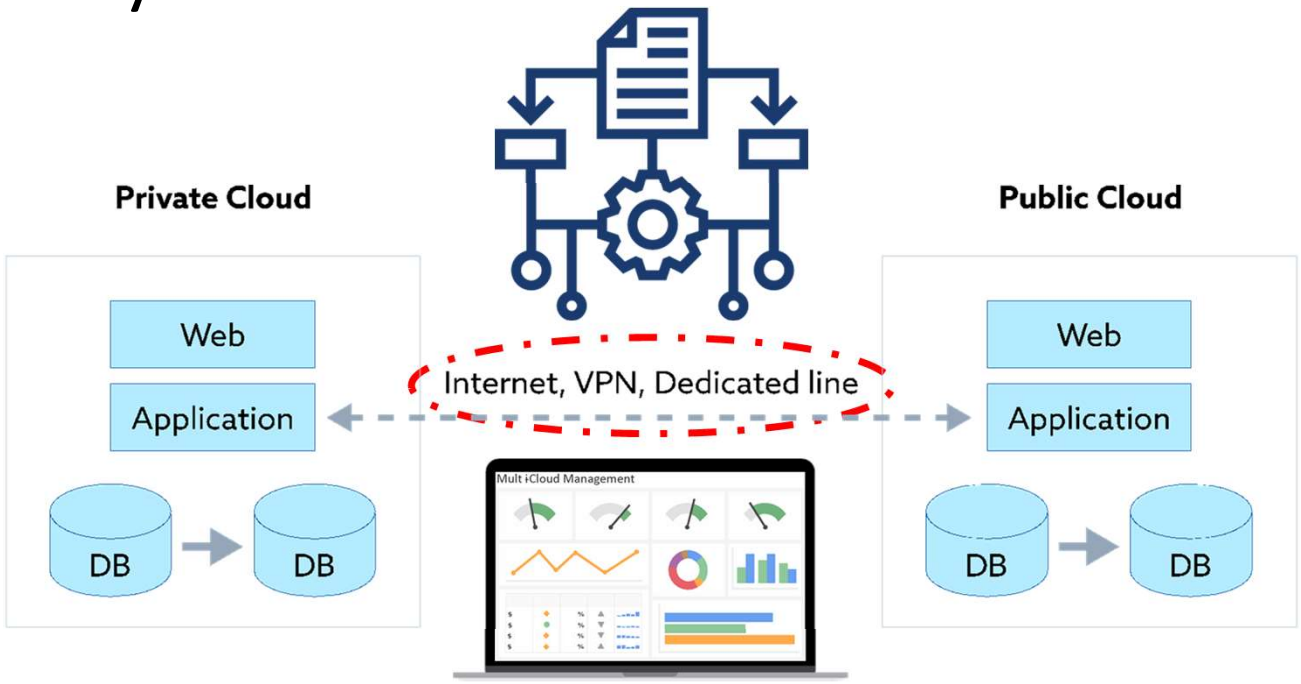
Business Value of the Hybrid Cloud for Enterprises

- An effective way to enjoy the benefits of public cloud without disrupting critical and core legacy services on private cloud
- Possible effective means to securely use cloud technologies
- Leveraging cloud resources at optimal costs



Hybrid Cloud Implementation

- Layer 3 Network Interworking
- Multi-Cloud Management Enabled by Cloud Broker
- Consistent Hybrid Cloud



Shared Responsibility in Hybrid Clouds

	On-premises/ Private Cloud	Public Cloud		
		IaaS	PaaS	SaaS
Data	Customer	Customer	Customer	Customer
Applications	Customer	Customer	Customer	CSP
Runtime	Customer	Customer	CSP	CSP
Middle Ware	Customer	Customer	CSP	CSP
Operation System	Customer	Customer	CSP	CSP
Virtual Network	Customer	Customer	CSP	CSP
Hypervisor	Customer	CSP	CSP	CSP
Servers	Customer	CSP	CSP	CSP
Storage	Customer	CSP	CSP	CSP
Physical Network	Customer	CSP	CSP	CSP

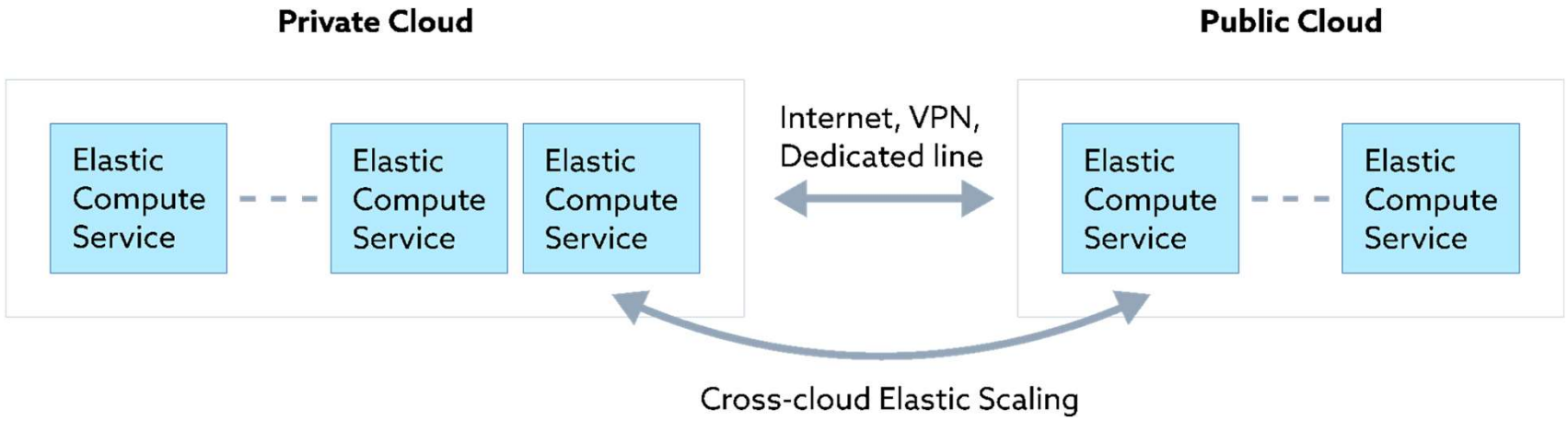
Hybrid Cloud Risks

- Distributed Denial of Service Attack (DDoS)
- Data Leakage
- Perimeter Protection Risks
- Compliance Risks
- Misaligned Service Level Agreements (SLAs)
- Misalignment of Cloud Skill Sets
- Gap in Security Control Maturity
- Comprehensiveness of Security Risk Assessment

Hybrid Cloud Threats & Vulnerabilities

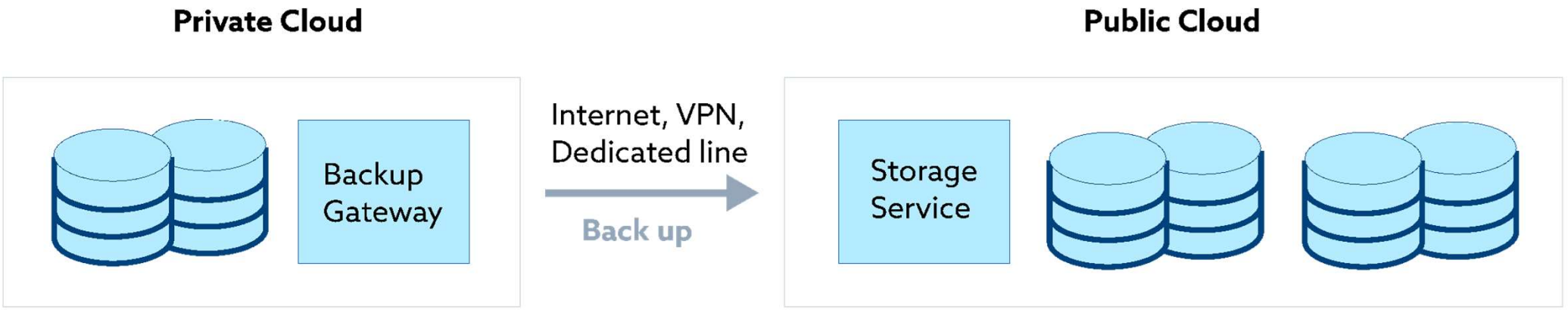
- Threat
  - Malicious Insider
- Vulnerabilities
  - Poor Encryption
  - Impacted Operational Processes
  - Network Connectivity Breaks
  - Decentralized Identity & Credential Management
  - Siloed Security Management

Use Case: Workload Expansion (Bursting)



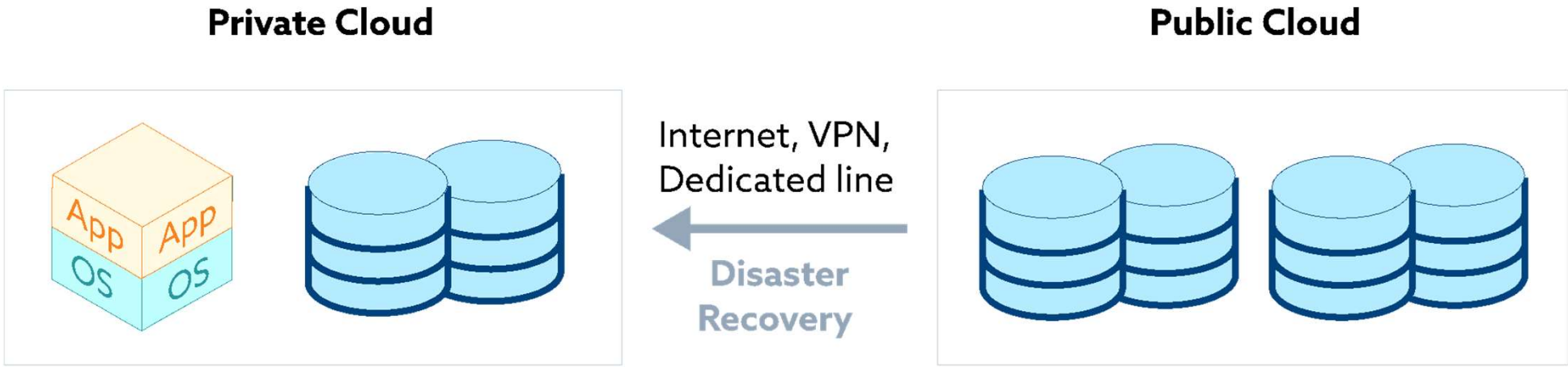
- Key risks, threats, and vulnerabilities
  - DDoS:
  - Data leakage
  - Impacted operational processes
  - Decentralized identity & access lifecycle management
  - Compliance risks
  - Network connectivity breaks

Use Case: Backup



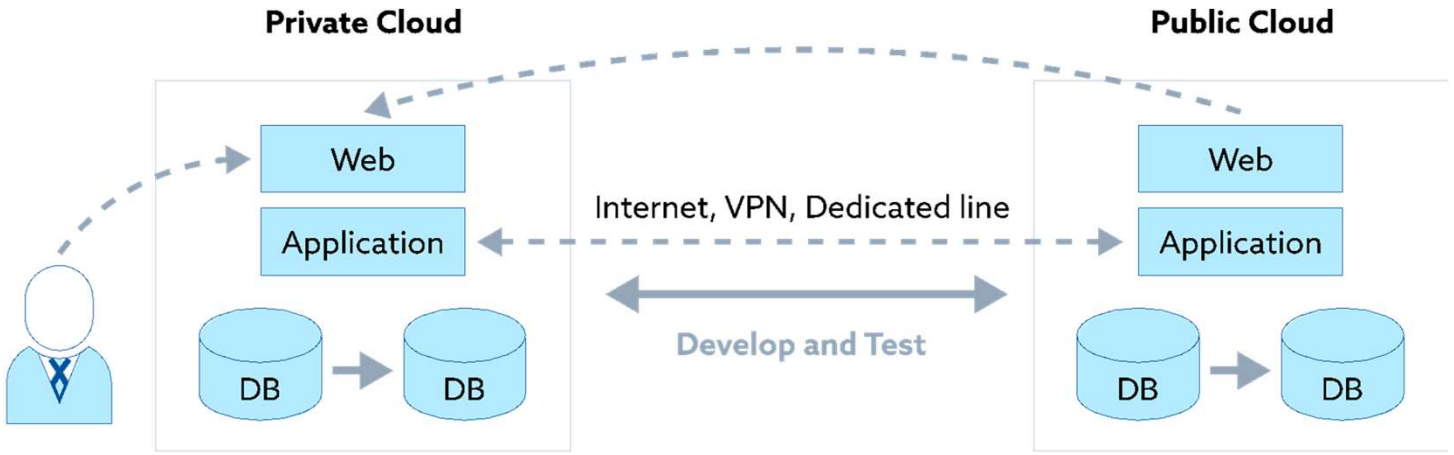
- Key risks, threats, and vulnerabilities
  - Data leakage
  - Compliance risks
  - Network connectivity breaks

Use Case: Disaster Recovery (DR)



- Key risks, threats, and vulnerabilities
  - Data leakage
  - Compliance risks
  - Network connectivity breaks
  - Insufficient testing of DR plans & tools

Use Case: Layered Deployment

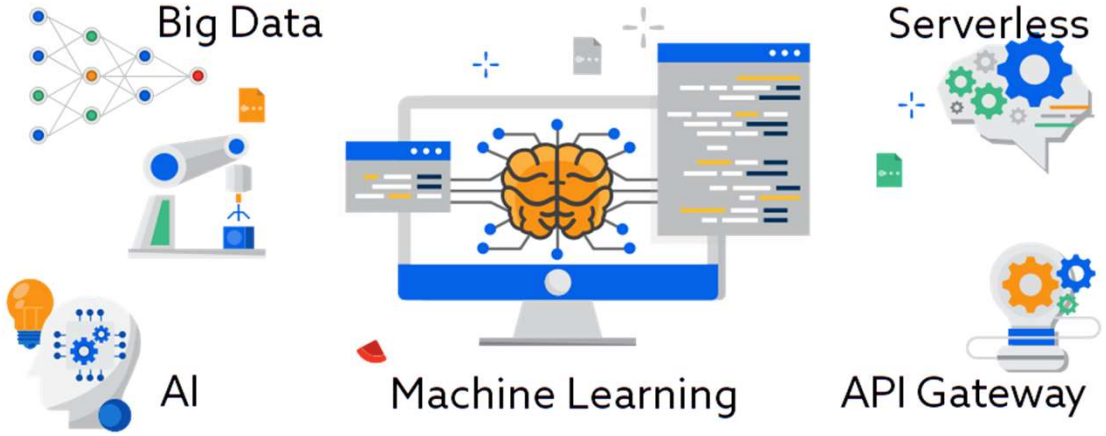


- Key risks, threats, and vulnerabilities
  - DDoS:
  - Perimeter protection risks
  - Network connectivity breaks

Use Case: Application Container Technology

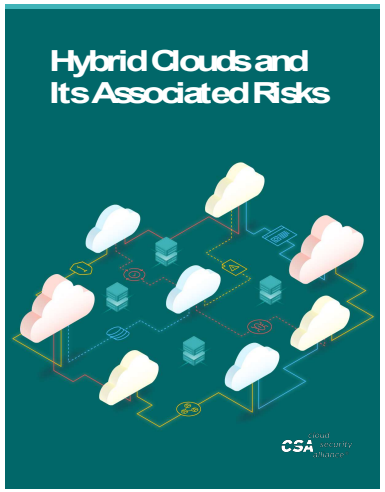
- Key risks, threats, and vulnerabilities
  - Perimeter protection risks
  - Gaps in cloud skill sets and security control maturity

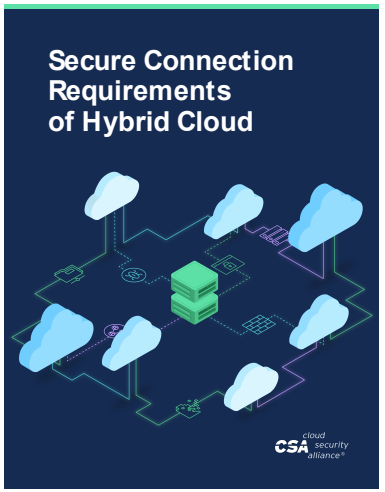
Use Case: Extend New IT Capabilities



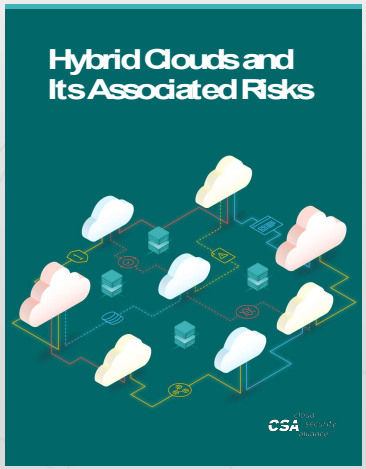
- Key risks, threats, and vulnerabilities
  - Compliance risks
  - Impacted operational processes, misaligned SLAs, gaps in cloud skill sets and security control maturity
  - Non-unified APIs

Research papers

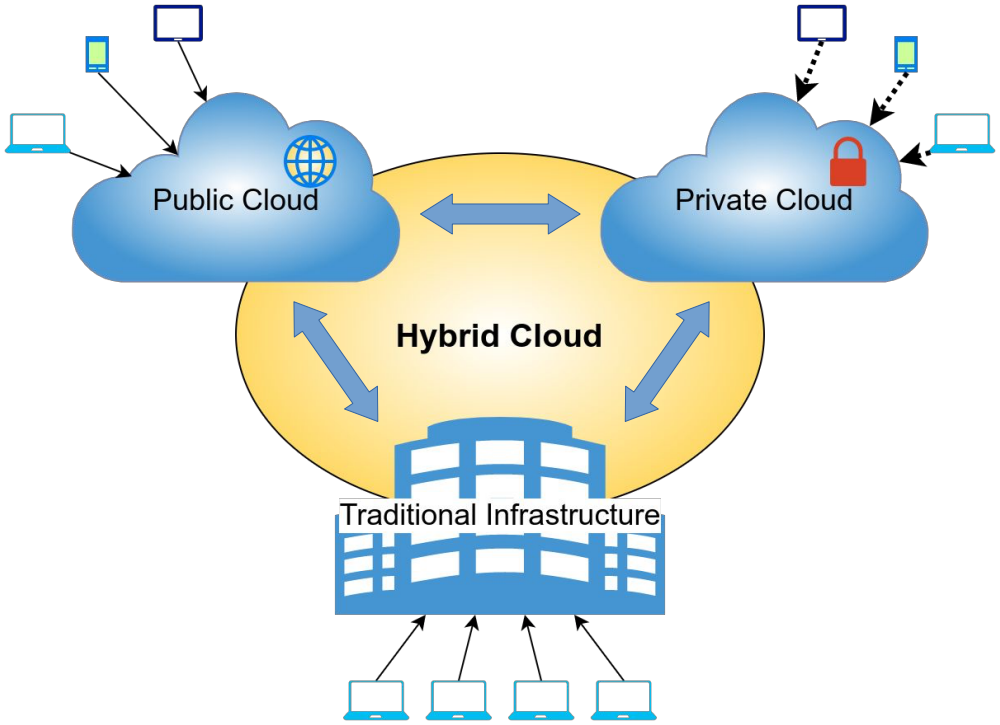




Research papers



Hybrid Cloud Architecture



cloud security alliance®

Cross-Cloud Security Capabilities

Cross-Cloud Perimeter Security

Cross-Cloud Transmission Security

Cross-Cloud Storage & Compute Security

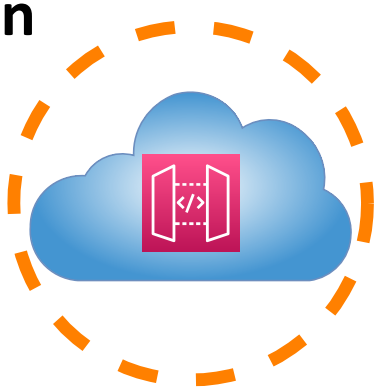
Cross-Cloud Management Security

cloud security alliance®

Cross-Cloud Perimeter Security

Perimeter Protection

Access Control



Interface Security

cloud security alliance®

Cross-Cloud Transmission Security

Network Connection

Communication Transmission

cloud security alliance®

Cross-Cloud Storage & Compute Security

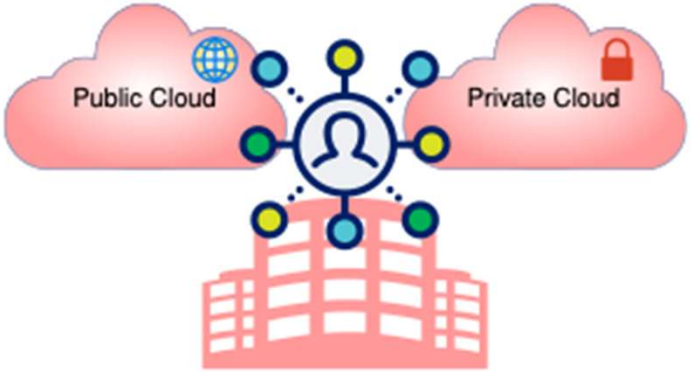
Data Storage

Compute Resources

Backup & Restore

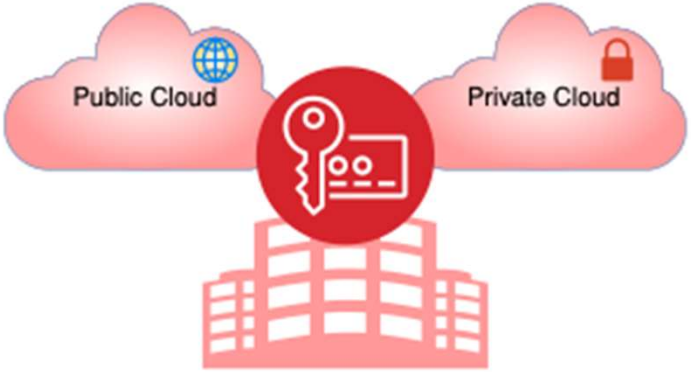
cloud security alliance®

Cross-Cloud Management Security (1/2)



Identity Authentication

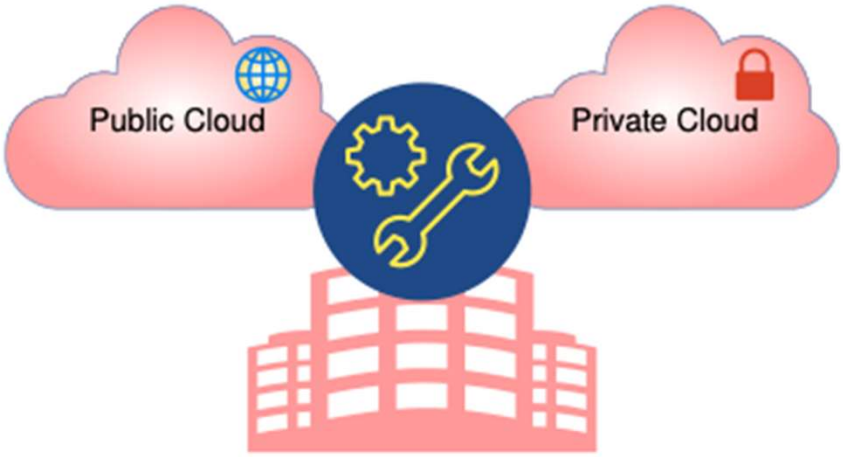
Authorization Management



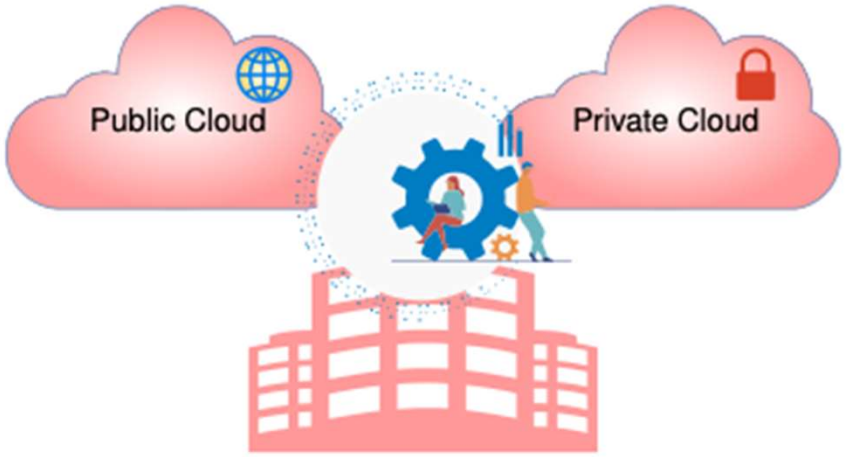
Key Management

cloud security alliance®

Cross-Cloud Management Security (2/2)



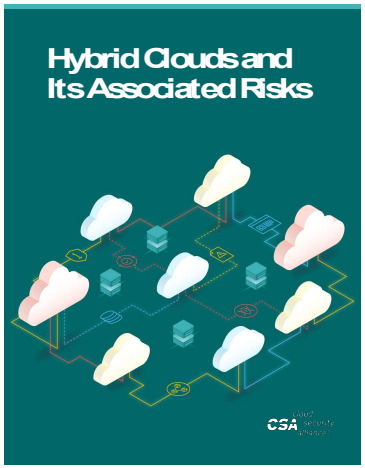
Operation & Maintenance

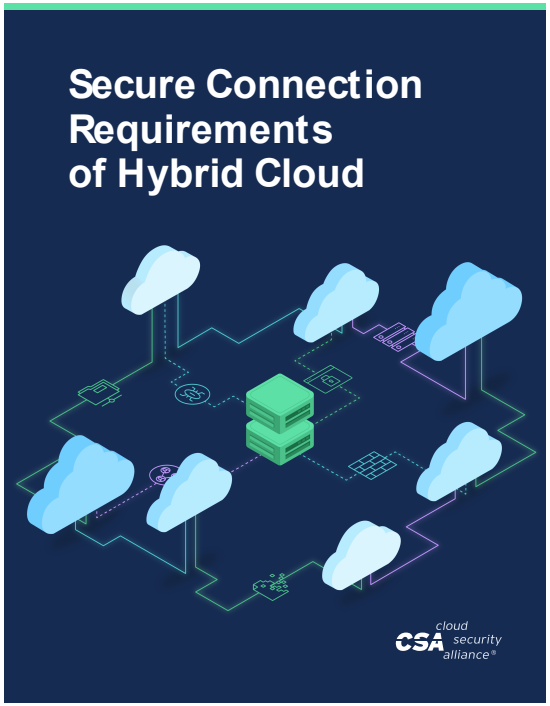


Operation Management

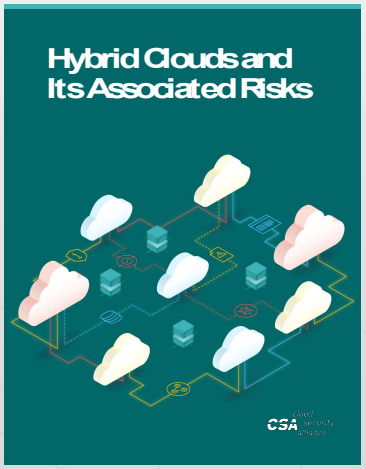
cloud security alliance®

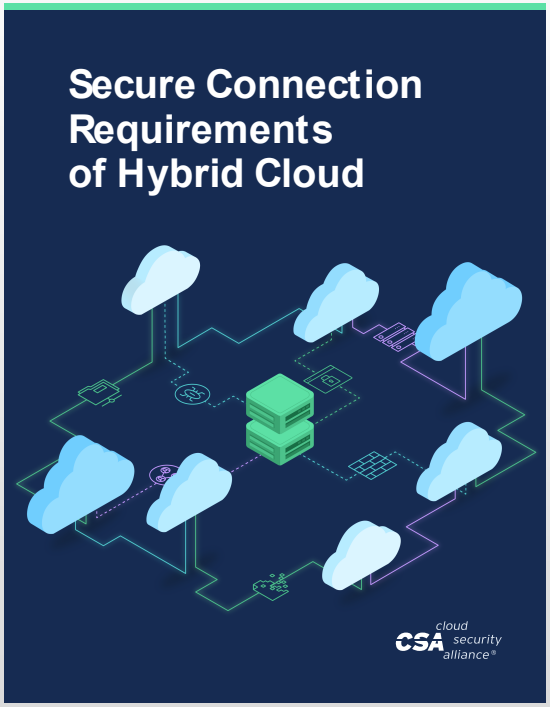
Research papers





Research papers





Contents

- Mitigation Measures for Risks
- Mitigation Measures for Threats
- Mitigation Measures for Vulnerabilities
- Conclusion

Mitigation Measures for Risks

1. Mitigate DDoS
2. Mitigate Data Leakage
3. Improve Perimeter Protection
4. Compliance
5. Aligned SLAs
6. Alignment of Cloud Skill Sets
7. Overall Considerations for Security Control Maturity
8. Comprehensiveness of Security Risk Assessment

Mitigation Measures for Risks

1. Mitigate Distributed Denial-of-Service Attacks (DDoS)

- Evaluate
- Plan
- Deploy
- Provide

Mitigation Measures for Risks

2. Mitigate Data Leakage (Ⅰ)

- Data classification
- Establish data security system and process assurance protocols
- Classify key data in advance
- Access control technologies and management methods
- Audit data Lifecycle
- Secure data interfaces

Mitigation Measures for Risks

2. Mitigate Data Leakage (Ⅱ)

- Data-sharing platforms
- Avoid plaintext transmission
- Isolate data transmission
- Control the unauthorized exfiltration
- Use the pseudonymization technique
- Add breach notifications or alerting mechanisms

Mitigation Measures for Risks

3. Improve Perimeter Protection (I)

- Utilize whitelisted devices for device-level authentication
- Consider geo-fencing
- Implement virtual security protection through in-depth network and security convergence
- Maintain APIs and add a statement for API security controls

Mitigation Measures for Risks

3. Improve Perimeter Protection (Ⅱ)

- Centralized security management and integrated customization of security policies
- Bind security policies to services
- Monitor security events
- Use strict access control policies
- Authenticate third-party applications for accessing cloud service interfaces
- Use an authentication credential

Mitigation Measures for Risks

3. Improve Perimeter Protection (Ⅲ)

- Encrypt the interface access connection
- Protect the credentials, keys, and tokens used for interface authentication and authorization
- Scan all traffic
- Verify all parameters inputted through the interface
- Compile the result code returned by the interface
- Set a threshold for the access frequency and access duration of the interface

Mitigation Measures for Risks

4. Compliance

- Specify which compliance standards apply and ensure compliance status
- Substantiate compliance through collaborative work
- Identify sensitive data involved in services in advance
- Evaluate information provided by public cloud
- Report on configuration statuses and risk levels for public and private cloud
- Engage in continuous compliance assessment and monitoring

Mitigation Measures for Risks

5. Aligned Service-Level Agreements (SLAs)

- The SLA covers overall services
- Users document requirements and thoroughly investigate hybrid cloud providers
- Specify and detail user service expectations in the SLA

Mitigation Measures for Risks

6. Alignment of Cloud Skill Sets (I)

- Use a Unified cloud management platform (CMP)
- The CMP isolates tenant data and enables access control measures
- The CMP provides a vendor-neutral interface
- The CMP should have a robust Identity aggregation, federation mechanism and attribute/policy-based access control
- Management planes integrate with public cloud providers cost management APIs and allow custom cost metrics definitions

Mitigation Measures for Risks

6. Alignment of Cloud Skill Sets (Ⅱ)

- Management planes are extensible
- Up-skilling internal staff capability and skill sets
- Sourcing vendors with the necessary skill sets and experience
- Establish personnel credentials and qualifications
- Attestations on compliances are generally publicly available
- SOC reports can be obtained to ensure adequate controls for SaaS options

Mitigation Measures for Risks

7. Overall Considerations for Security Control Maturity

- Understand the security control maturity
- Utilize security gap analysis to track weak security areas

Mitigation Measures for Risks

8. Comprehensiveness of Security Risk Assessment

- Asset-based risk management
- Integrate the hybrid cloud environment and implement risk assessment and prevention
- Conduct a periodic vulnerability assessment
- Log monitoring must be activated
- Software must be updated to the latest version
- View and track the security data in a unified manner

Mitigation Measures for Threats

1. Mitigate Malicious Insider (I)

- Comprehensive monitoring and auditing measures
- Create an enterprise risk identification and mitigation plan
- Stop all unauthorized access attempts
- Ensure that the least privilege mode is set and applied
- Delete or disable unnecessary and expired accounts promptly and avoid sharing accounts

Mitigation Measures for Threats

1. Mitigate Malicious Insider (Ⅱ)

- Establish a strict password control mechanism
- Strictly restrict access to key assets of the organization
- Establish internal behavior security monitoring and analysis methods
- Conduct annual incident response drills or tabletop exercises
- Develop broad insider threats awareness in security training.

Mitigation Measures for Vulnerabilities

1. Encryption
2. Seamless Operational Processes
3. Network Connection Assurance
4. Centralized Identity and Access Lifecycle Management
5. Integrated Security Management

Mitigation Measures for Vulnerabilities

1. Encryption (Ⅰ)

- Consider the respective characteristics of asymmetric and symmetric encryption

- Protecting data at rest:
  - Employ HSMs or external devices to generate encryption keys
  - Utilize TPMs
  - Use automated encryption
  - Consider two layers of protection
  - Use full disk partition encryption
  - Maintain encryption keys separately from the cloud environment

- Protecting data in motion
  - Use IPSec
  - Encrypt data flows and sessions

Mitigation Measures for **Vulnerabilities**

2. Seamless Operational Processes

- Review security and operational processes
- Pay particular attention to align the processes

Mitigation Measures for **Vulnerabilities**

3. Network Connection Assurance

- Have a clear network architecture review of the hybrid cloud
- Single points of failures (SPOFs) are identified and eliminated
- Monitor SLAs for network services and perform regular testing for BCPs/DRPs at the network layer

Mitigation Measures for **Vulnerabilities**

4. Centralized Identity and Access Lifecycle Management

- Use the unified identity management tools
- Use role-based access for public and private cloud environments
- Use modern authentication protocols and multi-factor authentication
- Monitor and verify all access rights
- Decouple the unified identity management from public and private clouds

Mitigation Measures for **Vulnerabilities**

5. Integrated Security Management （I）

- Ensure effective integration of different management teams
- Take steps to establish an organizational cloud center of excellence
- Organizational strategy for cloud adoption
- Change organizational structural to align with the cloud computing paradigm
- Ensure that the cross-platform management tools and policies are consistent

Mitigation Measures for Vulnerabilities

5. Integrated Security Management （Ⅱ）

- Define rules for configuration, installation, and access control for sensitive data/applications
- Define end-to-end access control, user management, and encryption policies
- Use automated configuration management tools

Conclusion

- Aspects of determining hybrid cloud security measures
- Systematic design requires a complete end-to-end security solution
- Other Considerations

Documentatie en referenties

- Website Peter van Eijk
  www.clubcloudcomputing.com
- (CSA Circle community)
  https://circle.cloudsecurityalliance.org
- (Werkgroep en downloads)
  https://cloudsecurityalliance.org/research/working-groups/hybrid-cloud-security/ www.jointcyberrange.nl)
- www.jointcyberrange.nl

Thank you!

cloud security alliance®

Bedankt

Voor uw bezoek aan de presentatie

Zijn we niet te afhankelijk van de Cloud

Graag ontvangen wij uw Feedback !

PvIB Platform voor InformatieBeveiliging