LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Threats In Healthcare Cloud Computing

02/04/2021

TLP: WHITE, ID#202102041030

Agenda

- Cloud Computing
- Covid-19
- Cloud Service Providers
- Cloud Models
- Cloud as a Service
- Shared Responsibility Model
- Misconfigurations
- Threat Actors Targeting Cloud
- NIST Framework
- Reducing Risks
- Summary
- References

Image source: wire19

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Cloud Computing:

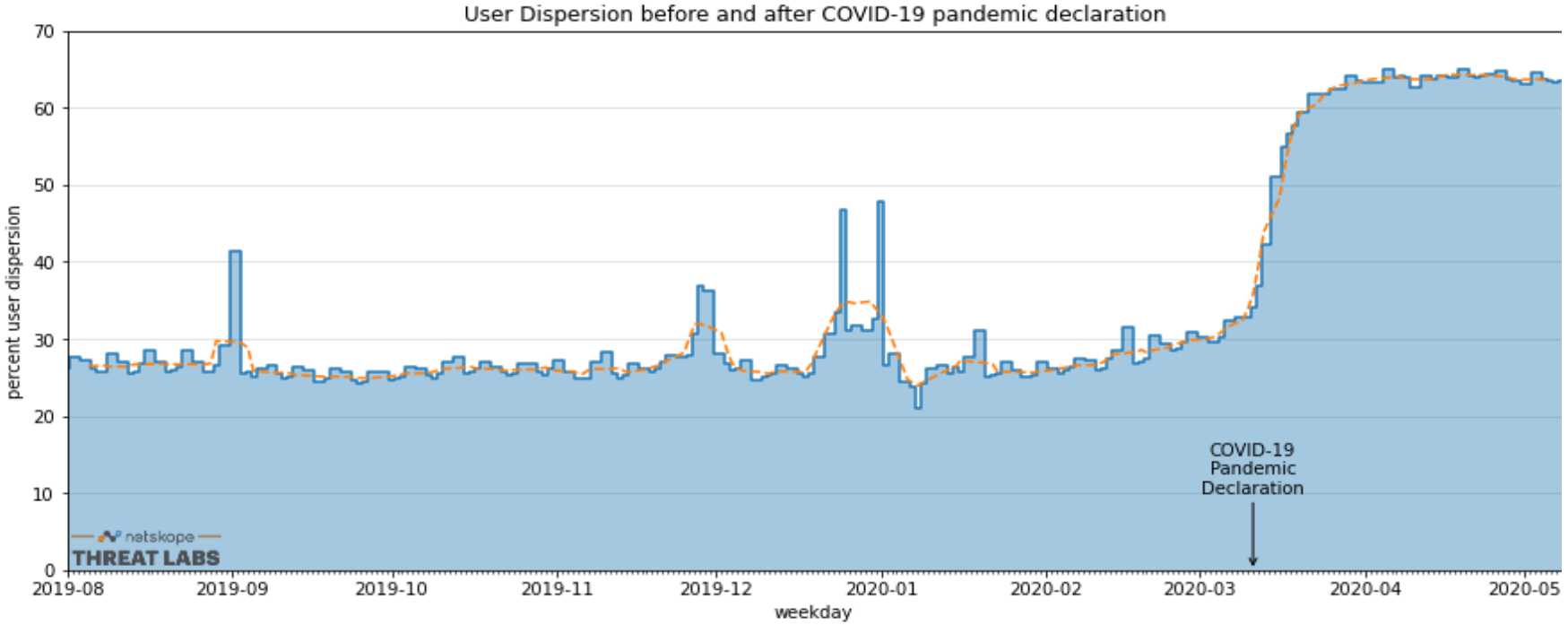
The delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

Cloud computing in the Healthcare market is estimated to grow from

$20 to $50 billion

by 2025.

Existing factors driving cloud transition further accelerated due to the COVID-19 pandemic. Cloud spending rose 35% during the first quarter of 2020.



McAfee researchers analyzed data from 30 million McAfee cloud global customers across all sectors, including healthcare, for their Cloud Adoption & Risk Report. The analysis found that the second-most targeted industry in relation to cloud threats was healthcare. Malicious IPs from China, Iran, and Russia were detected.

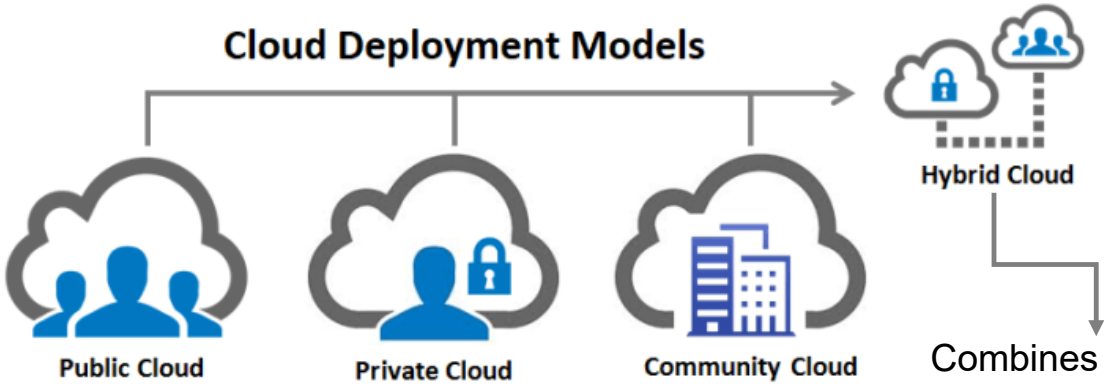
CSP Risks

- Outsourcing can be a valid approach to lowering the initial cost of deploying new IT-based services, and shortening the time to which such investment yields tangible benefits
- However, a proper risk assessment must be reviewed before outsourcing

Things to consider when selecting CSPs:

- Experience and technical expertise of key personnel
- Governance and compliance policies and practices, including vetting processes
- Quality and frequency of security and privacy awareness training
- Account management practices and accountability
- Adoption rate of new technologies
- How often management procedures and processes are changed
- Are the underlying mechanisms used to ensure privacy and security standards/commitments being maintained?

Cloud Models



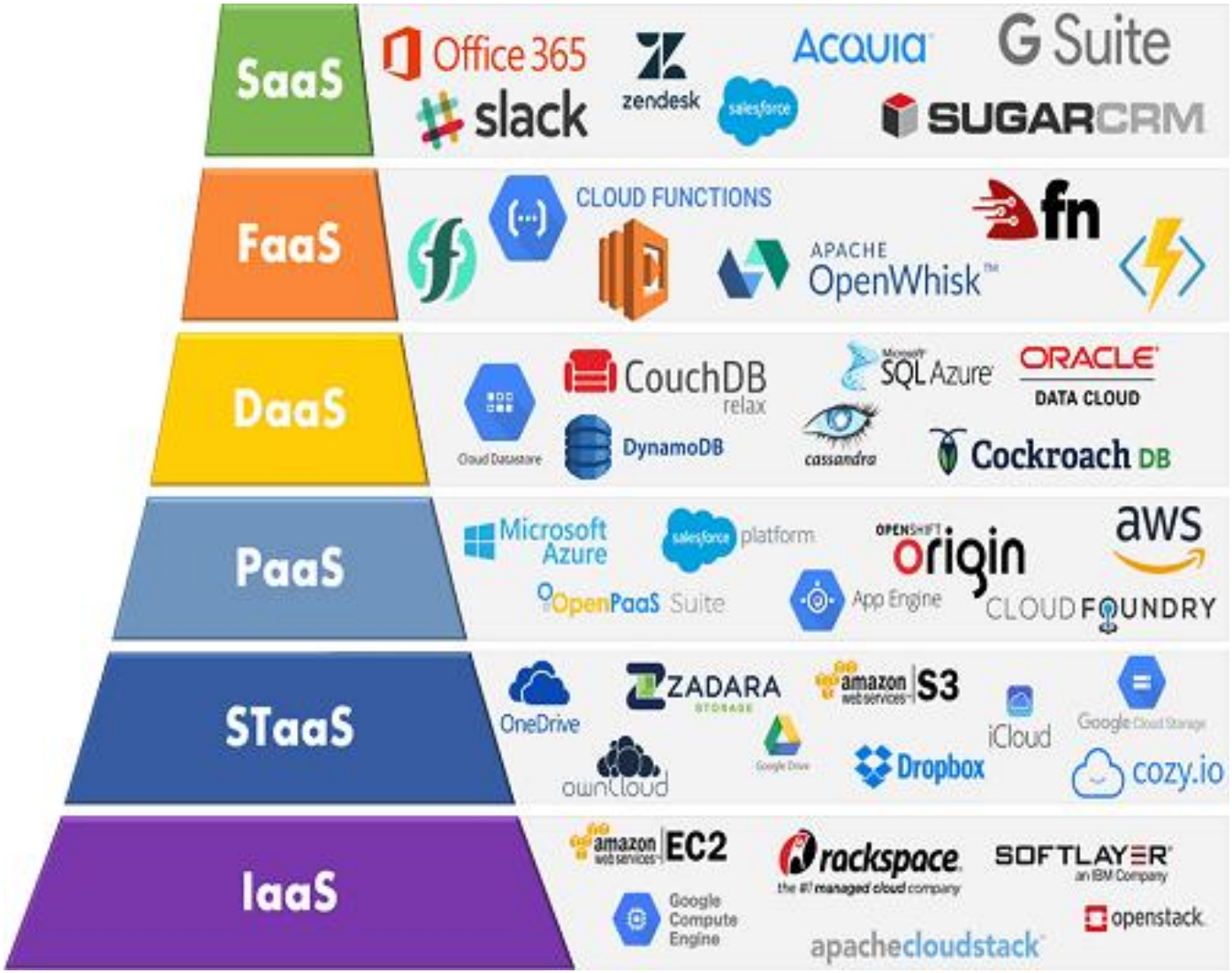
Combines on-premises infrastructure—or a private cloud—with a public cloud. Hybrid clouds allow data and apps to move between the two environments.

An open system where storage or software are available for free or pay-per-use, and can be accessed via Internet.

Consists of cloud computing resources used exclusively by one business or organization.

A multi-tenant platform that allows several companies work on the same platform, given that they have similar needs and concerns.

Cloud as a Service



Software

Function

Data

Platform

Storage

Infrastructure

Shared Responsibility Model

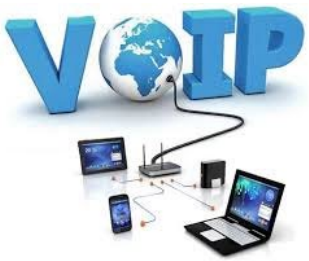
On premises (Traditional)	Infrastructure (IaaS)	Container (PaaS)	Abstract (SaaS)
Data	Data	Data	Data
Application	Application	Application	Application
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Your responsibility

Cloud Service Provider's responsibility

Image source:TrendMicro

The Summer 2020 edition of the *Accurics State of DevSecOps* report found that misconfigured cloud storage services were increasingly commonplace in 93% of cloud deployments.



Researchers discovered databases of a cloud-based Voice over IP telecommunications vendor containing more than 350 million customer records – including names, contact details, and in some cases, sensitive health information – stored online without the need for password authorization to gain access.

Researchers discovered a misconfigured Amazon S3 storage bucket, leaking over 60,000 patient records with protected health information tied to the cardiac data network.

Addressing Cloud Vulnerabilities

- Identity and Access Management (IAM) Roles
- Identity and Access Management Trust Policies
  - Permissions granted at the organization level
  - Permissions granted at the folder levels
  - Permissions granted at the project level
- Network Misconfiguration
  - Routing Rules
  - Private Subnet Routes
- Firewall Rules
  - ICMP Access
  - Outbound Access
  - Access to Non-HTTP/HTTPS Ports
  - Inbound Access on Uncommon Ports

65-70%

of all security issues in the cloud start with a misconfiguration.

APT37 was seen distributing a cloud-based RAT variant of RokRat to steal data from a victim's machine and send them to cloud services.

Chimera Group is now targeting Cloud services. The group has been using cloud storage web services such as Dropbox, Google Drive, and OneDrive and remote services such as VPN and Citrix, and a few specific tools named PsLogList, NtdsAudit, and Mimikatz.

**If information is successfully extracted from these tools, Pass-the-PRT attack is possible.*

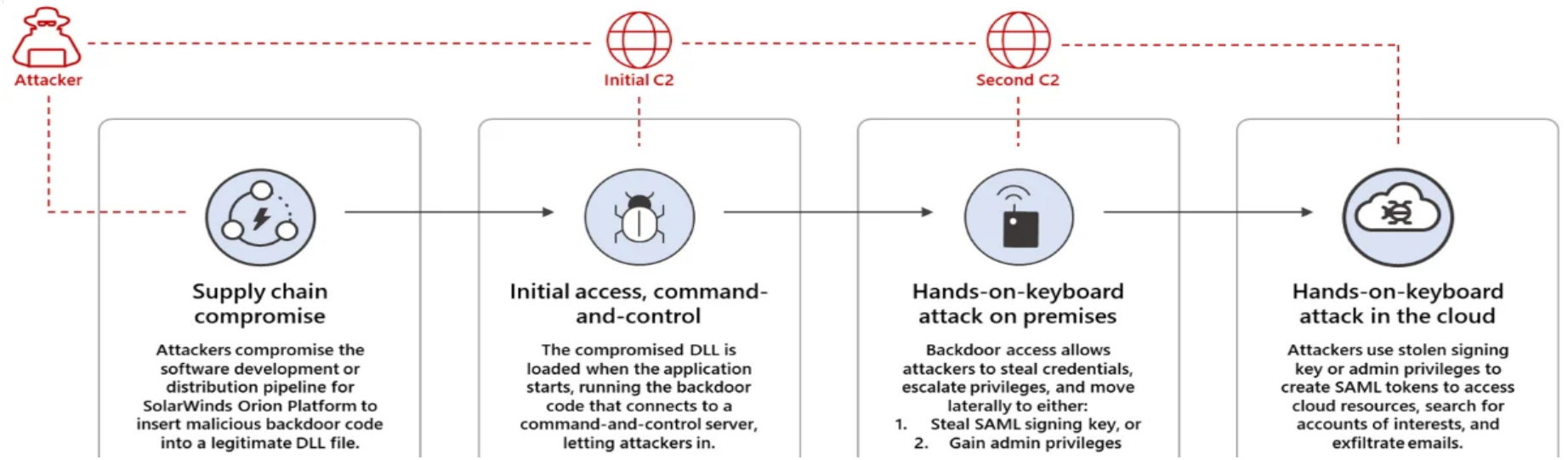
The suspected Russian hackers behind the massive SolarWinds attack attempted to hack CrowdStrike through a Microsoft reseller's Azure account, but were ultimately unsuccessful.

Example 1: How Threat Actors Infiltrate the Cloud

Companion alert to AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

CISA observed an APT actor using compromised applications in a victim's Microsoft 365 (M365)/Azure environment.

CISA also observed an APT actor utilizing additional credentials and Application Programming Interface (API) access to cloud resources of private and public sector organizations.



Example 2: How Threat Actors Infiltrate the Cloud

Stage 1: Forging a trusted authentication token used to access resources that trust the on-premises identity provider

Stage 2: Using the forged authentication token to create configuration changes in the Service Provider, such as Azure AD (establishing a foothold)

Stage 3: Acquiring an OAuth access token for the application using the forged credentials added to an existing application or service principal, and calling APIs with the permissions assigned to that application

Detection Method 1: Correlating SP login events with corresponding authentication events in ADFS and DCs

Detection Method 2: Identifying certificate export events in ADFS

Detection Method 3: Customizing SAML response to identify irregular access

Detection Method 4: Detecting malicious ADFS trust modification

https://us-cert.cisa.gov/ncas/alerts/aa21-008a

Stage 4: Once access has been established, the threat actor Uses Microsoft Graph API to conduct action on objectives from an external RESTful API (queries impersonating existing applications)

The NIST Cyber Security Framework (CSF) consists of standards, guidelines, and best practices to manage cybersecurity related risks. The NIST core identifies five key cybersecurity functions to organize recommended security controls into actionable work streams. As organizations adopt increasingly complex multi-cloud and hybrid cloud environments, attempting to apply the NIST CSF five key cybersecurity functions can be a challenge.

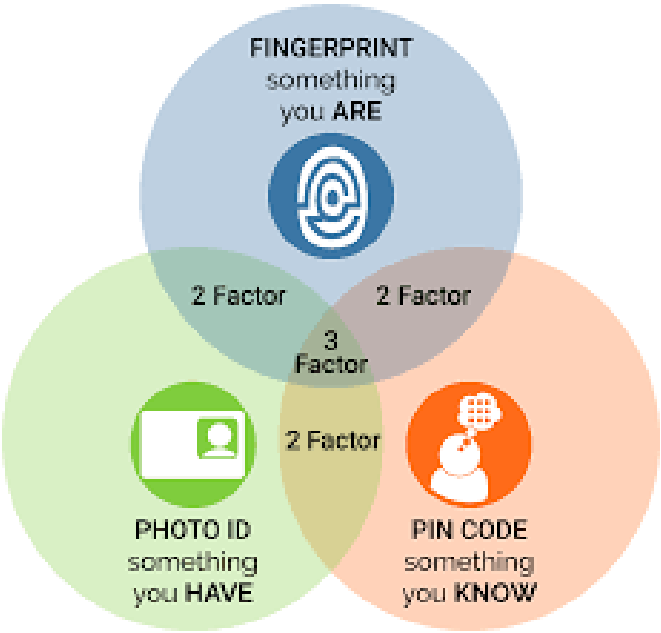
NIST Function	Challenge
Identify	Relationships between cloud entities can be very tough to see and visualize.
Protect	Choosing security tools and services to protect your infrastructure without creating a huge vulnerability.
Detect	Making sense of the data.
Respond	Analyzing incidents takes skill and time.
Recover	If your platform does not have the ability to deliver a complete and accurate picture of the attacks, recovery effects will also be incomplete.

Setup Correct Cloud Portfolio: Take a closer look at your selected cloud services to ensure what is or will be covered to reduce security gaps.

Cloud VPNs: Maintain conditions, permissions, and profiles of VPN policies for remote access**.** Create secure firewall rules for traffic that travels over Cloud VPN, and create strong pre-shared keys.

Multi-Factor Authentication: By providing an extra barrier and layer of security that makes it incredibly difficult for attackers to get past, MFA can block over 99.9 percent of account compromise attacks (according to Microsoft).

Secure Interfaces and APIs: From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent the security policy.



Keep multiple backups: The best way to thwart ransomware is to have multiple backups of data.

Prepare a Disaster Recovery Plan: A robust and tested disaster recovery plan can mitigate ransomware risks and minimize downtime/disruption.

Secure data at endpoints: If a ransomware attack manages to get through your security armor, your data at endpoints will be the first thing to get impacted. If these are hijacked, the chances of the changes being synced to cloud storage are very high.

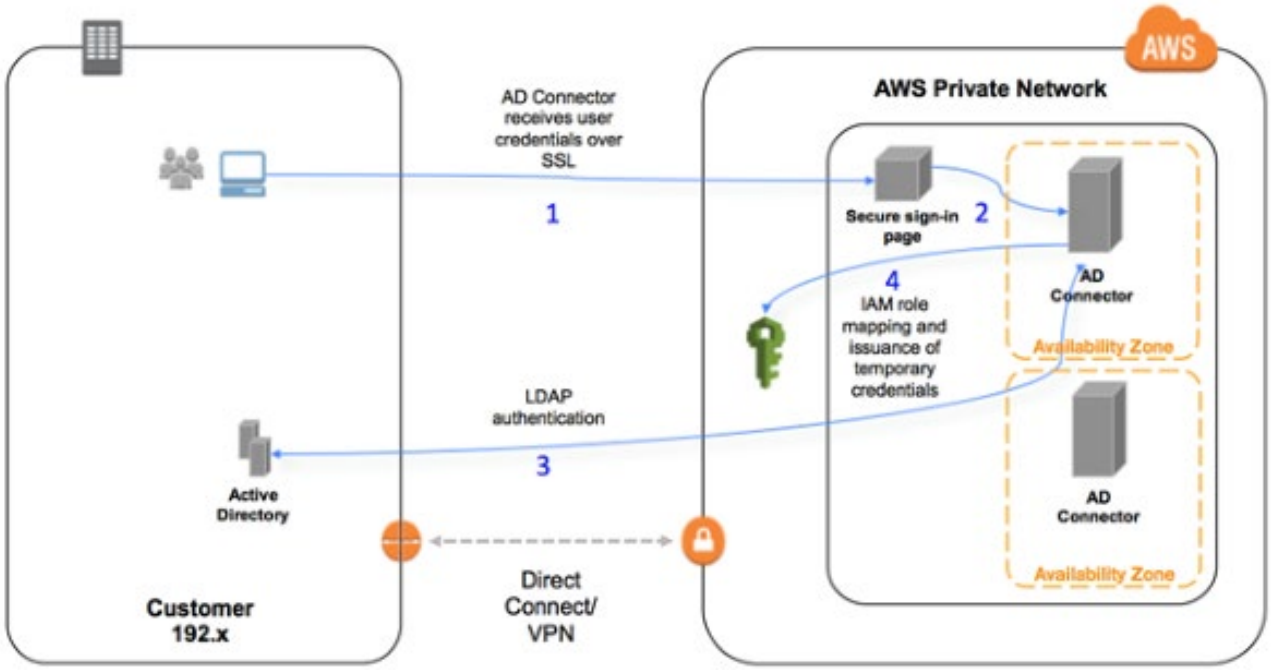
Encrypt data in transit and at rest: Data is not just vulnerable when resting in the cloud, but also while in transit. Encrypting the data can ensure it cannot be used by criminal minds even if they steal it.

Active Directory (AD)

Proactively assesses who has access to what: permissions, privileged groups, sensitive groups, Group Policy Objects and data.

In Hybrid setups, default configurations of AD connectors and AD connector account permissions (varies between CSP) can give attackers roundabout access to AD.

Authentication flow and network path



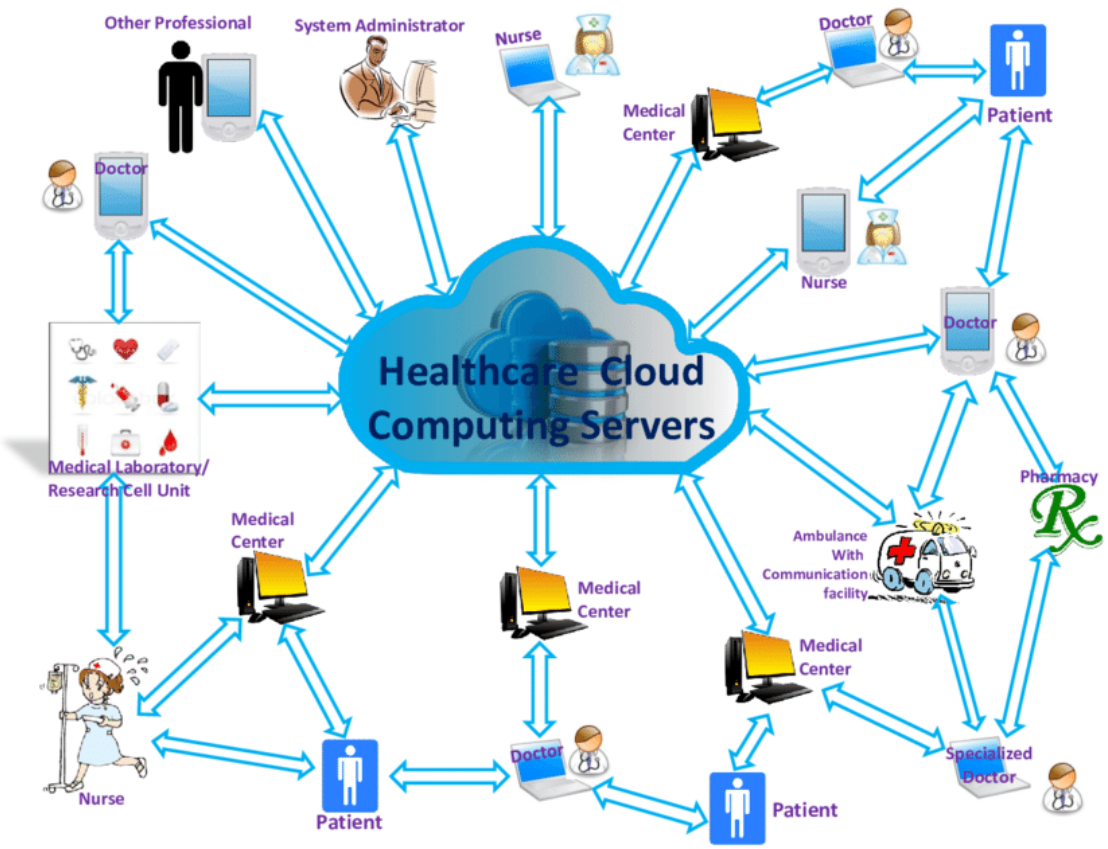
Resources for AD Connectors:

https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account

Summary

- As the Healthcare Sector takes steps to prevent the further spread of COVID-19 by providing remote options, the demand for cloud solutions has increased at a rapid rate.
- Special interest in the Healthcare Sector has heightened within threat actor groups due to the current state of affairs.
- Compromising certain on-premise tools, devices, or accounts could consequently give unauthorized access to cloud services.
- With bad cyber hygiene, the possibility of a cloud database breach, unauthorized access/disclosure, or ransomware attack increases significantly.



Reference Materials

References

Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
https://us-cert.cisa.gov/ncas/alerts/aa21-008a

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Top 7 security mistakes when migrating to cloud-based apps
https://www.csoonline.com/article/3602609/top-7-security-mistakes-when-migrating-to-cloud-based-apps.html?upd=1611328290397

Microsoft: SolarWinds hackers' goal was the victims' cloud data
https://www.bleepingcomputer.com/news/security/microsoft-solarwinds-hackers-goal-was-the-victims-cloud-data/

The Top Worry In Cloud Security for 2021
https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html

Top Health IT Security Challenges? Medical Devices, Cloud Security
https://healthitsecurity.com/news/top-health-it-security-challenges-medical-devices-cloud-security

CISA: Poor Cyber Hygiene Exploited to Compromise Cloud Security Services
https://healthitsecurity.com/news/cisa-poor-cyber-hygiene-exploited-to-compromise-cloud-security-services

Multi-Factor Authentication Blocks 99.9% of Automated Cyberattacks
https://healthitsecurity.com/news/multi-factor-authentication-blocks-99.9-of-automated-cyberattacks

One simple action you can take to prevent 99.9 percent of attacks on your accounts
https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

References

CLOUD THREAT REPORT 2H 2020
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit-42-cloud-threat-report-2h-2020.pdf

Top cloud providers in 2021: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players
https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

Disadvantages of Cloud Computing
https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

Misconfiguration on the Cloud is as Common as it is Costly
https://www.infosecurity-magazine.com/opinions/misconfiguration-cloud/

4 Common Cloud Misconfigurations & What To Do About Them
https://www.extrahop.com/company/blog/2019/4-common-cloud-misconfigurations-and-what-to-do-about-them/

Understanding policies
https://cloud.google.com/iam/docs/policies#policy-best-practices

Concepts related to access management
https://cloud.google.com/iam/docs/overview

What Companies Using Cloud Services Need To Know About Their Risk Responsibilities
https://www.bitsight.com/blog/what-companies-using-cloud-computing-providers-need-to-know-about-their-risk-responsibilities

Behind The Data Breach: Understanding Cloud Security And Misconfigurations
https://www.cshub.com/cloud/articles/behind-the-data-breach-understanding-cloud-security-and-misconfigurations

References

99 percent of all misconfigurations in the public cloud go unreported
https://www.zdnet.com/article/99-percent-of-all-misconfiguration-in-the-public-cloud-go-unreported/

Cloud Service Providers
https://rmas.fad.harvard.edu/cloud-service-providers

25 Must-Know Cloud Computing Statistics in 2020
https://hostingtribunal.com/blog/cloud-computing-statistics/#gref

10 Future Cloud Computing Trends To Watch In 2021
https://www.crn.com/news/cloud/10-future-cloud-computing-trends-to-watch-in-2021?itc=refresh

Can you meet customer demand for cloud-based computing?
https://www.pwc.com/us/en/industries/tmt/library/covid19-cloud-infrastructure.html

The biggest healthcare data breaches reported in 2020
https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-reported-2020

Enterprise Public Cloud Adoption Stifled by Privacy, Security Concerns
https://healthitsecurity.com/news/enterprise-public-cloud-adoption-stifled-by-privacy-security-concerns

What's at Stake with Healthcare IoT and Cloud? Unnecessary Risk
https://healthitsecurity.com/news/whats-at-stake-with-healthcare-iot-and-cloud-unnecessary-risk

Speeding Pharma's Time to Market with Managed Cloud Services
https://healthitsecurity.com/news/speeding-pharmas-time-to-market-with-managed-cloud-services

Cloud Mitigation for Ransomware, as COVID-19 Spurs Cyberattacks
https://healthitsecurity.com/news/cloud-mitigation-for-ransomware-as-covid-19-spurs-cyberattacks

References

Remote Attacks on Cloud Service Targets Rose 630% Amid COVID-19
https://healthitsecurity.com/news/remote-attacks-on-cloud-service-targets-rose-630-amid-covid-19

350M Voicemails, Health Details Exposed by Misconfigured Database
https://healthitsecurity.com/news/350m-voicemails-health-details-exposed-by-misconfigured-database

Medical Software Database Exposes Personal Data of 3.1M Patients
https://healthitsecurity.com/news/medical-software-database-exposes-personal-data-of-3.1m-patients

Remote Work Increasing Exponentially Due to COVID-19
https://www.netskope.com/blog/remote-work-increasing-exponentially-due-to-covid-19

Data Breaches Caused by Misconfigured Servers Within a Healthcare Environment
https://www.atlantic.net/hipaa-data-centers/data-breaches-caused-by-misconfigured-servers-within-a-healthcare-environment/

Study finds misconfigured cloud storage services in 93% of cloud deployments analyzed
https://www.techrepublic.com/article/study-finds-misconfigured-cloud-storage-services-in-93-of-cloud-deployments-analyzed/

GE Healthcare Launches Health Cloud on AWS, Improving Collaboration and Patient Outcomes
https://aws.amazon.com/solutions/case-studies/ge-healthcare/

Azure AD Connect: Configure AD DS Connector Account Permissions
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account

How to Connect Your On-Premises Active Directory to AWS Using AD Connector
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

References

What the NIST Framework Misses About Cloud Security
https://www.infosecurity-magazine.com/opinions/nist-framework-misses-cloud/

Guide to Computer Security Log Management
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Applying NIST Cybersecurity Framework to Cloud
https://www.cloudoptics.io/applying-nist-cybersecurity-framework-to-cloud/

Chimera
https://attack.mitre.org/groups/G0114/

Chimera Group Now Targeting Cloud Services
https://cyware.com/news/chimera-group-now-targeting-cloud-services-4db01161

CLOUD BACKUPS FOR RANSOMWARE ATTACK PROTECTION AND RECOVERY
https://storagepipe.com/blog/cloud-backups-ransomware-attack-protection-recovery/

Reaching for the cloud: Can ransomware infect cloud storage?
https://parablu.com/reaching-for-the-cloud-can-ransomware-infect-cloud-storage/

CrowdStrike Fends Off Attack Attempted By SolarWinds Hackers
https://www.crn.com/news/security/crowdstrike-fends-off-attack-attempted-by-solarwinds-hackers?itc=refresh

Security management in Azure
https://docs.microsoft.com/en-us/azure/security/fundamentals/management

Upcoming Briefs

- Malicious Use of Email Marketing Services
- A Retrospective Look at Healthcare Cybersecurity in 2020

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm EST at **202-691-2110.**

Questions