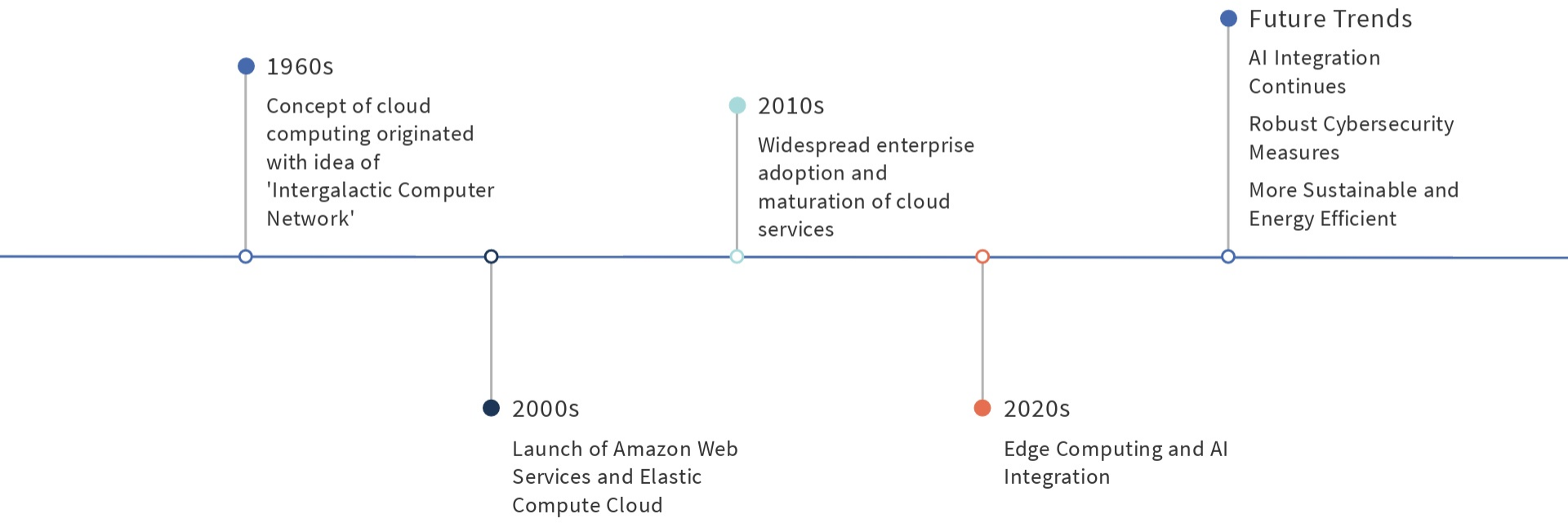

CLOUD COMPUTING
AND DATA SECURITY

HISTORY OF CLOUD COMPUTING



CLOUD COMPUTING MODELS

Public cloud

On-demand services available to the public

Private cloud

Dedicated cloud infrastructure for a single organization

Hybrid cloud

Combination of public and private cloud

Different cloud models provide options based on access, scale, and control

COMMON CLOUD PROVIDERS

AWS

Amazon Web Services provides a comprehensive set of cloud services including computing, storage, networking, database, and analytics.

Azure

Microsoft Azure provides IaaS, PaaS, SaaS, and hybrid cloud services for deploying and managing applications and services.

Google Cloud

Google Cloud Platform offers computing, storage, networking, big data, machine learning, and application services.

There are many major cloud providers to choose from like AWS, Azure, and Google Cloud when building cloud-based solutions.

BENEFITS OF CLOUD COMPUTING FOR BUSINESS

Reduced costs

Cloud computing reduces infrastructure and IT costs by eliminating the need for expensive hardware purchases.

Improved mobility

Cloud computing enables employees to access data and applications from anywhere with an internet connection.

Enhanced collaboration

Cloud-based apps like Google Workspace facilitate real-time collaboration and communication across teams and departments.

Better security

Leading cloud providers offer robust security tools and practices to protect sensitive financial data.

In summary, migrating accounting and finance systems to the cloud provides significant benefits including cost savings, flexibility, collaboration, and security.

Cloud Computing

DATA SECURITY CONCERNS

COMMON THREATS AND VULNERABILITIES IN CLOUD SERVICES

Insecure APIs

APIs act as doorway to the cloud, so any vulnerabilities can be exploited

Weak identity, credential and access management

Improper validation and weak passwords make cloud resources vulnerable

Insecure interfaces and APIs

Flawed user and admin interfaces of cloud services can be exploited

Proper access controls, updated systems and secure coding practices can help mitigate these threats.

IMPACT OF DATA BREACHES

Data breaches impact customer trust

Customers lose confidence in a company's ability to protect their data after a breach.

Breaches damage brand reputation

Negative publicity from a breach harms a company's brand reputation and public image.

Breaches lead to financial losses

Breaches cost money for legal fees, fines, and lost business.

Data breaches have far-reaching impacts on businesses, from eroding customer trust to damaging brand reputation to incurring major financial losses.

COMPLIANCE ISSUES

Compliance issues

Focusing on industry standards relevant to CPAs, like SOC 2, FTA Safeguards Rule

SOC 2 type 1 & 2 audits

SOC 2 audits focus on confidentiality, privacy, availability, security, and processing integrity

FTA Safeguards Rule

Covers data security program, access controls, encryption, employee training, intrusion detection, and more

Compliance standards like SOC 2 and FTA Safeguards provide assurance to clients that firms have proper controls in place.

Cloud Computing

CLOUD SECURITY BEST PRACTICES

SELECT A SECURE CLOUD DATA PROVIDER

Microsoft Azure

Offers robust security features like encryption, role-based access control, and compliance certifications.

Amazon Web Services

Provides a wide range of security tools and strong encryption for data at rest and in transit.

Google Cloud

Leverages encryption, access controls, and advanced threat detection to secure customer data.

IBM Cloud

Uses cryptographic technology and customizable access policies to protect sensitive data.

Alibaba Cloud

Employs anti-DDoS protection, vulnerability scanning, and compliance with regulations.

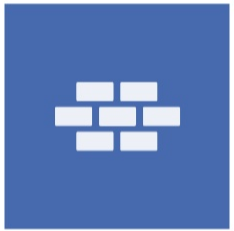
Oracle Cloud

Offers robust identity management, data encryption, and advanced security monitoring capabilities.

Implementing Strong Authentication and Access Controls for Cloud Data Hosting

- **Enable multi-factor authentication**
  Require users to authenticate with a second factor like a security key or one-time password in addition to username and password
- **Use role-based access controls**
  Restrict user access to only necessary data based on their job role and responsibilities
- **Encrypt data at rest and in transit**
  Use encryption to protect data stored on cloud servers and while moving between client and server

CLOUD DATA SECURITY



Conduct regular security audits

Schedule comprehensive audits of your cloud architecture, configurations, access controls, etc. to find security gaps.

Have an incident response plan

Document and regularly test response procedures for security incidents like data breaches, DDoS attacks, etc.

Review logs and alerts

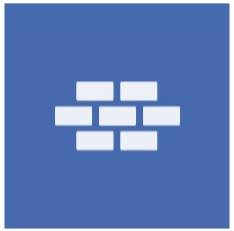
Continuously monitor logs and alerts from cloud providers to detect anomalies and potential threats.

Regular security audits and incident response planning are crucial for protecting your cloud data and architecture.

MOVING TO THE CLOUD DOES NOT MEAN YOU OFFLOADED YOUR CYBERSECURITY RESPONSIBILITIES

Install endpoint protection

Install anti-virus, anti-spyware, and other endpoint protection tools to secure devices



Enable firewalls

Configure host-based and network firewalls to filter traffic and connections

Patch and update

Regularly install latest security patches and updates on all endpoints

With proper endpoint hardening and ongoing maintenance, organizations can reduce their endpoint attack surface and improve their overall security posture.

MALWARE INFECTION VECTORS

Phishing emails

Hackers can send phishing emails with malicious attachments or links to install malware.

Drive-by downloads

Visiting compromised websites can trigger drive-by downloads to install malware without any action from the user.

Malicious attachments

Malware can be distributed through malicious email attachments.

Always be cautious about unsolicited emails, links, file downloads and ads to prevent malware installation.

ZERO TRUST CYBERSECURITY MODEL

Never Trust. Always Verify.

Implementing a Zero Trust model with strong identity and device verification enhances security for cloud access from managed and unmanaged devices.

MIKE FARLOW

comtechnc.com

mike@comtechnc.com

RAFE MARTIN

comtechnc.com

336-338-7328

rafe@comtechnc.com

Book a Meeting at www.rafe365.com