

North America Community Meeting 2023





North America Community Meeting 2023



Cloudy With a Chance of Breaches

Where CHD May Be Hiding and at Risk



Presented by:
Anton Abaya, CISM, CISA, PCI QSA
Professional Services Manager - Governance, Risk, and Compliance

Agenda

- **Introduction**
- **Rapid Cloud Growth & Security Challenges**
- **Case Studies: Real-World Cloud Cardholder Data Environments**
- **Key Takeaways**

About Me

Anton Abaya

- **WILDLY PASSIONATE** in All Cybersecurity and PCI DSS
- Professional Services Manager of GRC Team, vCISO, and Cloud Security
- Principal Consultant
 - PCI QSA: 15+ years
 - Penetration Tester / Red Teamer / Social Engineer
 - Developed Our **Cloud Security Assessment Methodology**



About Converge Technology Solutions



60+

Locations

Serving North America & Europe



>4,000

Clients



700+

Vendor
Partnerships

30+ Years of
Cybersecurity Experience

NOW



200+

Cybersecurity
Resources



4,000+

Professional Service
Engagements



>10,900

Threat Hunts



70,000

Security Alerts
Investigated

2023
YTD



89

Cybersecurity
NPS Score

Cloud Growth & Security Concerns



Cloud Security Market Size to Reach USD 106.02 Billion [2022-2029] | 18.1% CAGR

According to Fortune Business Insights, the global Cloud Security Market Size is projected to hit USD 106.02 Billion in 2029, at CAGR of 18.1 % during forecast period [2022-2026]; Rising Adoption of Cloud Computing Solutions & Applications to Augment Market Growth

Source: Global News Wire

CLOUD SECURITY CONCERNS

Growing adoption of cloud computing has brought forth a lot of security concerns for the IT professionals



Source: Prisma

Breaches in the Cloud

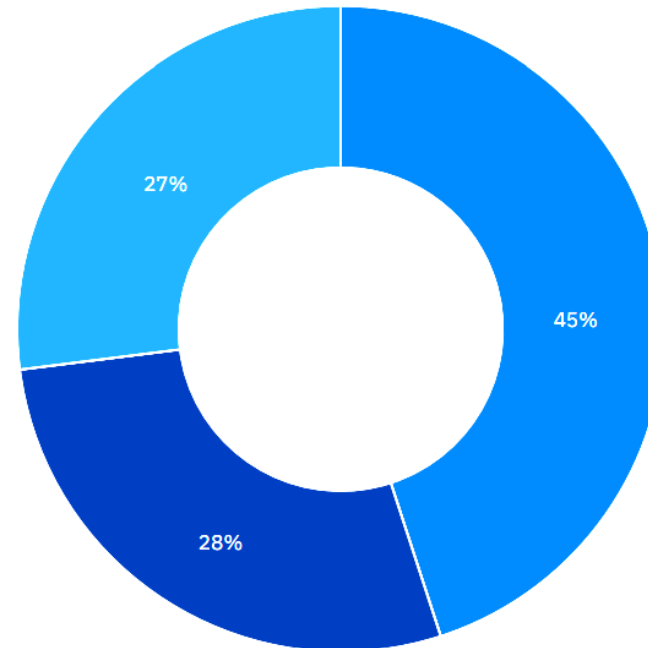
45%

Share of breaches that occurred in the cloud

43%

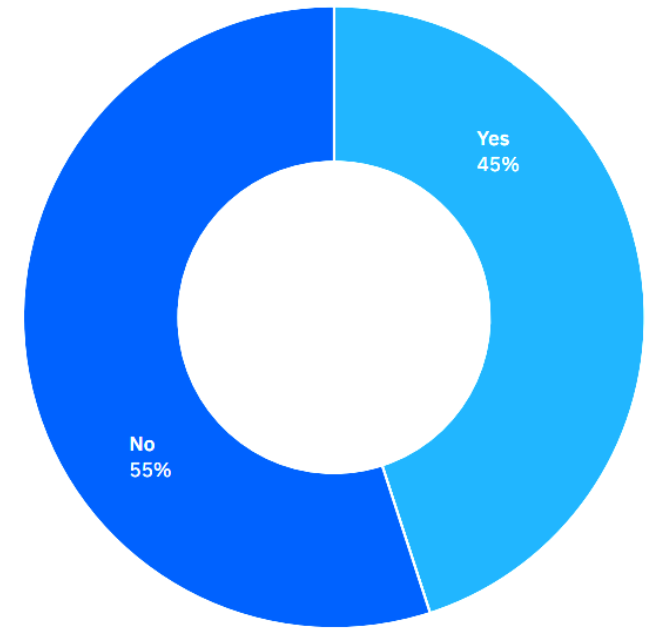
Share of organizations that were in early stages or had not started applying security practices to safeguard their cloud environments

What best describes your IT operating model?



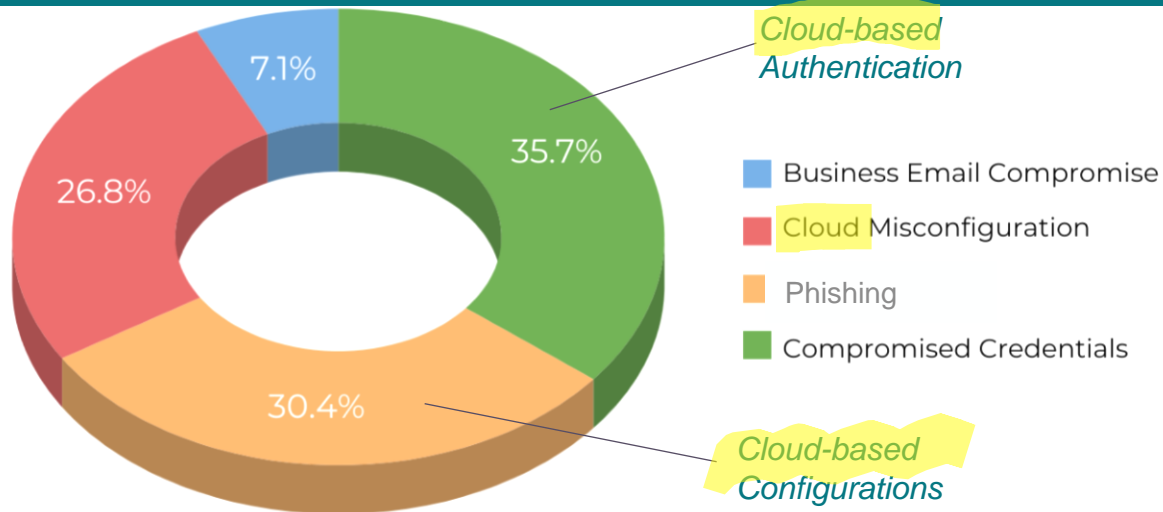
■ Hybrid cloud ■ Completely on-premises ■ Completely cloud

Did the data breach occur in the cloud?



Breaches in the Cloud

Initial Attack Vectors for a Data Breach



According to Ponemon 2021

ustadatastorage.com | 706. 793. 0186



More Data Points on Data Breaches

45% of Breaches Were Cloud-Based

Nearly half of all breaches occurred in the cloud – and those that occurred in the public cloud were costlier. While hybrid cloud environment breaches cost an average of \$3.8M, the average cost in private clouds was \$4.24M and in public clouds it was \$5.02M!

The Crazy Cost of a Data Breach

A data breach is an expensive matter. Per IBM, the average costs of breaches by type are:

- \$4.35M - The average total cost of a data breach
- \$4.82M - The average cost of a critical infrastructure data breach. Critical infrastructure includes financial services, industrial technology, energy, transportation, communication, healthcare, education and public sector

transportation, communication, healthcare, education and public sector
infrastructure includes financial services, industrial technology, energy,

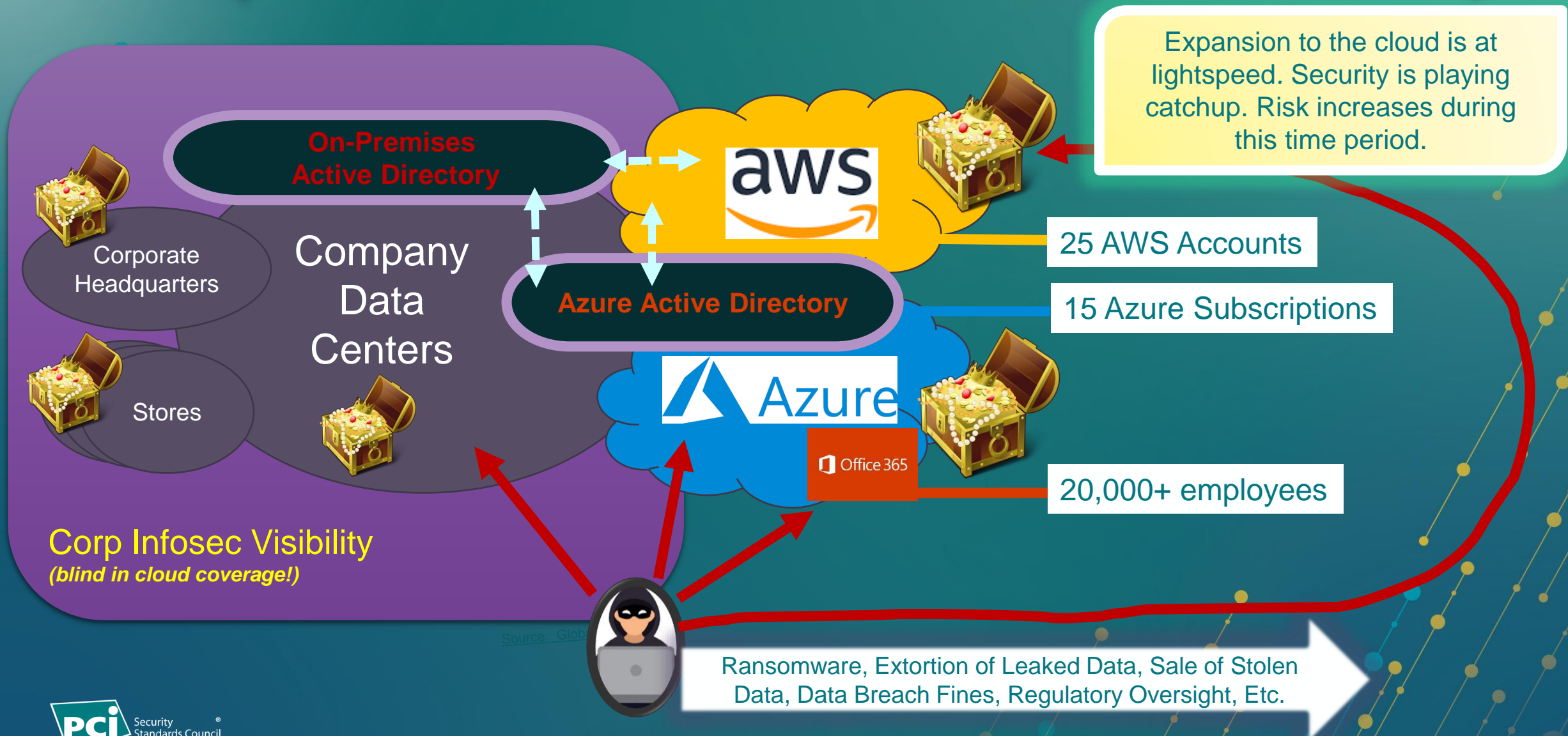
- \$4.82M - The average cost of a critical infrastructure data breach. Critical infrastructure includes financial services, industrial technology, energy, transportation, communication, healthcare, education and public sector
- \$4.35M - The average total cost of a data breach



Source: AugustaDataStorage



Example: Real-World Cloud Attack Landscape



Example: Real-World Cloud Attack Landscape

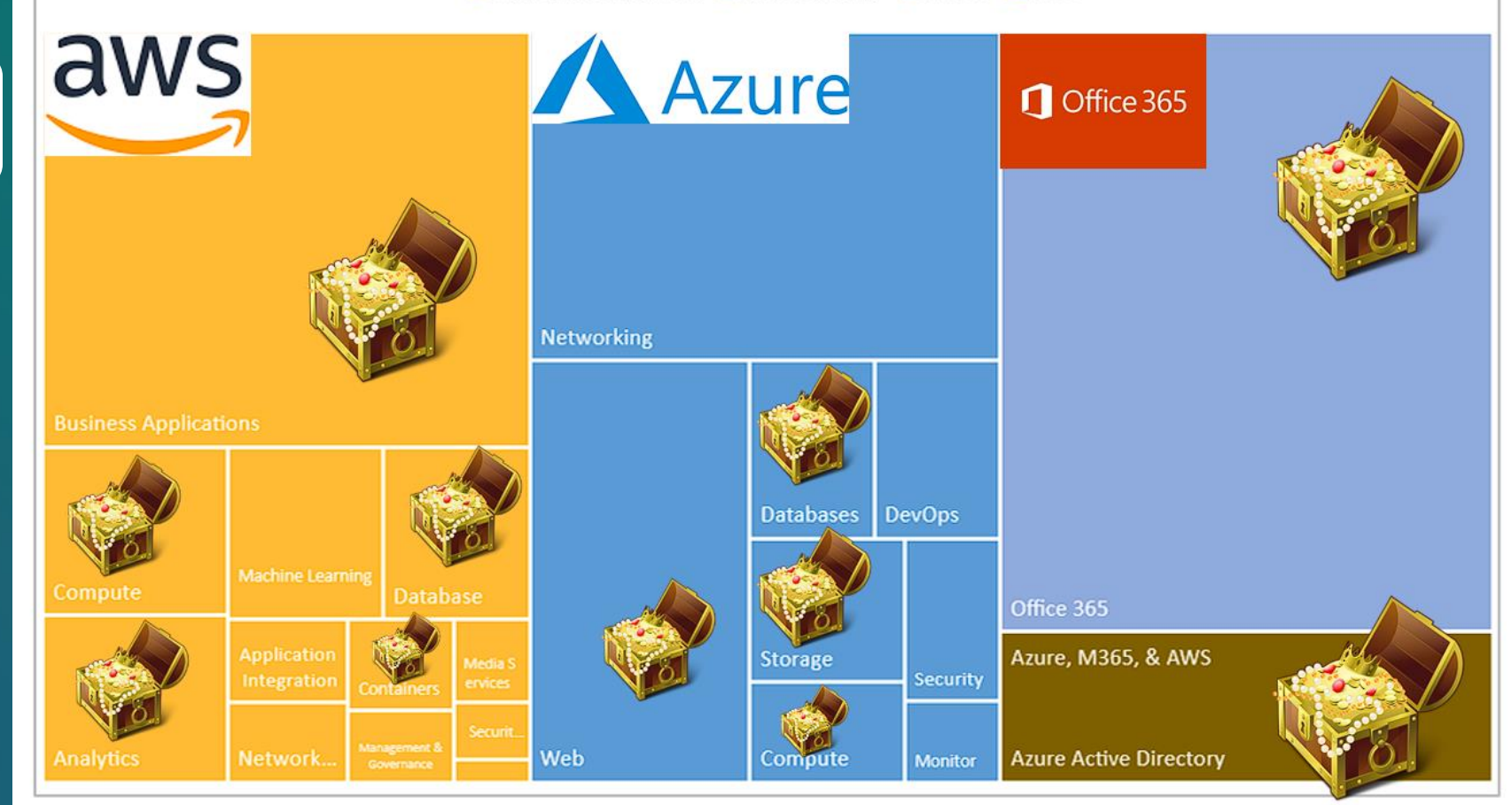


There are **unique attack vectors** for EACH of these.

Security issues
(cloud control plane
misconfigurations)
found affecting all
these areas.

Azure, Microsoft 365, and AWS Cloud Usage and Deployment

■ Azure, M365, & AWS ■ Microsoft 365 ■ Azure ■ AWS



Real-World Examples

PUBLIC internet exposure of cloud storage account. **(DATA BREACH)**

Using Azure Storage Explorer, the Blob container was confirmed to be accessible anonymously on the internet. Within this Blob were numerous Virtual Hard Disk (.vhd) files that are presumed to contain **sensitive information**.



The screenshot shows the Microsoft Azure Storage Explorer interface. The account is identified as 'Converge Technology Solutions' with email 'AAbaya@accudatasystems.com'. The current view is a blob container named 'snapshot'. A table lists several files, all of which are Virtual Hard Disk (.vhd) files. A yellow callout box highlights the text 'Virtual Hard Disk files open on the Internet!'. A red box highlights the file list table.

Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Type	Size	Status	Remaining
...sDisk_27122022.vhd			12/27/2022 7:45 AM	Page Blob		20.01 GiB	Active	
...sDisk_27122022.vhd			12/27/2022 7:44 AM	Page Blob		20.01 GiB	Active	
...Disk_27122022.vhd			12/27/2022 7:21 AM	Page Blob		20.01 GiB	Active	
...Disk_27122022.vhd			12/27/2022 7:21 AM	Page Blob		20.01 GiB	Active	
...sDisk_27122022.vhd			12/27/2022 6:21 AM	Page Blob	application/octet-stream	12.00 GiB	Active	
...sDisk_27122022.vhd			12/27/2022 6:18 AM	Page Blob	application/octet-stream	12.00 GiB	Active	
...sDisk_27122022.vhd			12/27/2022 6:15 AM	Page Blob	application/octet-stream	12.00 GiB	Active	
...ataDisk_27122022.vhd			12/27/2022 6:14 AM	Page Blob	application/octet-stream	64.00 GiB	Active	

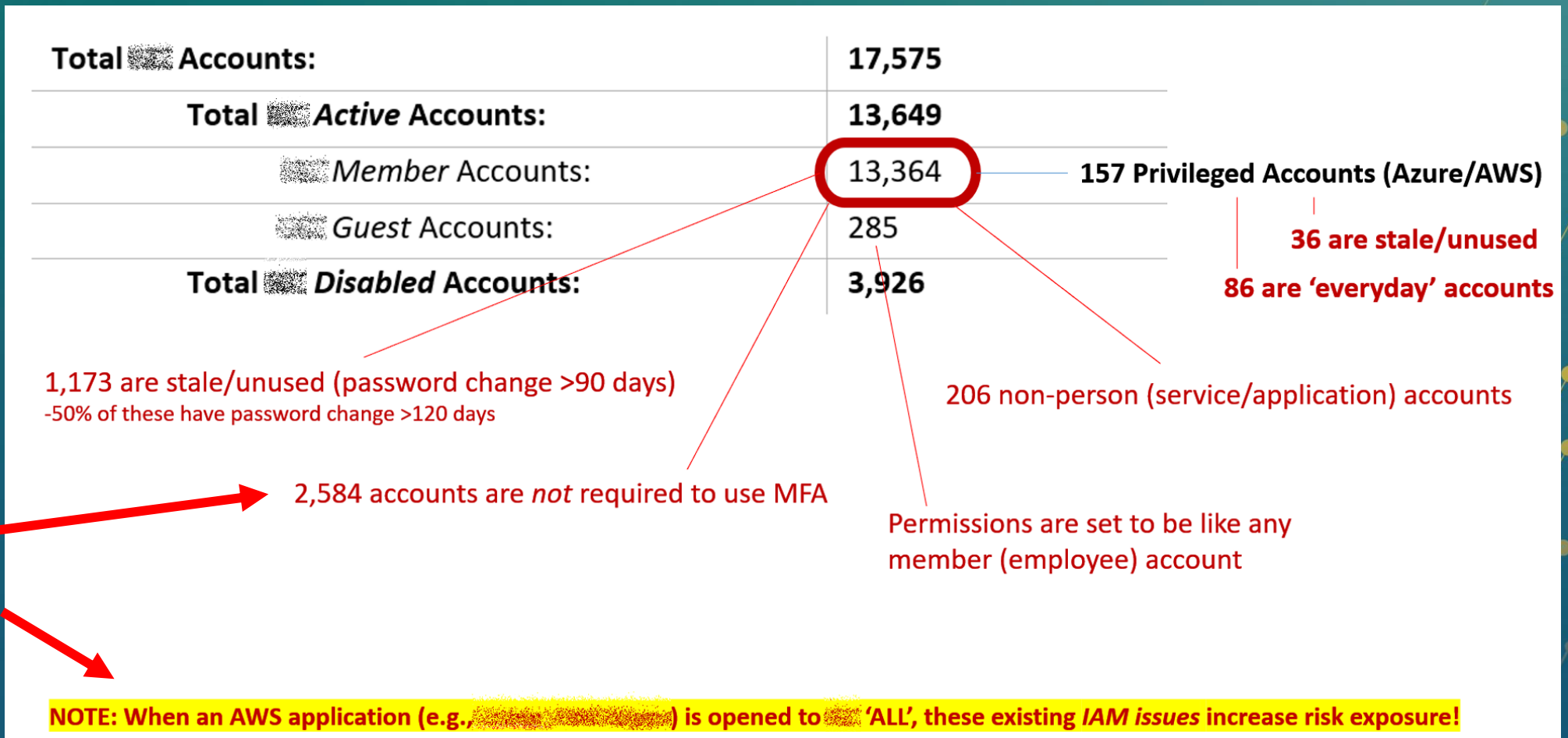
Real-World Examples

Identity access management (IAM) issues in the cloud.



(DATA BREACH)

Password: 'Company123'



Real-World Examples

Shadow cardholder data environment discovered.



The screenshot shows the Microsoft Compliance Manager 'Data classification' interface. The browser address bar displays 'compliance.microsoft.com/dataclassification?viewid=contentexplorer'. The left sidebar contains navigation options: Home, Compliance Manager, Data classification (selected), Data connectors, Alerts, Reports, Policies, and Trials. Below these are 'Solutions' including Catalog, App governance, Communication compliance, and Data loss prevention.

The main content area is titled 'Data classification' and includes tabs for 'Sensitive info types', 'EDM classifiers', 'Content explorer' (selected), and 'Activity explorer'. A search bar contains the text 'credit'. Below the search bar, a table lists 'Sensitive info types' with 'Credit Card Number' highlighted in a red box, showing a count of '28053'. To the right, an 'All locations' table lists various storage locations with their respective file counts, also highlighted in a red box:

Sensitive info types		All locations	
<input type="checkbox"/>	Credit Card Number 28053	<input type="checkbox"/>	Name 4 items
<input type="checkbox"/>		<input type="checkbox"/>	Exchange 16794
<input type="checkbox"/>		<input type="checkbox"/>	OneDrive 10372
<input type="checkbox"/>		<input type="checkbox"/>	SharePoint 881
<input type="checkbox"/>		<input type="checkbox"/>	Teams 6

Real-World Examples

Database as a Service exposed on the internet (to any other tenant).

A+ for effort!



F for execution?

A screenshot of the Azure portal interface for an SQL server's networking settings. The page is titled 'sql | Networking' and shows various configuration options. A green arrow points from the text 'A+ for effort!' to the 'Selected networks' radio button, which is highlighted with a green box. A red arrow points from the text 'F for execution?' to the 'Allow Azure services and resources to access this server' checkbox, which is checked and highlighted with a red box. The 'Public network access' section has 'Selected networks' selected. The 'Firewall rules' section contains a table with three rules. The 'Exceptions' section at the bottom has one checked exception: 'Allow Azure services and resources to access this server'.

Home > sql | Networking

SQL server

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following r

Public network access

Disable

Selected networks

Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By defa

Virtual networks

Allow virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network rule

Rule	Virtual network	Subnet	Address range	Endpoint status	Resource group	Subscription	State

Firewall rules

Allow certain public internet IP addresses to access your resource. [Learn more](#)

+ Add your client IPv4 address (96.127.127.94) + Add a firewall rule

Rule name	Start IPv4 address	End IPv4 address	
ClientIPAddress_2021-12-07_03:42:21	132.147.253	132.147.253	
ClientIPAddress_2021-12-07_08:42:55	96.127.127.94	96.127.127.94	
	132.147.253	132.147.253	

Exceptions

Allow Azure services and resources to access this server

Real-World Examples

Suspicious Global Administrator account



Home > [redacted] Inc. > Global administrator

Global administrator | Assignments

All roles

« + Add assignments × Remove assignments ↓ Download assignments ↻ Refresh ↗ Manage in PIM | ❤️ Got feedback?

✖ Diagnose and solve problems

Manage

- Assignments
- Description

Activity

- Bulk operation results

Troubleshooting + Support

- New support request

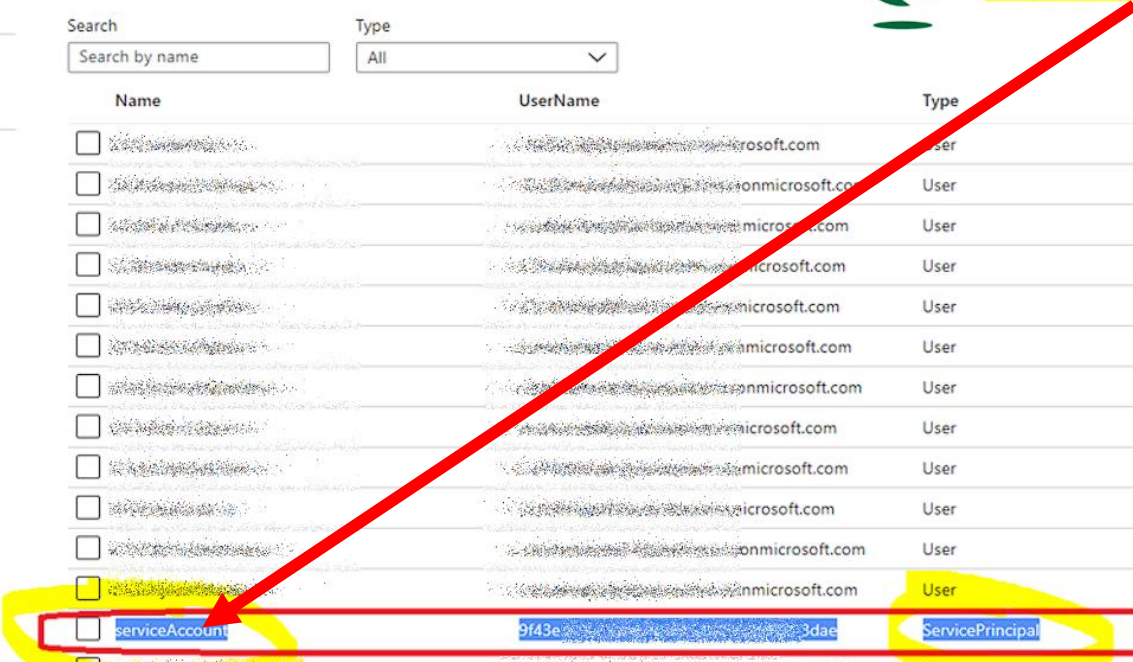
Warning: You currently exceed the recommended number of Global administrator assignments. →

Info: You can also assign built-in roles to groups now. [Learn More](#)

Search: Search by name | Type: All

Name	UserName	Type	Scope
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input checked="" type="checkbox"/>	[redacted]@onmicrosoft.com	User	Directory
<input checked="" type="checkbox"/>	serviceAccount	ServicePrincipal	Directory
<input type="checkbox"/>	[redacted]@microsoft.com	User	Directory
<input type="checkbox"/>	[redacted]@icrosoft.com	User	Directory

Highly suspicious service principal



Real-World Examples

Supply chain attack vector via MSP.



NOBELIUM targeting delegated administrative privileges to facilitate broader attacks

In the observed supply chain attacks, downstream customers of service providers and other organizations are also being targeted by NOBELIUM. In these provider/customer relationships, customers delegate administrative rights to the provider that enable the provider to manage the customer's tenants as if they were an administrator within the customer's organization. By stealing credentials and compromising accounts at the service provider level, NOBELIUM can take advantage of several potential vectors, including but not limited to delegated administrative privileges (DAP), and then leverage that access to extend downstream attacks through trusted channels like externally facing VPNs or unique provider-customer solutions that enable network access. To reduce the potential impact of this NOBELIUM activity, Microsoft encourages all of our partners and customers to

admin.microsoft.com/A

Home

Users

Groups

Billing

Settings

Domains

Search & intelligence

Org settings

Integrated apps

Directory sync errors

Partner relationships

Setup

Health

Partner relationships > [redacted] USA, Inc

[redacted] Inc

Your partner is a Reseller who can buy on your behalf. The roles assigned to them allow them to manage y

Partner information

[redacted] Inc

[redacted]

US

[redacted]

Relationship type

Reseller

Roles

Global Administrator

Helpdesk admin

Supply chain attack vector

Real-World Examples

Leaked AWS API keys on GitHub public repo (owned by developer).



```
github.com [redacted] src/main/resources/app[redacted]
[redacted] /src/main/resources/application.properties
[redacted] Merge branch 'master' of https://github.com/[redacted]
[redacted] [redacted]
[redacted]
21 spring.data.elasticsearch.engine.host=[redacted]
22 spring.data.elasticsearch.engine.port=443
23 spring.data.elasticsearch.engine.username=[redacted]
24 spring.data.elasticsearch.engine.password=[redacted]
```

Real-World Examples

Shadow cardholder data environment discovered.



Amazon S3 console interface showing a bucket named 'connect' containing a file named 'analysis/Voice/analysis.json'. The file is highlighted in blue. The console shows the file's properties, including its size (23.7 KB) and type (json).

The file content is displayed in a Notepad window, showing a JSON array of objects. The following objects are highlighted with red boxes:

- Object 1: `{ "BeginOffsetMillis": 518990, "Content": "Okay 6011 062-945-0113 25 three digits.", "EndOffsetMillis": 543620, "Id": "d559435-6868-40ea-9a5a-830a5e76-0404-486e-a03a-564c271b5cb3", "ParticipantId": "AGENT", "Sentiment": "NEUTRAL", "LoudnessScore": [80.4, 85.7, 83.55] }`
- Object 2: `{ "BeginOffsetMillis": 518990, "Content": "Oh it's all good. Yes ma'am.", "EndOffsetMillis": 543620, "Id": "d559435-6868-40ea-9a5a-830a5e76-0404-486e-a03a-564c271b5cb3", "ParticipantId": "CUSTOMER", "Sentiment": "POSITIVE", "LoudnessScore": [81.96, 80.55, 48.85] }`
- Object 3: `{ "BeginOffsetMillis": 518990, "Content": "Alright, I don't need that. But uh I'm gonna read this card back to you to make sure I have it", "EndOffsetMillis": 543620, "Id": "d559435-6868-40ea-9a5a-830a5e76-0404-486e-a03a-564c271b5cb3", "ParticipantId": "CUSTOMER", "Sentiment": "NEUTRAL", "LoudnessScore": [80.4, 85.7, 83.55] }`

A 'Find' dialog box is open, showing the search term '6011' and the 'Find Next' button. The search results in the Notepad window show the following matches:

- 6011 062-945-0113
- 6011 062-945-0113
- 6011 062-945-0113

The bucket properties section shows 'Bucket Versioning' is enabled. The management configurations section shows 'Replication status' is 'When a replication rule is applied to an object the replication status indicates the progress of the operation.'

Key Takeaways – Clearer Skies Ahead

Let's make cloud less cloudy.

1. Perform a Comprehensive **Cloud Security Assessment**
2. Perform a **Data Discovery, Privacy, Protection Assessment**
3. Enable **Cloud-Native** Security, Compliance, and Governance Tools and/or Use Third-Party Security Solutions (Multicloud)
4. Secure All **Authentication Directories and MFA** and **Vault All Secrets**
5. Enable Comprehensive Cloud Control-Plane Logging/Monitoring
6. Create **Guardrails or Blueprints** to Control Security Misconfigurations
7. Control/Limit **Developer** Access to the Cloud