



On the Highway To Cloud Security Hell:

Protecting User and Technical Accounts in the Public Clouds

Klaus Haller, AXA Schweiz
CSA & SIGS Special Event
Insights into Zero Trust
11.4.2024

Prettysleep1/Pixabay





Klaus Haller

Senior Security Architekt AXA CH

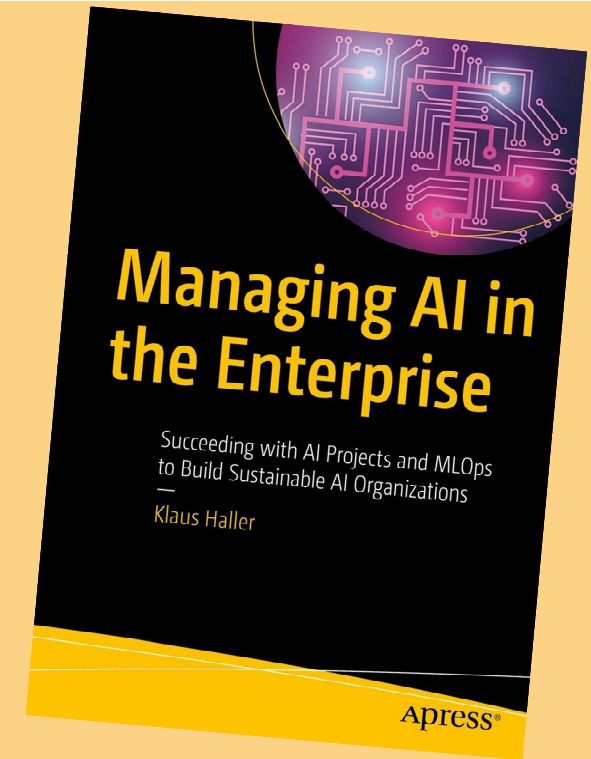
Cloud Security

Security & Analytics /AI

Security Reviews for Large Projects
and Programs

Encryption

Workplace





The World Changes

Hans/Pixabay



Mapping Cloud Access Variants

BaZuuH/Pixabay



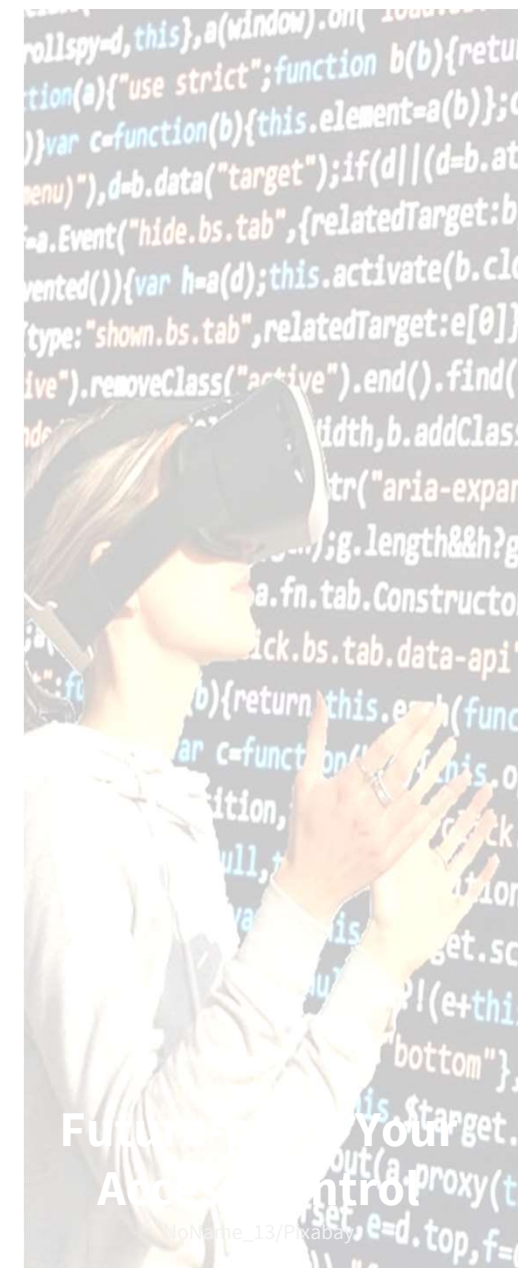
Understanding the new Risks

PublicDomainPictures/Pixabay



Future-proof Your Access Control

NoName_13/Pixabay





IT Automation, IT Automation, IT Automation

The Rise of Technical Accounts

Think about OS or database installations or cloud configurations ...

Accounts everywhere

Cloudification of our Workloads:

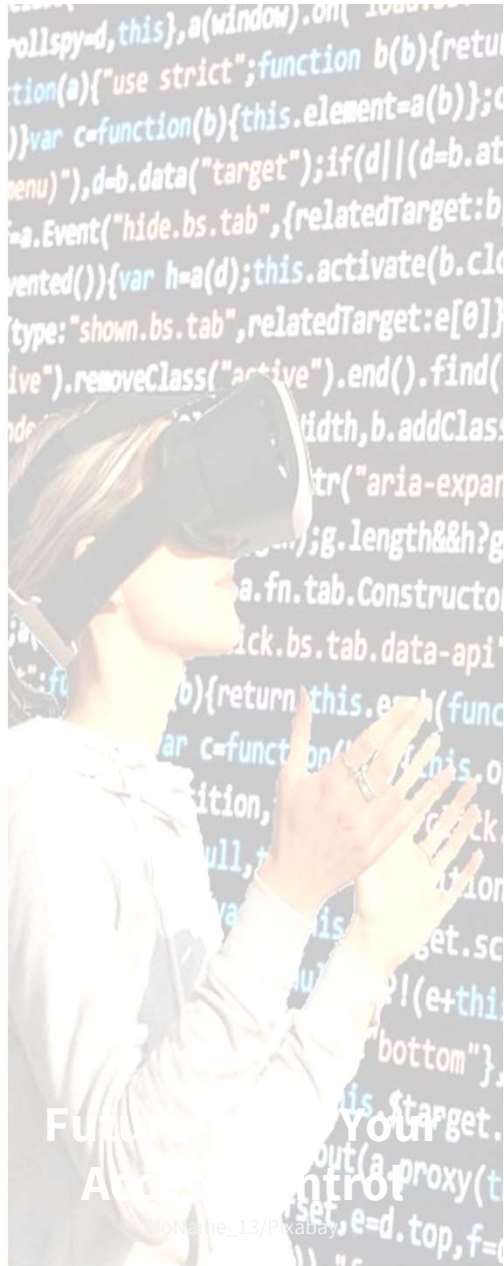
IaaS, PaaS (e.g., S3, Cloud Function), SaaS (M365)

Identity is the new perimeter

The World Changes

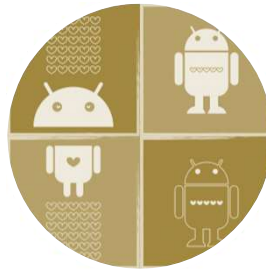
Hans/Pixabay







Software-as-a-Service



Platform-as-a-Service



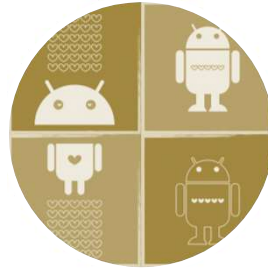
Infrastructure-as-a-Service



Software-as-a-Service

Application Layer

- Users including Super Users ?
- API Access (in/out) 💣



Platform-as-a-Service

Application Layer

- Users including Super Users (✓)
- API Access (in/out) 💣

Cloud

- Portal / GUI
- API Access



Infrastructure-as-a-Service

Application Layer

- Users including Super Users (✓)
- API Access (in/out) 💣

Cloud

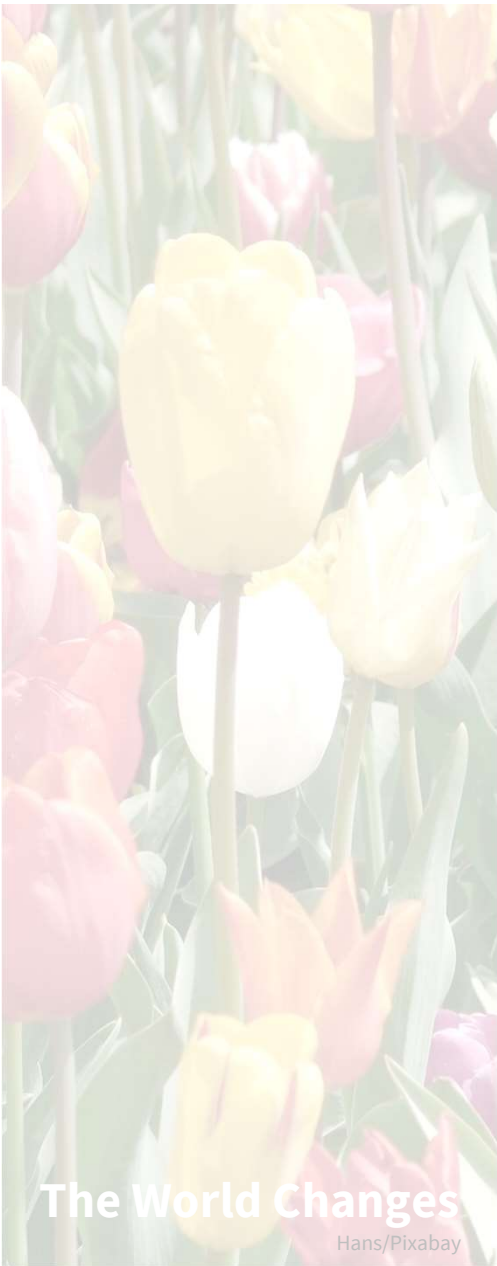
- Portal / GUI
- API Access



VMs / OS Layer

- Personal Users
- Admin Users
- Technical Users
- (Shared Users)





The World Changes

Hans/Pixabay



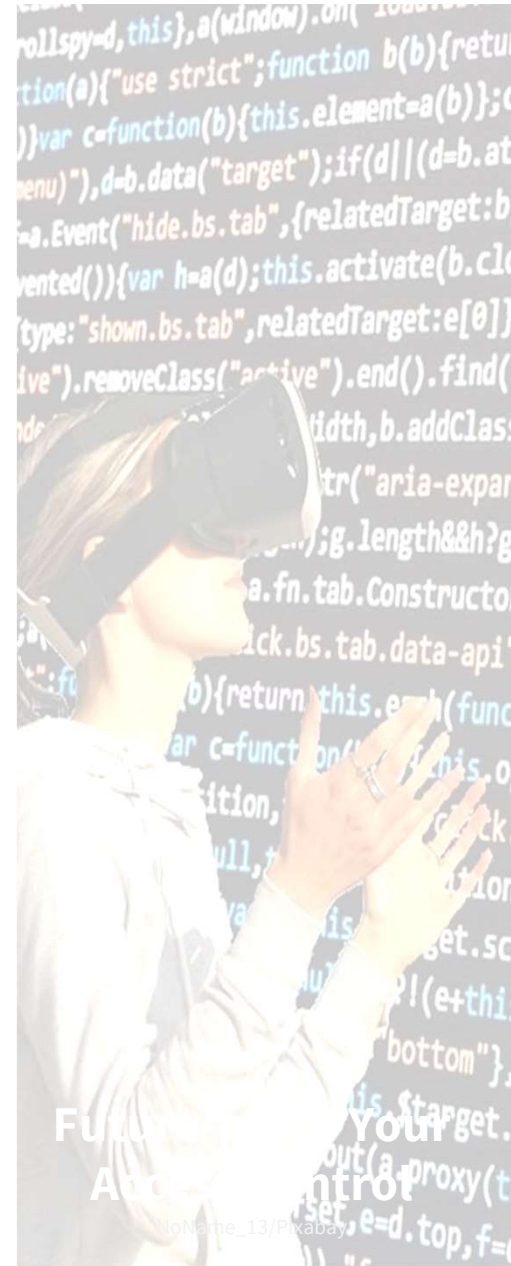
Mapping Cloud Access Variants

BaZuuH/Pixabay



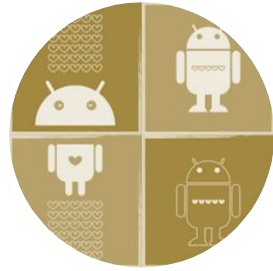
Understanding the new Risks

PublicDomainPictures/Pixabay

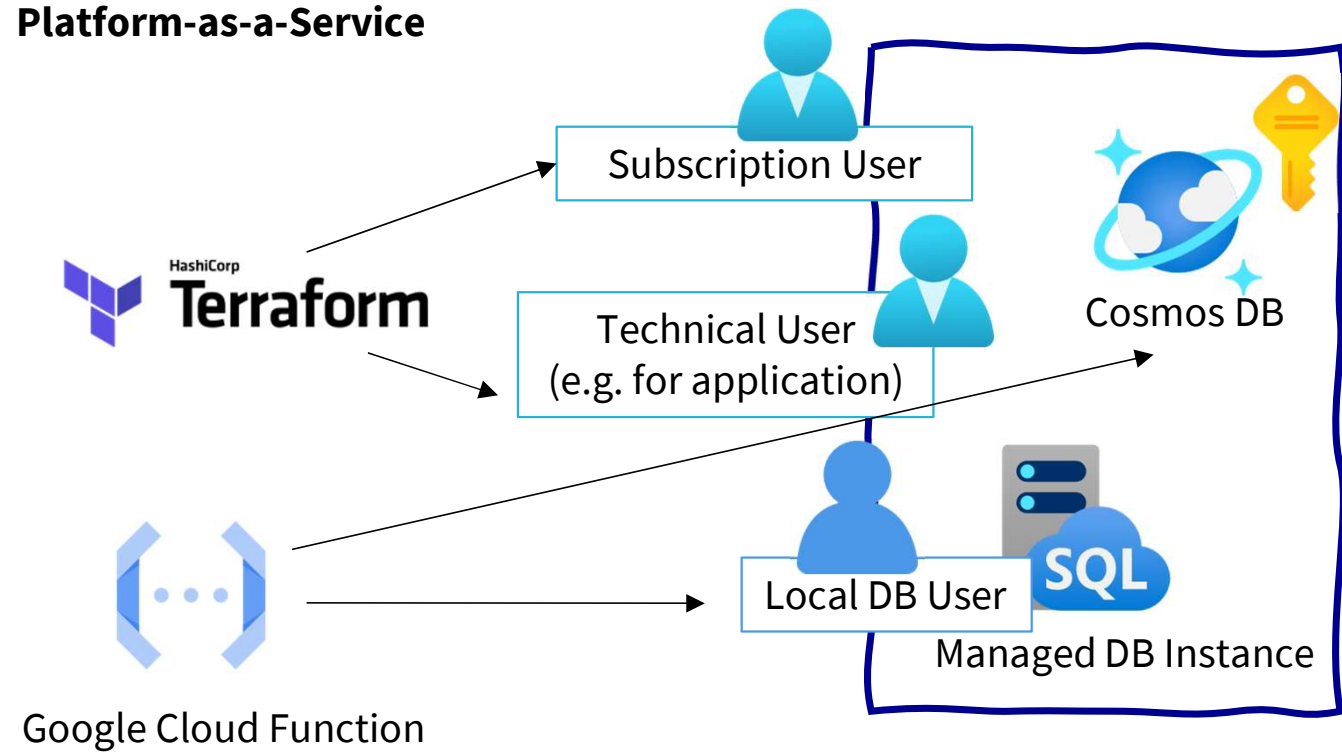


Future of Your Account Control

loName_13/Pixabay



Platform-as-a-Service



Microsoft Azure

All services > Azure Database for PostgreSQL flexible servers >

New Azure Database for PostgreSQL Flexible server

Microsoft

⚠ Server names, networking connectivity method and backup redundancy cannot be changed after server is created.

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the resource.

High availability

Zone redundant high availability deploys a standby replica in a different zone with automatic failover capability. You can also specify high availability options in 'Compute + storage'.

Enable high availability ⓘ ☐

Authentication

ℹ Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

Select the authentication methods you would like to support for accessing this PostgreSQL server. PostgreSQL authentication allows you to create and use a ROLES (usernames) and use a password to authenticate. Enabling Microsoft Entra authentication allows you to create ROLES based on your Microsoft Entra account and generate an authentication token with which to authenticate. [Learn more](#)

Authentication method

☒ PostgreSQL authentication only

☒ Microsoft Entra authentication only

☐ PostgreSQL and Microsoft Entra authentication

Admin username * ⓘ

Password * ⓘ

Microsoft Azure

All services > Azure Database for PostgreSQL flexible servers >

New Azure Database for PostgreSQL Flexible server

Microsoft

⚠ Server names, networking connectivity method and backup redundancy cannot be changed after server is created.

✖ Basics Networking Security Tags Review + create

Configure networking access and security for your server.

Network connectivity

You can connect to your server by specifying a public IP address specified below or from within a selected virtual network.

Connectivity method ⓘ

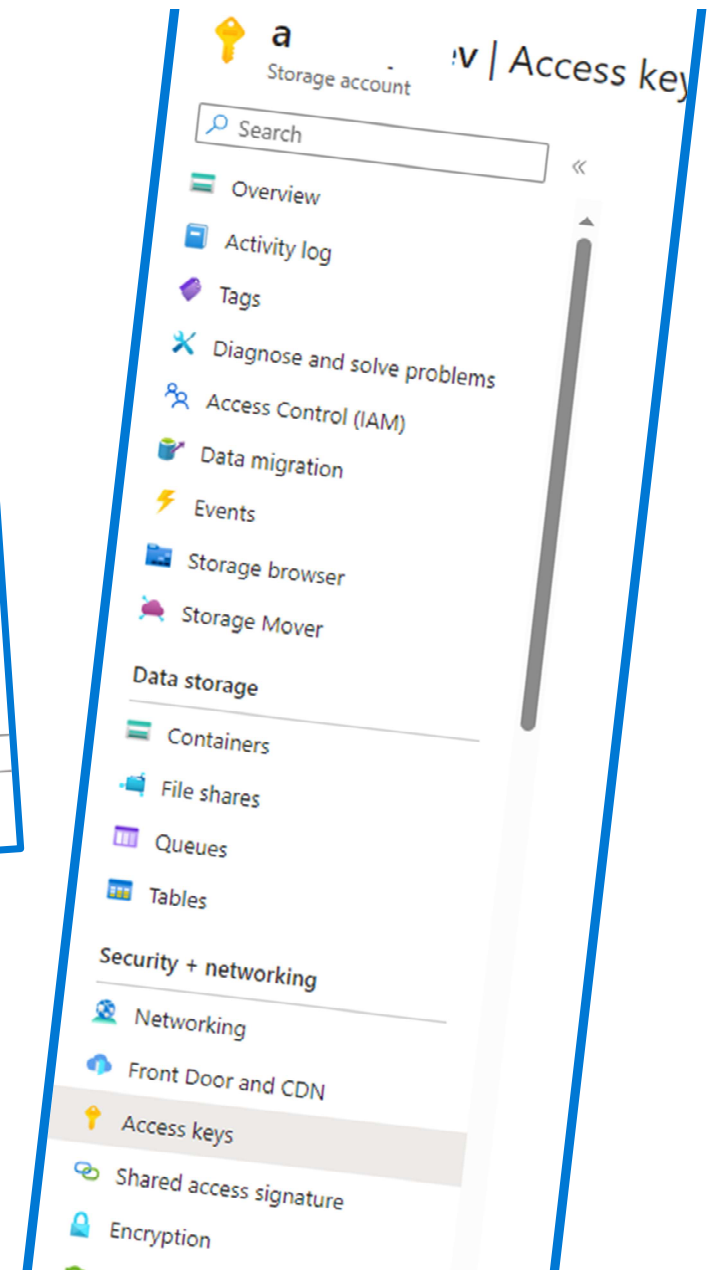
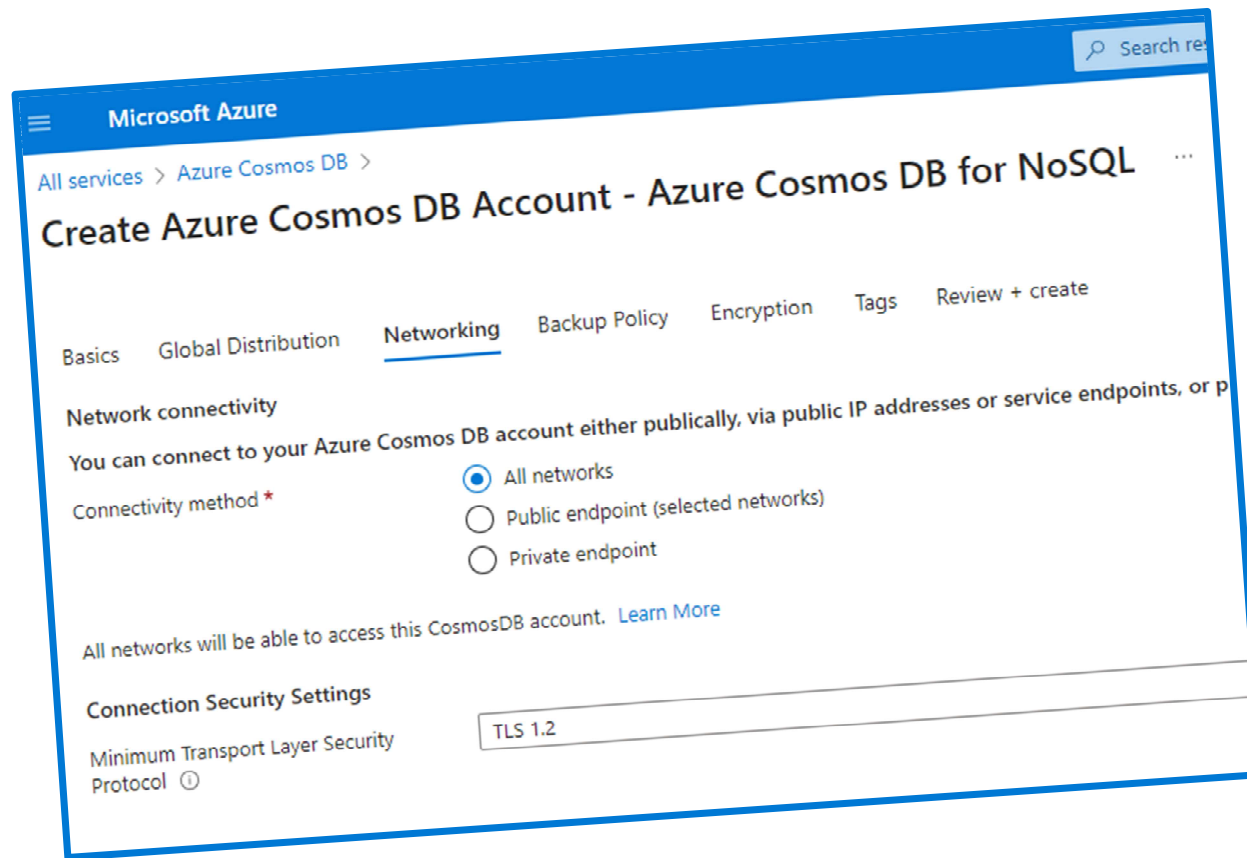
☒ Public access (allowed IP addresses)

☐ Private access (VNet Integration)

ℹ Connections from the IP addresses configured in the Firewall rules below will have access to this server. By default, no public IP addresses are allowed. [Learn more](#)

Firewall rules

Inbound connections from the IP addresses specified below will be allowed to port 5432 on this server.





Understanding the new Risks

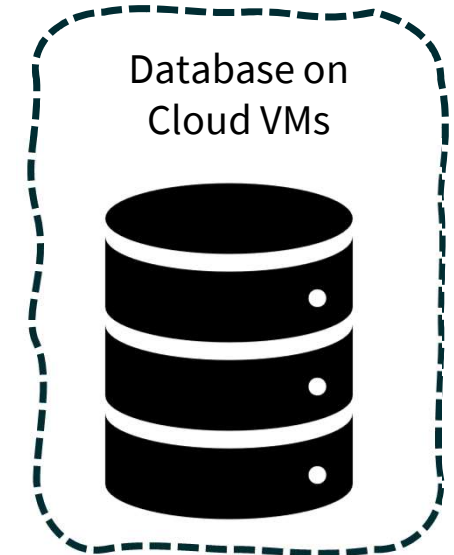
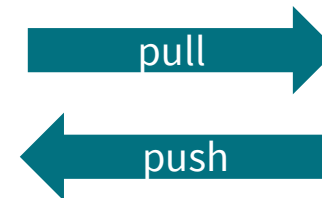
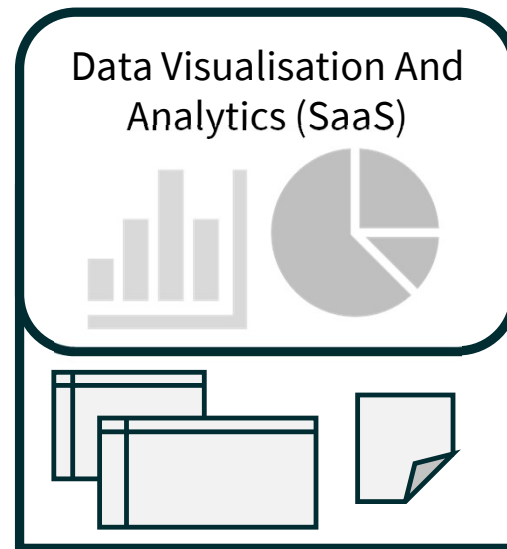
PublicDomainPictures/Pixabay



Software-as-a-Service



Infrastructure-as-a-Service

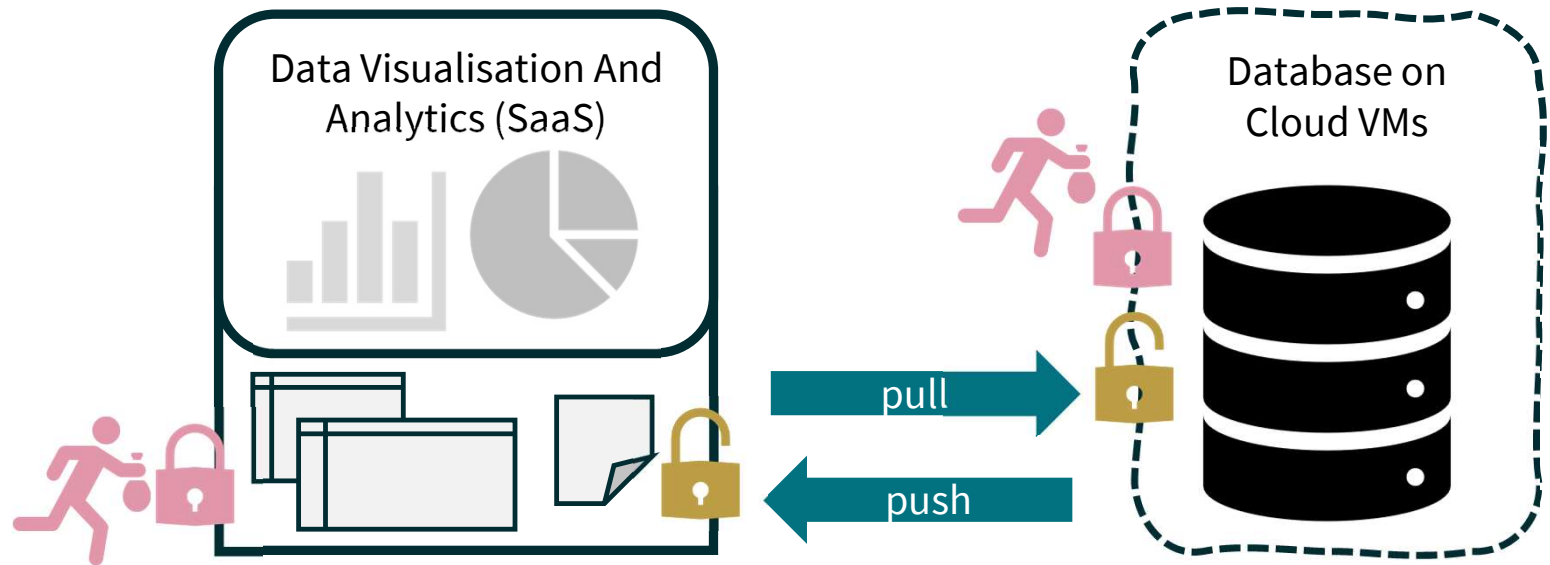




Software-as-a-Service



Infrastructure-as-a-Service





What is the crucial difference for
securing
technical accounts
compared to securing
personal accounts
?



What is the crucial difference for
securing
technical accounts
compared to securing
personal accounts
?

No MFA for Technical Accounts!
PaaS / SaaS have direct internet exposure.



DARK READING

Capital One Attacker Exploited Misconfigured AWS Databases

After bragging in underground forums, the woman who stole 100 million credit applications from Capital One has been found guilty.

[...]

Prosecutors noted that Thompson specifically used a scanner to look for AWS misconfigurations, in which database authentication required for access to databases of 30 entities, including cases planting cryptocurrency mi

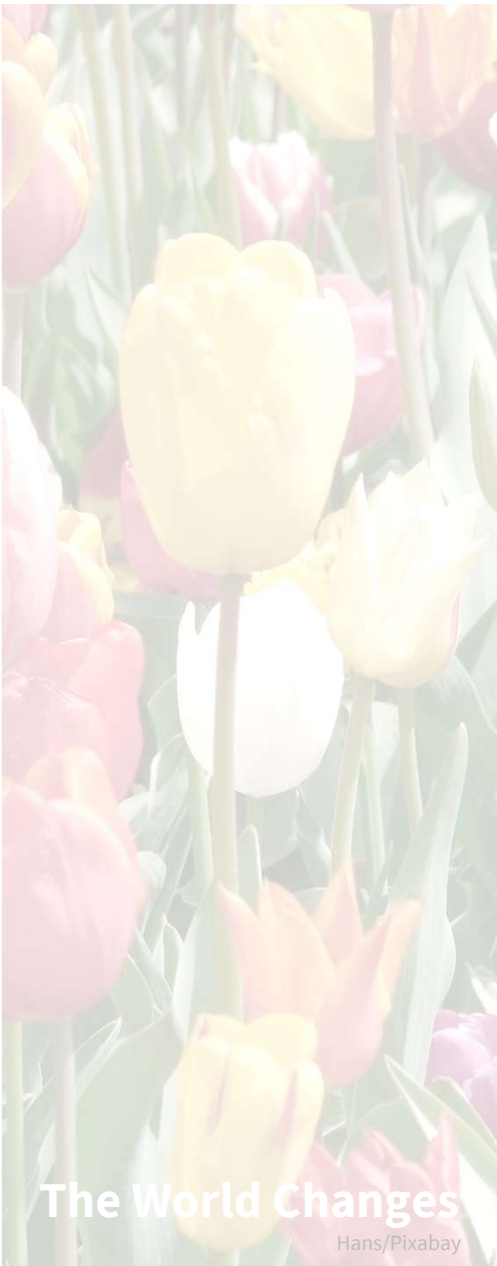


Zeljka Zorz, Editor-in-Chief, Help Net Security
July 12, 2023

Chinese hackers forged authentication tokens to breach government emails

Share    

Sophisticated hackers have accessed email accounts of organizations and government agencies via authentication tokens they forged by using an acquired Microsoft account (MSA) consumer signing key, the company has **revealed** on Tuesday.



The World Changes

Hans/Pixabay



Mapping Cloud Access Variants

BaZuuH/Pixabay



Understanding the new Risks

PublicDomainPictures/Pixabay



Future-proof Your Access Control

NoName_13/Pixabay

Securing Technical Accounts

Authentication / Identity

Access Key / User & Password ...

Certificate...

Managed Identity

Network

... VPN-Tunneling

... IP Restriction

... Private Link / VPC Service Control

Authentication / Identity

Access Key / User & Password ...
Certificate...



Managed Identity

Securing Technical Accounts

+



Network

... VPN-Tunneling
... IP Restriction
... Private Link / VPC Service Control



VPN Tunnel
VPN + Certificate
Certificate
Access Keys

Financial Loss →	<10k	<50k	<100k	<1Mio	>1Mio
Data Breach → ↓ Likelihood	<1000 customer records & no PII	<10k customer record, <100 PII records	<100k customer record, <10k PII records	<1mio customer record, <50k PII records	more
Less than every 50 years	Risk accepted	Risk accepted	Risk accepted	Document risk	Requires management approval
every 50 years	Risk accepted	Risk accepted	Document risk	Requires management approval	Requires management approval
every 10 years	Document risk	Document risk	Requires management approval	Requires management approval	Inacceptable
every 5 years	Document risk	Requires management approval	Inacceptable	Inacceptable	Inacceptable
More than 1 per year	Requires management approval	Inacceptable	Inacceptable	Inacceptable	Inacceptable



The World Changes

Hans/Pixabay



Mapping Cloud Access Variants

BaZuuH/Pixabay



Understanding the new Risks

PublicDomainPictures/Pixabay



Future-proof Your Access Control

NoName_13/Pixabay



LinkedIn