TIME TO STOP INSIDER THREAT

Cyber Security Insider Threats

Growing in Frequency and Impact

Increased 44% over the last two years

Involved in 30% of serious data breaches

Core Issue - who are you?

Existing MFA Methods are Vulnerable and regularly exploited

Privileged Access Control needs unequivocal Identity recognition

MFA Weakness

SMS Messages	Despite being susceptible to SIM Swap, Interception and Phishing attacks, this is still widely employed
Mobile MFA App	If the client is a mobile and the MFA App is on the same device, it is not Multi-factor Authentication
Biometric MFA	Latest AI assisted tools create realistic videos and voices after brief sampling of victims, making a passable cloned voice with 60 seconds of training audio and then have text-to-fake voice! Biometrics fail the crucial test –recovery from compromise- run out of irises very quickly
Passwordless Methods	If an Android mobile device is already compromised by malware, initializing Passwordless authentication could potentially expose the private key to cloning. This is a significant vulnerability because Mobile devices often serve as both the authentication factor and the client
FIDO2 type Devices	FIDO2 type devices have an open specification which can expose attack vectors. If the validation of the Attestation Key is bypassed by User choice, browser setting or an extension, a forged FIDO2 device allows an attacker to self-provision their MFA

Insider Threat Policy

User Activity Monitors

User Behaviour Analytics

Anomaly Detection with AI

Privileged Access Management

Disadvantages

False Positives

Higher Administration Costs

Negative “Big Brother” Climate

Less flexible Operational Modes

Privileged Access Vault becomes the Target

Deterrence – Best Solution

Removing plausible deniability of Access

Immediate Detection cloned secrets (Credentials, Private keys, Biometric)

Unique attribution of Access

The CASQUE Deterrent

Real-Time Clone Detection

CASQUE immediately detects and prevents clone attempts

Insider Threat Deterrence

Prevents malicious insider actions by eliminating plausible denial

Patent-Backed Innovation

Protected by US and EU patents with no third-party dependencies

Quantum Resilient

Immune to quantum computing, meets NIST’s highest assurance

Seamless Integration

Works with existing deployments with federated Identity provision

CASQUE Challenge- Response

Dynamically makes random for new key in Smartcard on each User Interaction

Nothing fixed secret for a Hacker to target or for a complicit Insider to disclose

NFC contactless on Mobiles

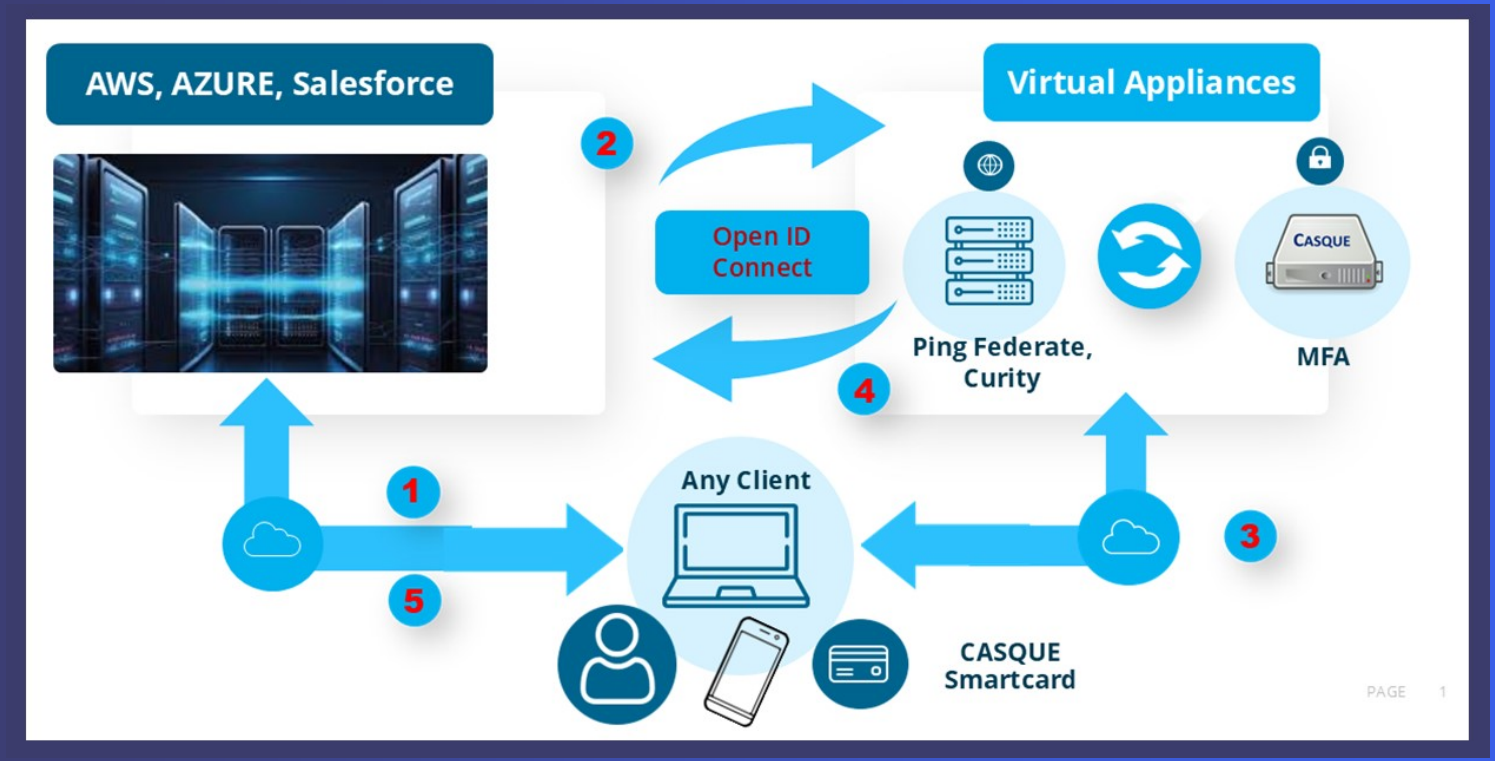
Challenge presented as QR image on Laptops

No need for Card readers, works on any client, any OS

MFA Authentication with frictionless User experience

Radical MFA without the vulnerabilities of existing methods

CASQUE Integrates with existing Infrastructure



TIME TO STOP INSIDER THREAT

Info at casque.co.uk