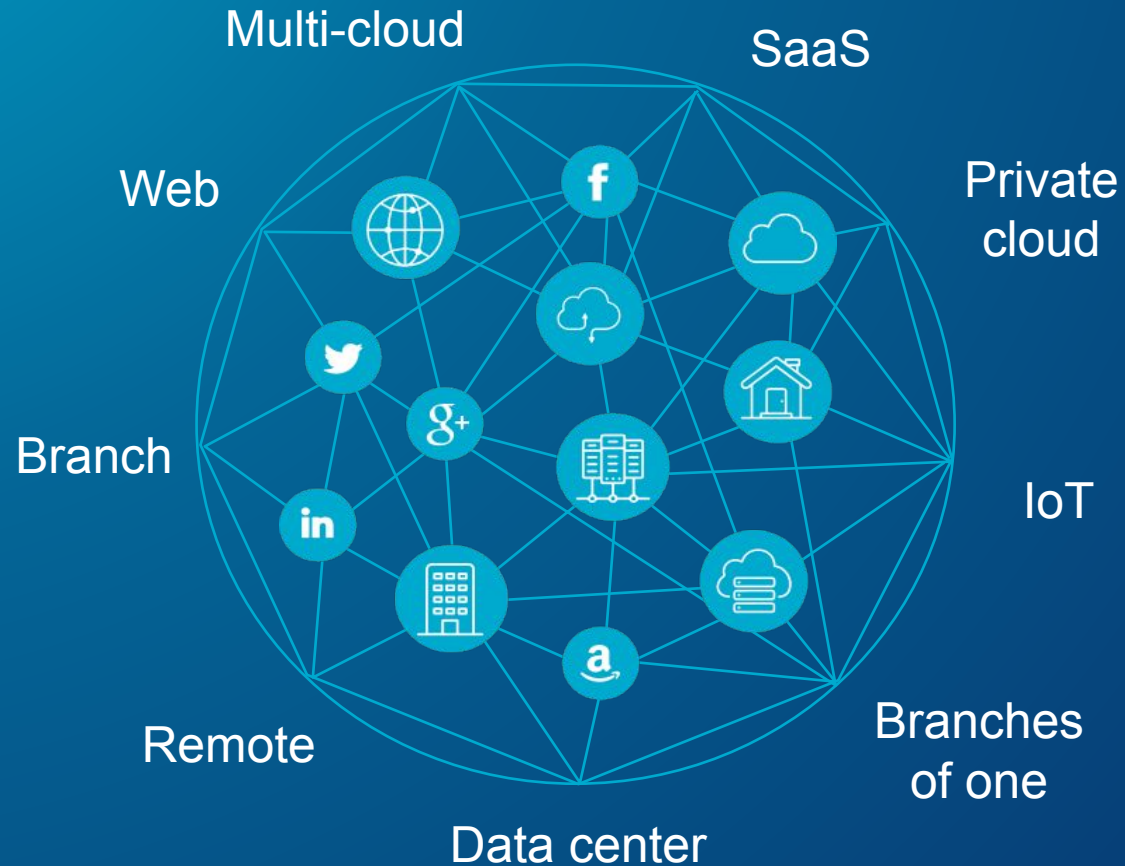


Security & Networking ReAI imagined

Secure and accelerate cloud, data, & AI everywhere

Krishna Narayanaswamy – Cofounder & CTO Netskope

Users, apps, and data are everywhere



- **75%+** of traffic is SaaS and cloud delivering 50% of threats
- **2,400+** SaaS apps for average enterprise — most shadow IT
- **95%** of traffic is encrypted where threats and data hide

Explosion of Generative AI

ChatGPT Sprints to One Million Users

Time it took for selected online services to reach one million users



* one million backers ** one million nights booked *** one million downloads
Source: Company announcements via Business Insider/LinkedIn

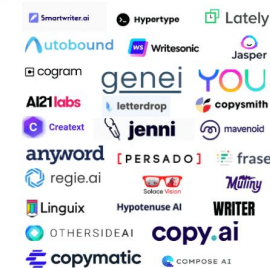


statista

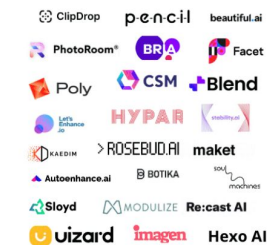
THE GENERATIVE AI STARTUP LANDSCAPE

ANTLER

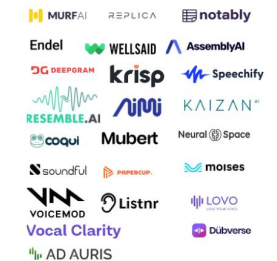
TEXT



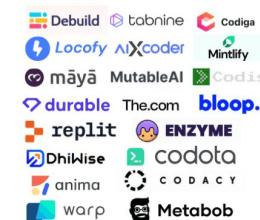
IMAGE



AUDIO



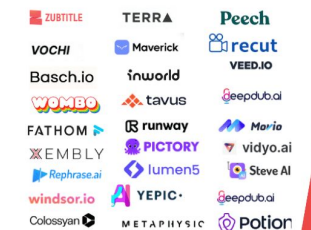
CODE



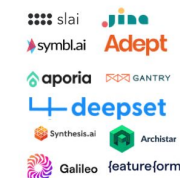
CHATBOTS



VIDEO



ML PLATFORMS



SEARCH



GAMING



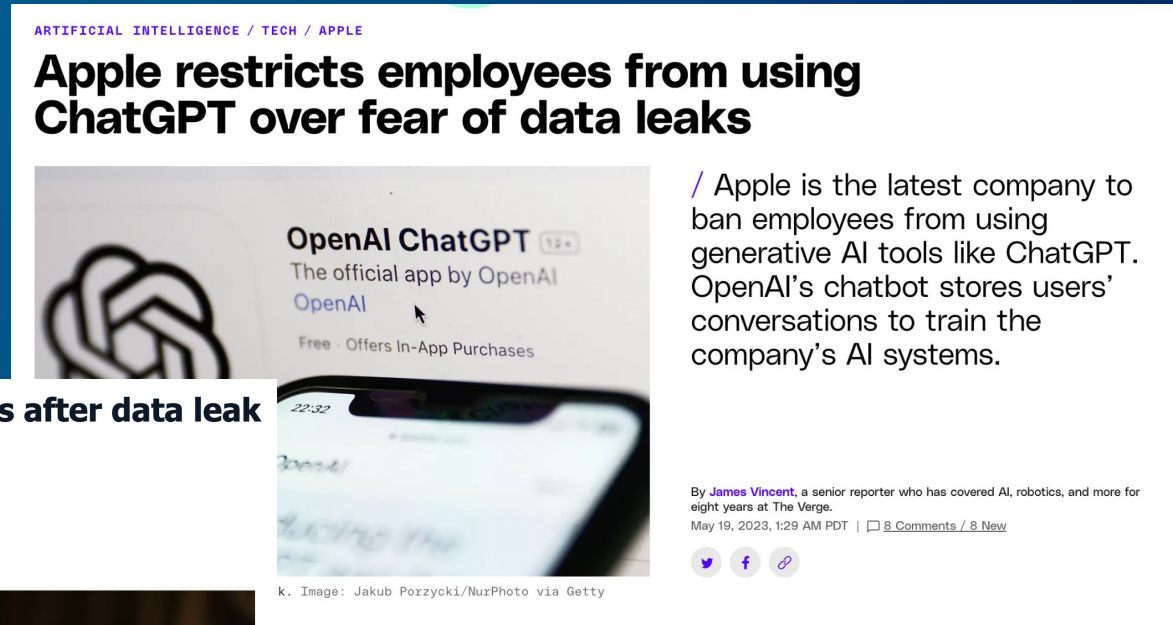
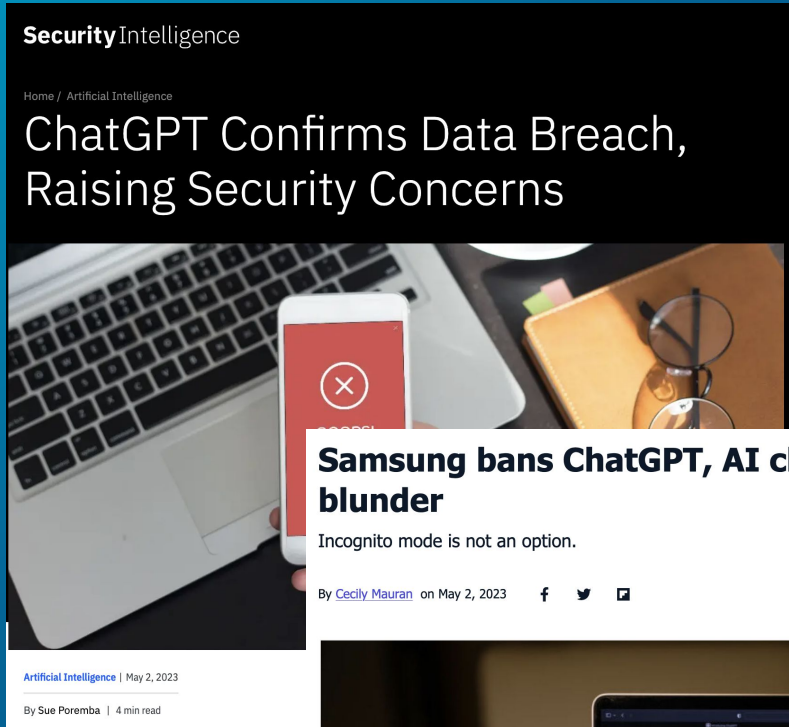
DATA



Data is at Risk in AI Apps

Amazon Warns Employees to Beware of ChatGPT

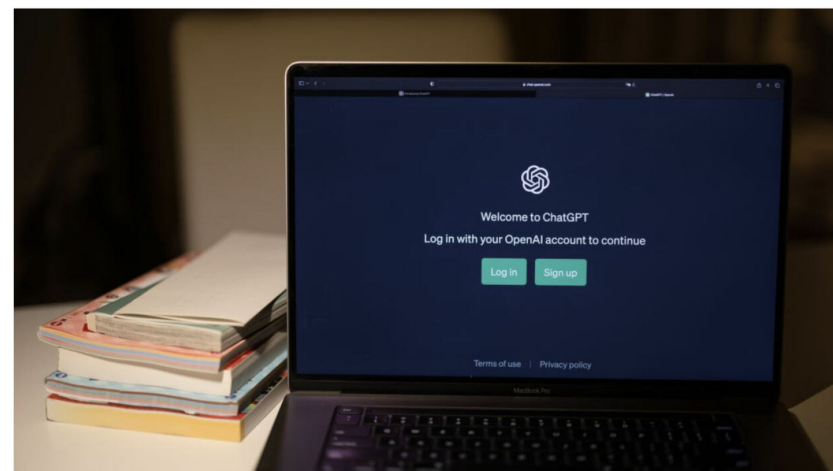
At the same time, OpenAI's Chat GPT gave correct answers to interview questions for a software coding position.



Samsung bans ChatGPT, AI chatbots after data leak blunder

Incognito mode is not an option.

By Cecily Mauran on May 2, 2023



Samsung joins other companies that have banned or restricted ChatGPT because of data breach risks. Credit: Getty Images



JPMorgan Chase, Verizon, Citigroup, and Goldman Sachs Block Access to ChatGPT

By IBL News - February 27, 2023

SaaS GenAI Adoption Continues To Skyrocket

Widespread AI Adoption

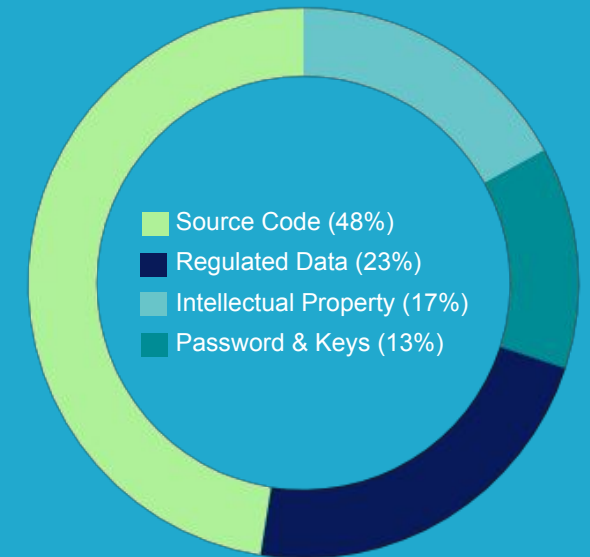
89% Actively Using SaaS GenAI Apps

Rise of Shadow AI

60% Are Using Personal GenAI Accounts at Work

Sensitive Data Risk

Top four types of data sent to GenAI apps



Source: Netskope Threat Labs, Cloud and Threat Report: Shadow AI and Agentic AI 2025

Source: Netskope Threat Labs Cloud and Threat Report: Generative AI, 2025

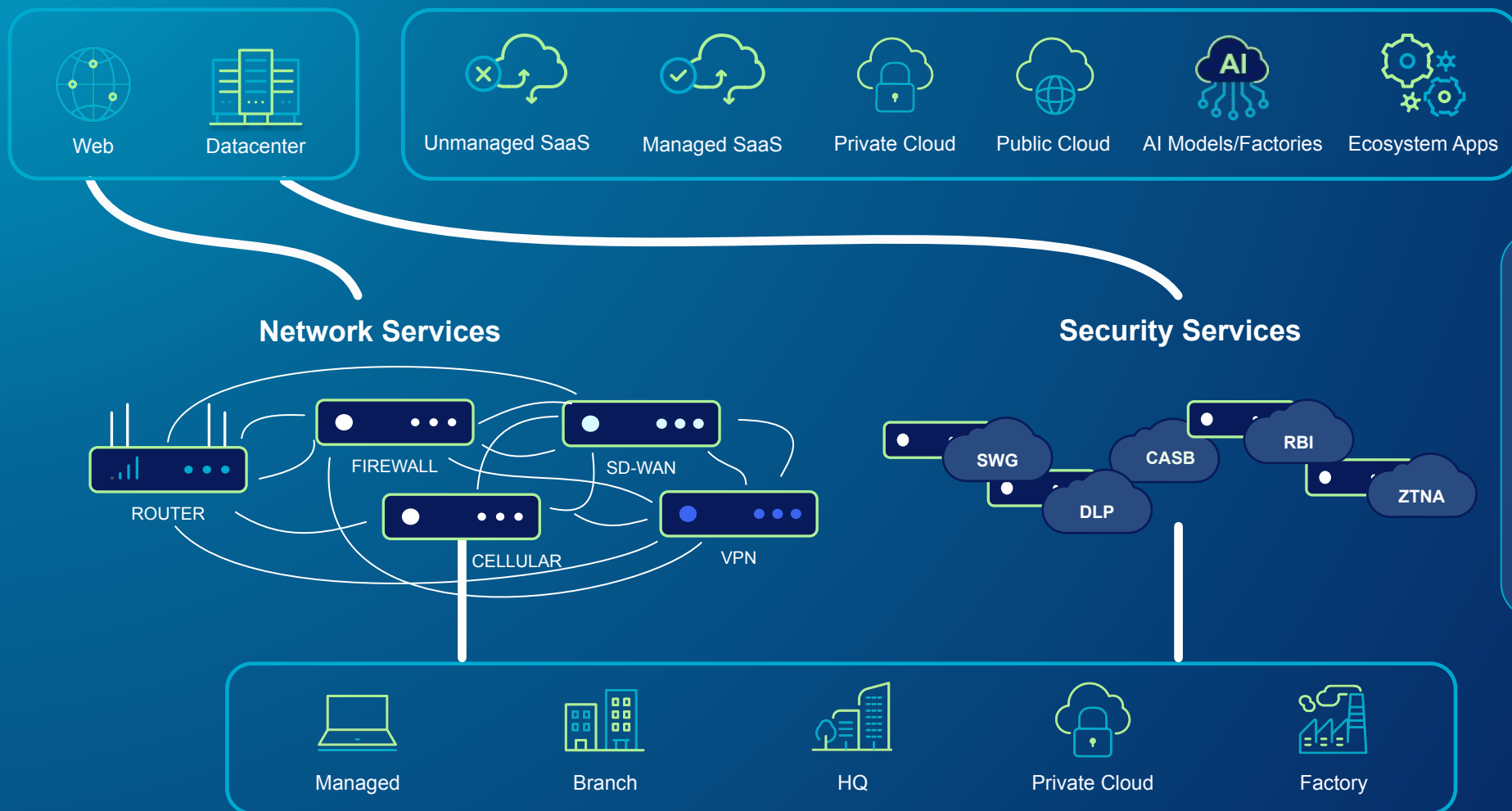


A man in a dark suit stands with his back to the camera, hands on his hips, looking down a road that splits into two paths. To the left, a green arrow-shaped sign points left with the word 'ALLOW' in white. To the right, a green arrow-shaped sign points right with the word 'BLOCK' in white. The scene is set against a blue sky with white clouds and a green grassy field.

ALLOW

BLOCK

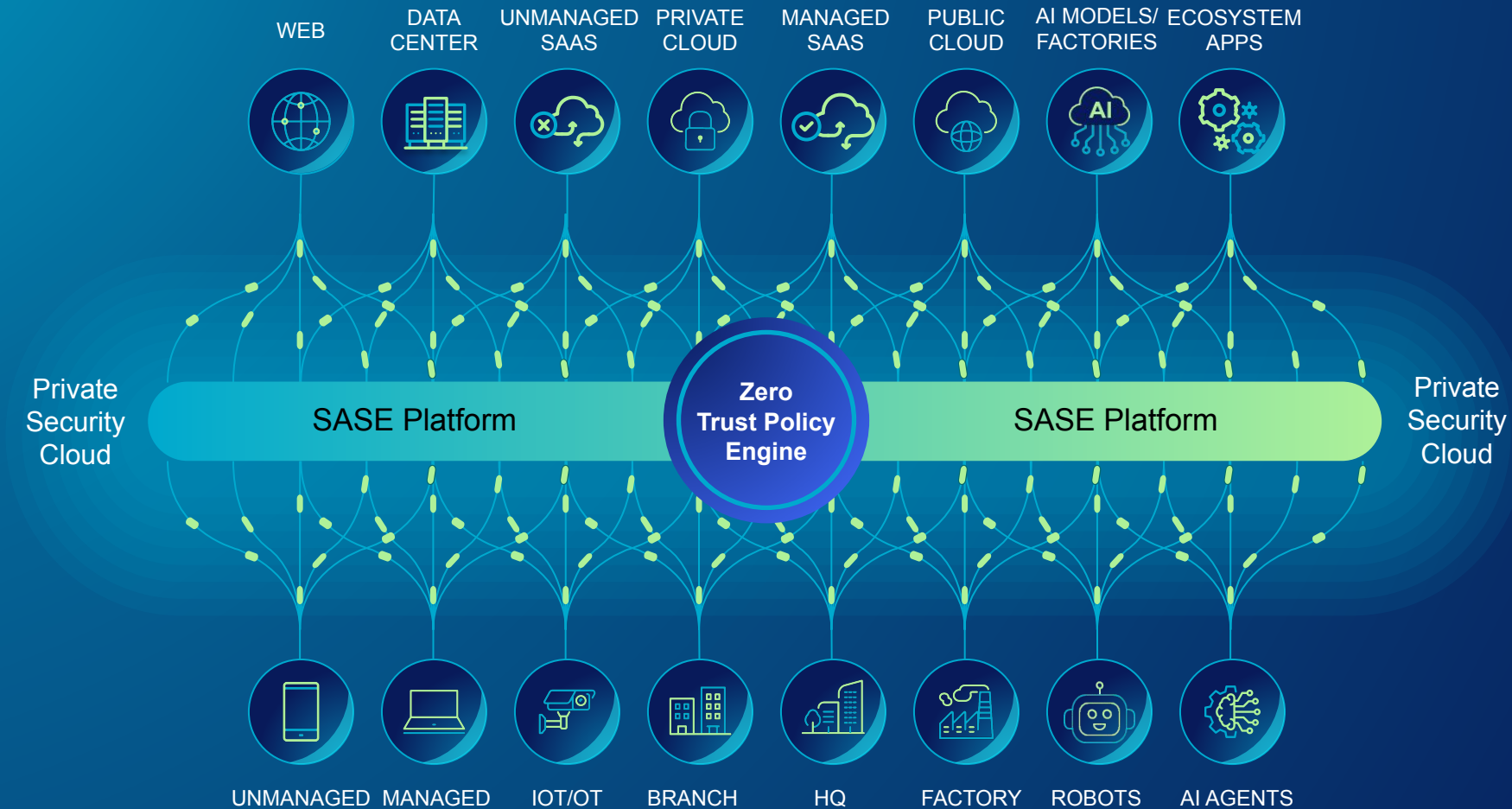
Legacy Infrastructure Can't Address the Modern Digital Landscape



✗ Siloed and cumbersome security and networking services create operational complexity and security risks

✗ Underlying legacy networking infrastructure often suffers significant performance degradation when advanced services enabled at scale

Redefined Security and Networking



The Language of the Internet Has Fundamentally Changed



Static, monolithic webpages

Mid-1990s to Early 2000s

Firewall



Some dynamic content

Early 2000s to 2010s

Next Generation Firewall
Secure Web Gateway



Data-Rich, Interactive, Dynamic Applications / Websites

AI and Cloud Era

Modern Security, Networking, Analytics Platform
(Netskope One)

Language

HTML

HTML with form-data and SOAP (XML)

REST API, MCP, A2A, GraphQL (JSON)

Visibility

Ports, IP addresses, protocols

Limited application, user, device

Application, identity, location, device, behavior, data risk, content, activity

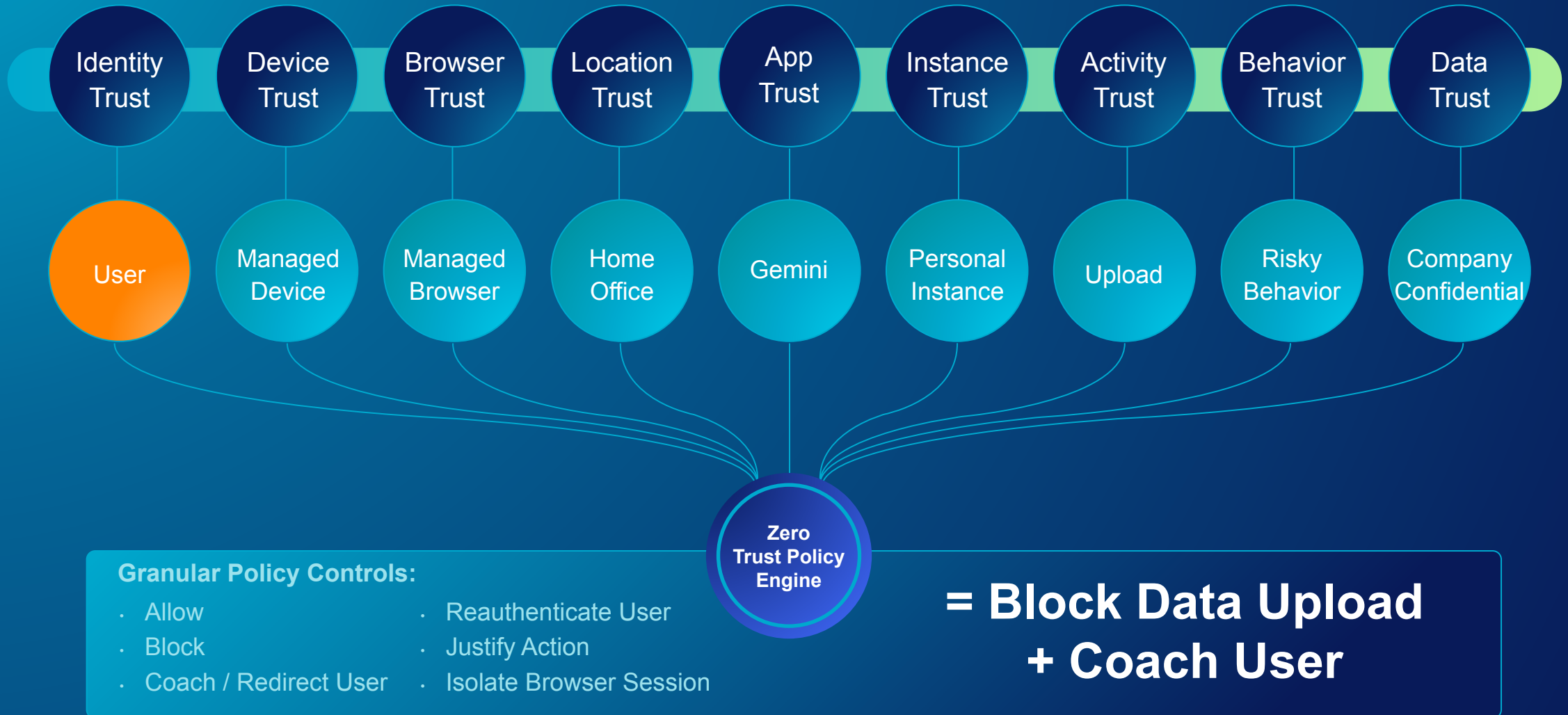
Control

Block / allow apps, static rules

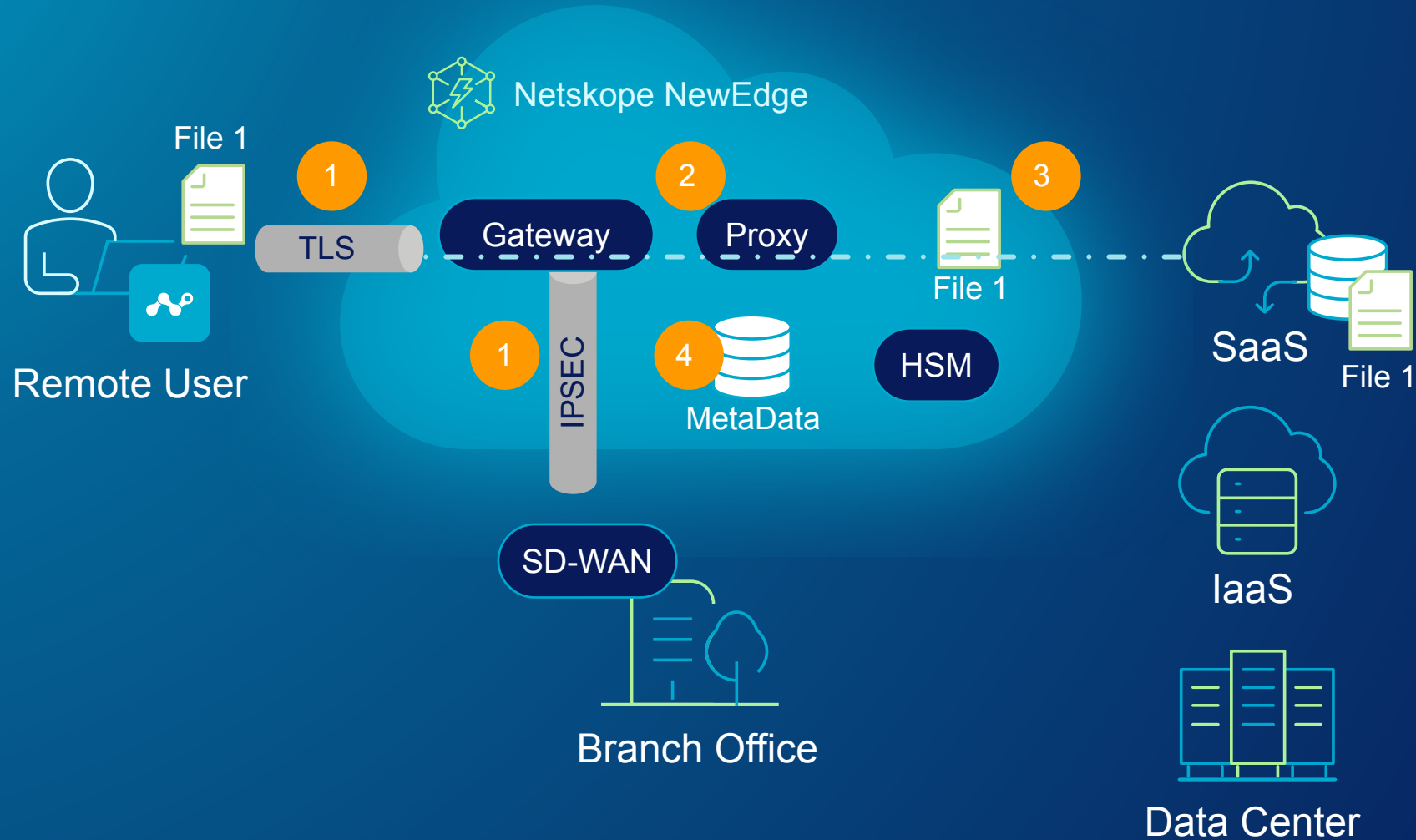
Block/Allow apps, websites w/ rudimentary control

Granular, contextual, risk-based, real-time

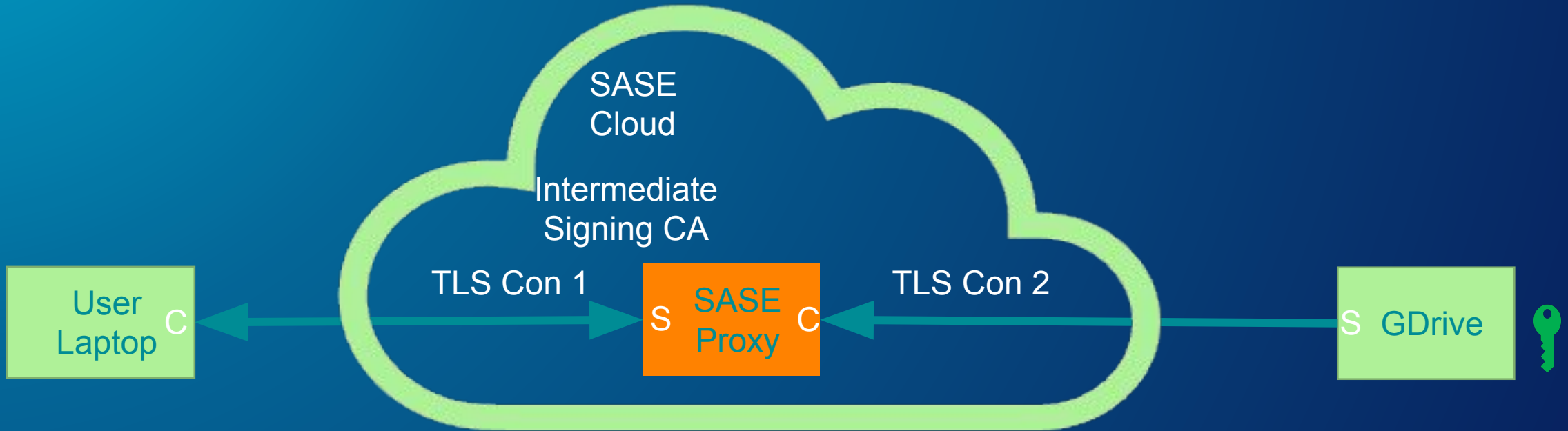
Adaptive Security Architecture :: User



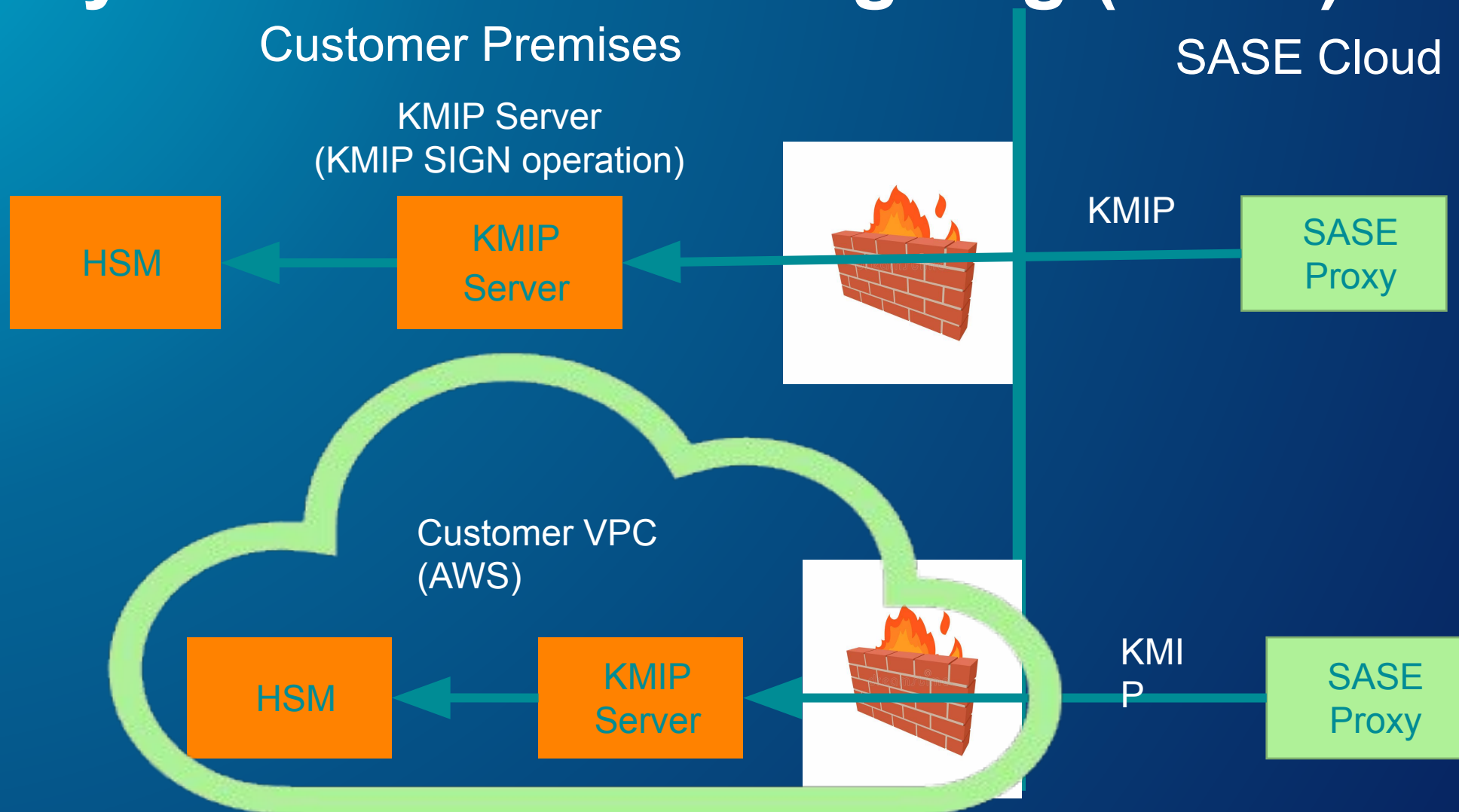
Encryption in the SASE platform



TLS Broker – Certificate Handling (OpenSSL)



Proxy Intermediate CA signing (KMIP)



The path to post-quantum cryptography (PQC)



Encryption in the Age of Quantum

Symmetric Encryption

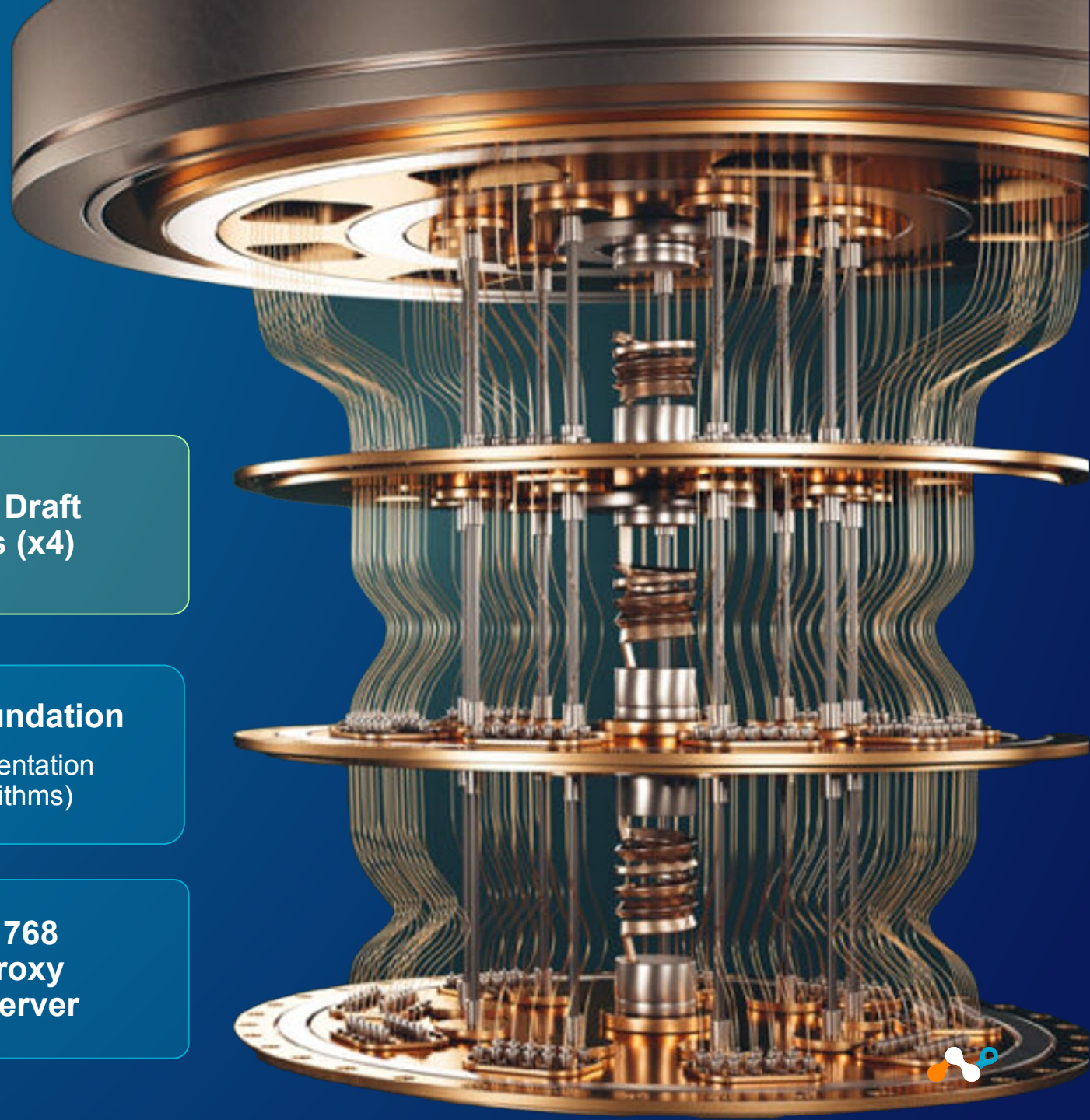
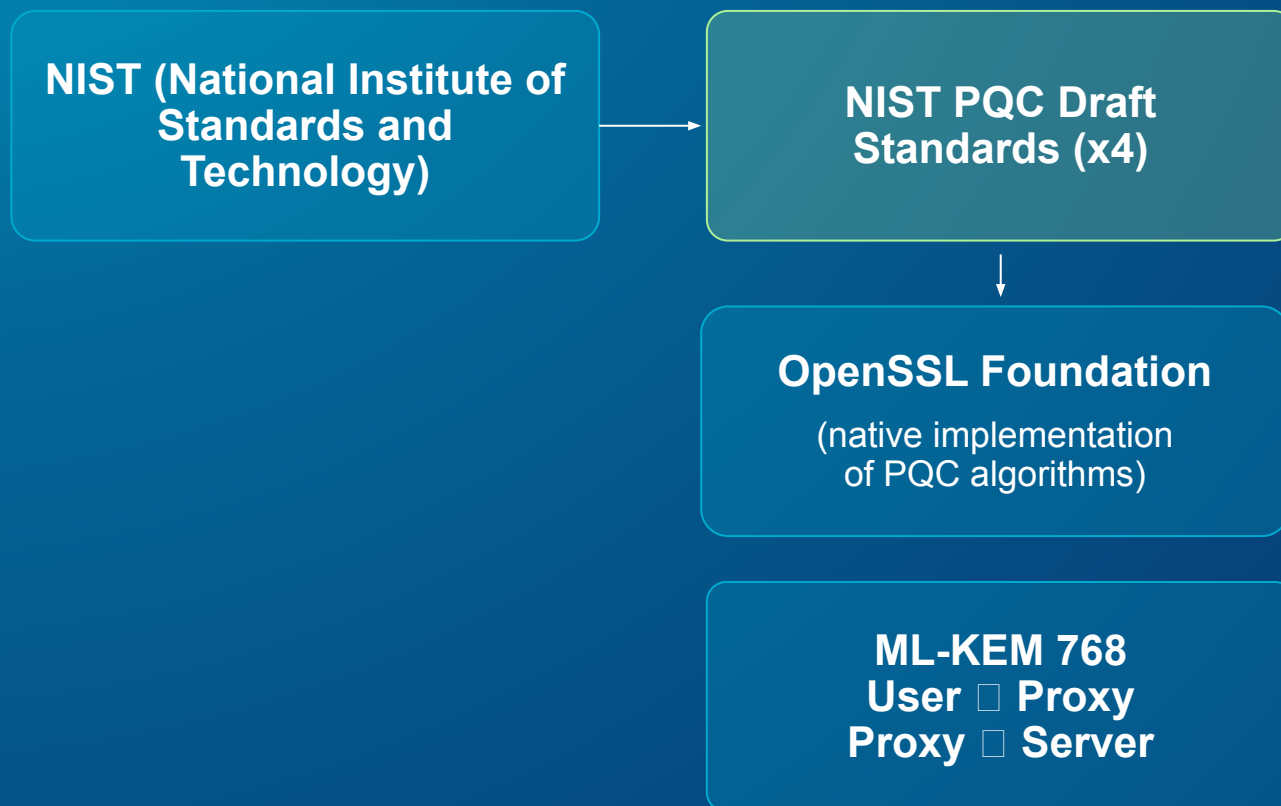
How it works	One key encrypts & decrypts
Think of it as	A shared safe —same key opens it
Used for	Fast data encryption (files, backups, VPNs)
Pros	Fast, efficient for large data
Cons	Key sharing is a risk

Asymmetric Encryption

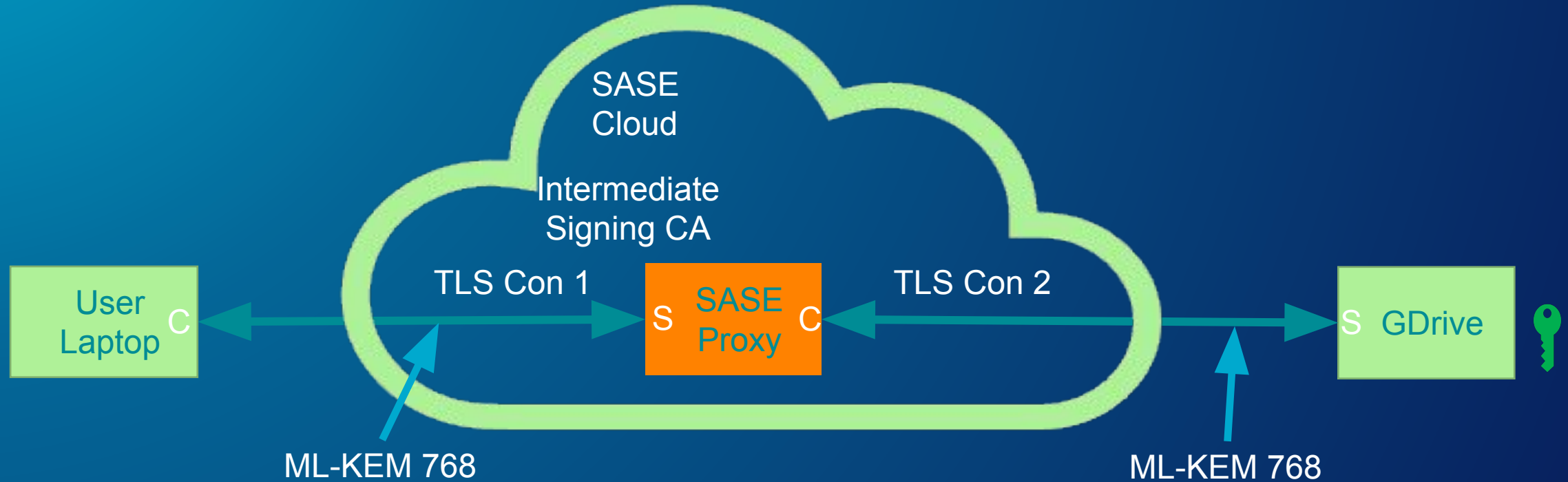
Public key encrypts, private key decrypts
A locked mailbox —anyone can drop in, only you can open
Secure communication (SSL/TLS, email, digital IDs)
No need to share private key
Slower, breaks with quantum computing



PQC Readiness Options



PQC Negotiation (OpenSSL)



Key Takeaways

Emerging Risks

- SaaS/IaaS/PaaS
- Gen AI and LLM Apps
- Quantum Computing



Emerging Risks

- SASE Security Platform
- Context Aware Zero Trust
- Safely Enable Apps



Enabling Tech

- SSL/TLS - OpenSSL
- Key Mgmt - KMIP



Thank You



linkedin.com/in/krishna-narayanaswamy



krishna@netskope.com