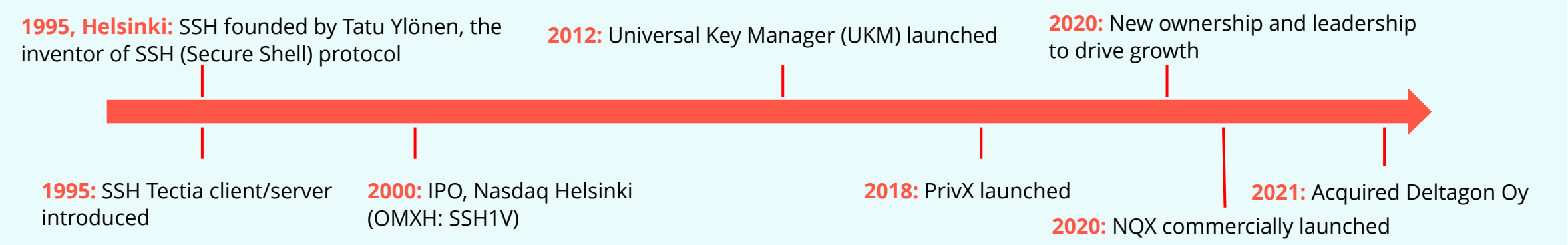
SSH.COM

SSH Communications Security

Securing the connected car

10.6.2021

25+ years of history of innovation in cybersecurity technology



Over **5M annual unique website visitors** proves that SSH thought leadership is sought after every day

SSH.COM IS TRUSTED BY

***also trusted by 2 of the top 10 car manufacturers**

WESTERN UNION | Walmart | OCBC Bank | SAP | Disney | IRS | SWISS

Motivation: IoT & OT face increasing cyber threats

74%

…of data breaches start with digital keys in the wrong hands

83%

…of organizations do not have robust processes to control their digital keys

95%

…of cloud breaches in 2020 were predicted to be due to customer vulnerabilities

How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed

Cyber attack hits Tower Semiconductor

Maersk had to reinstall 45,000 new computers after hacker attack

How a ransomware attack cost one firm £45m

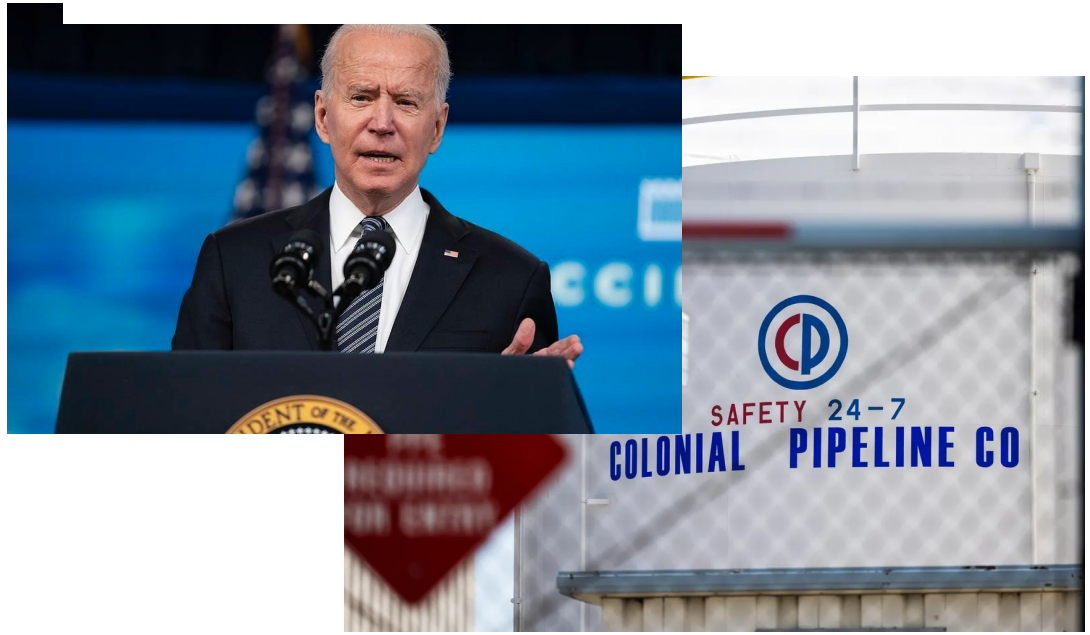
How to make sure that the right persons or applications have access to right resources at right time?

Source: IBM, Gartner

Zero Trust: the new norm for critical access

Cybersecurity

Biden Proposes Billions for Cybersecurity After Wave of Attacks



"The Federal government must lead the way and increase its adoption of security best practices, including by employing a **zero-trust security model** *[…]"*

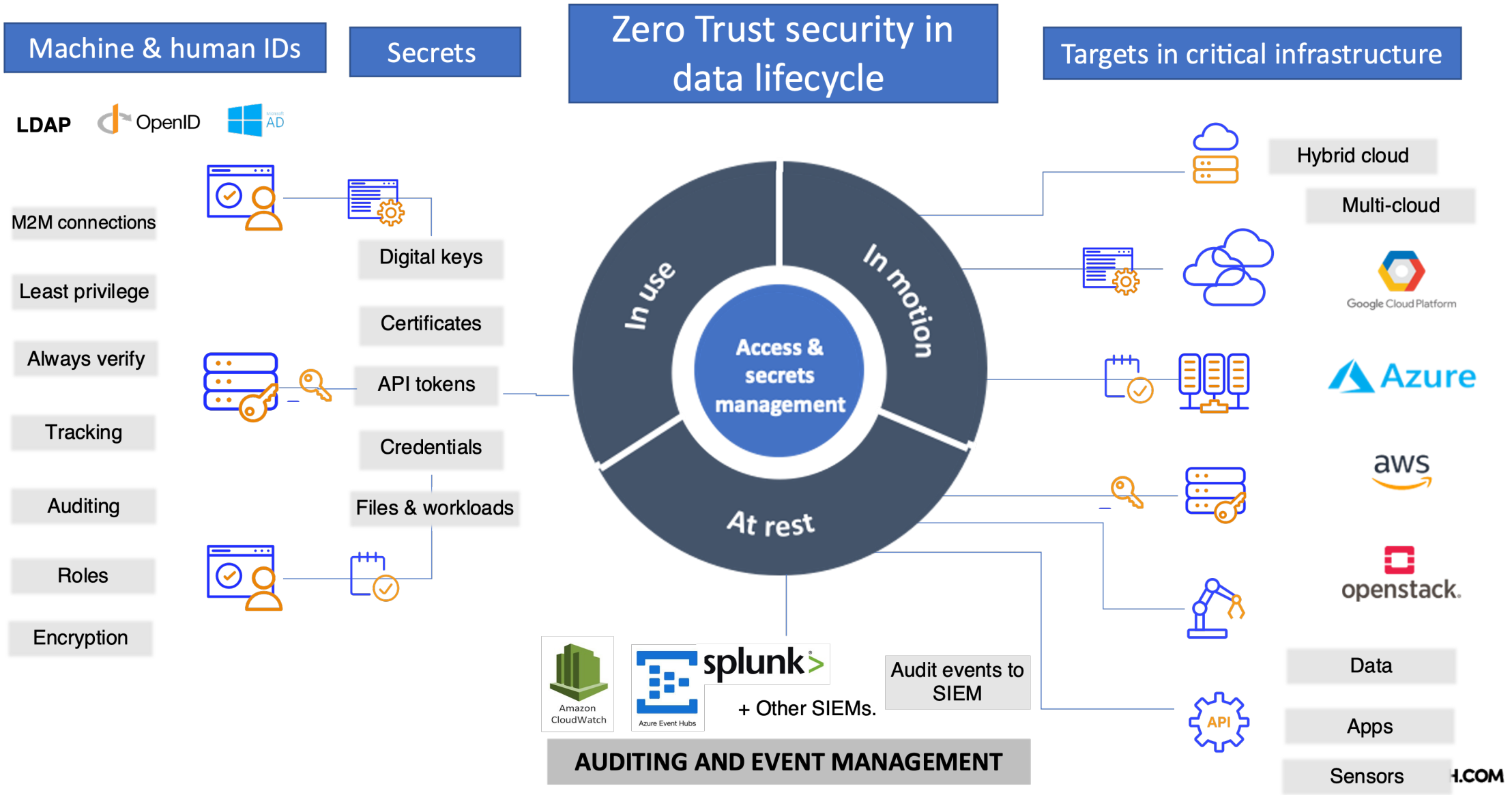
Zero Trust:

- Eliminates data breaches by managing trust from organization's network architecture
- "Never trust, verify real-time all the time".
- Get away from static passwords
- Leverage network segmentation, prevent server hopping, provide application-level threat prevention

pwd1234

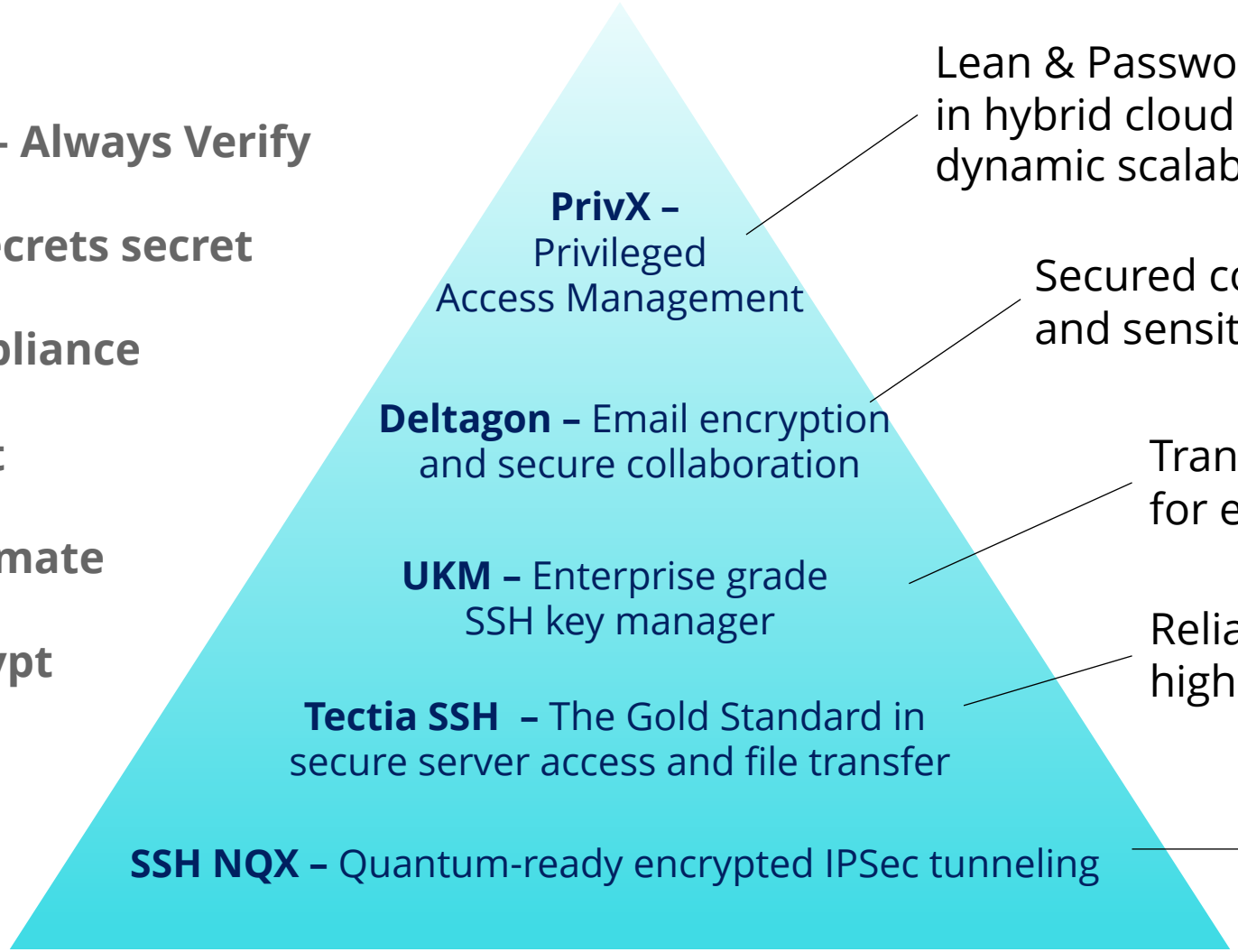
BUT…
Many "Remote access" and M2M solutions lack the granularity and control needed for Role-based & Just-In-Time Access

SSH Zero Trust: access and secrets management



Our solutions – cybersecurity in layers

1. **Never Trust – Always Verify**
2. **Keep your Secrets secret**
3. **Always Compliance**
4. **Always Audit**
5. **Always Automate**
6. **Always Encrypt**



Lean & Passwordless access to resources in hybrid cloud environments with dynamic scalability and HA

Secured communications for valued and sensitive data in daily use

Transparency and compliance for enterprise server estates

Reliability and robustness for high-volume data transactions

Critical infrastructure protection

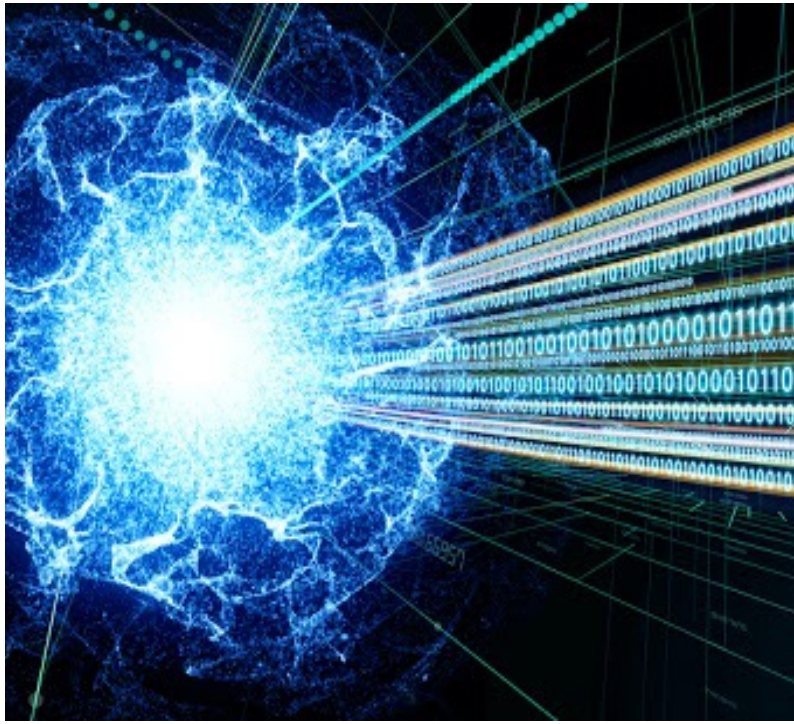
Post-Quantum Cryptography (PQC)

All current data encryption is based on traditional algorithms like Diffie-Hellman and RSA, which are vulnerable to attacks by quantum computers (QCs)

All protocols are vulnerable if the **algorithm** is vulnerable (TLS/HTTPS/FTPS, SSH/SFTP etc)

QCs exist right now in the cloud where anyone can access with a reasonably low cost

With a rapid growth of quantum computing resources, QCs will soon become a threat to traditional cryptography



1

SSH will be Quantum ready with our new set of algorithms

QCs will not have a specific advantage against Quantum ready algorithms

2

To make our implementation extra secure, we have a hybrid algorithm approach

- Traditional algorithm (ECDH) protects against traditional attacks
- Quantum ready algorithm protects against quantum attacks

3

PQC algorithms are under development

NIST PQC final round candidates:
Saber
CRYSTALS/Kyber
FrodoKEM

Zero Trust & PQC for securing automotive data and the ecosystem

IPR management and malicious code prevention

Fleet management & vehicle access

DevOps & CI/CD pipeline – GitHub/ GitLab

TLS / X.509 Certificate and SSH key based identification

Software / firmware updates

Emergency **112** & road assist communication security

Road infrastructure security & digital access

E-vehicle charging station network management

“Vehicle to X” communication

Maintenance equipment and shop service provider network access

Vehicle to vehicle communication

Use cases: securing mobility and logistics

Maritime engine diagnostics access from IoT cloud

- **SSH** / **RDP** access to marine vessels over satellite link
- PrivX provides tracking of user identities and transparency into the sessions, securing the VPN tunnel from unsanctioned use

Rail logistics / interactive user interface solutions

- Customer challenge: how to secure transactiont data traffic from POS terminals across 600 multinational locations
- SSH solution: Secure and encrypted file transfers over **SSH tunneling**

Sea-port infrastructure engineering remote access

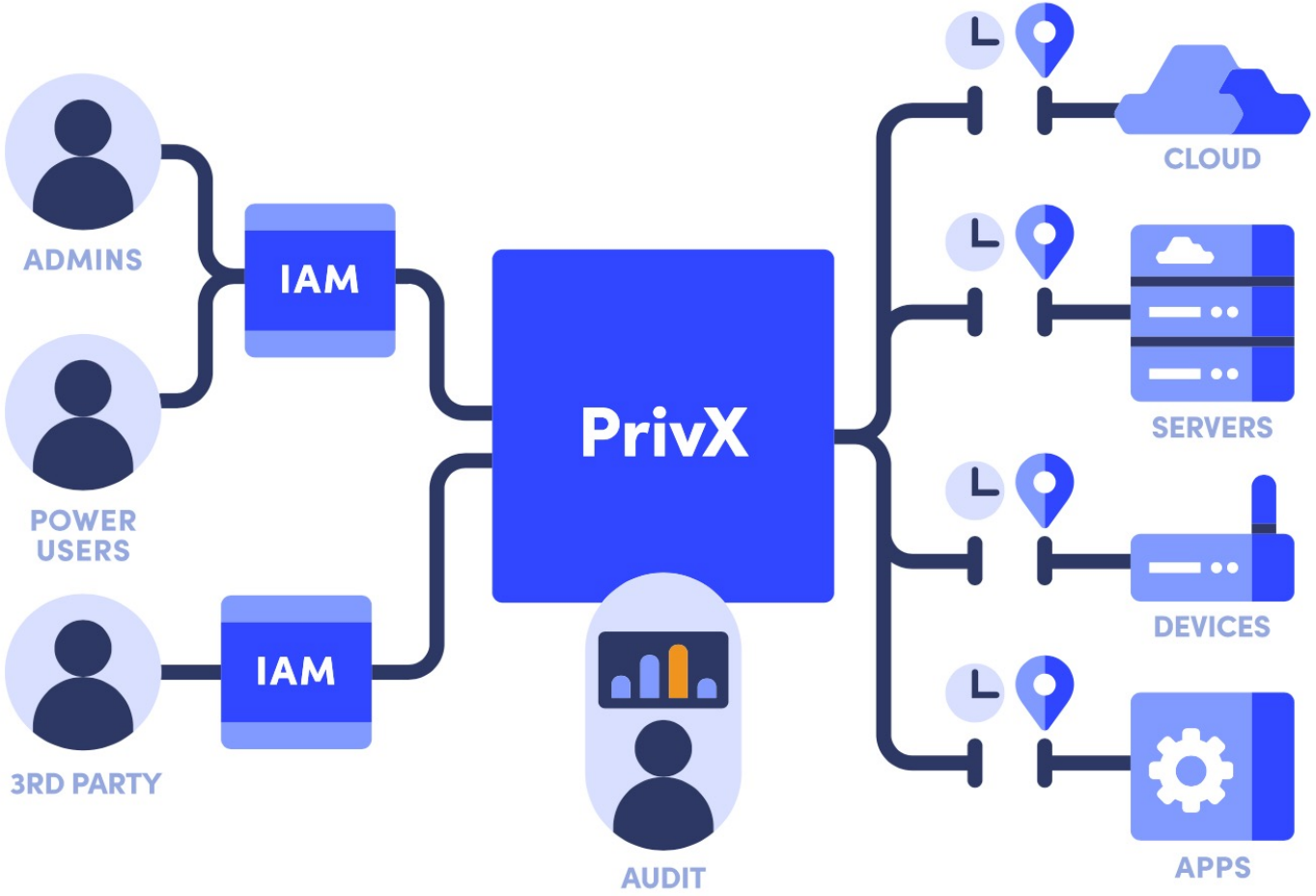
- **VNC** and **RDP** connectivity to on-target remote terminals running PLC systems
- Role-based access to data center servers for in-house and 3rd party engineering staff

Privileged Access Management for DevOps

- DevOps has become essential to many organizations looking to become more responsive and innovative.
- Application developers and other agile teams increasingly need **privileged access to essential tools.**
- **PrivX** is an alternative to conventional shared account password management technology by providing a **certificate authority based Just-In-Time access**.
- Access is **faster**, onboarding and offboarding of privileged users is quick and there are **no passwords** (or other credentials) **to issue or lose**.

kuppingercole ANALYSTS LEADERSHIP COMPASS *2/2021*

Role-based DevOps CI/CD access to GitHub and other cloud-based resources



- ✓ Access control to targets through roles
- ✓ User identities are always verified from AD
- ✓ MFA is used
- ✓ User never sees the secrets
- ✓ Sessions are recorded
- ✓ Audit trails created
- ✓ No permanent access rights
- ✓ On-boarding and off-boarding are automated
- ✓ Access approval is based on workflow
- ✓ Shared accounts on targets are secured by PrivX
- ✓ … and it boosts productivity