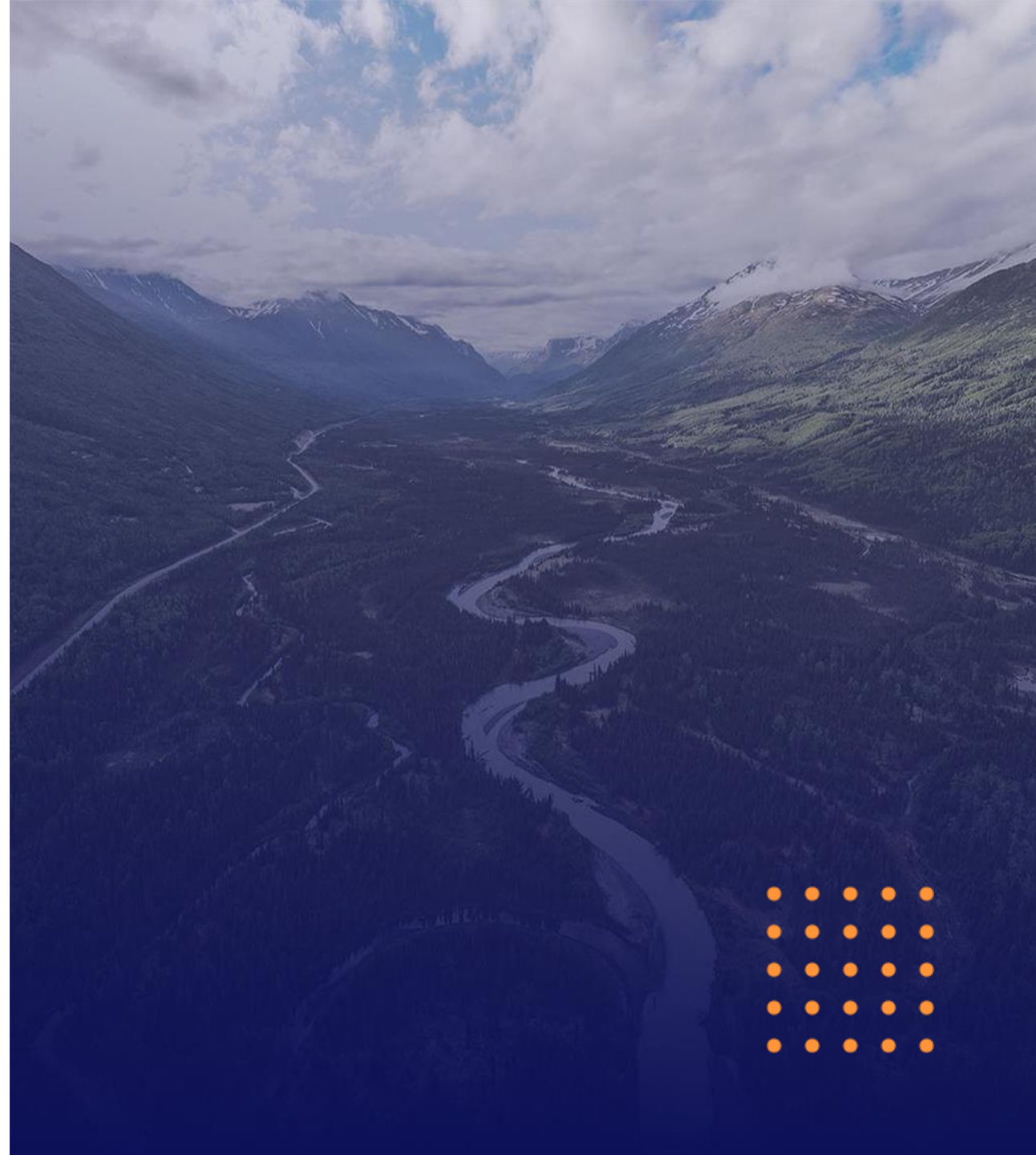

Passwordless Authentication –

The next new normal in secure digital transformation and better data protection through “Post Quantum Cryptography”

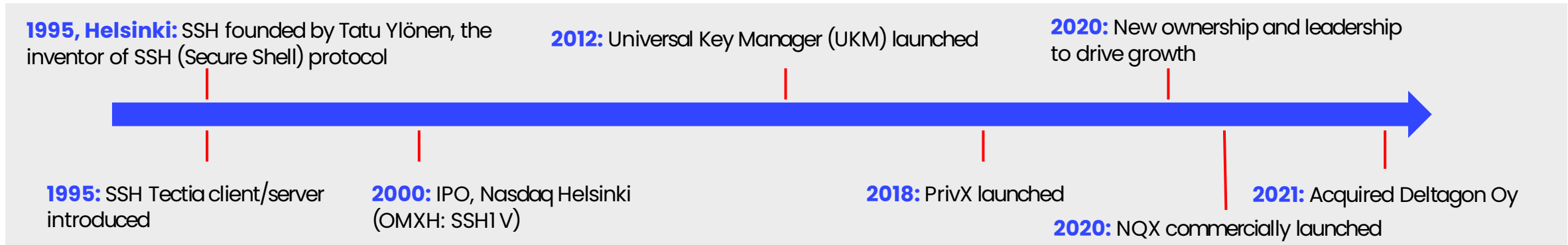
Ricky Ho
Vice President

 **SSH.COM**



SSH.COM

25+ years 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

Who is SSH.COM?

PrivX® –
the next generation cloud &
privileged access gateway.

**Universal SSH Key Manager®
(UKM)** –
the #1 SSH Key Risk Assessment,
Management and Automation tool.



Tectia® Client/Server –
the gold standard commercial product in
secure access and file transfers from the
inventor of the SSH protocol

Sec@GW® –
email encryption solution secures your
communication straightforwardly.



A cybersecurity pioneer since 1995

SSH.COM developed the SSH protocol which
today remains one of the cornerstones of
Internet security.



References



The Washington Post






The Future of Authentication

- Passwordless



World Economic Forum – The Future

Passwordless Authentication: The next breakthrough in secure digital transformation

Download PDF 

Cybercrime is set to cost the global economy \$2.9 million every minute in 2020 and some 80% of these attacks are password-related. Knowledge-based authentication – whether with PINs, passwords, passphrases, or whatever we need to remember – is not only a major headache for users, it is costly to maintain. For larger businesses, it is estimated that nearly 50% of IT help desk costs are allocated to password resets, with average annual spend for companies now at over \$1 million for staffing alone.

<https://www.weforum.org/whitepapers/passwordless-authentication-the-next-breakthrough-in-secure-digital-transformation/>

Passwordless is Everywhere




FIDO2/WebAuthn

And more...

Benefits of Using Passwordless Authentication

- Better user experience:
 - Passwordless authentication eliminates all of the troubles connected to remembering complicated passwords
- Improved security for users and organizations:
 - Difficult for a cybercriminal to get into your account as there are no passwords to be hacked
- Quicker login process:
 - Eliminate the old traditional way, like fill out long forms, take complicated steps, and be forced to create an account...etc



Most of it are usage for
causal users & business
users

How are about my privileged
users, my admin, my
engineers...etc



The future is passwordless ...



1

1990s

Move passwords to
encrypted & secret vault

Manage & limit access

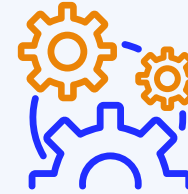


2

2000s

Obfuscate
shared account
passwords

No more sharing



3

2010s

Manage & rotate
passwords

Where policy mandates and not
yet ready for the next step



4

2020s-Now!

Move to
passwordless world

Dynamic Privileged Access (DPA)
instead of static

Challenges for Easy and Safe Access

Multiple tools for secure cloud access



OT/IoT

Too many different systems (IAM/PAM)



ISO 27001(A.9), PCI
DSS, SOX COBIT,
BASEL III, NIST,
SANS CIS CSC,
ISACA , NIS Dir,
GDPR, IEC 62443

Regulations

Data protection

Users come and go, roles & authorities
change

Making changes is slow , laborsome and
expensive



Password, key and token chaos

Misuse, IP protection, ransomware

Users make mistakes and forget

Complex to control 3rd Party/service provider access

How to make sure that the right persons have access to right resources on right level at right time?

Reduce the number of secrets to manage

No more vault based password management!!

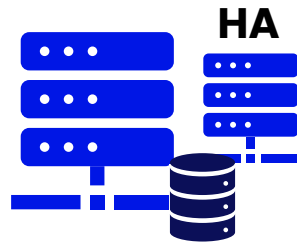
USERS, APPLICATIONS

- No agents on the clients
- No leave-behind credentials to manage (passwords, keys)
- Web based access



PAM

JIT authentication with ephemeral certificates that automatically expire



HOSTS

- No agents on the targets
- No configuration changes to the environments



Users Need Access to Critical Data and Resources

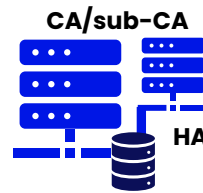
USERS, APPLICATIONS

Users and user groups are automatically synced from AD/LDAP or federated from OIDC providers (JIT)



PrivX™

Users and user groups are mapped to roles automatically (RBAC)



RESOURCES

Applications, network devices, servers
Access control to accounts on targets is done through roles (JEA)



Consoles, HR/Salary, SoMe, Finance

How to make sure that the **right persons** have access to **right resources** on **right level** at **right time**?

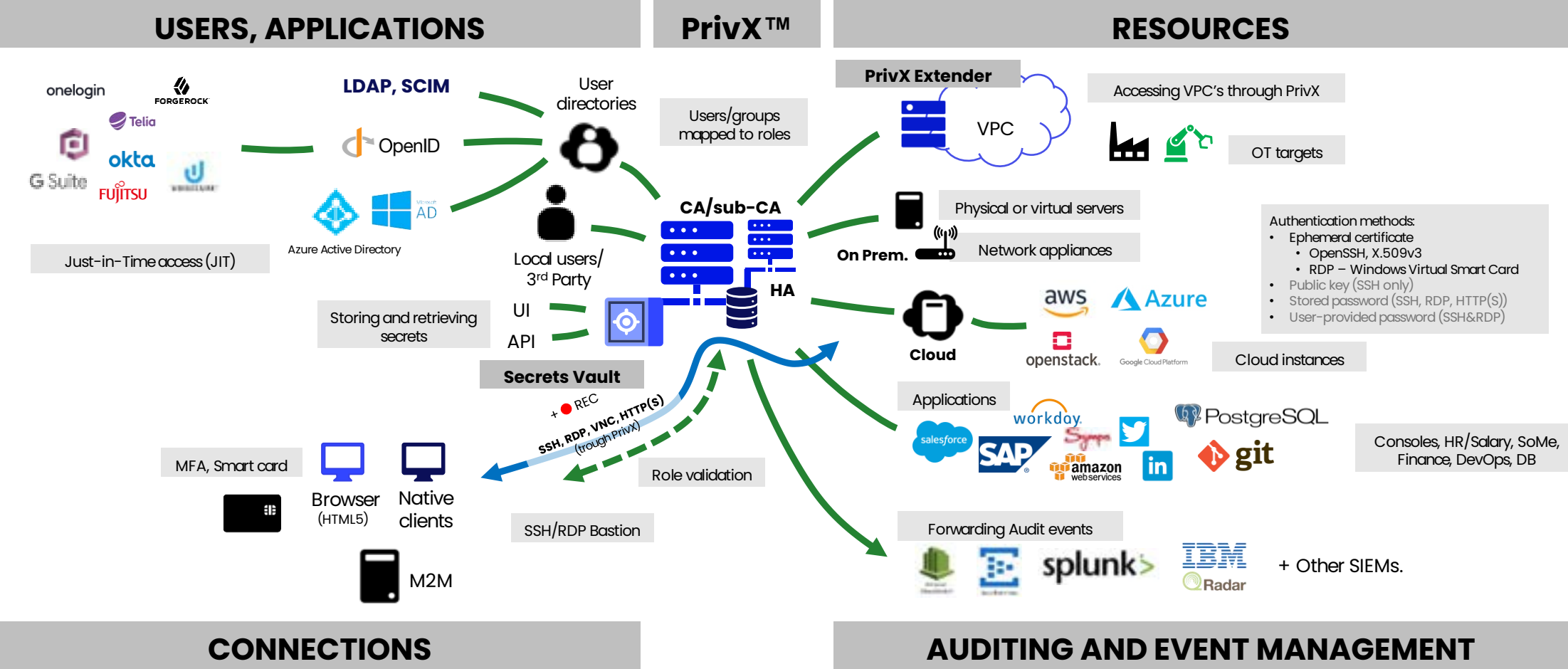
Connections are allowed based on user's current role
Connection can be established with one click from up-to-date list of resources (SSO)

CONNECTIONS

Automate audit events alerting and reporting
There is always a trace of individual user who made the connection. Audit events can be integrated with external systems i.e., SIEMs

AUDITING AND EVENT MANAGEMENT

How Does PrivX Work?



Differentiation

- Passwordless instead of Vault based
- Just-in-time access instead of always-on
- Ease of integration w/ target systems instead of configuration changes needed
- Purely agentless solution for both Passwordless & password based
- Future proof solution for cloud adoption & automation
- Ease of management product instead of bulky/endless deployment

Passwordless, keyless & frictionless = Manage less!

1

**Enhance productivity with
less secrets to manage**

2

**Reduce complexity by
eliminating processes**

3

**Keep your environment
lean, clean & immutable**

4

Always recorded



SSH Tectia

- Post Quantum Cryptography (PQC)



Quantum Computers Attacks



- All encryptions are decryptable, just matter of time
- Quantum computers exist right now
 - They are in the cloud where anyone can access with a reasonably low cost
- Overall increase in cybercrime and the financial capabilities of cybercriminals (currently over 1 trillion p.a. estimated to grow to 10 trillion p.a. by 2025)
 - Especially ransomware attacks
- All protocols are vulnerable if the algorithm is vulnerable (TLS/HTTPS/FTPS, SSH/SFTP etc)
- All current data encryption is based on traditional algorithms like Diffie-Hellman and RSA, which are vulnerable to attacks by quantum computers
- **Hack NOW, decrypt later**

Quantum Readiness

We are now Quantum ready with our new set of algorithms

- Quantum computers will not have a specific advantage against Quantum ready algorithms

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

Algorithms developed

- Based on NIST PQC (post quantum crypto) final round candidate algorithms
 - Saber
 - Streamlined NTRU Prime
 - CRYSTALS/Kyber
 - FrodoKEM

**Come and see our
demo at our booth#1**

