



SECURITY AGAINST YOU: HOW HACKERS TAKE OVER YOUR SECURE SHELL ENVIRONMENT

Elba Horta

Regional Sales Manager , Southern Europe

elba.horta@ssh.com

WE ENABLE, MONITOR & MANAGE ENCRYPTED NETWORKS



Quick Facts:

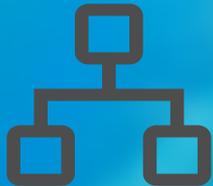
- Inventors of the SSH protocol
- Finnish Listed Company: NASDAQ OMX Helsinki (SSH1V)
- 3,000 customers including 7 of the Fortune 10

What We Do:

- Secure Shell Access Controls & Key Management
- Privileged Access Management
- Data-in-Transit Encryption

ENABLE

Tectia™ SSH



SSH Communications Security

MONITOR

CryptoAuditor™



MANAGE

Universal SSH Key Manager™



OUR CUSTOMERS

FINANCIALS



RETAIL



GOVERNMENT



UTILITIES & TRANSPORT



G2000/ENTERPRISE



Mercedes-Benz



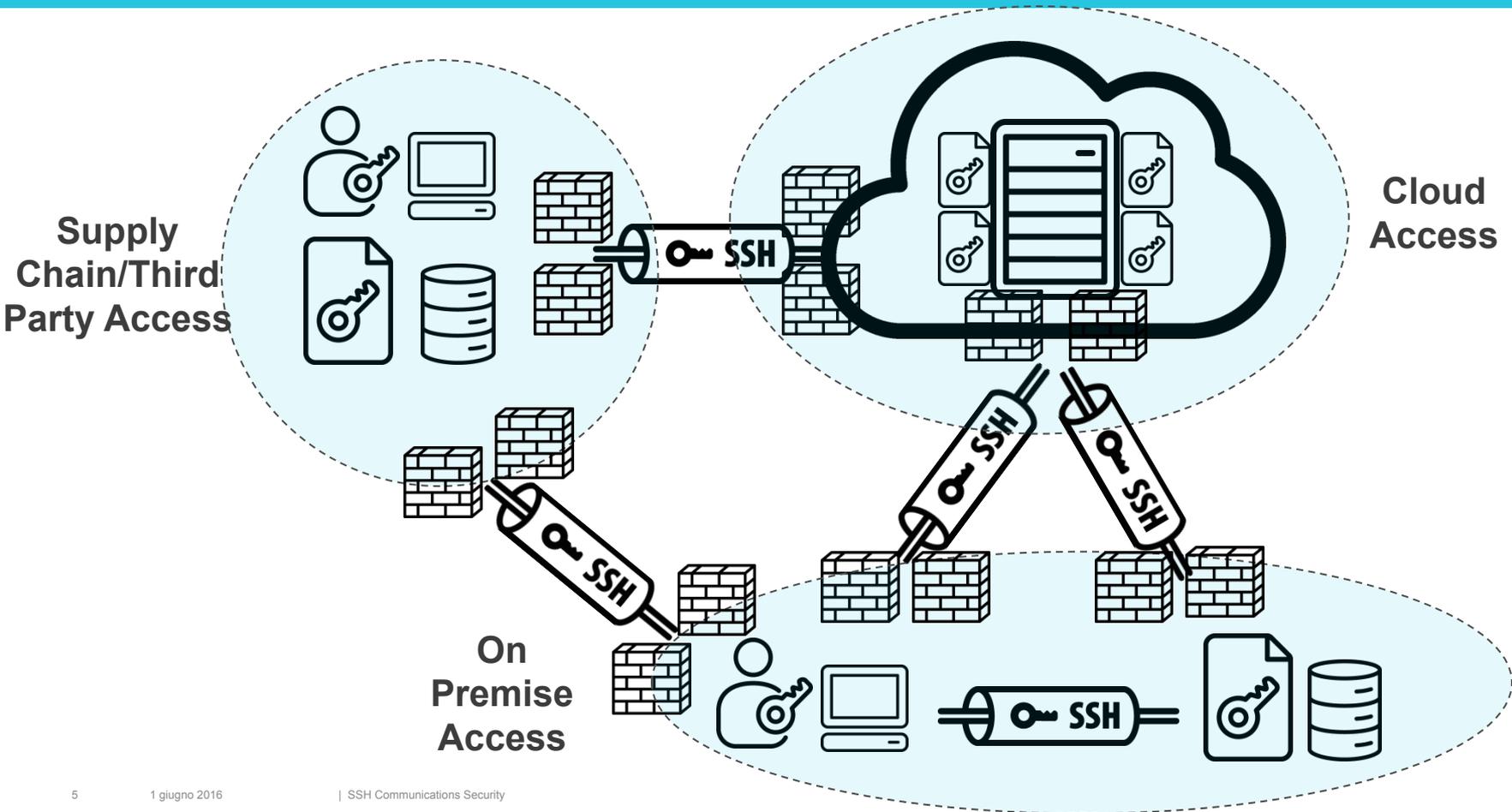


**KEEP
CALM**

AND

**ENCRYPT
EVERYTHING**

WHAT DOES ACCESS HAVE TO DO WITH SSH? EVERYTHING



HOW HACKERS TAKE OVER YOUR SECURE SHELL ENVIRONMENT

20 years of unmanaged SSH

No user key restrictions!

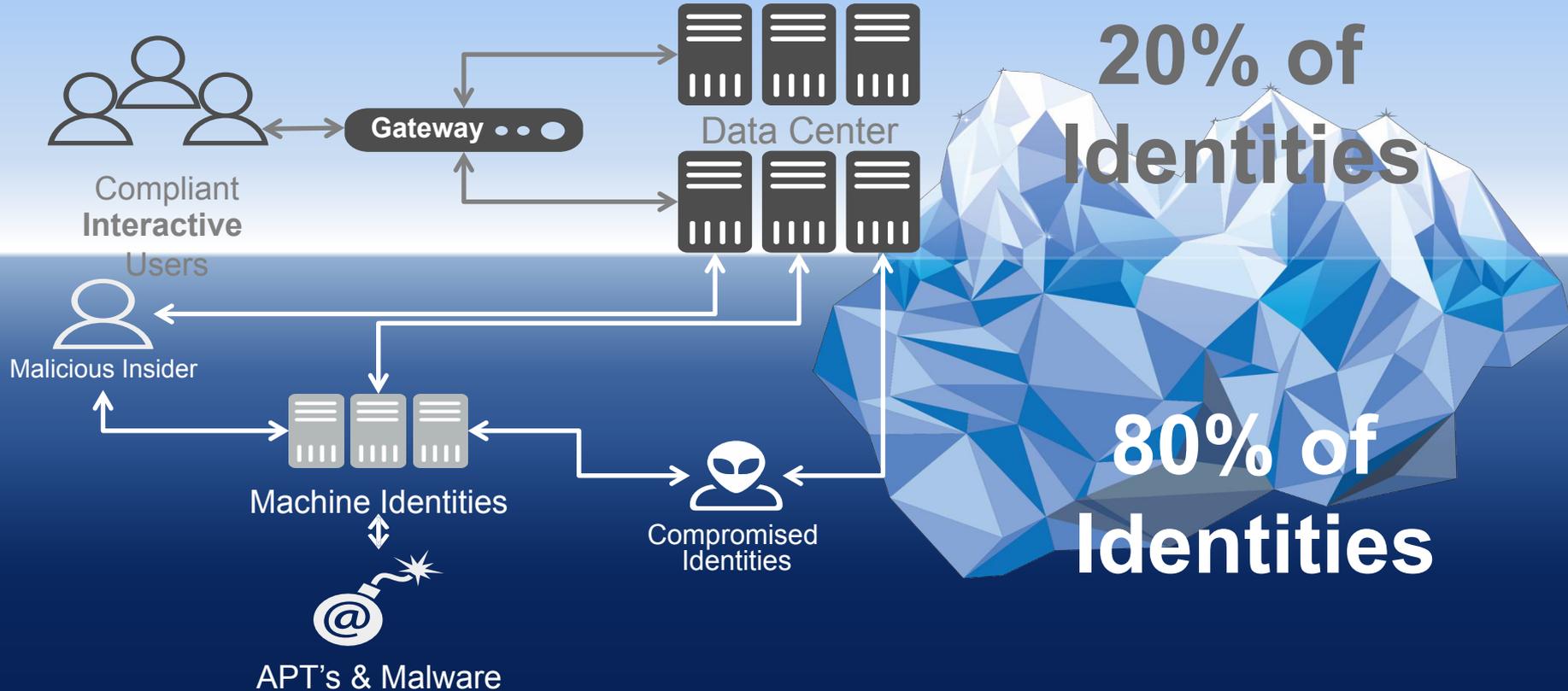
- move or copy private keys
- No expiration date

No explicit association between
a private key and an identity

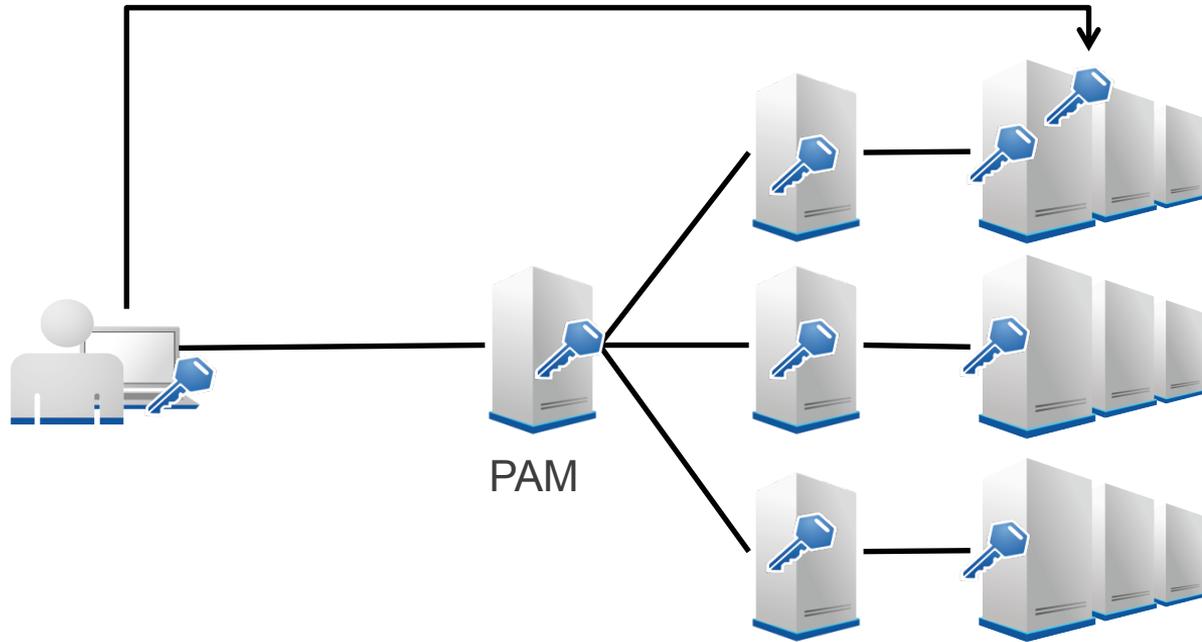
What governance? – key
creation, tracking and removal



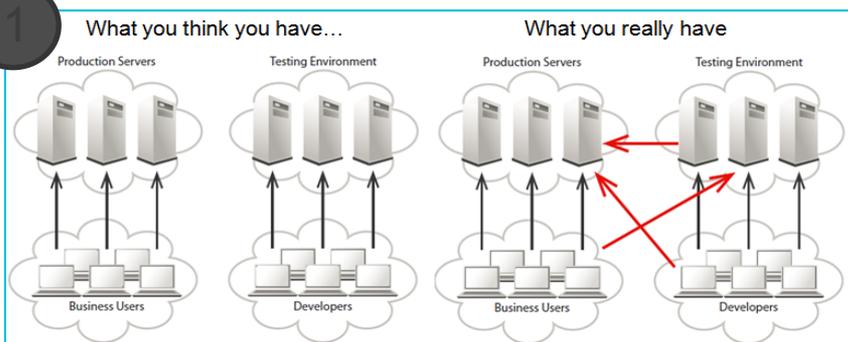
TAKING ADVANTAGE OF WHAT YOU DO NOT SEE



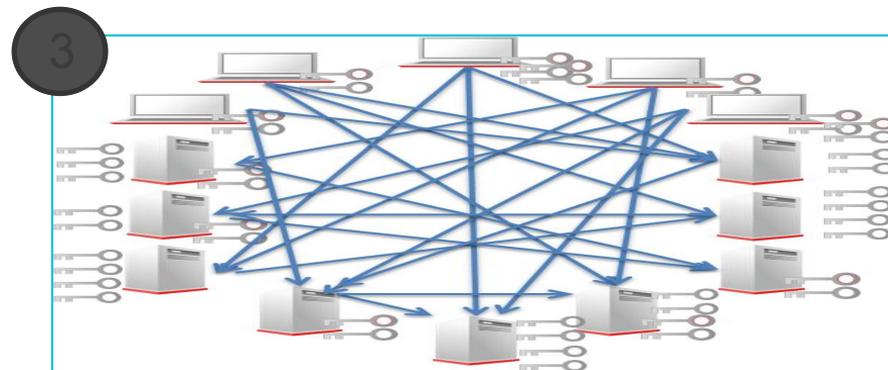
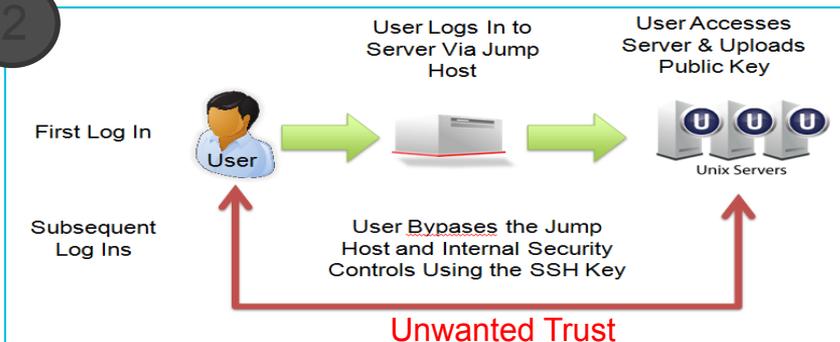
BYPASSING PAM



HOW HACKERS TAKE OVER YOUR SECURE SHELL ENVIRONMENT



1. Development to production
2. Bypassing security controls
3. Unmanageable mesh of trust



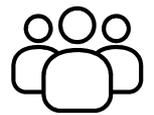
Universal SSH Key Manager



- Hosts, Users, SSH Keys and Trust-Relationships



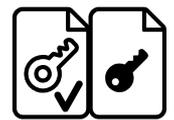
- Logins and Key Usage
- Unauthorized Operations



- Relocate Keys and Lock Down Servers



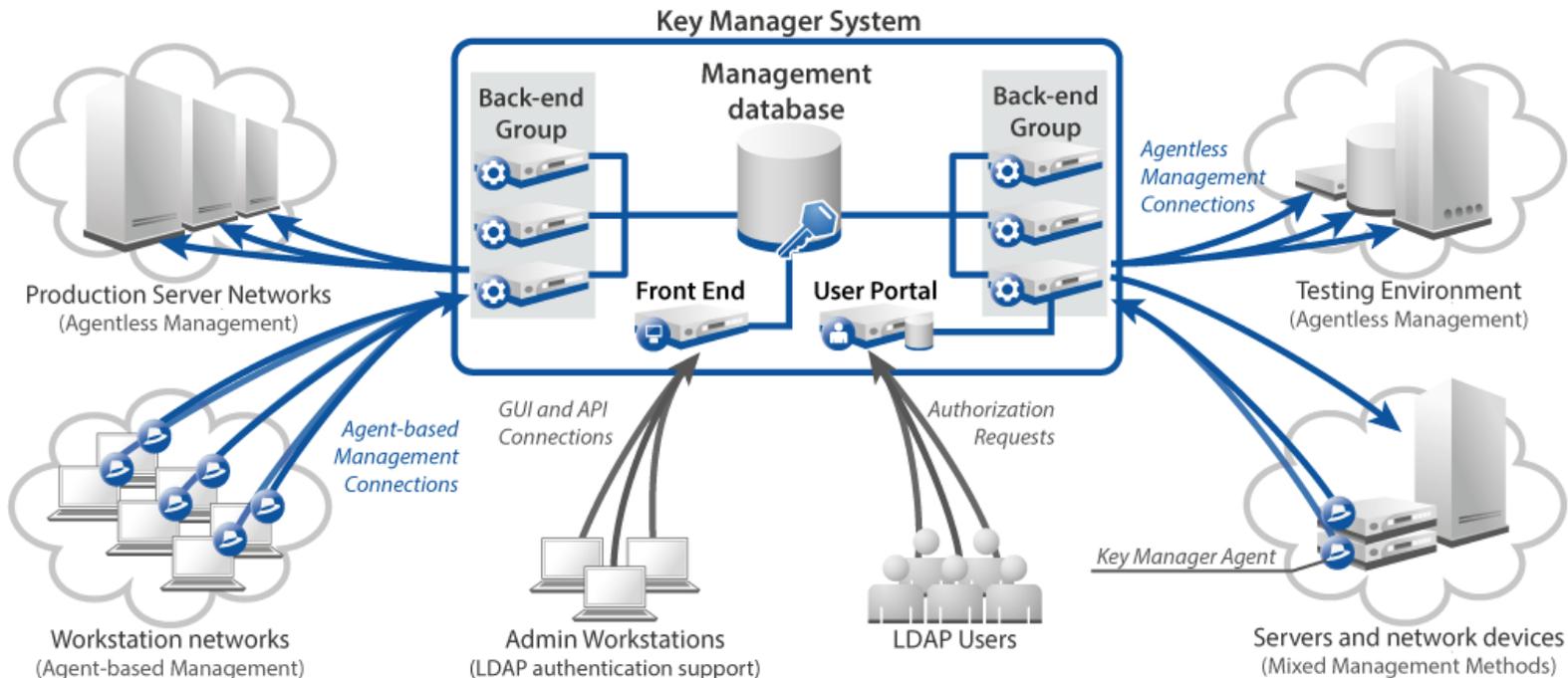
- Remove Obsolete Keys



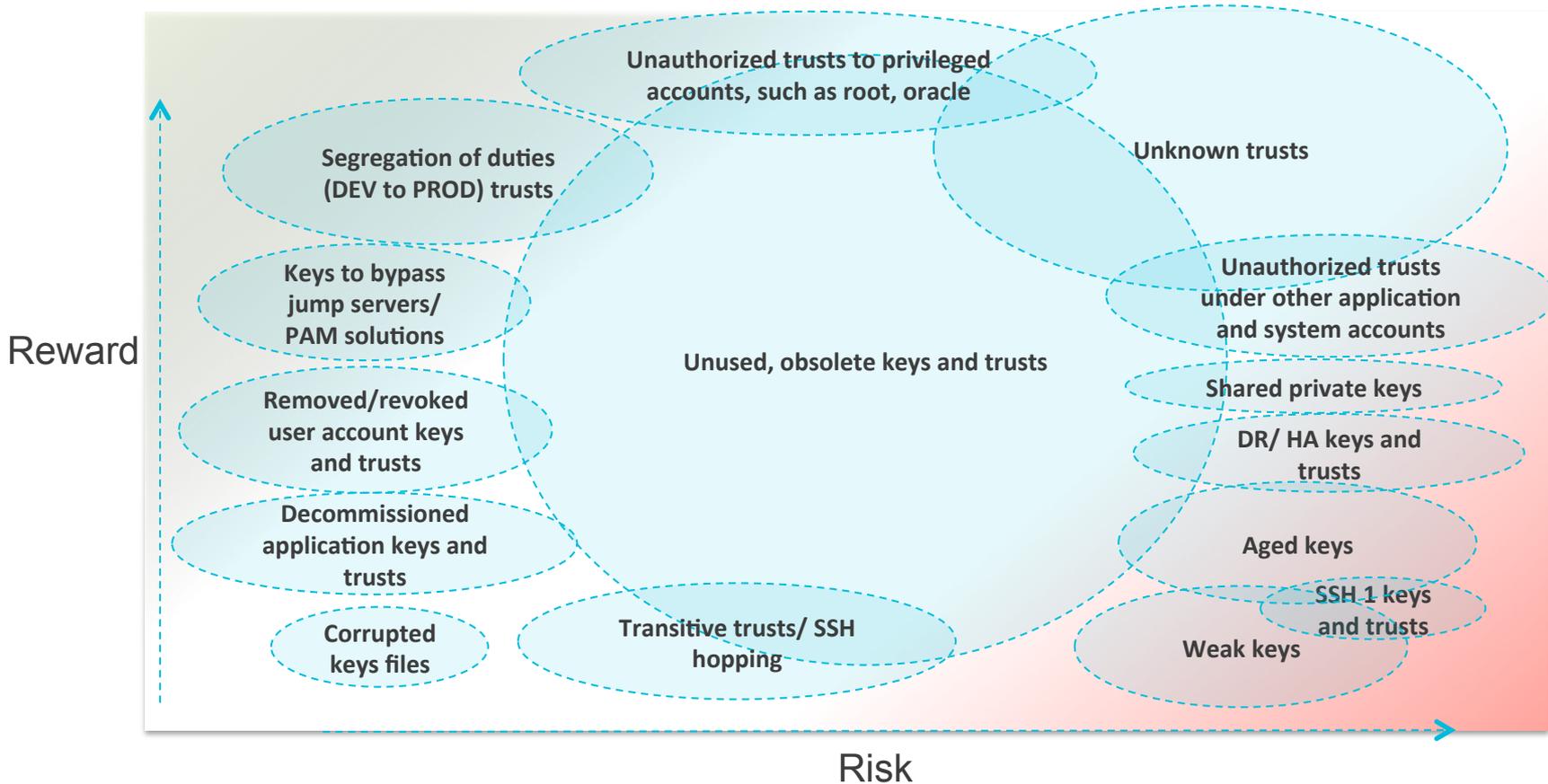
- Automate Life Cycle and Management of Your SSH



UNIVERSAL SSH KEY MANAGER ARCHITECTURE



THE RISK VS. REWARD IN POLICIES, REMEDIATION AND ROTATION



Success Case #1 Global Bank



Over 10,000 servers on their network

**1.5 million Secure Shell User Keys
identified**

**10% or 150,000 User Keys were
unknown**

AND ALSO HAD ROOT ACCESS

**No ability to monitor and enforce Secure
Shell user access**

Failed SOX & MAS Audit

UNIVERSAL SSH KEY MANAGER - LIVE DEMO

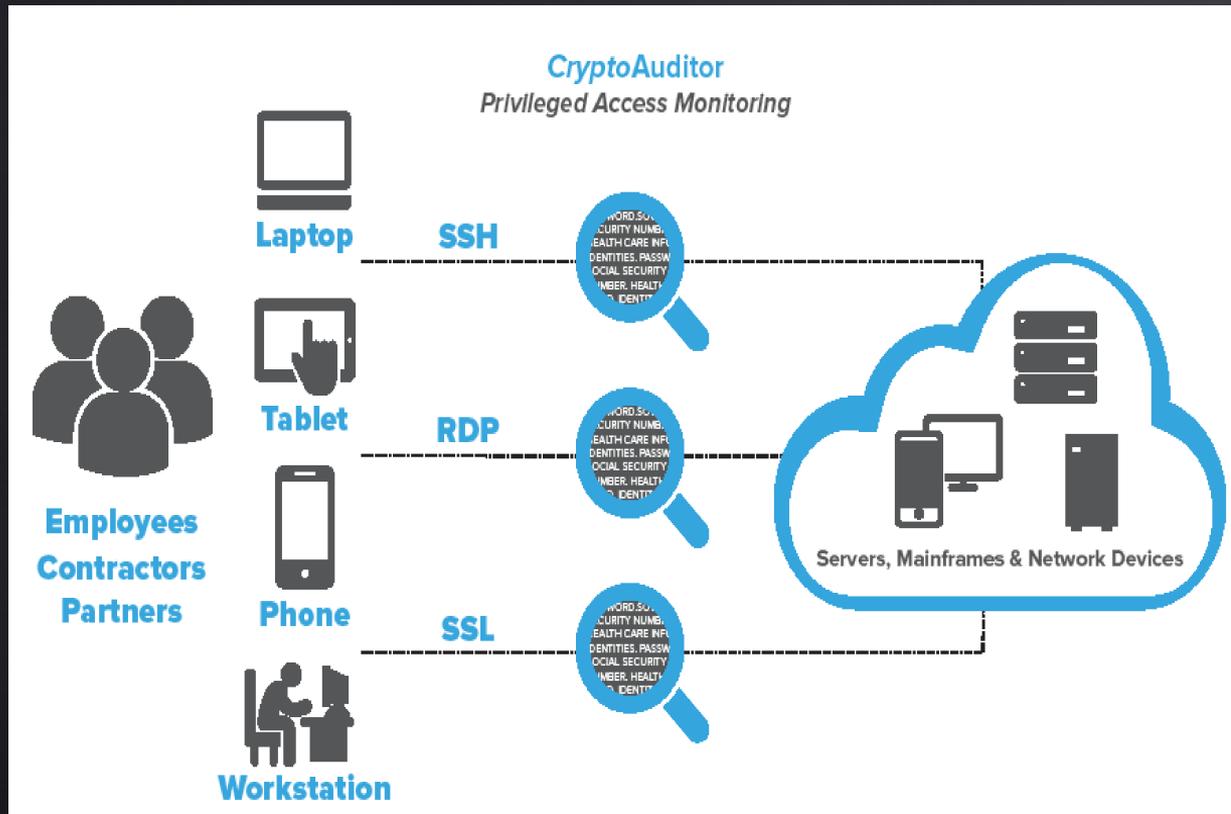


Linux servers in two segments: Production and Development
Various users including root

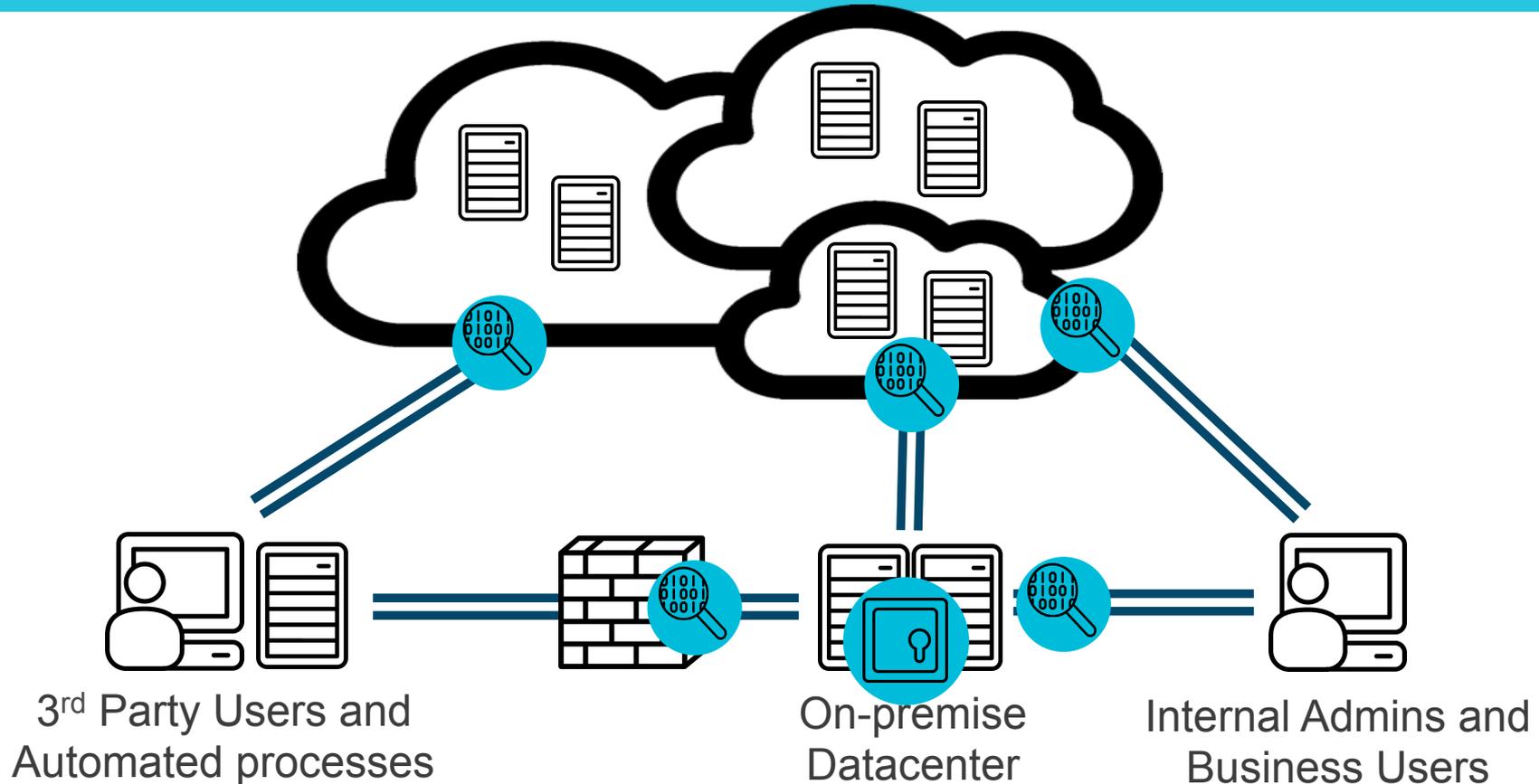
WHAT ABOUT THIRD PARTY OR INTERNAL ADMIN ACCESS?

CryptoAuditor

THE PARADOX: BLINDED BY ENCRYPTION



CRYPTOAUDITOR - DISTRIBUTED IN-LINE MONITORING, CENTRALIZED VISIBILITY AND POLICY ENFORCEMENT



Transparent
Agentless

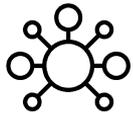
Strong
Authenticate

Audit
Encrypted
Traffic

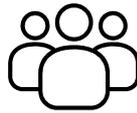
Integrate

Manage

- Installs in hrs, inline virtual appliance
- Bastion or transparent modes



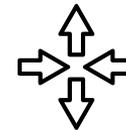
- Combined access control with LDAP, OTP, SecurID, Certificates...
- Usermapping



- Audit SSH, SSL, RDP, SFTP
- Central Forensic Video repository



- Send visible traffic to DLP, IDS, AV, SIEM...



- Real Time Actions, Alerts and Reporting





Success Case #2 Financial Institution

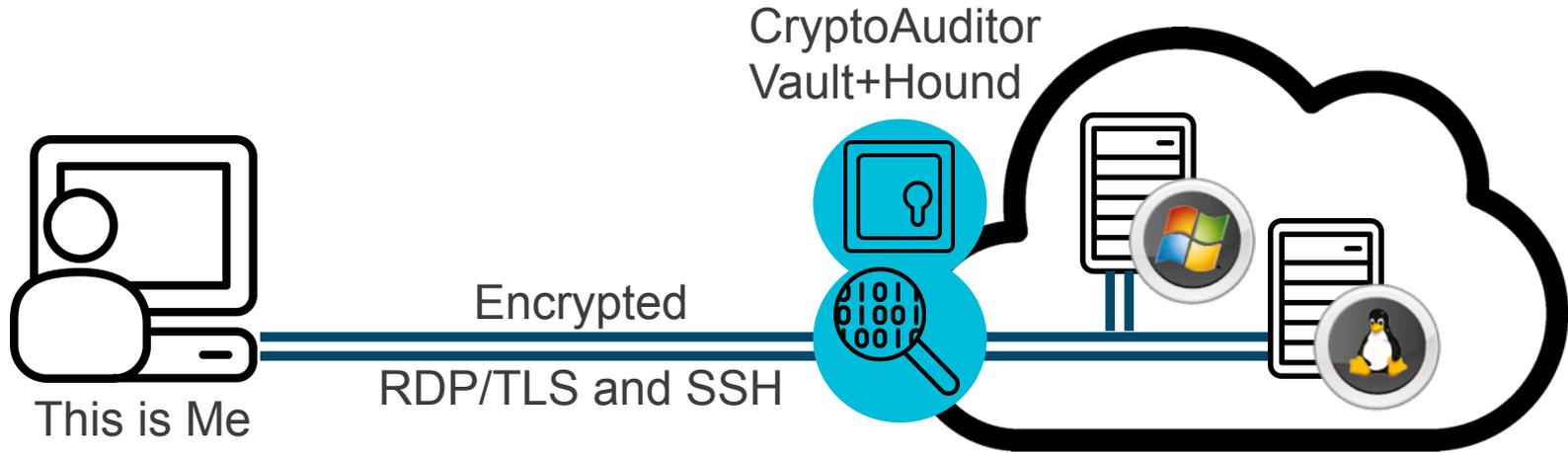
Multiple Data Centers

Many third party vendors and internal administrators

No ability to monitor their remote connections nor encrypted traffic content

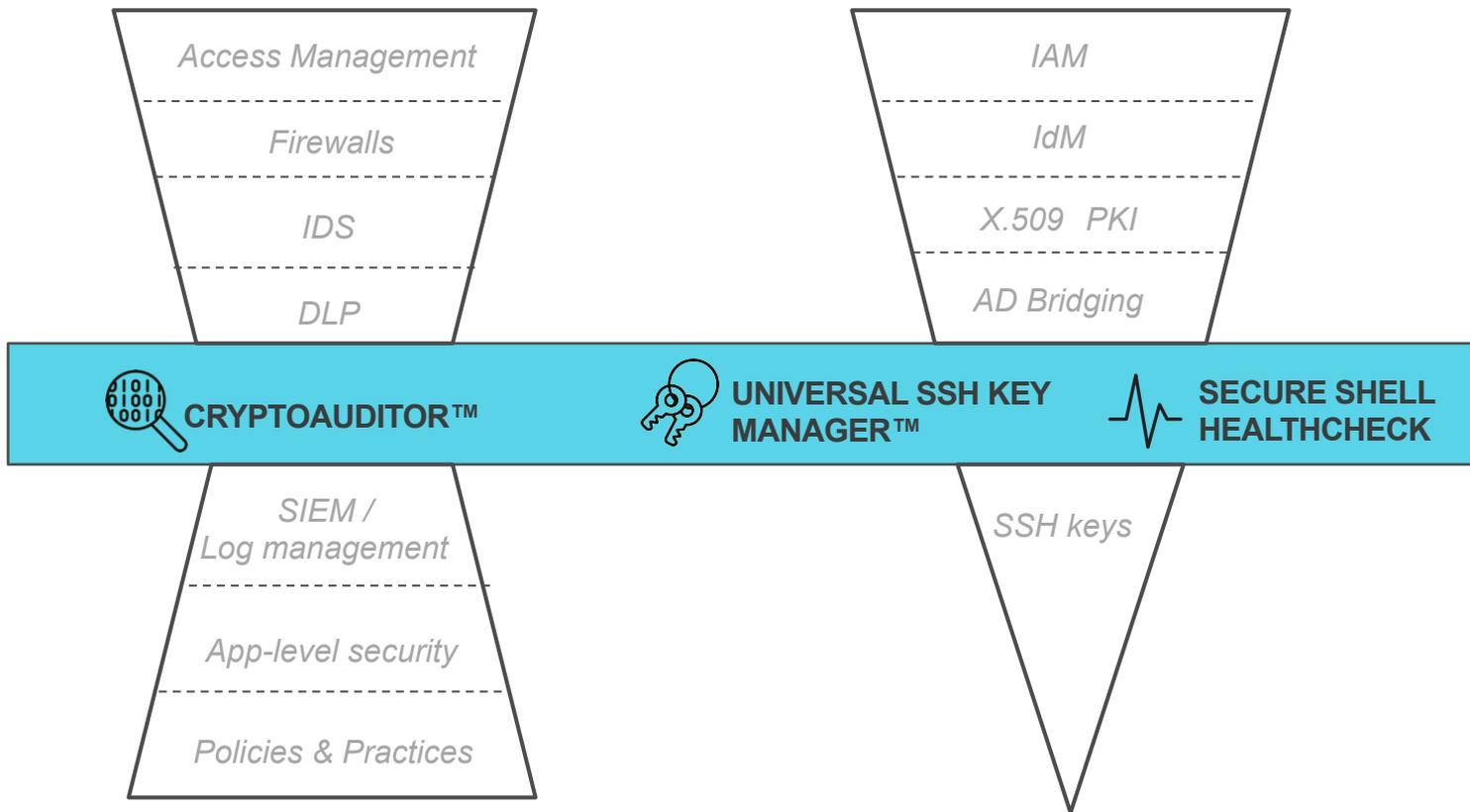
Must be PCI-DSS compliant

CRYPTOAUDITOR - LIVE DEMO



Transparent monitoring of remote terminal SSH access

FILLING THE GAPS IN YOUR PAM



POLL #1

What is your biggest concern regarding privileged access and encrypted data flows?

1. Monitoring and control of cloud access
2. Monitoring and control of internal admins?
3. Monitoring and control of 3rd party/ vendor access
4. Monitoring and control of automated M2M access
5. Inspection of encrypted incoming/ outgoing sessions and content

POLL #2

Where am I with my environment

1. I have tools in place that meet all my current and near term requirements
2. I have tools in place, but those do not address all the new needs I have
3. I don't have such tools in place, and there is no immediate need either
4. I don't have such tools in place and I'm searching for one.

What can *you* do now?

Try for yourself!

www.cryptoauditordemo.com

www.ukmdemo.com

NEXT STEPS

- **Be proactive! Download the free trial versions of Universal SSH Key Manager and CryptoAuditor**
- **Create a Project or use the flow of an existing project**
- **Contact Us or our partners**



THANK YOU

Contact:
elba.horta@ssh.com