PRIVILEGED ACCESS MANAGEMENT (PAM)

Controlling Access and Authorization enabling Interoperability

thycotic

JOSEPH CARSON (CISSP)

Chief Security Scientist | Thycotic

- 25+ Years Experience in Enterprise Security
- (ISC)² Information Security Leadership Award (ISLA®) Winner 2018
- Top 100 CISO's in 2020
- Security Professional of the Year 2020 and Blogger Finalist
- Frequent speaker at Cyber Security events globally
- Adviser to several governments, critical infrastructure, finance and maritime industries
- Author of 5 books including award winning Cybersecurity for dummies, Least Privilege for dummies and our latest Privileged Access Cloud security for dummies.
- Certified FX/MM Trader
- Implemented one of the worlds largest banks Grid Computing Farms

What is privileged access?

- Also Non-human accounts
- Local administrator
- Unix ROOT
- Service accounts
- Domain administrator
- CISCO Enable
- Application/SaaS Accounts
- Batch job/scheduled tasks/chron jobs
- Normal User Accounts with access to sensitive data

Admin/Security/ Helpdesk/3rd Party

Apps/API/RPA/ Service Accounts

Int./Ext. Business User or 3rd Party

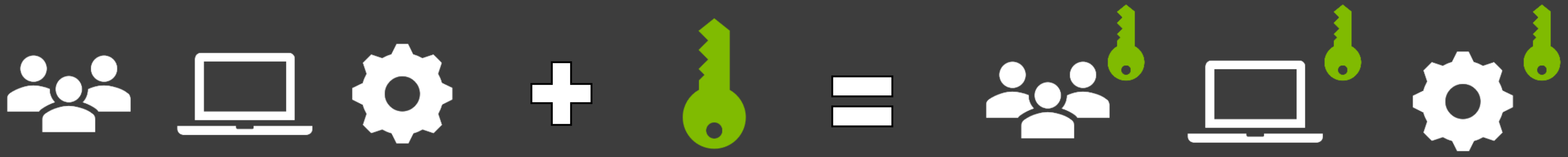
ALMOST ALL USERS ARE NOW PRIVILEGED USERS

Common Breach Causes

- Poor access management
- Insecure applications and APIs
- Misconfigured cloud storage
- Distributed Denial of Service (DDOS) attacks
- Overprivileged users
- Shared credentials
- Password only security controls
- Securing third-party access and remote employees
- Shadow IT

What can we do to reduce the Risks?

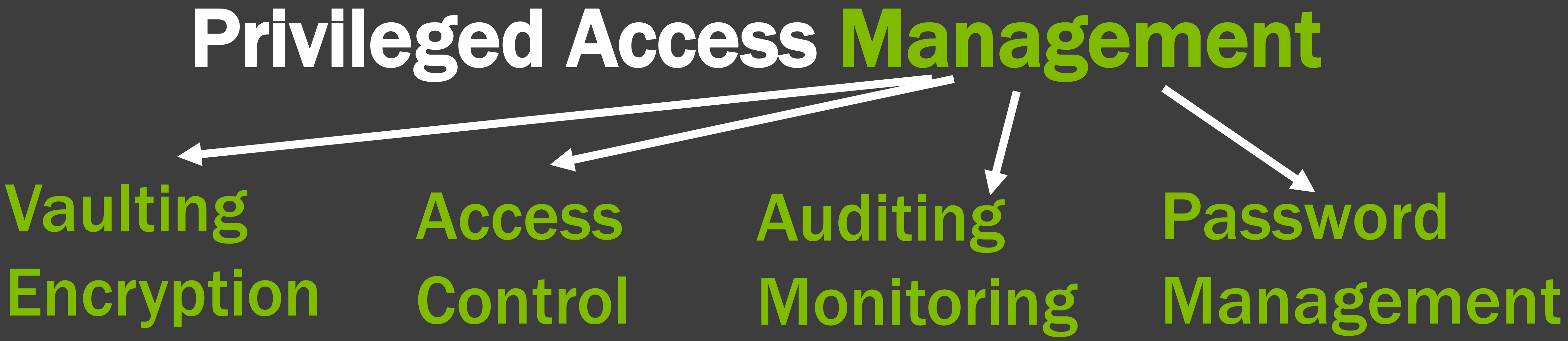
Privileged Access Security



Users, Computers, Applications

PRIVILEGE

PRIVILEGED Users, **PRIVILEGED** Computers
PRIVILEGED Applications



Privileged Access **Management**

- Vaulting Encryption
- Access Control
- Auditing Monitoring
- Password Management

Privileged Access Management

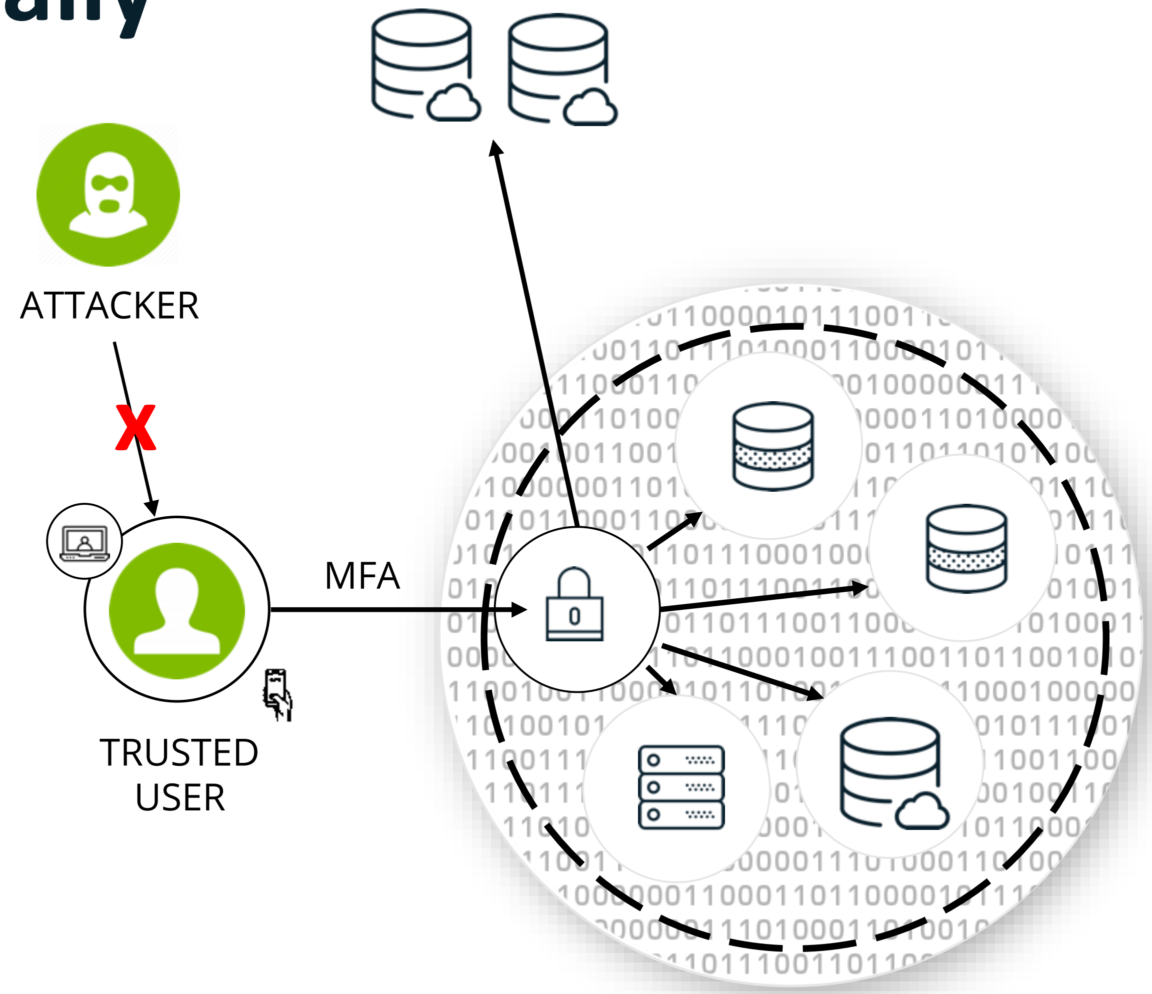
- IAM Integrations
- Integrations with Enterprise Solutions, like SIEM and Systems Management
- Multi-Factor Authentication
- Securing DevOps
- Remote Access Integration
- API for automation and seamless integrations
- Session Launching and Recording
- Principle of Least Privilege Enforcement
- Enforce Zero Trust based on Adaptive Risks

No longer about managing a privileged account but enabling secure usage of privileged access.

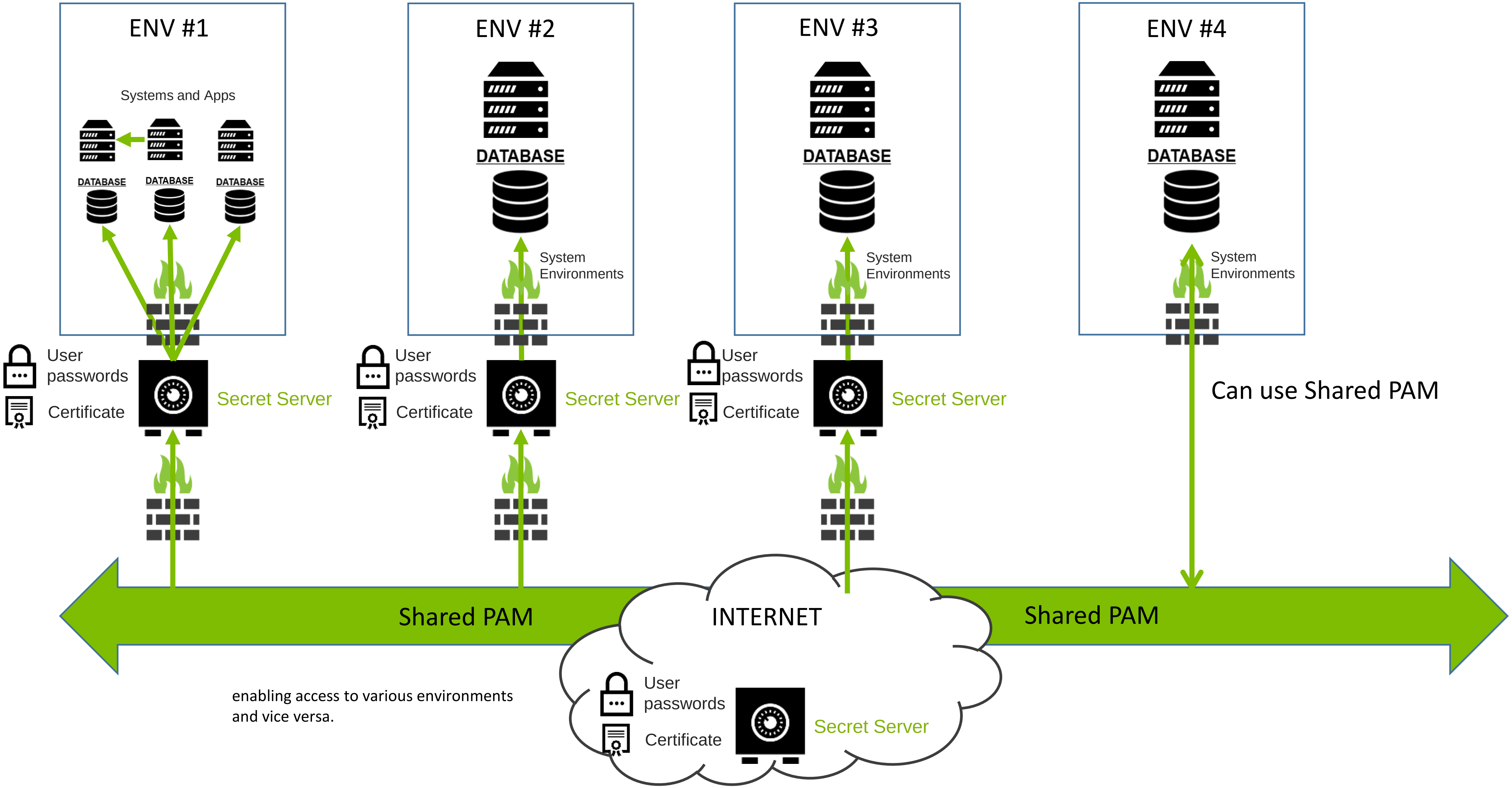
Classifying Trust Dynamically

Adaptive Security

1. Secure Digital Identity
2. Multi fA (Trust Level)
3. Secure Privileged Access
4. Secure Data Vaults
5. Check Reputation
6. Check Behavior
7. Check Risks
8. Secure Access to both On Prem and Cloud



Thycotic PAM Enabling Interoperability between environments securely



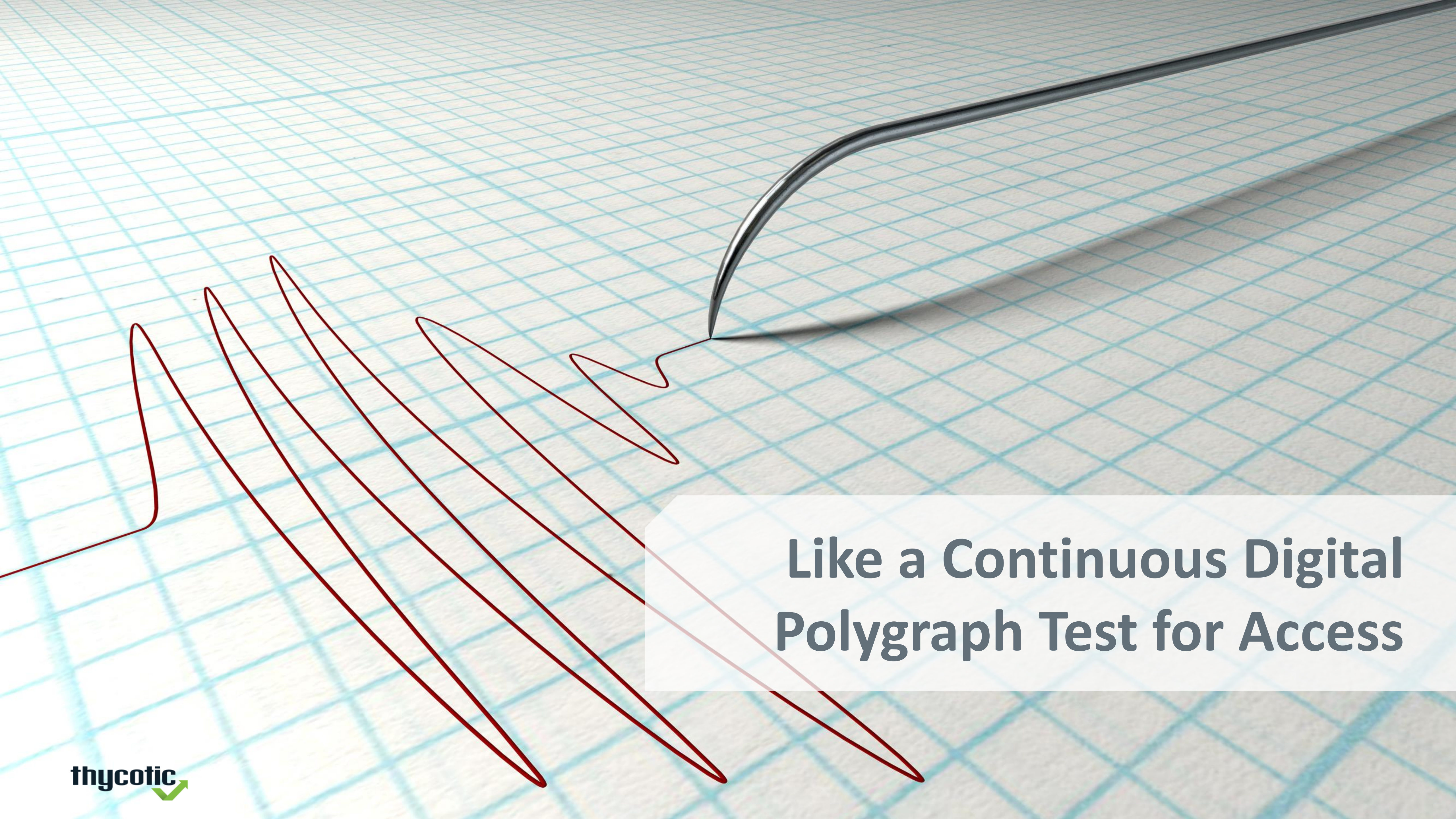
enabling access to various environments
and vice versa.

Zero Trust

Zero trust assumes any user or system that accesses the network, services, applications, data, or systems must be verified. To gain authorized access, trust must be earned by the prospective user through verification.

BUILDING DIGITAL TRUST

thycotic



Like a Continuous Digital Polygraph Test for Access

”Understanding hacker techniques and processes is the best way to defend against cyber attacks, and focusing on business risks is the best way to get security budget.“

– Joseph Carson