VECTORZERO™

Unrivaled *Security*

Addressing Residual Risk Beyond NIST 800-53-5:

Automated Moving Target Defense, Confidential Computing & Post-Quantum

Oregon Cyber Resilience Summit

10.4.23

Andrew Blume

VP of Sales

Andrew Blume ‘12

Go Ducks!

Unrivaled *security without complexity or compromise*

VectorZero

Technical staff are cleared, former IC Officers

100% US-Owned & Operated

All code developed in Reston, Virginia

What is NIST 800-53-5

Over 1,000 Security Controls

Unrivaled *security without complexity or compromise*

Attack Vectors & Methods

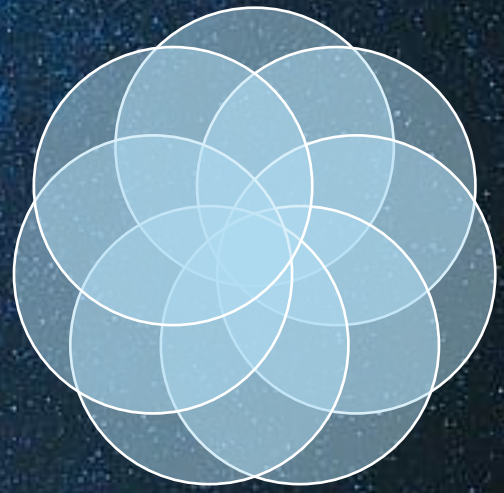
And Practical Organizational Needs

Protecting Against:

- Advanced Persistent Threat
- Side-Channel Attacks
- Cloud Threat Actor
- Quantum Computing Decryption
- Insider Threat
- Privileged Software Attacks
- Legacy Vulnerability

Requirements:

- Chain of Trust Edge to Cloud
- Rapid Build / Tear Down
- Data Governance / Confidential Secure Collaboration
- Low to High Transfer
- Ease of Integration & Use
- Managed Attribution
- Encrypted Analysis



Beyond NIST 800-53-5

Automated Moving Target Defense

Stand up high assurance, zero trust, NIST 800-53-5, enclaves within minutes from anywhere

Confidential Compute

Data protected while in process & memory without compromising speed or useability

Post Quantum

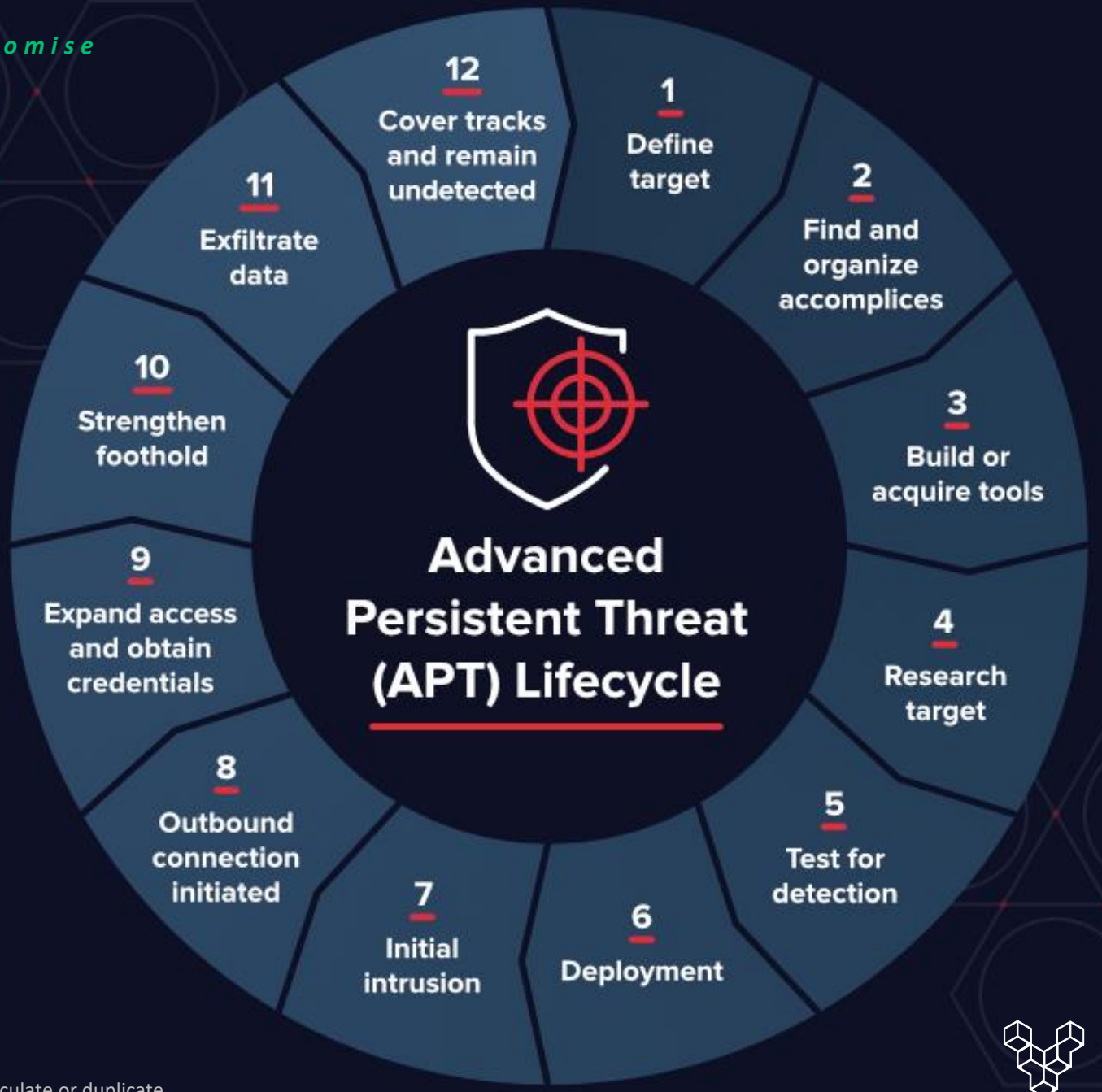
Cryptographic systems that are secure against quantum computers

APT Anatomy

Long Shelf-Life Breaches

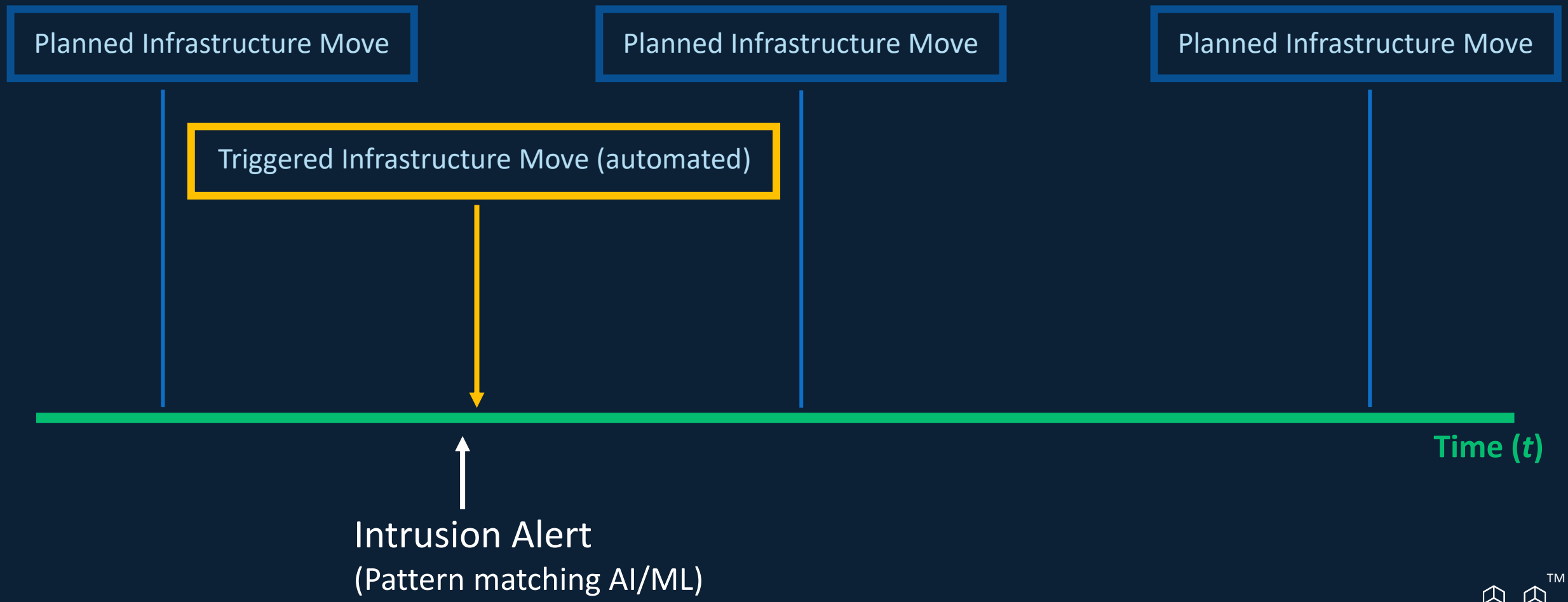
273 Days*

IBM 2022 Cost of a Data Breach Report



Automated Moving Target Defense (AMTD)

Preventing adversaries from gaining a foothold by changing your infrastructure



Unrivaled ***security without complexity or compromise***

The Moving Components

Each AMTD move orchestrates changes in:

- API gateway servers configurations
- Backup NoSQL database endpoint
- Certificate manager server configuration
- Cisco firewall
- Palo Alto firewall
- Content delivery network configuration
- CSP network firewalls
- DNS configuration
- DNSSec configuration
- Isolated virtual networks
- Network address translation gateways
- NoSQL database repository
- NoSQL database endpoint
- Object storage endpoint
- Object storage repositories
- Routers
- Subnets
- Switches
- Threat detection configuration
- TLS certificates
- VPN servers by region
- Web application firewalls for content
- Additional security policy check against NIST 800-53-4 configuration
- App (IAM) accounts
- App (IAM) group
- App (IAM) policies
- Asymmetric encryption key
- Auditing accounts
- Auditing log repository
- Backup Auditing log repository
- Backup NoSQL database repository configuration
- Backup services configuration
- Hardware Security Module configuration
- (IAM) accounts
- (IAM) policies
- Identity Access Management (IAM) group
- Operating system logging repository
- Security group configuration
- Security policy checks configuration
- Sensitive data machine learning
- Symmetric encryption keys
- VPN certificates
- Web application firewalls for authentication & authorization
- Object storage repository security policy

Ephemeral Vaults, Infrastructure As Code

An Automated Moving Target Defense

Provision Vault In Minutes

Servers
Networking
Storage
Accounts
Firewalls
Encryption Keys

Run Workload Fully Encrypted

Deploy any analytics, AI/ML, or other tools

Save Data in Storage, Deprovision Vault

Reducing attack surface to near zero, and destroying any implanted malicious code

Provision *New* Vault with Saved Data & Users

Patched, updated, & available anywhere on the public fabric

Post Quantum

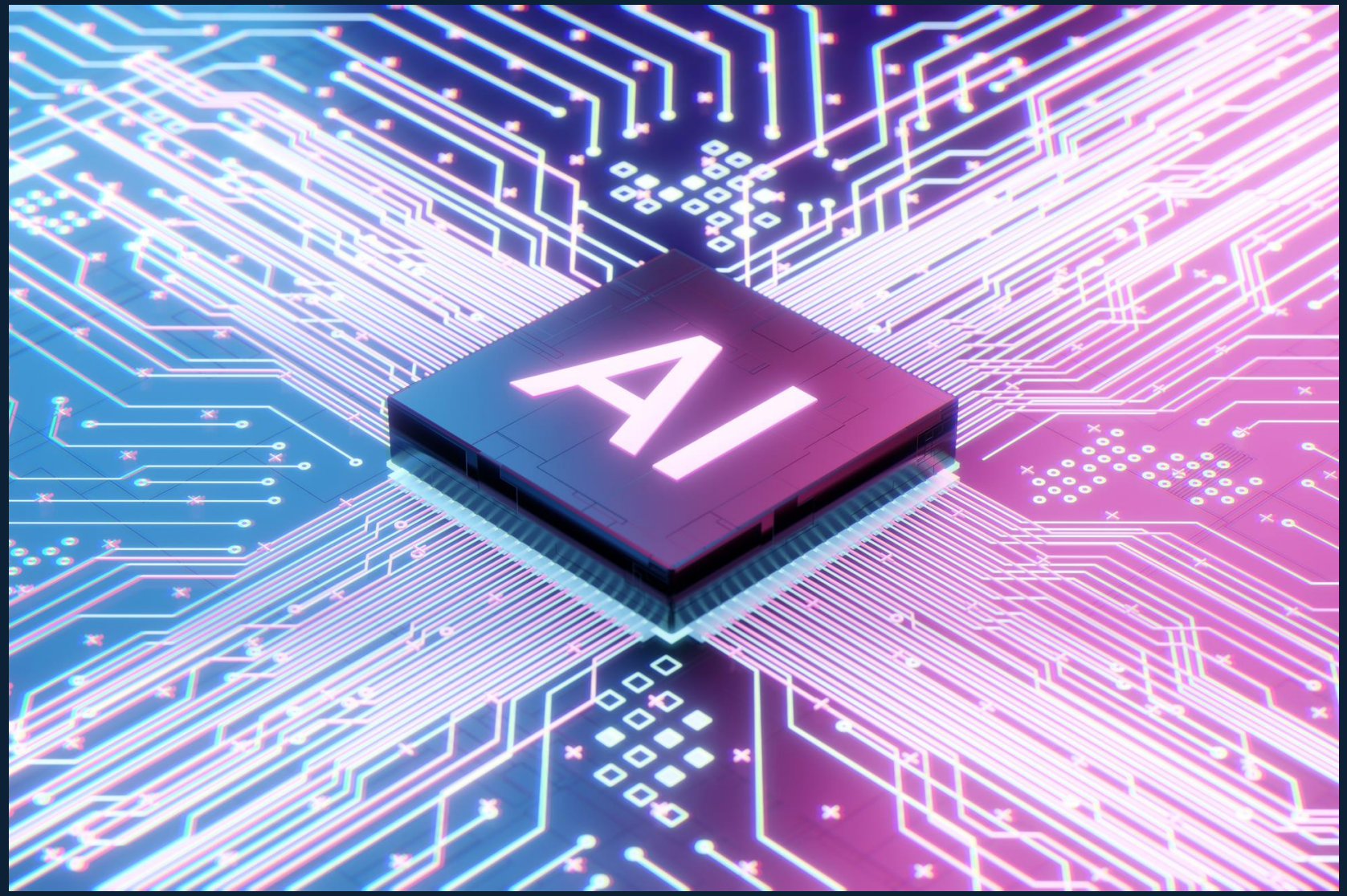
Post Quantum Encryption

With software-defined AMTD, we rapidly and easily interchange encryption algorithms.

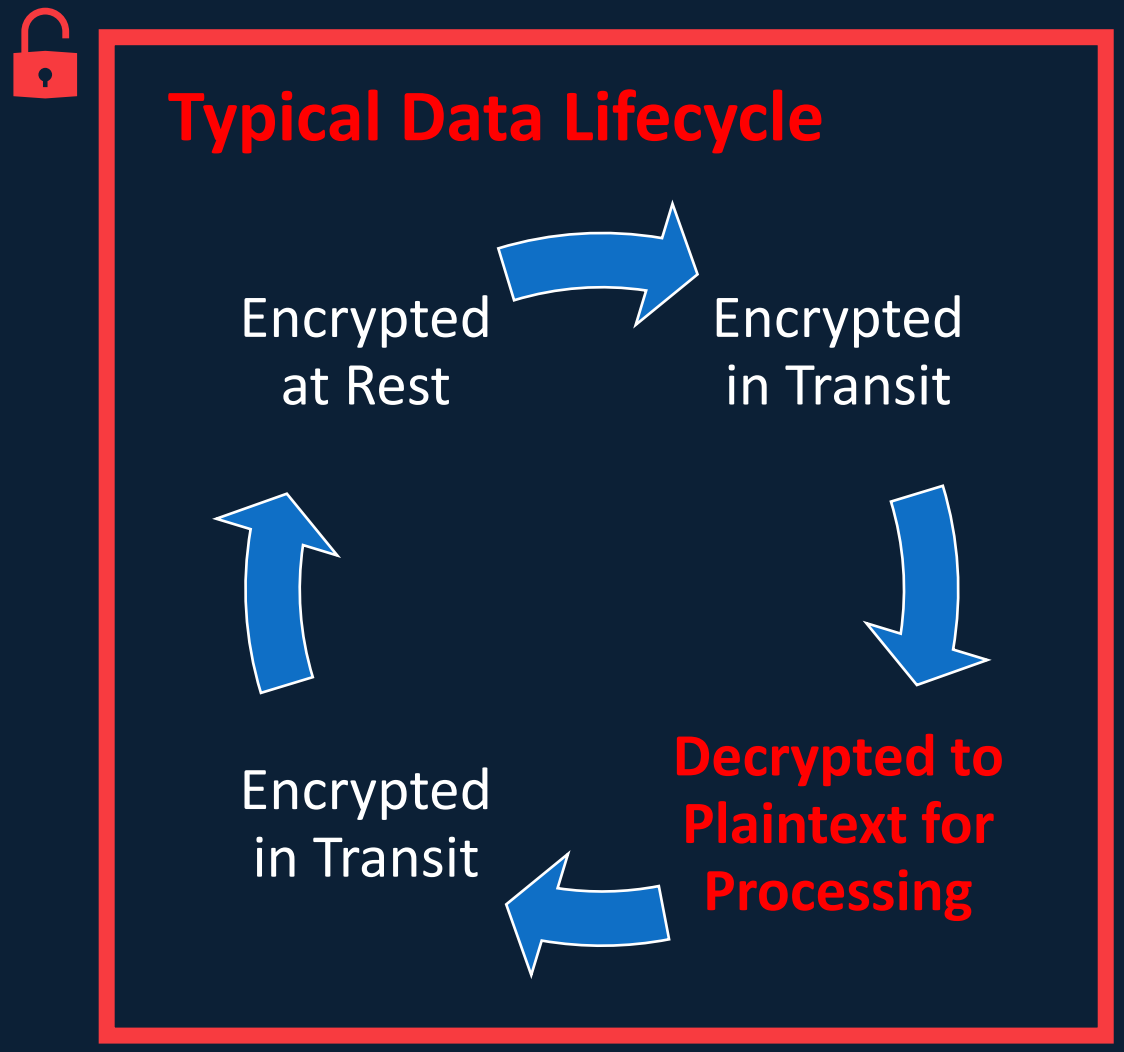
- FIPS 140-2 L3
- BIKE
- Kyber
- S2n-tls
- S2n-quic
- Elliptic Curve
- Fully Homomorphic
- Other algorithms

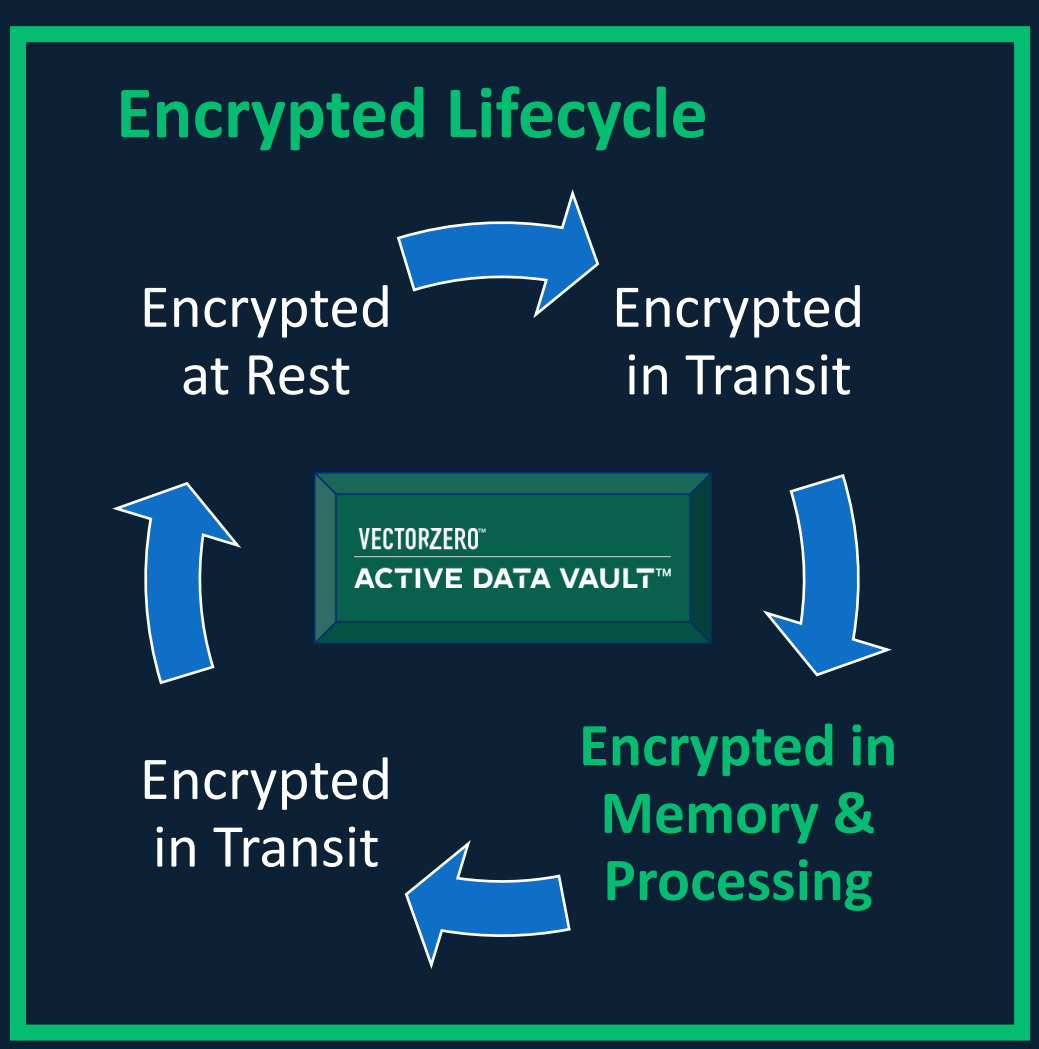
Compatible with existing + future post-quantum algorithms

What About AI



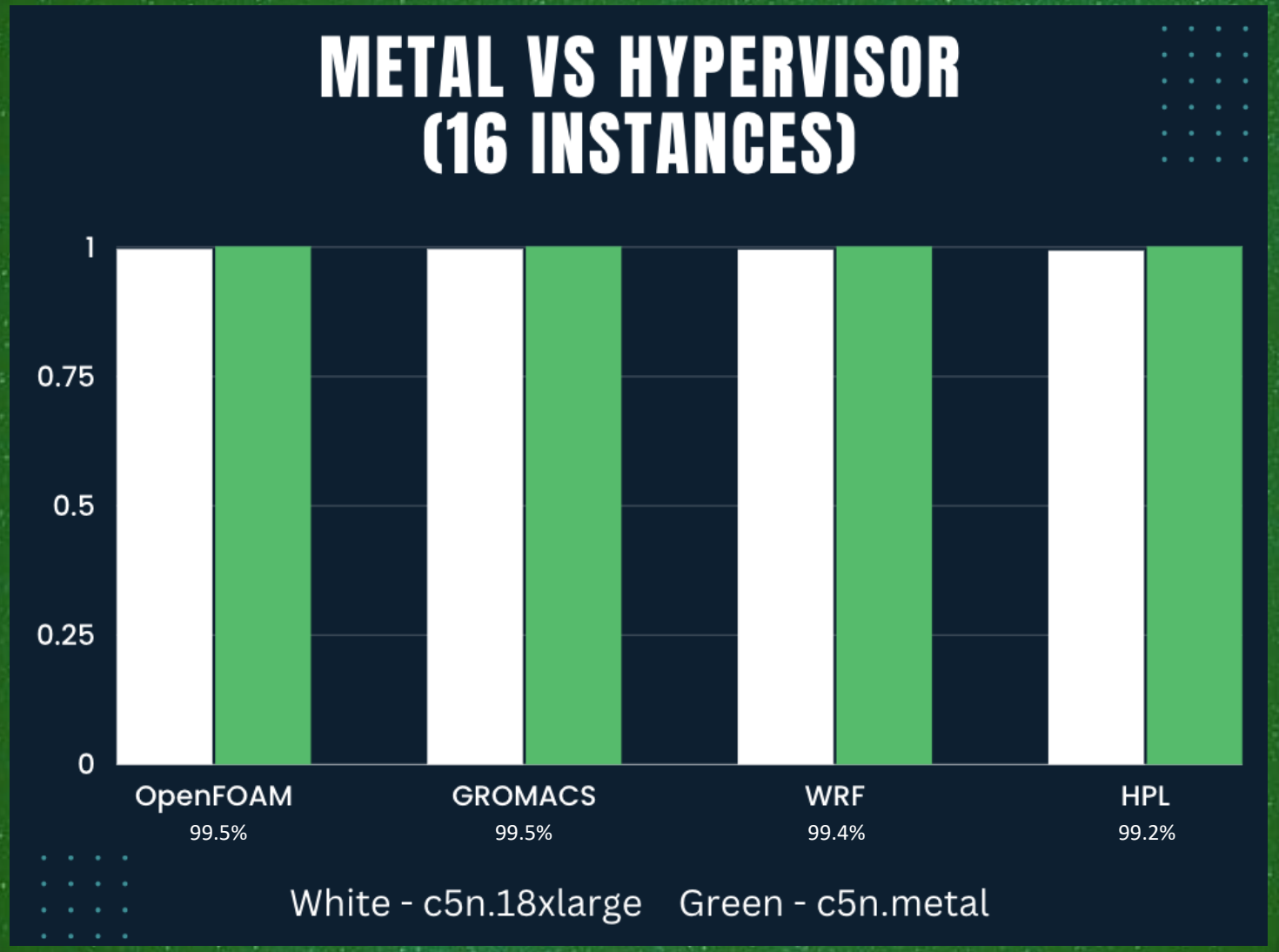
Confidential Computing





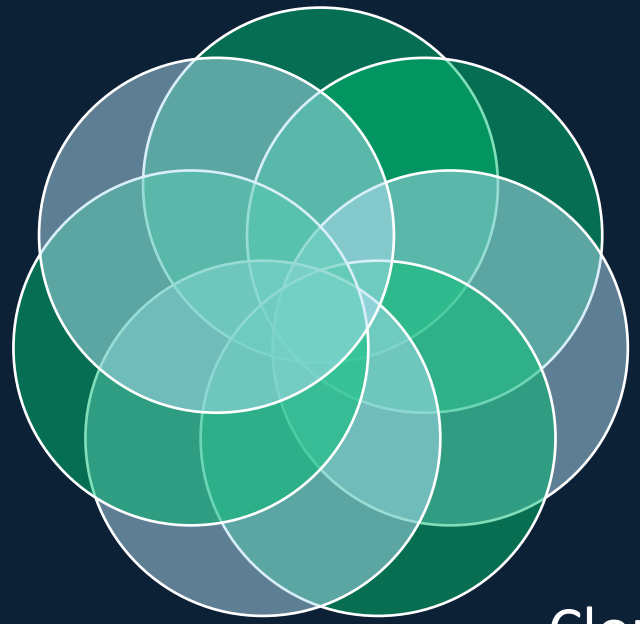
Confidential Computing Performance Overhead

AWS Comparison of Bare Metal vs Amazon Confidential Computing (1)



Insider Threat & Community Behavior

Data is accessible to your protected workload, yet unreadable to:



Platform Administrators

Threat Actors

Data Scientists

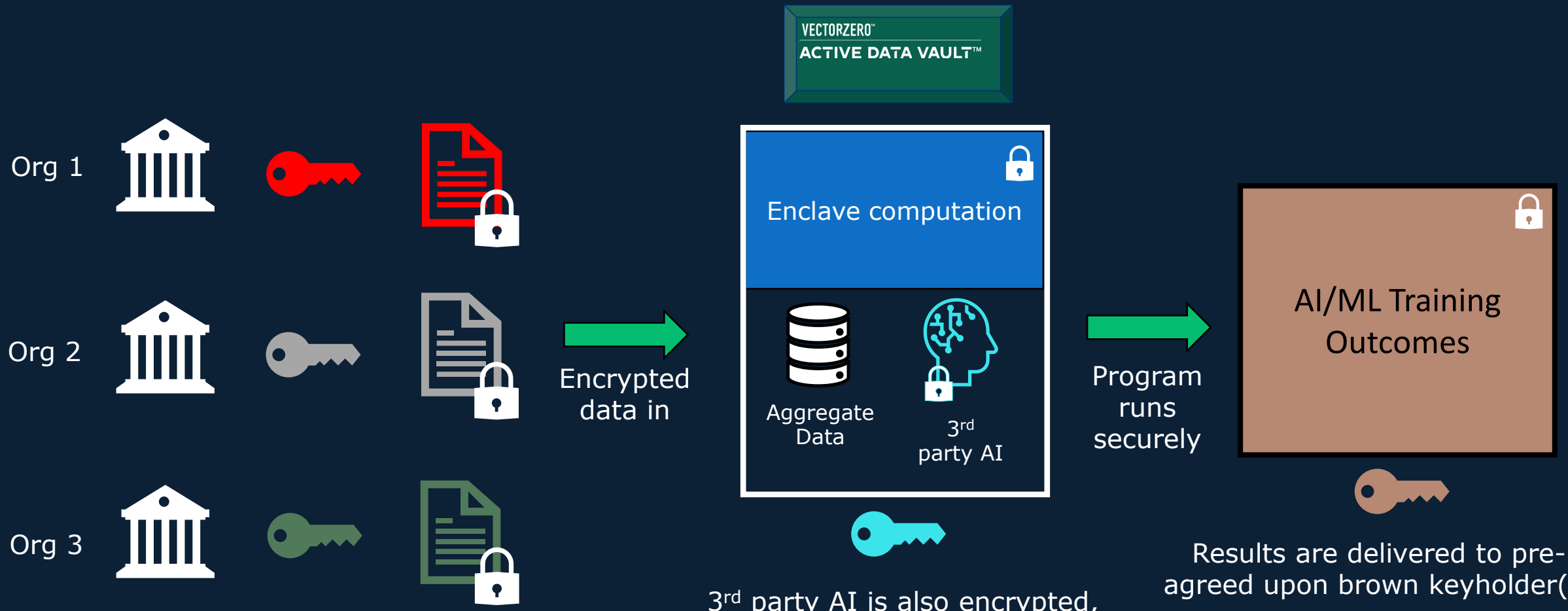
3rd Party Partners

Data Engineers

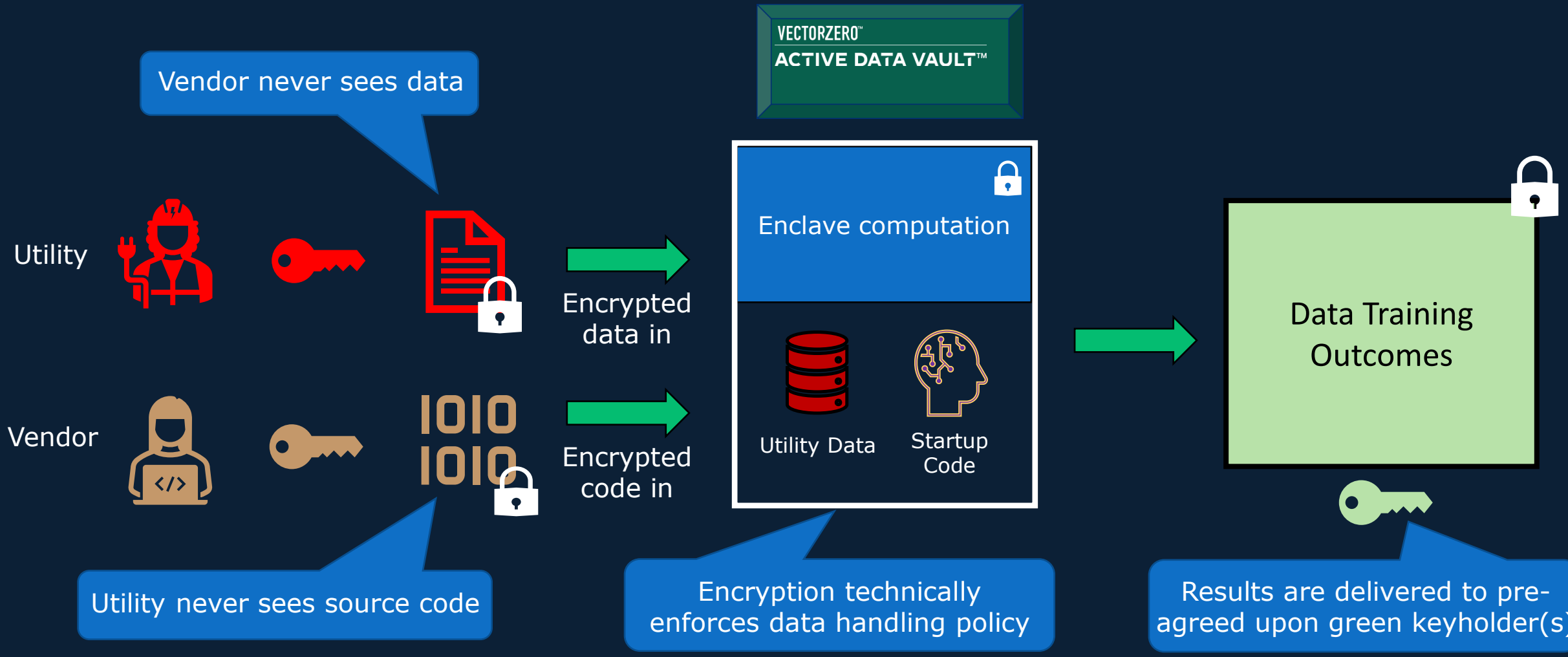
Hypervisors

Cloud Service Providers (Paige Thompson)

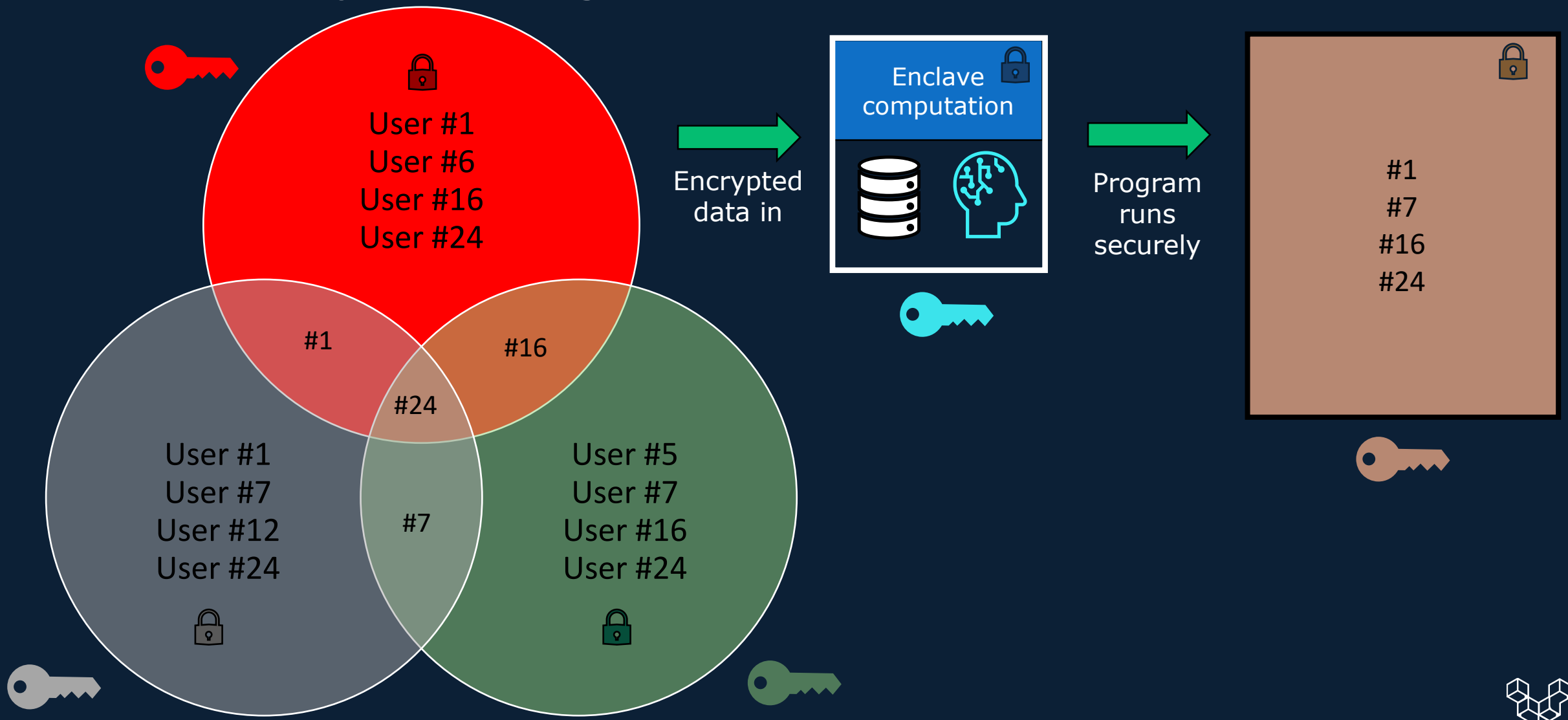
Secure Multi-Party Computation (SMPC) Example: AI/ML Training



Secure Multi-Party Computation Example: Utility Innovation



SMPC Example: Finding Common Devices



Attestation: Don’t Trust, Authenticate

Authentication for Supply Chain & Servers

- ADV takes measurements of CPU, bootloader, firmware, OS, software, and data.
- ADV uses AI/ML to adjudicate attestation measurements against corporate security policy.
- If adjudication is successful then release compute, connection, data, or key.

Technical Trust Vectors

Verify more, trust less with supply chain attestation

Typical Technical Trust Vectors

- CPU Manufacturer
- Motherboard
- Boot Loader
- Firmware
- Operating System
- Software Vendors
- Cloud Service Provider

Confidential Computing Technical Trust Vectors

- CPU Manufacturer

Beyond NIST 800-53-5

Automated Moving Target Defense	**Stand up high assurance, zero trust, NIST 800-53-5, enclaves within minutes from anywhere**
Confidential Compute	**Data protected while in process & memory without compromising speed or useability**
Post Quantum	**Cryptographic systems that are secure against quantum computers**

EPRI Pilot Demonstration

Cyber Physical

- Secure isolated backups for configuration files & other sensitive data
- NERC CIP ready cloud environments & migrations
- Secure Multi Party Computation (SMPC)
- Secure AI/ML

Thank You

VECTORZERO™

Unrivaled *Security*

Andrew Blume
VP, West Coast Sales

Andrew.Blume@vectorzero.ai
818-429-2357

MADE IN THE USA