OpenSSL CONFERENCE

KEYFACTOR

INFOSEC GLOBAL
a Keyfactor company

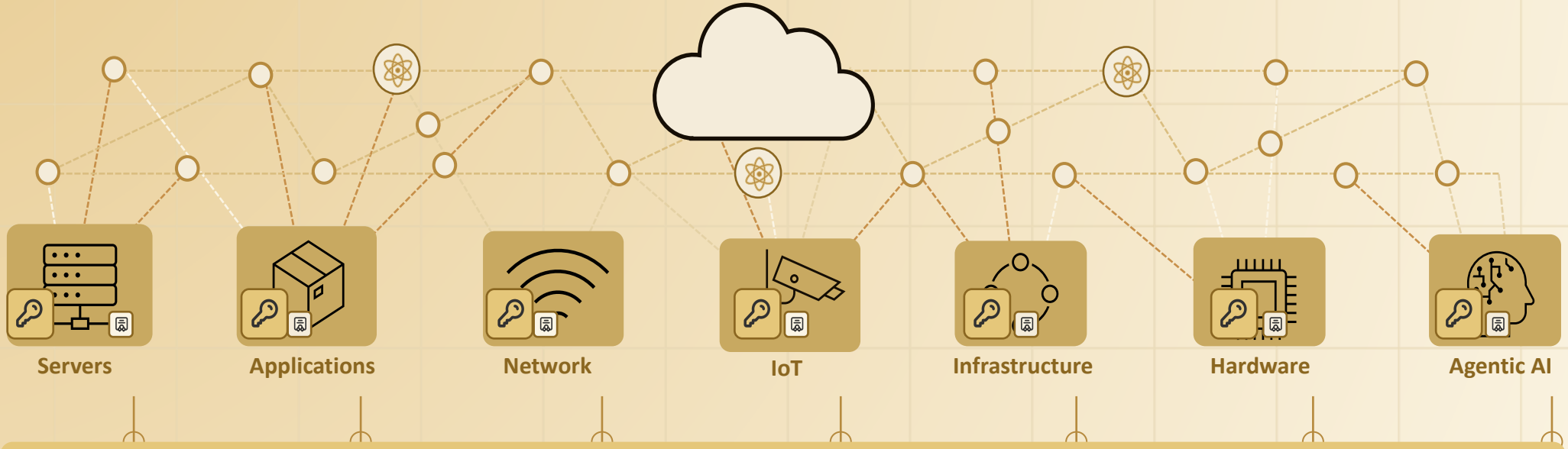
From Hidden Cryptography to Enterprise Risk

Securing Ecosystems for Cryptographic Compliance and Post-Quantum Readiness

Dr. Vladimir Soukharev, VP, Cryptographic Technology, Keyfactor

15-Oct-26

Cryptography is critical infrastructure



Certificates & Identities

Keys & Secrets

Ciphers & Algorithms

Libraries & More

PKI, CLM, IAM

Cryptographic risk is a blind spot for CISOs and boards

More than half of enterprises aren’t actively monitoring their cryptographic assets.

Wakefield Research, June 2025

OpenSSL CONFERENCE

Five dimensions of cryptographic risk

1

Cryptographic Risk

Vulnerabilities

Are weak, outdated or insecure cryptography still in use?

2

Cryptographic Risk

Keys in the Wild

Do we know where all our sensitive keys are, and how they are protected?

3

Cryptographic Risk

Compliance

Are we exposed to fines due to lack of cryptographic visibility and controls ?

4

Cryptographic Risk

Quantum

Are we prepared to migrate to Post-Quantum Cryptography ?

5

Cryptographic Risk

Malicious Code

Could attackers exploit strong cryptography against us?

Business Impacts

- Balance Sheet Exposure
- Regulatory Compliance
- Operational Resilience

OpenSSL CONFERENCE

Why cryptographic risks are hard to manage

CRYPTOGRAPHIC RISK
Implementation Failure

Weak design or vulnerable cryptographic components

CRYPTOGRAPHIC RISK
Operations Failure

Poor key and certificate management, overlooked cryptographic configuration.

CRYPTOGRAPHIC RISK
Data Protection Failure

Failure to protect sensitive data with strong, compliant encryption.

Enterprise App

Configuration

Compute

In-Transit

Authentication

3rd Party Dependencies

Identities

Hardware

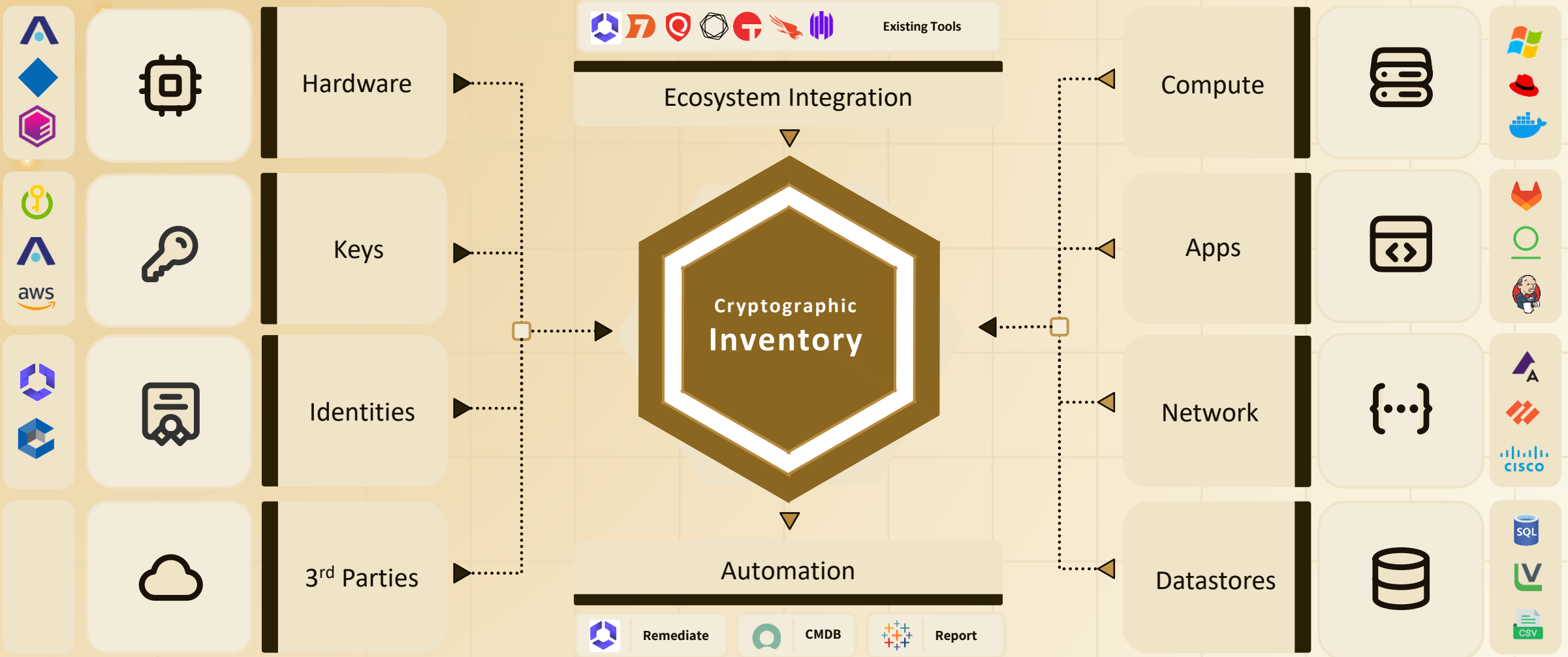
At-Rest

Signing

Technical Impacts | High Costs | Manual Workload | Long Migration | High Fragmentation

How to identify and prioritize cryptographic risk

A golden source for cryptographic inventory



Map your cryptographic inventory journey

Phase 1

Design

Get Executive Support, define Scope, use-cases, priority & objectives.

Phase 2

Validate

Explore, define, and validate the Inventory Approach to prioritize implementation.

Phase 3

Productize & Learn

Productize Initial Use-Cases within high value environment.

Example Ecosystem

GitLab · CROWDSTRIKE · tenable · KEYFACTOR

Phase 4

Expand & Automate

Scale Use-Case through Automation & Start Remediation.

Example Ecosystem

servicenow · Azure · JFrog ARTIFACTORY · aws

Phase 5

Scale with Confidence

Scale Deployment to additional Use-Cases & Ecosystem.

Example Ecosystem

Strategic Vendors Long-Term Partnership

Automated discovery reduces risk and supports compliance

Compliance drivers | Cryptographic inventory matters

Organizations face **tightening regional and industry-specific regulations** requiring cryptographic visibility

NIST / FIPS 140-3

Mandates validated cryptography tracking.

CMMC / FedRAMP

Requires visibility into cryptographic modules.

EU PQC Roadmap & OMB M-23-02

Inventories of quantum-vulnerable systems.

GDPR & ISO 27001

Strong encryption controls and auditability.

CBOM vs. Cryptographic Inventory

	CBOM (Cryptographic Bill of Materials)	Cryptographic Inventory
Scope	Focuses on built-in cryptographic capabilities within a specific software release	Provides an enterprise-wide view of all cryptographic assets, usage, and risks
Data Sources	Derived from source code or a software bill of materials (SBOM)	Aggregates data from live systems, applications, devices, and infrastructure
Visibility	Lists algorithms, libraries, and supported key sizes	Includes keys, certificates, protocols, configurations, policies, vulnerabilities
Operational Insight	Static view only; does not show how cryptography is actually used	Provides full context — shows how, where, and why cryptography is applied
Update Frequency	Updated only when software is released	Continuously updated as systems, policies, and infrastructure change
Strategic Value	Supports audit readiness for individual applications	Enables holistic cryptographic risk management, compliance reporting, and post-quantum readiness

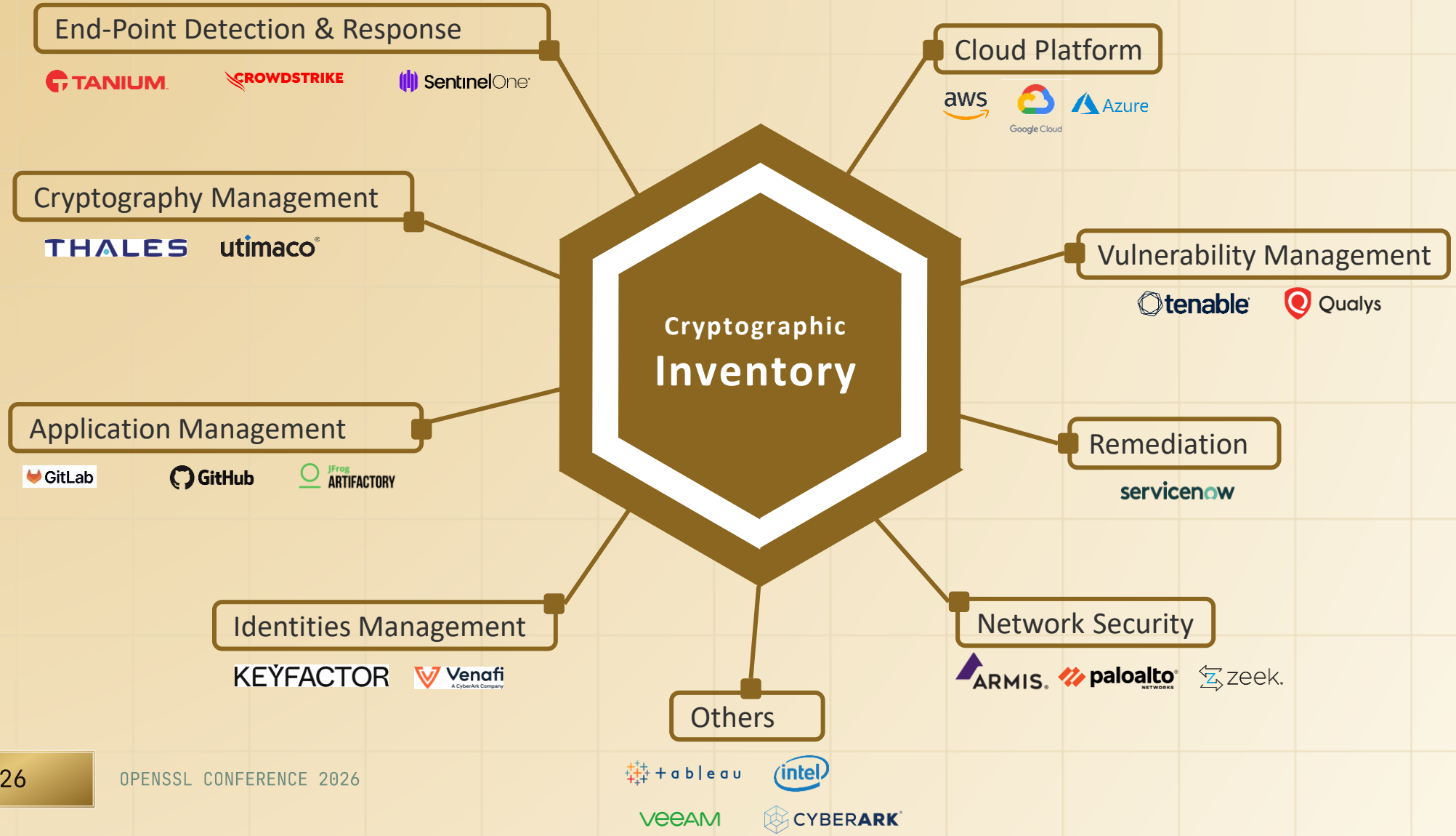
A CBOM is foundational, but a cryptographic inventory is strategic.

CBOM gives visibility into what's built in.

A cryptographic inventory delivers continuous insight into what's deployed, configured, and at risk.

Requirements for building a complete cryptographic inventory

Requirement 1: Leverage the corporate ecosystem



Requirement 2: Enable a complete inventory

Keys Inventory

- SSH Keys
- RSA & ECC Keys

Tokens Inventory

- JWT Tokens
- JWE Tokens

Keystores Inventory

- Key Stores
- Trust Stores

Certificates Inventory

- Root CA
- Intermediate CA
- SSL / TLS
- Personal Certificate
- S/MIME Encryption
- Digital Signing
- Time Stamping

Cryptographic Libs Inventory

- Classical Libraries
- PQC Ready Libraries

Algorithms Inventory

- Classical Algorithms
- Post-Quantum Algorithms

Ciphers Inventory

- Crypto Protocols
- Cipher Suites

Locations

- Hosts
- Applications
- Network
- KMS, HSMs
- And more

Requirement 3: Streamline resolution processes

Cryptographic
Compliance

Detect Issues

Cryptographic
Prioritization

Prioritize Findings

Cryptographic
Actions

Build Actions

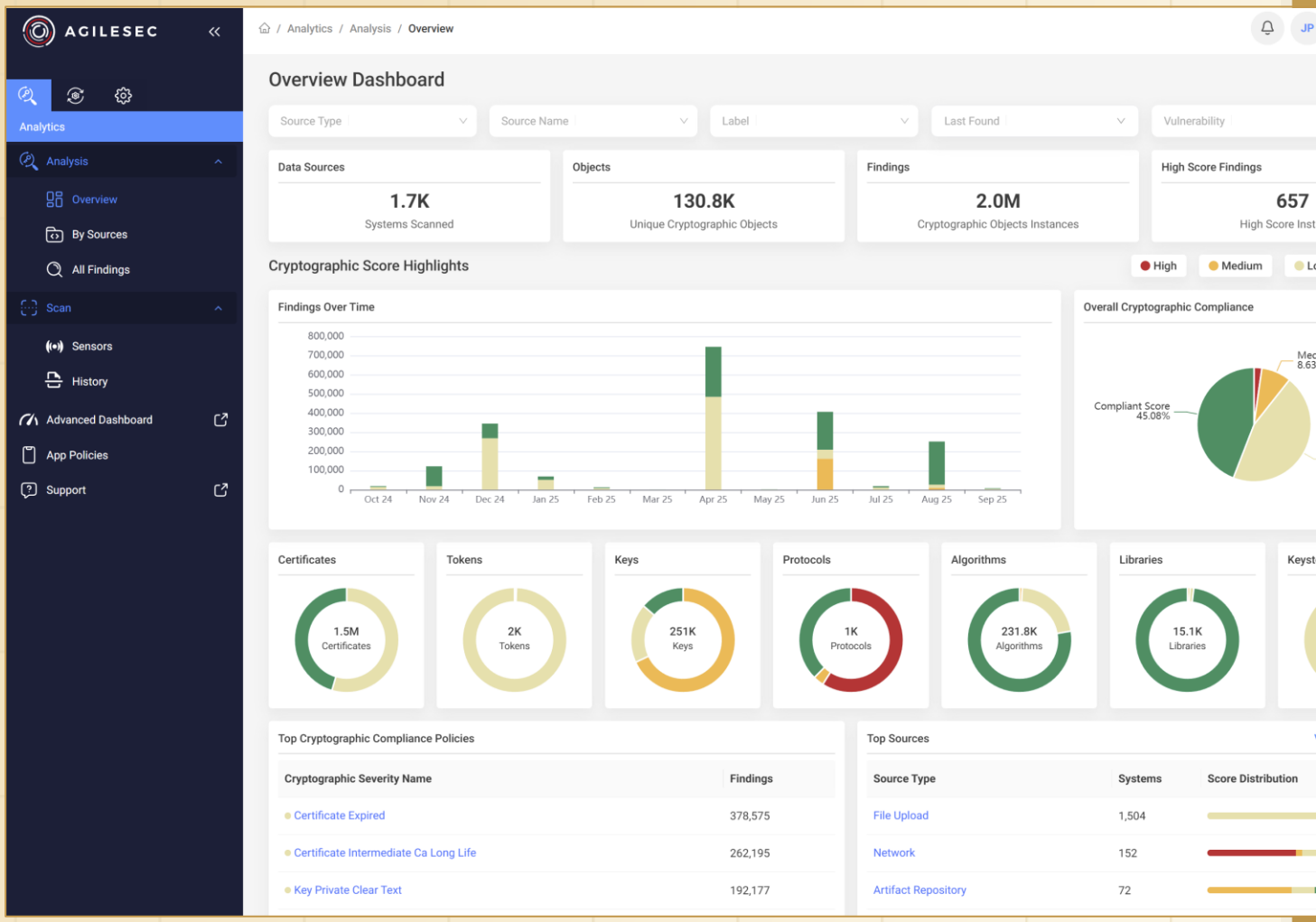
Cryptographic
Workflows

Accelerate Response

OpenSSL CONFERENCE

Requirement 4: Operationalize cryptographic management

Visibility	Flexibility	Interoperability
Automation	Scalability	Security
Remediation	Reporting	Integration



A framework for the journey from risk to resilience

From discovery to resilience

Phase 1

Discovery

Gain visibility into cryptographic assets

Focus on high risk zones and infrastructure

Utilize existing security tools

Phase 2

Inventory

Centralize inventory of assets into single view

Correlate assets with systems and apps for context

Enrich inventory with metadata (risk scoring, compliance status)

Phase 3

Risk Reduction

Identify risks and vulnerabilities

Prioritize remediation based on impact and exposure

Enable actionable insights and ownership

Phase 4

Enablement

Ingrain policy into development and IT workflows

Continuously monitor to drive accountability

Proactively report security posture to stakeholders

Phase 5

Resilience

Ensure readiness for new mandates, threats, PQC

Automate workflows and risk remediation

Continuously detect and respond to risks and vulnerabilities

Cryptographic posture management platform

Identities | Certificates | Tokens | Algorithms | Libraries | Protocols

Inventory

Build an inventory of cryptography hidden in complex infrastructure

Discover

Analyze

Analyze cryptographic vulnerabilities, compliance gaps and Quantum Threat.

Agile Platform

Control

Automate

Automate cryptographic remediation processes.

Remediate

Monitor

Monitor evolution of cryptography and PQC deployment.

Ecosystem

Thales | Azure | Copilot | Entrust | Tanium | Keyfactor | AWS* | Others

Crowdstrike | Utimaco | ServiceNow | Artifactory | Gitlab | Github | Venafi

OpenSSL CONFERENCE

Discover
Cryptography Inventory

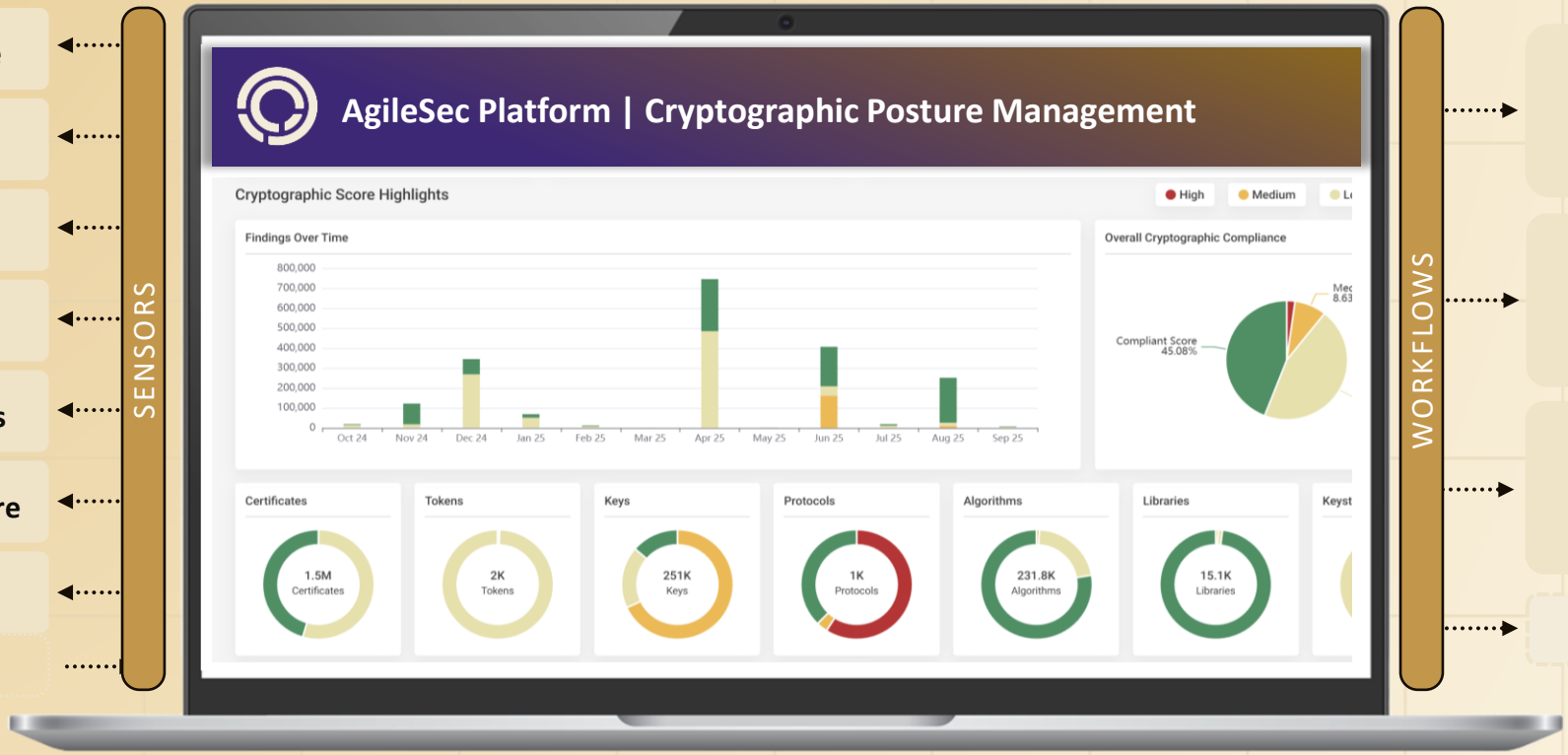
Control
Cryptographic Vulnerability & Compliance

Remediate
Cryptographic Automation

MANAGED & UNMANAGED

- Compute
- Apps
- Network
- IoT & OT
- Identities
- Data Store
- Cloud
- And More

SENSORS



WORKFLOWS

- Compliance
- Response
- CMDB
- And More

INTEGRATIONS

Crowdstrike · Utimaco · ServiceNow · Artifactory · Gitlab · Github · Venafi · Thales · Azure · SentinelOne · Veeam · Tanium · Keyfactor · AWS · Others

Cryptographic Sample Analyzed

Independent technical scans of applications of leading global enterprise platforms

OpenSSL CONFERENCE

Application	Key issues 2025	Key issues 2026	Progress
Top Video App	Certificate: distrusted WoSign/StartCom and Symantec-era CAs in bundled trust store Algorithm: DES, 3DES, RC2 Certificate: 28 SHA-1 signed Certificate: Chinese-operated roots bundled	Certificate: distrusted WoSign/StartCom and Symantec-era CAs still bundled Algorithm: DES, 3DES, RC2, Tiger Certificate: 6 SHA-1 signed	Improved
Global Wealth Giant	Algorithm: widest insecure set (DES, RC4, 3DES, DH-768, IDEA) Certificate: SHA-1 weak-key app signing certificate Library: unsupported OpenSSL 1.1.1w Certificate: test CA shipped	Algorithm: widest insecure set (DES, RC4, 3DES, DH-768, IDEA, RC2, GOST 28147, Blowfish, Tiger) Library: unsupported OpenSSL 1.1.1w Certificate: MD2-signed weak-key certificate Certificate: SHA-1 weak-key app signing certificate Certificate: 15 SHA-1 signed Certificate test CA shipped	WORSE
Top Payment App	!!!JWT Token: no expiration (HS256)!!! Certificate: SHA-1 weak-key self-signed (195 occurrences) Algorithm: RC4, 3DES, RC2	!!!Key: Ed25519 and X25519 private keys in clear text!!! Algorithm: DES, 3DES, RC4, IDEA, MD2, GOST, Blowfish Certificate: SHA-1 weak-key self-signed (109 occurrences) Library: GmSSL (Chinese SM algorithms) JWT Token: 5 expired HS256 tokens embedded	WORSE

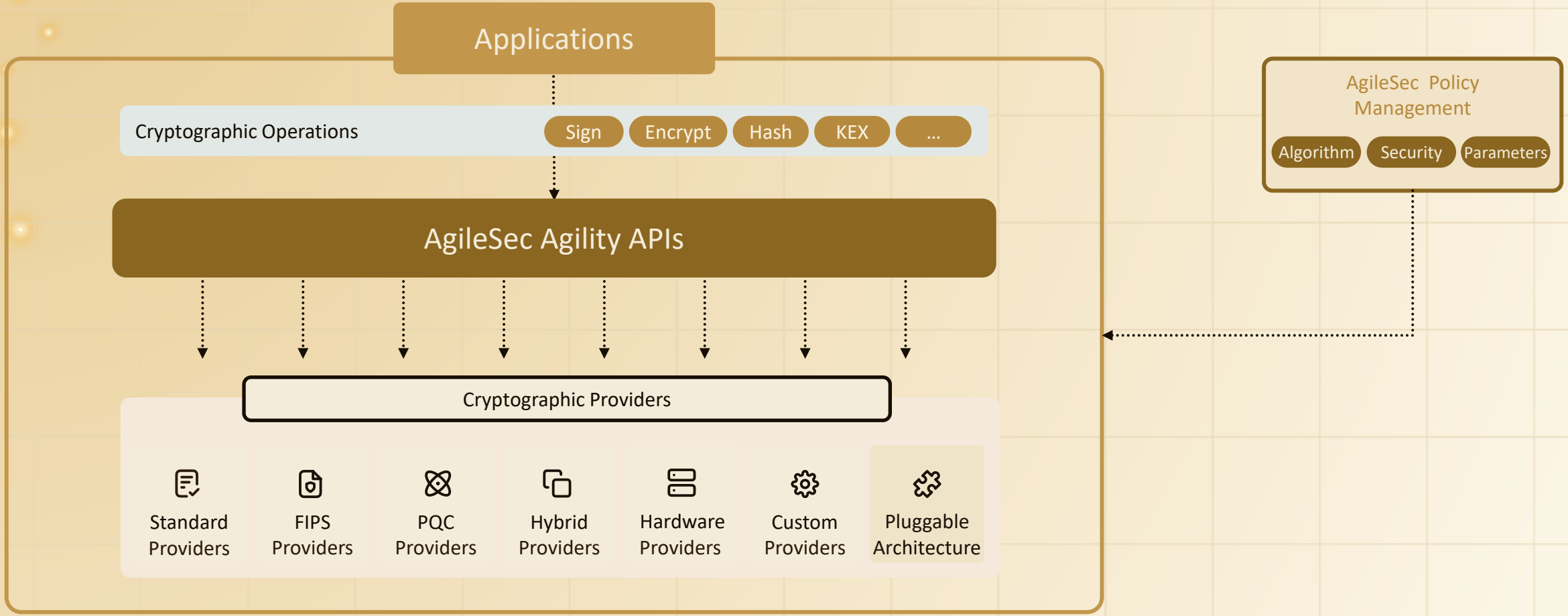
Cryptographic Sample Analyzed

Independent technical scans of applications of leading global enterprise platforms

OpenSSL CONFERENCE

Application	Key issues 2025	Key issues 2026	Progress
Global Forex Giant	!!!JWT Token: no expiration (ES256)!!! Certificate: app signing certificate is SHA-1 with a weak key Certificate: 6 SHA-1 roots Algorithm: MD5, Blowfish	!!!JWT Token: no expiration (ES256), unchanged!!! Certificate: app signing certificate SHA-1 with a weak key Certificate: 6 SHA-1 roots Algorithm: MD5, Blowfish	UNCHANGED
Global Health Platform	Algorithm: DH-768 Algorithm: RC2, Blowfish Algorithm: heavy MD5/SHA-1 use Certificate: signing certificate subject is all "Unknown"	Algorithm: DES, 3DES, RC4, IDEA, GOST, DH-768 Library: OpenSSL 3.3.2 (end of life) Certificate: 4 expired payment SDK certificates Certificate: signing certificate subject is all "Unknown"	WORSE
Top E-Commerce Giant	Algorithm: 3DES Certificate: SHA-1 signed Amazon.com certificate Certificate: expired timestamp certificates	Algorithm: 3DES, Blowfish Certificate: SHA-1 signed Amazon.com certificate Certificate: expired timestamp certificates	UNCHANGED/SLIGHTLY WORSE
Top AI Platform	!!!JWT Token: no expiration (HS256)!!! Algorithm: MD5, SHA-1 Certificate: copy signed by Uptodown, not the Platform	Algorithm: RC2, MD5, SHA-1 Certificate: 4 expired payment SDK certificates	MIXED

Cryptographic agility architecture



OpenSSL CONFERENCE

KEYFACTOR

Dr. Vladimir Soukharev
VP of Cryptographic Technology, Keyfactor