INFOSEC GLOBAL FEDERAL

AgileSec™ Analytics

Cryptographic Discovery, Remediation & Control

Cryptographic Agility Management

In today's evolving digital landscape, organizations are facing a multifaceted challenge when it comes to effectively managing cryptography. Cryptographic assets play a pivotal role in safeguarding sensitive data and securing digital operations. However, a lack of visibility into these cryptographic objects, their associated risks, and the absence of a centralized inventory pose significant hurdles, especially to prepare the transition to cryptographic agility and post-quantum security.

As quantum computing technology advances, traditional cryptography faces obsolescence, emphasizing the urgency of effective cryptographic agility management. This imperative is not just about addressing current cryptographic vulnerabilities but also preparing for a crypto-agile and post-quantum cryptographic future. In this context, cryptographic agility management is vital for maintaining data security, compliance, and operational integrity, making it indispensable in today's cyber-threat landscape.

Key Steps Towards Cryptographic Agility Management

Centralized Inventory

A company must build and maintain a centralized inventory of all managed and unmanaged cryptographic assets deployed across its digital footprint.

Continuous Assessment

The cryptographic inventory is continuously assessed against the company's cryptographic policy to find weaknesses or compliance gaps.

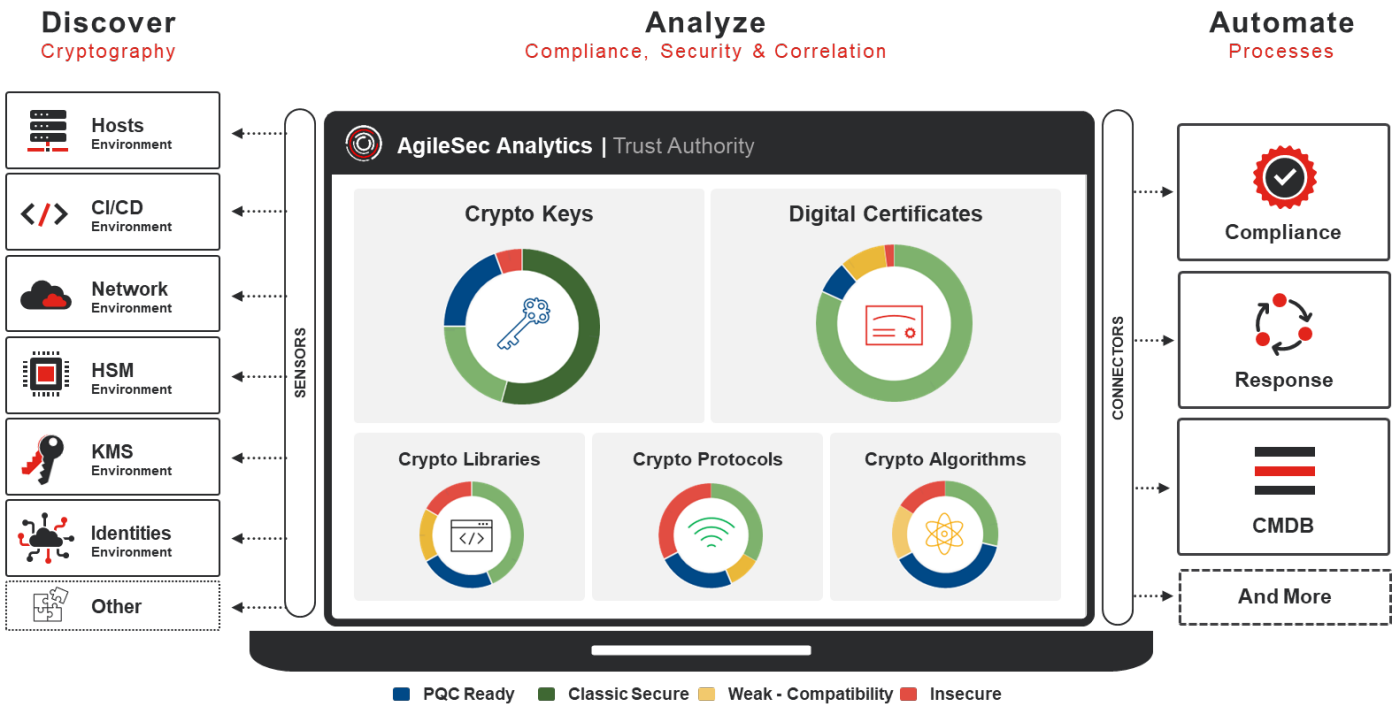
Swift Remediation

In the event of an unpredictable cryptographic compromise, a company must be able to react and swiftly mitigate the new cryptographic risk.

INFOSEC GLOBAL FEDERAL

Solution Summary

AgileSec Analytics is an innovative enterprise-grade security solution designed to enable companies to build a comprehensive inventory of all cryptographic assets deployed across their digital footprint. The Solution automatically reports cryptographic weaknesses and compliance gaps based on established security policies. The Solution is highly flexible and can seamlessly integrate with a variety of technologies and systems already deployed within the organization.



Discover

AgileSec Analytics collects cryptographic information from multiple sources and creates a centralized inventory of all cryptographic objects detected and used.

Analyze

AgileSec Analytics continuously analyzes cryptographic inventory to pro-actively identify potential cryptographic vulnerabilities, misuse or compliance breaches.

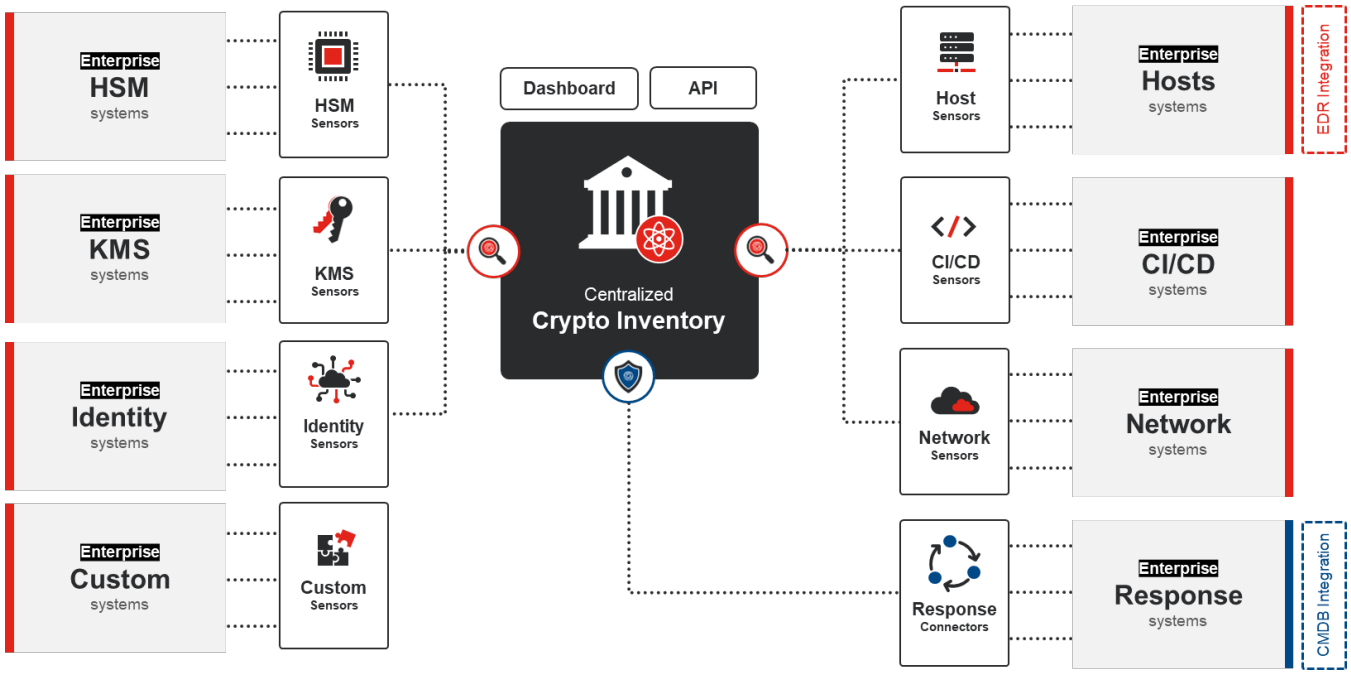
Automate

AgileSec Analytics integrates with 3rd party systems to automate processes, including remediation of cryptographic vulnerabilities, and enrichment via CMDB and risk reporting in existing GRC tools.

INFOSEC GLOBAL FEDERAL

Ecosystem Integration

AgileSec Analytics builds a **centralized cryptographic inventory** using lightweight sensors that collect cryptographic information from multiple types of technologies. A typical enterprise deployment involves the collection and correlation of managed and unmanaged cryptographic objects that are deployed across critical systems, including but not limited to:



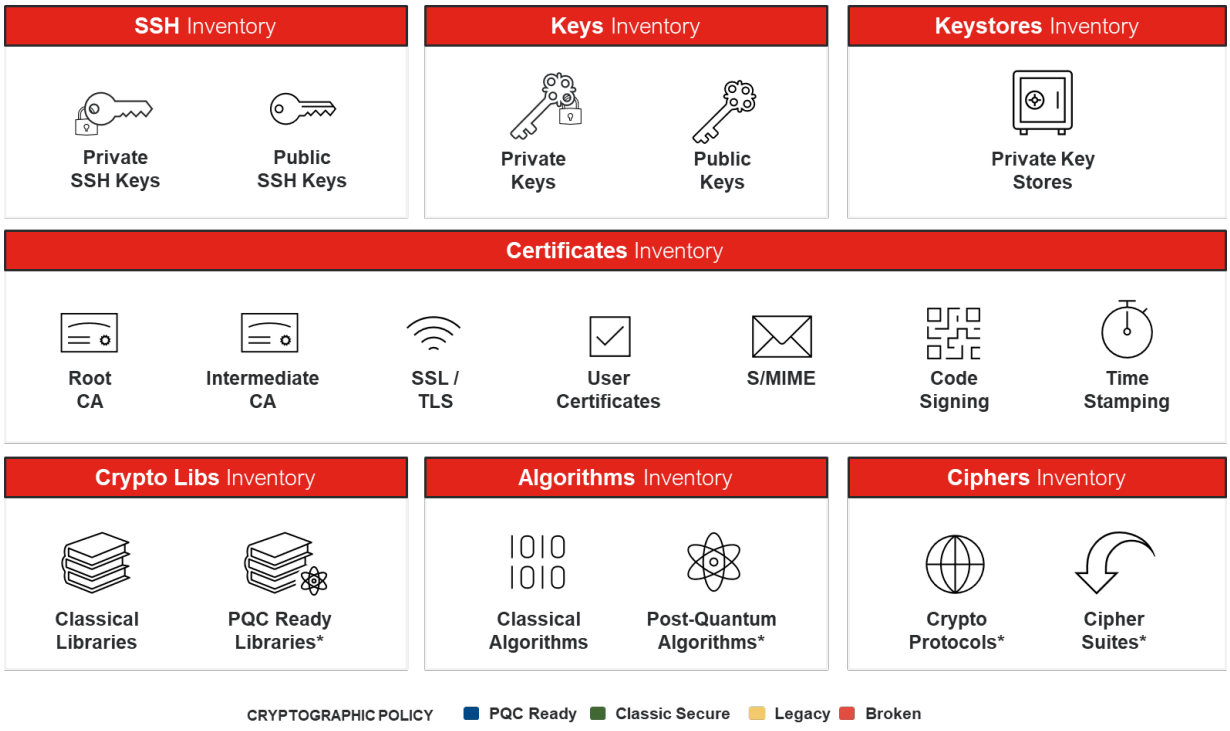
Key Sensors and Connectors to Collect and Synchronize Cryptographic Data

- **Host Sensor** collects cryptographic material in filesystems, running network processes and certificate store hidden in crown jewel systems.
- **Network Sensor** collects the cryptographic material exposed by SSH and TLS network interfaces across network infrastructure.
- **KMS Sensor** collects cryptographic keys and X509 Certificates configured and managed via key management system for further correlation.
- **CI/CD Discovery** collects cryptographic material embedded within binary objects and any applications present in a CI/CD pipeline.
- **HSM Sensor** collects cryptographic keys present in Hardware Security Modules via PKCS#11 or APIs interfaces.
- **Identities Sensor** collects X509 Certificates and public keys present within PKI, Identity and Certificate Management Systems
- **Custom Sensor** collects cryptographic information from custom data sources via API or other scanning approach.
- **Response Connectors** streamlines the remediation process of cryptographic vulnerabilities and CMDB integration via 3rd party tools.

INFOSEC GLOBAL FEDERAL

Cryptographic Inventory

AgileSec Analytics builds an inventory of machine identities and cryptographic objects discovered across the different environments of an organization. The cryptographic inventory focuses on providing deep insights in the following type of cryptographic objects:



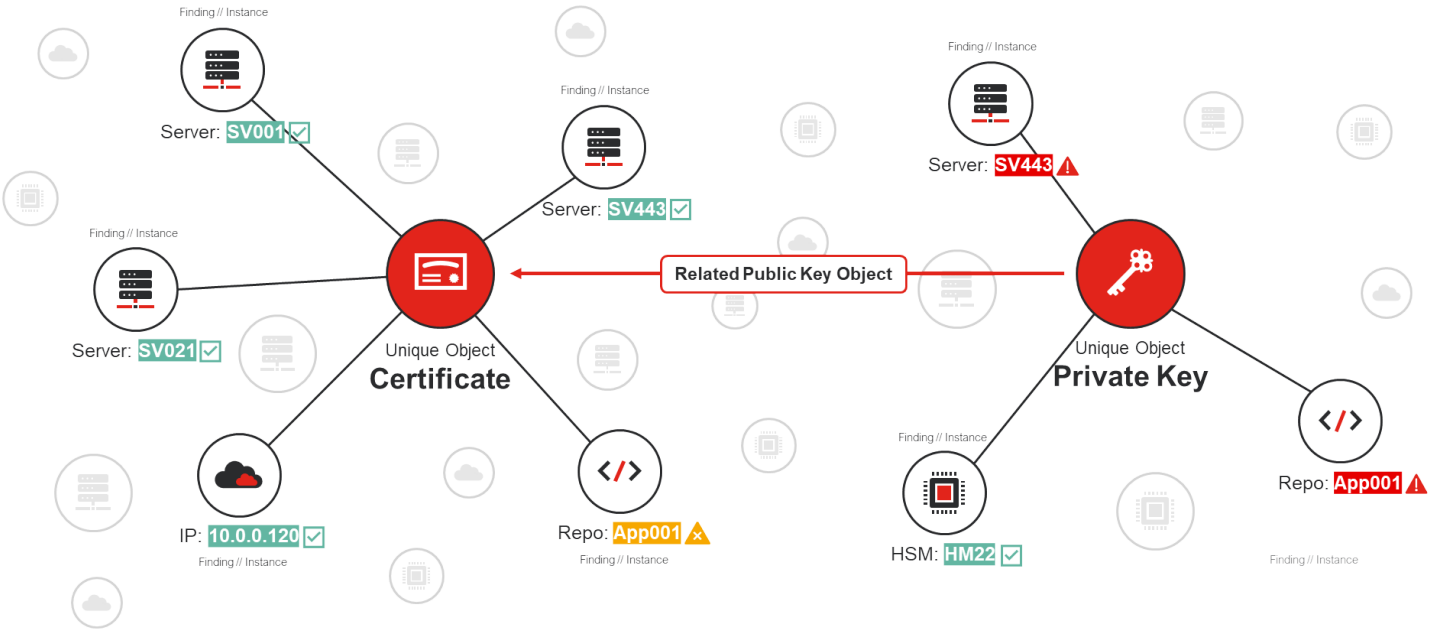
Cryptographic Objects Collected, Inventoried and Analyzed

- **X509 Certificates -** Inventory of all types of certificates deployed into an infrastructure, including Root CA, Intermediate CA, Network TLS, Personal, Authentication, Code Signing, Time Stamping and more Certificates.
- **Cryptographic Key -** Inventory of all cryptographic keys that are deployed into an infrastructure, including Private Keys, Public Keys and SSH Keys in multiple formats.
- **Keystores -** Inventory of all cryptographic keystores that are deployed into an infrastructure, including java keystore, PKCS keystores, certificate store and more.
- **Cryptographic Libraries -** Inventory of all cryptographic libraries that are deployed into application and systems, including OpenSSL, Bouncy castle and more.
- **Cryptographic Algorithms -** Inventory of cryptographic algorithms that are implemented into applications, including standards, PQC or foreign algorithms.
- **Cryptographic Protocols -** Inventory of all cryptographic protocols, versions and cipher suites configured in network interface, including TLS and SSH.

INFOSEC GLOBAL FEDERAL

Cryptographic Correlation

AgileSec Analytics applies advanced correlation between the cryptographic objects discovered and their unique instances. Cryptographic Correlation is a key value proposition of the Solution that enables companies to proactively assess how cryptographic material is being used and map the different cryptographic dependencies.



Cryptographic Correlation Capabilities and Use Case Examples

- **Unique Identifier** is a crucial mechanism of the solution to uniquely identify cryptographic objects and their instances across a digital footprint.
- **Unique Objects** include unique keys, certificates or crypto material discovered independently from their location within the ecosystem.
- **Unique Instances** represent the exact location and systems that are containing a unique cryptographic object.
- **Associated Objects** represent cryptographic objects that are used by other objects, like a certificate that is using a specific public key.
- **Orphan Objects** are cryptographic objects that have no association with any other cryptographic objects discovered.
- **Object Reuse** is an example of useful correlation to proactively detect the unexpected reuse of cryptographic material for multiple purposes.
- **Duplicate Secret Key** is an example of useful correlation to proactively identify and prevent the leakage of secret private keys.
- **Expired Object in use** is an example of useful correlation to proactively detect instances and usage of keys that are supposed to be expired.

INFOSEC GLOBAL FEDERAL

Cryptographic Reporting

AgileSec Analytics provides advanced reporting, dashboarding and data presentation capabilities. It integrates several predefined customizable dashboards to meet specific requirements. The solution offers the following core reporting capabilities:

Cryptographic Dashboard and Reporting

- **Inventory -** Explore, search, review and analyze all cryptographic object and their unique instances detected within multiple systems.
- **Vulnerability -** Automatically flag cryptographic objects that are subject to a known cryptographic vulnerability.
- **Compliance -** Automatically flag cryptographic objects that fail to meet specific cryptographic requirements or specifications.
- **Cryptographic Score -** Automatically assess the priority of cryptographic objects that are vulnerable and create a ranking for remediations.
- **Alerting -** Create specific alerts with detailed and contextualized remediation strategies for cryptographic objects with high scores.
- **Progression -** Monitor the resolution of cryptographic vulnerabilities and improvement of the company's cryptographic posture.
- **Ownership -** Automatically differentiate cryptographic objects that belong to the company from 3rd parties and operating systems.
- **PQC Migration -** Support the creation of dedicated plans to migrate to post-quantum security and cryptographic agility.

INFOSEC GLOBAL FEDERAL

Cryptographic Policy Engine

AgileSec Analytics Policy Engine is used to continuously monitor the cryptographic inventory to identify weaknesses or compliance gaps. The Policy Engine has different phases to assess the technical severity, and the relevancy of the cryptographic findings. It applies a cryptographic scoring to mark priority cryptographic findings and generate alerts with detailed information and contextual background on the vulnerabilities.

Cryptographic Inventory ▶ Severity Assessment ▶ Relevancy Assessment ▶ Score Assignment ▶ Alerting Creation

Example of Cryptographic Policies to Flag Weaknesses and Compliance Gaps

- **Insecure Key Size.** Use of insecure key length in sensitive cryptographic material.
- **Vulnerable Key.** Use of compliant key with a known vulnerability or attack vector.
- **Disclosed Key.** Use of compliant key which is known to be part of RFC, test code or other public source.
- **Insecure Algorithm.** Use of insecure cryptographic algorithm to perform cryptographic operation.
- **Quantum Vulnerable.** Use of quantum vulnerable algorithm to perform cryptographic operation.
- **Leaked Secret Key.** Leakage of secret key into systems without appropriate protection.
- **PQC Algorithm.** Use of post-quantum algorithm to perform cryptographic operation.
- **Vulnerable Library.** Use of vulnerable cryptographic library in system or application.
- **End-of-Life Library.** Use of end-of-life cryptographic library in system or application.
- **PQC Ready Library.** Use of cryptographic library that include post-quantum algorithms.
- **Key Reuse.** Reuse of keying material for different purposes or for multiple cryptographic objects.
- **Expiring Certificate.** Use of hidden certificate that is set to expire within a short time period.
- **Blocklist Certificate.** Use of Certificate that is part of known blocklist and shall be removed.
- **Long Life Certificate.** Use of Long Life Certificate to perform sensitive cryptographic operations.
- **Compromised Certificate.** Reliance of Certificate that is known to be compromised.

And more…

INFOSEC GLOBAL
FEDERAL

About Infosec Global

ISG is a fast-growing cybersecurity company providing innovative solutions in the field of cryptographic agility management, cryptographic discovery, and post-quantum cryptography. ISG has a global footprint with offices in Canada, Switzerland, and the U.S. The ISG team combines the best cryptography experts with seasoned business leaders experienced in building and growing new businesses globally.

Notable Facts About InfoSec Global

- Technology validated by NIST as part of the NCCOE PQC Migration Initiative.
- Established track record in cryptographic agility management since 2014.
- Achieved **FIPS** and **SOC2** Compliance and Certifications.
- Co-Author of **SPHINCS+ (SLH-DSA)** a new PQC algorithm under standardization by **NIST**.
- Working with top-tier global customers in **finance**, **insurance**, and **technology** markets.
- Strong practical experience deploying **crypto-agility** & **crypto-discovery** in complex environments.
- Established strategic alliances with large **OEMs** and **Global** channel partners.
- Led by crypto legends (**'Father of SSL'**) and seasoned successful entrepreneurs.
- More information at https://www.infosecglobal.com

Certifications

FIPS VALIDATED 140-2

AICPA SOC aicpa.org/soc4so

InfoSec Global Federal (USA)

8330 Boone Blvd.
Floor 8,
Tysons, VA
22182 USA

InfoSec Global Canada

2225 Sheppard Avenue East
Suite 1402,
Toronto, Ontario
M2J 5C2 Canada

InfoSec Global Switzerland

Hardturmstrasse 103
8005 Zurich
Switzerland