




AgileSec™ Analytics

Uncovering Certificates, Keys and Cryptography

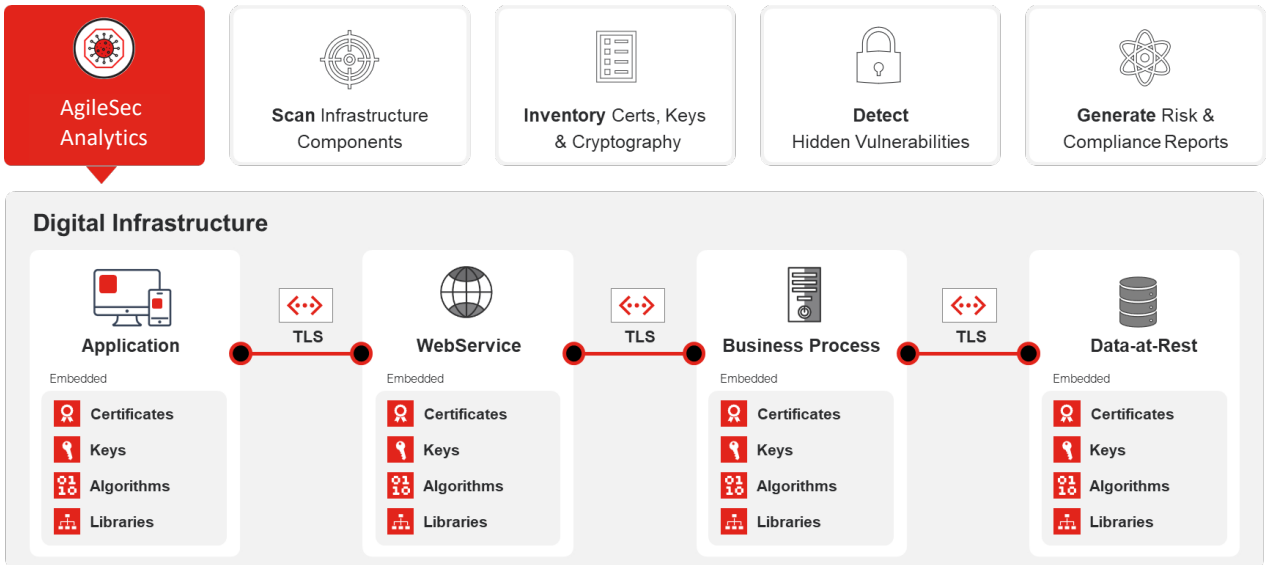
Sudden and unpredictable key, certificate or cryptographic compromises can leave companies at risk. Security and risk management leaders must start assessing their reliance on cryptography and build appropriate response plans.

Organizations need to be proactive in managing authorized and unauthorized uses of cryptography in order to protect the critical data entrusted to them. Today's digital business rely on digital certificates, keys and cryptography as their core security foundation to maintain digital trust, confidentiality, and authenticity. The security of financial transactions, distributed blockchains, IoT communications, and digital identities are susceptible to attack and fraud if cryptography is weak, outdated, or vulnerable to exploit.

IN-SECURE MANAGEMENT OF CERTIFICATES, KEYS OR CRYPTOGRAPHY		
Data Loss	Compliance Breach	Infrastructure Downtime
 <p>Use of strong cryptography is key to maintain confidentiality, integrity and authenticity of information. Use of broken cryptographic mechanisms can lead to substantial data breach.</p> <p>Q: Do I know my reliance on cryptography?</p>	 <p>New data protection regulations require companies to securely manage cryptography. Use of outdated cryptographic mechanisms is a breach of compliance.</p> <p>Q: Are my systems using compliant cryptography?</p>	 <p>Digital Certificates are key to establish trusted communication between users and digital services. Undetected expiring certificates can lead to downtime of such service.</p> <p>Q: Are all embedded certificates under my control?</p>

The Solution

AgileSec Analytics is a cryptographic discovery and analysis solution that quickly, easily, and automatically generates an inventory of certificates, keys and cryptographic mechanisms found in software applications, libraries, servers and network across the enterprise. It proactively hunts for hidden risks and vulnerabilities. AgileSec Analytics accelerates cryptographic compliance and post-quantum readiness for enterprises, governments and technology providers.



AgileSec Analytics reports information about cryptographic artefacts present within infrastructure:



Certificates | Analysis

- Prevent downtime of an infrastructure by detecting **expiring certificates**
- Prevent data breach by detecting **in-secure or fraudulent certificates**
- Prevent compliance breach by detecting **non-compliant certificates**



Keys | Analysis

- Prevent data breach by detecting **insecure or weak private keys**
- Prevent key disclosure by detecting **insecure key storage**
- Prevent compliance breach by detecting use of **non-compliant private keys**



Cryptographic | Analysis

- Prevent data breach by detecting **vulnerable cryptographic libraries**
- Prevent compliance breach by detecting **non-compliant algorithms (e.g. SHA1)**
- Support quantum-safe transition by detecting **quantum vulnerable algorithms**

Technical Capabilities

AgileSec Analytics can scan any system from applications, servers or infrastructure without requiring any source code. It detects the presence of certificates, keys and cryptographic mechanisms that are deeply embedded within applications. After building a complete inventory, AgileSec Analytics analyzes the findings and assigns a severity depending on potential vulnerabilities. Results are directly exported for further audit or used within existing infrastructure or processes for automation.

1. SCAN

- ✓ **Scan Applications**
 - Binary Applications (.exe, ..)
 - Archive (.zip, .rar, etc.)
 - Java applications (.jar, ...)
 - Mobile Application (.ipa, .apk, ...)
 - Firmware (.bin, ...), Libraries (.dll, ...)
 - Other binary files (*.*)
- ✓ **Scan Enterprise Servers**
 - Windows, Linux, Mac, ...
 - All folders, and binaries
 - Running Processes
- ✓ **Scan Infrastructure**
 - Internal LAN
 - Private / Public Cloud
 - Webservices and APIs

2. INVENTORY

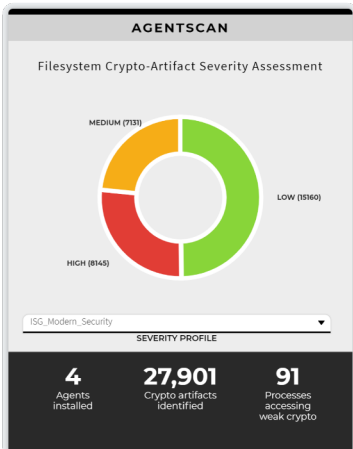
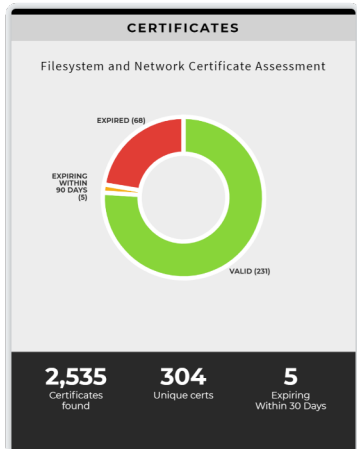
- ✓ **Certificates Inventory**
 - Generate Certificate Inventory
 - Certificates embedded in applications
 - Certificates present within host
 - PKCS, PEM & DER Format
- ✓ **Keys Inventory**
 - Generate Key inventory
 - Keys embedded in applications
 - Keys present within host
 - PEM Key Files
- ✓ **Cryptography Inventory**
 - Algorithms (AES, ECDH, ...)
 - Libraries (openssl, Botan, ...)
 - Protocols (TLS, ..)
 - Unknown Implementations of algorithms

3. ANALYZE

- ✓ **Certificate Analysis**
 - Certs by type (HTTPS, CA, ..)
 - In-Secure Algorithms
 - Expired Certificates
 - Not-Compliant (e.g. MD5)
 - Trusted / untrusted Certificate issuer
- ✓ **Key Analysis**
 - Type of Keys
 - Algorithms by Key
 - In-secure or weak Keys
- ✓ **Cryptography Analysis**
 - Un-Compliant and insecure algorithms
 - Vulnerable Library (e.g. Heartbleed)
 - Quantum Vulnerable Algorithms
 - List binaries impacted

4. INTEGRATE

- ✓ **Data Exportation**
 - Webservices & API
 - XLS and CSV
 - Syslog
- ✓ **Enterprise Policy**
 - Custom Risk Profile
 - Custom Compliance Reporting
 - Custom Alerting Rules
- ✓ **Enterprise Integration**
 - Automation & Alerting
 - SIEM Integration
 - Continuous Integration (C-I)
 - Agent Management Tool (Tanium,...)
 - Custom scan scripts



Quick Dashboard

AgileSec Analytics reporting functions provide both easy to understand top-level reports for leadership teams and in-depth analysis for technical staff. AgileSec Analytics provides at-a-glance answers to exposure and specific results for security and engineering teams with only a few clicks.

Enhanced Visibility

AgileSec Analytics uses powerful charts to enable technical teams to quickly analyze the situation and identify potential problems. Data integration can be customized to focus on key elements organizations would like to monitor and control.

- Invalid	0	0.0%
+ Expired	17	56.7%
- Expires in 1-30 Days	0	0.0%
- Expires in 31-60 Days	0	0.0%
- Expires in 61-90 Days	0	0.0%
+ Expires in 90+ Days	13	43.3%
- Not Yet Valid	0	0.0%

Actionable Results

AgileSec Analytics enables technical teams to quickly identify hidden critical vulnerabilities. Impacted files are highlighted to speed up the definition and execution of remediation plans.

- + NSS ver 1 8 86 i
- OPENSLL ver 4 8 209 i
 - Versions **4**
 - + 1_0_2 **32**
 - + 1_1_0 **5**
 - + 1_0_1 **3**
 - ♥ - 1_0_1[a-f] **2**
 - 8436358180598962027 | file:///home/isglocal/agilescan/juicy_crypto/curated_linux_files/libssl-1.0.1f.a
 - 8436358180598962027 | file:///home/isglocal/agilescan/juicy_crypto/curated_linux_files/libcrypto-1.0.1f.a
 - + Running Processes **8**
 - + Related Files **209**
- + SODIUM ver 2 0 5 i

Key Benefits

AgileSec Analytics is an enterprise grade solution that provides unique information about certificates, keys and cryptographic mechanisms hidden within a complex digital infrastructure, that can threaten digital safety. AgileSec Analytics uncovers critical information and provides key benefits to organizations:



Deliver Unique Information

Delivers unique information about certificates, keys and cryptography present within a digital infrastructure or embedded within applications.



Enhance Cyber Resilience

Detects hidden certificates, keys and cryptographic vulnerabilities that leave companies at risk and that can be exploited by attackers.



Prevent Infrastructure Downtime

Detects embedded certificates that are expiring and that can lead to unanticipated downtime of sensitive infrastructure or services.



Verify Compliance with Standards

Automates compliance controls required by industry specific regulations and continuously verifies usage of state-of-the-art mechanisms.



Prepare for Quantum Transition

Enables organizations to prepare their transition to new cryptographic standards (e.g. Post-Quantum) by mapping presence of cryptography.



Leverage Leading-Edge Detection

Unique capabilities to detect certificates, keys and cryptography within byte code independently from coding language and without source code.



Integrate Infrastructure

Integrates with different enterprise systems including Continuous Integration (CI), SIEM and any other system via API and webservice.



Ensure Minimal Operational Impact

Uses a lightweight scanning approach to minimize impact on operations and ensure seamless deployment through standard automation tools.

Deployment Use-Cases

AgileSec Analytics enables companies to reinforce their security and compliance controls over several use-cases. As AgileSec Analytics does not require access to source code, it can be easily deployed and integrated within a company's digital footprint and existing development processes. The principal deployment scenarios are the following:



SDLC Enhancement

Automate compliance and security controls during the development of new applications by internal or external developers to prevent release of systems with cryptographic, keys or certificates errors.



Cryptographic Discovery

Build and maintain an inventory of certificates and keys present within an infrastructure, including applications, servers and network, and to pro-actively detect potential problems.



Sensitive Systems Audit

Assess the security of a specific system or environment with specific emphasis on cryptography, keys and certificates and validate it complies with industry standards and regulations.



Post-Quantum Preparation

Map reliance on cryptographic mechanisms and prepare for seamless transition to new cryptographic standards (e.g. Post-Quantum) while minimizing operational impacts.



As the pioneer and leader in Cryptographic Agility Management solutions, InfoSec Global secures the world's digital assets by helping the way people discover, protect, control and future-proof their crypto assets with agile cryptography.. Powered by patented technologies and delivered through a "crypto-as-a-service" approach, InfoSec Global's solutions restore digital trust to enterprises, governments, and technology companies through crypto agility and a zero-trust framework. From crypto asset discovery and threat detection to rapid remediation and automated threat management, InfoSec Global reduces risk, enhances responsiveness, improves resiliency, and protects against future threats posed by quantum, AI and machine-learning technologies. Visit us at www.infosecglobal.com.

InfoSec Global Canada
2225 Sheppard Avenue East, Toronto ON, M2J 5C2
Canada

InfoSec Global Switzerland
Hardturmstrasse 103, 8005 Zurich
Switzerland

For More Information
www.infosecglobal.com | info@infosecglobal.com