



SIGNACERT AND VERACODE ANNOUNCE FIRST SOLUTION FOR END-TO-END SOFTWARE COMPLIANCE

May 19, 2009

Leaders in code validation and security verification collaborate to protect enterprises from software risk

Portland, OR and Burlington, MA May 19, 2009 — SignaCert, a leading provider of IT Compliance solutions based on whitelisting and Veracode, provider of the world's leading cloud-based Application Risk Management Platform, today announced a broad collaboration around their respective methods for code validation and security verification. This collaboration provides organizations with insight into the authenticity, integrity and security of software applications to implement centralized governance and controls to meet software compliance requirements.

"We have been focused with our partner, Veracode, on this for a long time," said SignaCert Founder Wyatt Starnes. "Software validation, based on best-of-breed code trust from our known-provenance attestation model, and Veracode's patented binary code security verification services are a natural fit. This is particularly important for our mutual government customers."

Both companies have seen strong traction in government markets, and both recently announced investments by In-Q-Tel, the independent strategic investment firm that identifies innovative technology solutions to support the mission of the broader U.S. Intelligence Community.

"Software is a strategic asset which is embedded in every modern data system and critical business process," said Mark McGovern, In-Q-Tel's Vice President of Digital Identity and Security. "It enables innovation and efficiency, but software is also complicated, hard to manage, and often represents the Achilles heel for security which malicious parties use to exploit a system. That makes software security a strategic issue for any enterprise. Integrated capabilities like those coming from Veracode and Signacert's collaboration will make it easier for enterprises to address this important issue and to deploy solutions for assessing, measuring and managing their software."

In February 2009, a consortium of Federal agencies and private organizations released the Consensus Audit Guidelines (CAG) that define the critical security controls needed to protect federal information systems and to implement continuous FISMA compliance. SignaCert and Veracode provide

Federal agencies with a comprehensive solution to meet the CAG's whitelist and application software security requirements.

SignaCert recently announced a significant arrangement with Microsoft for whitelist, or software "allow lists" that has resulted in a standardized and extensible Data Exchange Format (DEF). With the addition of Veracode's security verification, SignaCert will extend the DEF to support software security ratings directly from the Veracode Application Risk Management Platform.

The SignaCert & Veracode collaboration will include:

- An extended Data Exchange Format (DEF) that standardizes the protocol for combining integrity assurance and software security verification and ratings.
- Roadmap inclusion by SignaCert and Veracode enabling the support and delivery of integrity assessment and code security qualitative rankings with a standardized data representation.

"Software whitelisting and application security testing are key components in building a successful application risk management program," said Neil MacDonald, VP and Gartner Fellow. "Including security ratings as an attribute within software whitelist databases provides organizations with additional insight into an application for setting and enforcing application control policies."

"Organizations don't want to deploy insecure software, but haven't had any insight into the validation or verification of their applications," said Matthew Moynahan, CEO of Veracode. "This partnership lets organizations know the security and authenticity of software before making important and expensive deployment decisions."