The MobilityHub
SECURING DATA & APPS.

John Edwards

Startups Offer Mobile Security Innovation

John Edwards, Technology Journalist, 3/11/2013

With BYOD and other trends increasingly challenging enterprise security, a growing number of startups are working on technologies designed to help IT departments protect their organizations against a growing number of malware and related threats.

Under development

For example, Bluebox plans to attack the rapidly growing BYOD threat directly. According to its website, the company is "working to save the world from information thievery." It hasn't formally introduced its technology, but it's been reported that Bluebox has developed an improved method of protecting enterprise data on mobile devices, particularly BYOD gadgets.

Another enterprise security-oriented startup in stealth mode is CrowdStrike, which is promising to deliver "a new and innovative approach to solving today's most demanding cyber-security challenges." The company says its core mission is to "fundamentally change how organizations implement and manage security in their environment."

It's believed that CrowdStrike is planning to introduce technology that will not only identify attacks against enterprise networks from mobile devices and other sources, but also will be able to track down attackers, particularly individuals or groups trying to steal or harm data.

Who are you?

Secure identity management is the goal of ForgeRock. The company's Open Identity Stack creates a centralized provisioning and access management system covering enterprise, mobile, and SaaS applications. The product is designed to provide an alternative to traditional, closed-source identity management tools, which ForgeRock says are complicated, expensive, and incompatible with cloud and mobile devices.

By embedding encryption-based security technology directly into the integrated circuits placed inside mobile devices, Trustonic says it can help enterprises lock down virtual private networks, enhance mobile end user security, secure payment services, and even manage content delivered to consumers.

At the heart of Trustonic's strategy is the Trusted Execution Environment, a secure area located inside the mobile device's application processor. According to Trustonic, this area functions like a bank vault, with a strong door protecting the vault itself for hardware isolation. Within the vault, safe deposit boxes with individual locks and keys (software and cryptographic isolation) provide further protection.

Better malware detection

For Lastline, the challenge is creating an anti-malware technology that can work unobtrusively and reliably, particularly in mobile device-rich environments. Lastline's Previc offering is designed to provide real-time dynamic analysis of all incoming files and outgoing connections, thereby providing comprehensive protection against advanced malware sent over the web and within email. Every user is monitored in real-time for advanced malware infections, regardless of where the infection originated.

TaaSERA is working on advanced malware detection technology that exposes emerging attacks before breaches occur. The company's Attack Warning and Response Engine (AWARE) platform includes network, endpoint, mobile, and temporal event-based malware detection and risk modeling capabilities, as well as providing threat feed data on malicious IP addresses.

The AWARE platform integrates data feeds from third-party analysis tools, including whitelisting and binary analysis services. AWARE also aims to provide detailed forensic evidence of malware attacks and infections.

What other startups are you watching in mobile security? Let us know in the comments.