Boston-based Core Security Technologies has announced its latest product to help Amazon Web Services (AWS) customers perform on-demand penetration testing of their cloud-hosted systems. Core CloudInspect hopes to ease the minds of organizations concerned with the exploitation of deployed cloud systems and applications by providing an easy (and repeatable) test and measurement method. Having prototyped this service with Amazon over the past few months, Core is confident that this product will be the company's dip into the pool created by cloud architecture – and subsequent cloud security concerns.

**The 451 take**

We like that Core is thinking about its customers and their operational roadmaps – and not just Core's development roadmap. Many of Core's customers are likely looking to move at least some portion of their infrastructures into a cloud-hosted environment in the future. The risk of moving those systems outside of the protection of traditional on-premises security controls, however, continues to weigh heavily on the minds of many enterprise customers. Providing the ability to extend vulnerability management, penetration testing and risk identification to AWS-hosted machines may serve to lay some organizations' concerns to rest – or at least the portion relating to ongoing testing and validation of deployed systems. One thing that concerns us is that this integration with Amazon has no exclusivity. This means that every one of Core's competitors has the opportunity to emulate the company's model for AWS – or another cloud provider for that matter – and perhaps steal some of Core's thunder over the long run.

Core set out to create a product that allows customers of AWS to test and measure the vulnerabilities and exposures of their deployed cloud-based systems. Core CloudInspect is a SaaS-delivered penetration testing product for AWS-hosted instances that can identify security exposures of (and validate mitigating corrections to) both deployed applications and servers. Customers are not required to purchase a standard Core Impact or Insight Enterprise license since CloudInspect is deployed with an ad hoc test, authorization and payment workflow tightly integrated with Amazon's exiting APIs. Through the SaaS portal, customers must perform a one-time setup of CloudInspect that provides the requisite credentials to their cloud instances – using AWS access keys.

Once authorized, security assessments of customer-owned AWS instances can be launched along with name, type, status and any security groups they might belong to. It should be noted, however, that AWS micro instances cannot be tested because Amazon does not allow for testing of micro instances under its own licensing agreements. Web applications can be
tested simply by providing the URL of the website – provided that they are hosted on the instance selected during the initial host identification phase. Several report types are available, including an executive report that summarizes discovered vulnerabilities, a hosts report that details information gleaned from tested hosts and detailed reports for host and Web application vulnerabilities that were successfully exploited during the test represented in the Vulnerabilities Report and WebApps Vulnerabilities Report, respectively.

Payment for the scan is pushed off to Amazon's Flexible Payments Service – something that administrators of AWS services will likely be used to seeing. Authorized AWS users need simply provide their credentials to pay for the ad hoc scan and, upon completion of the payment process, the scan is launched. Core states that testing time varies depending on the size and number of instances and Web pages being tested – something that should not be a surprise to anyone who has ever conducted a vulnerability scan or penetration test against on-premises hosts and applications. The status and progress of the selected scan can be checked at any time through the CloudInspect portal interface.

Core anticipates initial pricing to be somewhere in the neighborhood of $20 per instance (and per test) but expects the pricing to increase over time as demand and future capabilities increase. Although CloudInspect cannot share the results of conducted tests with other pieces of Core's portfolio, the company does admit to having several roadmap discussions around closer cross-pollination of disparate products. We asked if Core's deployment was something that could be easily repeatable within another vendor's cloud or hosted architecture. The company admitted that the biggest barrier to transplanting the existing CoreInspect model to another provider was the UI experience and integration – although we suspect that, with enough time and money, Core would be happy to make such a model work for another provider.

**Competition**

Core Security will continue to face pressure from traditional competitors with penetration testing chops, such as SAINT Corporation and Rapid7 with its commercial Metasploit Express, Metasploit Pro and the company's flagship vulnerability management product, NeXpose – although none will have the tight integration with AWS afforded to Core. Since many traditional vulnerability management and penetration test tools will require prior authorization by (or at least registration with) Amazon prior to testing, the path of least resistance does not comparatively present itself as favorable to traditional players in the space. That being said, Core will continue to feel crowded by vulnerability management vendors like Lumension Security, Critical Watch, nCircle, Qualys, McAfee (Foundstone), StillSecure, Tenable Network Security, Trustwave, Secunia, Shavlik Technologies, Cenzic, eEye, GFI Software and Sweden's Outpost24, in addition to software performance test vendors Mu Dynamics and BreakingPoint Systems – although likely to a much lesser extent, given their typical use cases.

Specific to Web application penetration testing and vulnerability discovery, Core Security will likely encounter IBM (Ounce Labs and Watchfire), Hewlett-Packard (SPI Dynamics and Fortify Software), Protegrity (Kavado), Acunetix, Armorize Technologies, WhiteHat Security and Cenzic, among others. Competition also comes from companies like Gleg and Argeniss that offer commercially available exploits.