Core Security Technologies recently released two updates to its security test and measurement portfolio with version 11 of its CORE IMPACT Pro penetration-testing product and CORE INSIGHT Enterprise, its new risk-focused enterprise-testing platform. The company says it plans to continue to grow sales of its flagship IMPACT Pro product in 2011 and to make the market aware of INSIGHT Enterprise's capabilities. It is also making plans to push into the UK market and deeper into EMEA (having officially entered the EMEA market earlier this year) to bolster its sales and market penetration.

The 451 take

Putting its 'risk' foot forward is something new for Core Security – at least based on its past expertise. Providing continuous monitoring of assets and associated threat avenues may allow Core to tap new market opportunities where traditional pen testing is viewed by executives as a systems availability risk that's still hard to digest. For INSIGHT to succeed, integration is paramount. Core sees INSIGHT as a way to symbiotically improve security within organizations. By integrating with network and Web vulnerability scanning, patch management, ESIM, DLP, GRC and forensics products, Core believes it can help make those products more effective toward meeting the end-user organizations' security and compliance goals. To supplement existing integration avenues, we wonder if Core should seek out integration opportunities with security lifecycle management providers like Skybox Security, AlgoSec, Secure Passage, RedSeal Systems and Tufin Technologies, to name a few, in order to enhance INSIGHT's visibility into infrastructure changes that could adversely impact identified assets.

Boston-based Core Security hit the 1,000-customer milestone this year and has begun to realize its investment last January in its services offering and training programs. Building off strong 2010 growth – stating 20% year-over-year growth in the third quarter and a compound annual growth rate of 46% from 2004 through 2009 – the company is out to prove that it is not just a one-trick pony for penetration testing.

CORE IMPACT Pro version 11 adds the ability to detect and exploit configuration vulnerabilities in Cisco routers, and Core Security plans to expand supported network devices in future releases. The product also adds man-in-the-middle (MITM) attack capabilities to bolster its wireless testing support. Emulating the capabilities of the open source KARMA tools package – a set of tools that leverage 802.11 Evil Twin attacks to perform MITM attacks – IMPACT Pro can mimic a wireless access point and subsequently
launch attacks against connected systems. The release also includes client-side phishing enhancements that can be used to craft targeted emails resulting from discovered data on compromised systems or websites, as well as integration with several Web application scanners such as IBM's Rational AppScan, Hewlett-Packard's WebInspect and NT OBJECTives' NTOSpider.

Core's newest product, CORE INSIGHT Enterprise, builds off of the firm's penetration-testing heritage but is positioned (more correctly) as an enterprise security testing and measurement solution—a phrase the company would prefer to be aligned with instead of simply 'penetration testing.' Unlike IMPACT, INSIGHT looks to target users higher up the corporate ladder by providing validation of, and metrics for, deployed security controls. Instead of launching a penetration test against an identified asset directly, users are asked first to identify sensitive assets within the organization that they feel may be at risk for compromise. Using its strategically deployed 'auditor' appliances, INSIGHT proceeds to map avenues of compromise similar to those employed by a live attacker. Unlike a penetration test, this process is not a one-shot engagement. INSIGHT continues to test the identified assets and adjacent connecting tissue in order to validate that new attack vectors are not introduced that could put the assets at risk.

INSIGHT provides a straightforward dashboard aimed at CSO/CISOs to graphically identify assessment and risk trends for designated assets. Heat maps related to the status of operational areas display visual indicators of at-risk assets and can be sorted by geographic location, business unit, system category, data category or compliance area, as needed. The dashboard provides drill-down executive and technical reports allowing for deep-dive analysis of identified risks. CORE Security admits that its INSIGHT product is aimed at CISOs, IT and risk management users looking to manage and report on risk throughout the enterprise—unlike its IMPACT Pro offering, which is targeted at professional penetration testers. Ideally, the company sees its new products' sweet spot within networks with thousands of systems, applications and end users.

**Competition**

Core Security will continue to face pressure from traditional players with penetration-testing chops such as SAINT Corporation and Rapid7 with its commercial Metasploit Express, its newly released Metasploit Pro and its flagship vulnerability management product, NeXpose. Core Security will also feel crowded by vulnerability management vendors like Lumension Security, Critical Watch, nCircle, Qualys, McAfee (Foundstone), StillSecure, Tenable Network Security, Trustwave, Shavlik Technologies, Cenzic, eEye, GFI Software and Sweden's Outpost24, in addition to software performance-test providers 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), HP (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.