Boston-based Core Security Technologies says it's seeing progress in bringing the value of penetration testing to the enterprise masses. The roughly 180-person company now claims 950 paying customers and says it has seen around 20% top-line growth in the last year. A new version of Core Impact, 10.5, is part of that, as is a new product, Core Enterprise Test and Measurement (ETM), that will automate testing for strapped IT departments and produce reports and remediation recommendations for consumption at a higher executive level. Demand for professional services and support tied to its products is also on the rise, as enterprises look to nurture an internal penetration-testing capability.

**The 451 take**

We noted in a recent 451 ESP report on e-crime and advanced persistent threats that penetration-testing and forensic capabilities like those that Core offers will be increasingly important. Core's reports from the trenches seem to reinforce that. Strategically, the company sees some daylight between the capabilities of security information management (SIM) products, security incident response tools and the broader market for governance, risk and compliance wares. To fill in the gaps, it is offering its security testing and measurement offerings as a means to validate and measure the effectiveness of security controls and compliance. For now, Core is continuing to expand the reach of its Impact Pro penetration-testing product, while pushing more automated tools appropriate for non-practitioners in the enterprise audience.

We're confident that penetration testing in some form will be central to security planning and even compliance going forward, and that Core is well positioned to ride that wave. The key will be forging technology partnerships that allow its testing tools to add value to existing functions like vulnerability scanning, SIM and compliance monitoring. Beyond that, as it expands its enterprise offerings, Core will have to walk a fine line between satisfying the needs of its high-end users and a broader market of enterprise end users.

Core's announced improvements to its flagship product, Core Impact Version 10.5, include anonymous information sharing, with the ability to self profile for vertical-based information, support for Secure Content Automation Protocol (SCAP) and 64-bit encryption, and integration with Rapid7's open source Metasploit Framework. Metasploit integration broadens the set of exploits that Core users can choose from, while bolstering the value of Impact against competition from Metasploit Express, the new premium version of that platform.
The other big development is Core ETM, due out by the fourth quarter. That consists of two modules to automate penetration testing and is aimed at compliance-focused executive-level users and organizations without stable security or IT teams. The product is currently in alpha testing with six customers, and will move on to beta within the next several months and into general availability as a hard or soft appliance, or remotely managed, by the end of this year.

Core says business is good, with 20% year-over-year top-line growth. Federal business is strong, and the latest version of Impact Pro adds SCAP compliance for that market, which now accounts for 32% of Core's revenue. The company also claims a 150% increase in revenue from training and professional services, as customers look to build out their internal penetration-testing capabilities. That kind of attention to building up a sustained penetration-testing capability augers well for Core's long-term prospects, though the company's dual focus on serving high-end users and a much-broader but less-sophisticated population of enterprise end users could strain the its resources and message.

**Competition**

Core's main competition has traditionally come from the likes of Immunity Inc, Mu Dynamics, Saint Corporation and BreakingPoint Systems. Integration with Metasploit brings Impact into direct competition with the newly released Metasploit Express product from Rapid7.

In Web application penetration testing, the company will encounter a mix of pure-play and consolidated vendors. These include Qualys (a Core partner), WhiteHat Security, nCircle, Cenzic, Hewlett-Packard (SPI Dynamics) and IBM (Watchfire). Other players' kits in this segment include those from Protegrity (Kavado), Fortify Software, Acunetix, Armorize Technologies and Mayflower GmbH. Services like Gleg and Argeniss offer commercially available exploits. Free tools include the Metasploit framework as well as Nikto, Oedipus and WebScarab for testing of Web-based applications.