Core Security, with Impact at version 8 and customers above 800, hits its stride

Analyst: Nick Selby
Sector: Enterprise Software

Event summary

Over the years, as we've watched Core Security Technologies, we've questioned some of its approach and wondered whether the market for an in-house penetration-testing platform would grow quickly enough to sate Core's investors. Happily, the market for these tools is growing as mainstream enterprises become more aware of the need to regularly test not just network hosts and applications but also their forward-facing Web applications.

We believe Core is well suited to leverage the fact that penetration testing is rapidly shifting from cutting edge to early mainstream adoption in the enterprise. Since a leadership change in mid-2007, Core has given us some very encouraging progress metrics. A rising tide raises all ships, and this is an area we have long believed deserved to play a larger role in enterprise IT security.

The 451 Take

Since taking over the helm in 2008, Core president Mark Hatton has seen the company grow substantially. This is a multifaceted story and can't be boiled down to any single element, but the company has concentrated on financial fundamentals, sales and the reengineering of some of its flagship product to make it more enterprise friendly. While it won't let us be specific, Core has not just turned the corner, we believe, but is in fact showing strong growth in terms of customers, employee headcount and product development. Core is at the lead of and largely responsible for a new wave of adoption of penetration-testing tools within the enterprise. We have long said that pen testing may have enterprise legs, but will now say that the legs are here and steady.

Context

Unfortunately, the bulk of the updated financial information is stuff Core wants to keep under its hat. Headcount, it says, is up to 170 from 135 just about a year ago, and it claims its customers under current subscription have risen from 630 to more than 800. Of the total staff, it says about 50 are in North America and the remainder in Argentina. Of North American staffers, about 10 are technical with the rest in sales and marketing, while essentially all but a handful of administrative staff in Buenos Aires are technical.

The firm is not sharing average deal sizes. List price for an Impact license is $30,000; we feel safe with an average sales price of $20,000 and see that multiple licenses per customer are not infrequent. Most of the deals are direct sales, though the company has recently hired a business development staffer to look into channel sales. Unlike competitor Immunity Inc, which balances revenue between product sales, training and consulting work, Core says its consulting group is very small and training is mainly no-cost Web training. Though of course it engages in paid training and consulting, these are not, we understand, significant revenue sources on the whole.
Strategy

We think there are a few reasons for the rapidly increasing willingness among enterprises to consider buying pen-testing tools. First, of course, is the vastly improved awareness of vulnerable code in operating systems, applications and Web applications. Second, is a groundswell of movement in the world of infosec toward risk assessment. Third, the economy being in dire straits tends to focus the mind on fixing what you have before buying new gear, which leads to patching the stuff you've already got, which leads to a desire to test what you have to see whether it's any good.

Enter pen-testing platforms. Core has done an outstanding job of differentiation in its UI and reporting, which clearly articulates what has been a natural stratification in the world of pen-testing tools. At the top are fully automated tools like Core Impact, which has powerful functionality and can be used by experts – but is also, frankly, dead easy to work with and can be put safely in the hands of an inexperienced user without the danger of breaking too much. That means a lot.

The next layer down would be tools made for professional penetration testers or highly skilled internal pen testers, and we would say that space is owned by Immunity's Canvas (and to a growing extent Immunity Silica – more on that in a report soon). Beneath that would be free or very inexpensive tools that can satisfy the needs of essentially everyone from the consultant to the script kiddy – tools like the Metasploit Framework and a plethora of fuzzers and hacking tools.

For Core, continually improving the user experience on the one hand and being able to create consumable and concise reporting on the other is the key to expanding its enterprise presence. In the past, we've said that none of the players from the above-mentioned strata seem particularly keen to cross stratas. Core at this point is much like Larry Fitzgerald in Superbowl 43 – carrying the ball, hitting its stride and charging in what is basically an open field.

Products

In version 8, Core has worked to lay its foundation for a more broadly applicable enterprise offering, striving to address issues of scalability and usability with changes to the back end and front end. It has begun using SQL Express server for a back end and has changed its UI to be less bare-tree-like and more intuitive. We've not played with version 8, but have viewed the publicly available tutorials on the Core website and must say that the UI looks great and is easy to follow (we've used several earlier versions at some length).

Some of the usability improvements are simply around workflow: grouping and labeling of sets and subsets of hosts is a big one. So, too, has reporting been updated to avoid page after page – Core says it has played with layout and visualization to take into account vastly larger numbers of hosts, and added features like Delta reporting – when one runs the same tests against the same set or subset repeatedly, reports (Impact uses Crystal for output) can be run showing progress or change over time.

Technology

Core is pushing its Web application pen-testing capabilities, and we believe it is correct to do so – this is a vastly different beast from the increasingly crowded world of Web application vulnerability testing. In Web app pen testing, one finds holes and then exploits them to demonstrate the potential risk associated with a given vulnerability. Impact v8 has a bevy of cross-site scripting and blind SQL injection attacks, allowing users to crawl a website, select potentially vulnerable pages, attempt exploit, exploit, and then harvest information either by installing an agent or agentlessly popping a shell to attack the host OS. The Core functionality for rapid end-user testing is a good
example of appealing to the let's-fix-what-we-have tendency that is more prevalent now. Impact lets you do rapid tests of which users will open or even preview emails and thereby be owned.

**Competition**

As we've said, competition at Core's level is almost entirely from consultancies, and we'd bet dollars to donuts that the consultants are using Core, the less-expensive Canvas from Immunity, the free Metasploit Framework or, increasingly likely, one of each. The key differentiator between Core and Immunity is the enterprise readiness, scalability and, of course, the UI.

Canvas concentrates on architecture and fast exploit turnaround. **Saint Corporation** is another commercial competitor, but from what we've seen, not particularly troublesome. The free and open source Inguma framework, written in Python, competes primarily with Metasploit, but is really simply another toolset that's out there and not competitive in nature. Also out there are products based on Metasploit like Pentoo and Knoppix STD. **Skybox Security** simulates attacks but doesn't actually conduct the exploit.

Now that it's getting fully into this Web stuff, Core could see competition from pure-play Web app vulnerability-testing vendors **WhiteHat Security**, **Qualys**, **Cenzic** and – if they ever get round to doing anything with their products – **HP** (**SPI Dynamics**) and **IBM** (**Watchfire**). Other vendors' kits in this segment include those from **Protegrity** (**Kavado**), **Acunetix** and **Mayflower GmbH**.

**SWOT analysis**

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core has been around a long time, and under its new leadership is demonstrating a fiscal viability and sales and marketing oomph that will build on its strengths. We see no obvious direct competition to date.</td>
<td>As companies seek to shift from opex to capex, software sales could be threatened more than in the past by products and new offerings from consultancies, as well as professional services from competitors like Immunity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>With no obvious competition, Core has a seriously open road ahead and a market opportunity we must characterize as accelerating and significant.</td>
<td>The economy is a major threat as firms try to do more with less. Immunity, should it break its pattern and take on VC money to expand, could pose a not-insignificant threat – especially if bought by a large firm.</td>
</tr>
</tbody>
</table>

**About The 451 Group**

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company's analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com