REPORT REPRINT

Spirent evaluates enterprise security posture with CyberFlood Data Breach Assessment

PATRICK DALY

9 AUG 2018

The company recently announced Data Breach Assessment, the latest feature within its CyberFlood platform, representing its continued commitment to security over its legacy network-performance testing business.

451 Research®

Spirent recently announced Data Breach Assessment, the latest feature within the company's CyberFlood platform, representing its continued commitment to security over its legacy network-performance testing business. While revenue attributable to security continues to grow in both relative and absolute terms, network-testing revenue continues to decline, making the recent shift in focus seem increasingly appropriate.

THE 451 TAKE

CyberFlood's ability to model the performance impact of various security events provides a good deal of value to large enterprises with complex network and security architectures. The company continues to increase its value to customers by expanding its capabilities to the attacks most relevant to its customer base, which is exactly what it did with the launch of its breach-emulation feature, which focuses on more sophisticated multilayer attack campaigns. As of right now, there are few competitors with the breadth of security-performance testing offerings and depth of expertise that Spirent is able to offer, giving the company an early advantage in the market. As prospects for traditional network-performance testing dwindle, however, we expect an increasing number of those vendors to mimic Spirent's approach and pivot into security due to the natural technological overlaps, which could reduce the company's edge in the future. Nevertheless, Spirent looks poised to continue its current path as growth in security revenue drives growth in the company's top line.

CONTEXT

Spirent is an 82-year-old British company that is headquartered in Crawley, UK, and publicly traded on the London Stock Exchange. The company is currently led by CEO Eric Hutchinson, who has been with the company since 1983, was named CFO in 2000 and has held his current role since 2013. For much of its history, Spirent has focused on network-performance testing for networking equipment vendors, but in recent years has shifted its focus to emphasize security-performance testing. This began with the acquisition of Mu Dynamics in 2012, giving Spirent its initial security-testing capabilities, as well as a software platform to run all of its testing services that replaced the company's traditional hardware-based approach. In 2016, Spirent launched CyberFlood, its current security- and performance-testing platform, and created SecurityLabs, its ethical hacking unit that offers professional services such as penetration testing to its customers. The new breach-emulation feature within CyberFlood is just the latest in a string of developments that demonstrate Spirent's increasing shift away from its legacy business of network testing and into security testing.

Spirent's 2017 financial results were rather muted overall, but reflect the company's future direction in security testing. The company generated $454.8m in revenue across all of its lines of business, compared with $457.9m in 2016. For the network and security line of business, revenue similarly dropped by $1.2m year over year, although the company says that this was due to weak demand for Ethernet testing services offsetting the growth in its application security testing business, which includes CyberFlood and SecurityLabs. While Spirent does not break out its application security offerings separately from the networks and security line of business, the company stated in its 2017 10-k that application security revenue grew 20% from the prior fiscal year, making it the fastest-growing offering in Spirent's portfolio. Given this high growth, we expect Spirent to continue investing more heavily in security to offset some of the more mature areas of its business.

PRODUCTS

There are several different components to Spirent's portfolio of products and services, including CyberFlood, TestCloud and SecurityLabs. CyberFlood is Spirent's security- and performance-testing platform that enables its customers to emulate real application traffic at high rates to test vendor products and validate the enterprise security architecture against a variety of attacks. Many of CyberFlood's features rely on Spirent's TestCloud to operate. TestCloud is a library composed of up-to-date applications, attacks, and malware for all of a customer's web and mobile applications that enables CyberFlood to emulate customer environments when performing security and performance tests. SecurityLabs is the name given to Spirent's team of security professionals that provide managed vulnerability scanning and penetration-testing services to the company's customers across wired and wireless networks, web applications, mobile applications, and IoT devices.

The new breach-emulation feature within CyberFlood, named Spirent Data Breach Assessment, builds upon the platform's existing functionality and extends it to include the automation of purple team assessments. This allows Data Breach Assessment to perform safe penetration tests from emulated attackers to emulated targets – both controlled by CyberFlood – allowing enterprises to perform active monitoring within their networks. Data Breach Assessment also drives Spirent's IoT strategy – it enables enterprises to measure the security effectiveness of their IoT devices, which are notoriously susceptible to attack under different scenarios, as shown by recent events like WannaCry and Mirai bringing down Dyn. Assessments start with CyberFlood modeling the network's topology, at which point this solution runs a series of attacks against the network to emulate a data breach while capturing data on how the network and security infrastructure responds. Once an assessment is completed, Spirent correlates logs of the event with the attack scenarios run, and can notify customers whether their security products blocked and logged the event, blocked but did not log, logged but did not block, or neither blocked nor logged. From there, the customer can revise policies or change network settings and run the data breach emulation again to see if the result has improved.

STRATEGY

Spirent's plan is to leverage its existing competency in network-performance testing in order to pivot to higher-growth areas like security testing. The company is a founding member of NetSecOPEN, an industry group dedicated to defining open testing standards, which accomplishes the dual goal of enhancing its approach's credibility and the ability to influence future standards in-line with its product roadmap. Spirent provides different testing methodologies espoused by NetSecOPEN within CyberFlood. The company has also positioned itself not only as a method for improving security posture through testing, but also as a way for enterprises to evaluate the effectiveness of different vendor products before becoming customers.

COMPETITION

Spirent will primarily compete against network-load testing vendors and professional services vendors focused on penetration testing, bringing the company against a wide array of companies with different primary focuses and core competencies. While some may focus on application security and source code analysis, others focus on network or hardware hacking. Praetorian is an example of one professional services provider with a focus on penetration testing for IoT environments, and while it competes against Spirent's IoT strategy, Praetorian is too specialized to broadly compete with Spirent's entire portfolio.

The breadth of Spirent's capabilities makes it difficult to specifically say which vendors it does and does not compete against. However, we could begin to see an increasing number of network-performance testing vendors pivot their offerings to security testing to take advantage of new growth opportunities, as Spirent did with CyberFlood, giving rise to a market of direct competitors. Spirent can use the fact that there is not too much direct competition for CyberFlood's offering at the moment to gain early market share and potentially drive new top-line growth.

SWOT ANALYSIS

STRENGTHS

CyberFlood leverages Spirent's existing expertise in network-performance monitoring to provide valuable insight into how a company's network would perform under a variety of different attack scenarios.

WEAKNESSES

CyberFlood is likely an offering that caters to the security needs of large enterprises with complex architectures and money to spend on advanced testing, and is less likely to be adopted by the midmarket and SMBs.

OPPORTUNITIES

Spirent can leverage its early position in the security performance testing market to establish a foothold in the market and potentially drive new growth.

THREATS

There is already an incumbent base of network performance monitoring vendors that could easily pivot into CyberFlood's market in the same way that Spirent did, cutting down on the company's current competitive edge.