No. 23
25th April 2019

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

IBM Security and Cisco Mean Business

- IBM Security and Cisco are following through on their "power of two" announcement of two years ago. They are serious about their strategic alliance in cyber security.
- The two companies point to a recent win with a large multinational on the basis of a jointly-written RFQ as a key example of what they can achieve together.
- The offer of a 'single throat to choke' across sprawling multi-vendor environments resonates very well with the cyber security priorities of many enterprise customers.
- HardenStance tentatively estimates the alliance can generate incremental annual sales in the low single digits for the next 2 - 3 years but is unlikely to exceed that.
- The new partnership between Fortinet and Symantec may be partially competitive but is less likely to develop to the level that IBM Security and Cisco's has.

IBM Security and Cisco gave a joint webcast last week during which they provided an update on their alliance in the cyber security market. The session provided an update on the product integrations they've carried out across their cyber security portfolios and the breadth and depth of commercial collaboration they're engaging in now.

The most striking proof-point offered up is that IBM Security and Cisco have started submitting joint RFQs for some large cyber security contracts.

The most striking proof-point arising from the webcast is that IBM Security and Cisco have started submitting joint RFQs for large cyber security contracts. The example offered up is a multinational with more than a hundred sites and 40,000 employees. This customer asked the two companies to forego their own RFQs for a large compliance-related project in favour of submitting a joint one. According to Chris Smithee and George Mina, Program Directors for Strategic Alliances for Cisco and IBM Security respectively, they did as requested and won the contract.

The two companies issued their 'Power of Two' PR two years ago

It's coming up on two years now since the two companies first announced they were partnering up to "raise cyber security to the power of two." In June 2017 HardenStance published a short response to the announcement. The position HardenStance took was that up until then the '1.0' of these two companies' partnership had taken the form of nothing more than routine, tactical, product integrations. Partnership 2.0 - the 'power of two' announcement - promised a more strategic approach to a larger subset of integrations across their cyber security portfolios and across products and services.

The blog argued that the enhanced partnership had "undoubted promise" but that customers needed to wait and see "how 2.0 actually delivers on the ground." There was perhaps nothing especially insightful in those comments. Looking out to where the relationship might potentially go next, though, the blog also noted that "the opportunity of account-sharing is going to be pretty tempting, at some level at the very least." It also stated that "there might be grounds to be hopeful that account conflicts could be managed more easily between IBM Security and Cisco in a future 3.0 iteration [compared with some technology partnerships]."

The evidence offered up in last week's webcast suggests that this is indeed the trajectory the partnership is on now. IBM Security and Cisco do seem to have an alliance in cyber security that's worthy of the name. A 3.0 version of their partnership really does seem to be taking shape. It would appear they really do mean business.

This is non-trivial. Many technology alliances don't work. Moreover, at the time of the 'power of two' announcement two years ago, Cisco's cyber security business was still in the throes of a period of painful senior management churn. That can't have helped. Getting this far into executing on this alliance is therefore a significant achievement.

Key take-aways from the webcast

- The apparent willingness of the executive teams of both companies to combine the interests of their sales organizations to pursue new opportunities is key to the value they can bring to customers.
- As expected, the limited overlap in their product portfolios is helping. Cisco's portfolio is weighted towards prevention, threat detection and product. IBM Security's is weighted more towards incident response and services, including managed services. There isn't a lot of competition between their sales teams for the same dollar of revenue.

The strongest focus on portfolio integration has centred around integrating large parts of the Cisco portfolio with IBM's Q-Radar and Resilient platforms

- The size, brands and commitment to cyber security of the two partners gives an enterprise customer's own technology, operations, and finance teams a strong incentive to engage with them at a strategic level across sales, product and services. Many technology alliances can't provide that.
- Consulting services, including managed services, around consolidating sprawling multi-vendor environments is a major part of the value proposition and a key priority for many enterprise CISOs. Cisco's Chris Smithee captured the partners' goals succinctly in the webcast, stating: "we're not going to take your number of vendor relationships down from forty or more to just the two of us. But if we can get you down to counting the number of vendor relationships you have to maintain to a number you can count on the fingers of two hands, that's a big win for [a customer's] operations and finance teams, and for their C-suite."

The webcast provided a number of proof-points around portfolio integration:

- The strongest focus centres on integrating parts of the Cisco portfolio with IBM's market-leading Q-Radar SIEM and Resilient Incident Response (IR) platforms. Q-Radar now supports – ingests threat telemetry from - 25 Cisco products out of the box. Around a dozen Cisco security apps now run on the IBM Security App Exchange.

Figure 1: Integrated Technologies, Services and Threat Intelligence

	Products			
	Security Analytics	Incident Response	Threat Intelligence	Managed and Consulting Services
IBM Security	IBM QRadar SIEM	IBM Resilient	IBM X-Force	X-Force Threat Mgmt. & Security Hub
cisco Security	Firepower, ISE, Cloud (Umbrella, Cloudlock), Threat Grid, AMP for Endpoint, ESA/WSA, Stealthwatch	Threat Grid, Umbrella Investigate and Enforcement	TALOS	Firepower Threat Defense, AMP for Network, AMP for Endpoint, ISE, Threat Grid

Source: IBM Security/Cisco

- As part of its managed security services portfolio, IBM Security is now supporting Cisco's Firepower Threat Defence (FTD) Next Gen Firewall (NGFW) products as well as Anti Malware Protection (AMP) for networks (AMP4N) and for endpoints (AMP4E).

Support for Cisco's Identity Services Engine (ISE), Threat Grid and Umbrella are also on IBM Security's managed security services roadmap.

The alliance can make its mark in two main areas. The partners are now demonstrably better positioned to win vendor consolidation and multi-vendor consulting and management services together than they could on their own. Incremental sales can also come from gap-filling from across one another's portfolios.

Without hard data to draw on, HardenStance tentatively estimates the alliance can generate incremental sales in the low single digits for the next two to three years for each firm. Market factors will create a ceiling on that incremental growth rate which the alliance will have difficulty breaking through. Among those limiting factors are:

- Ongoing customer preferences for best of breed security products and/or preferring to manage their own multi-vendor networks.
- Customers preferring others to do their vendor consolidation and/or vendor management for them. This includes the larger Managed Security Service Providers (MSSPs) and other vendors. Among vendors, Palo Alto Networks and even Sophos have been acquiring product companies at a ferocious pace to strengthen their account positions as many enterprises look to rationalize their vendor partnerships.

Fortinet and Symantec's intent bares at least comparison with IBM Security and Cisco's 'Power of Two' announcement of two years ago.

Will Fortinet and Symantec go in a similar direction?

An important recent development in the vendor landscape is last December's announcement of an enhanced partnership between Fortinet and Symantec "to deliver the most robust and comprehensive cloud security service."

Fortinet and Symantec's intent with this bares at least some comparison with IBM Security and Cisco's "power of two" announcement two years ago. They too want to go beyond a limited, tactical, partnership to something more strategic. Also, it's quite narrowly focused on select product integrations – in this case on policy and threat sharing across their endpoint and network security domains via a single interface.

Eighteen months ago HardenStance made what proved to be a pretty accurate call as regards where the IBM Security and Cisco partnership could or would go next. A relevant question now is whether Fortinet and Symantec will evolve in that same direction. Two years from now, will Fortinet and Symantec be as integrated in their approach across their own organizations, portfolios, products, consulting services and managed services including across multi-vendor environments?

Answer: probably not. For any cyber security company – be it IBM Security or any other – Cisco offers an unrivalled global enterprise account footprint. Any prospective partner would want to move heaven and earth for privileged access to Cisco's portfolio, accounts and management team. Conversely, IBM Security is highly respected as a leading cyber security player in both products and services. As an emerging player, Cisco needed – arguably still needs – the boost to its credibility that comes from partnering a cyber security leader like IBM Security, especially one with such a complimentary portfolio.

There's no such disparity in account footprints or cyber security kudos between Fortinet and Symantec. Hence the logic of prioritizing one another to the level of combining strategically across their organizations doesn't look as compelling. Put differently, Fortinet-Symantec 2.0 won't necessarily evolve to a 3.0 as IBM Security and Cisco have.

The Fortinet and Symantec partnership is unlikely to meet IBM Security and Cisco head-on on a regular basis. Where they do meet, Fortinet and Symantec will retain the upper hand. This is because their partnership is committed to piling on additional value into their core endpoint security and NGFW products spaces where they're typically more competitive than the joint IBM Security and Cisco offering. The IBM Security and Cisco alliance can certainly generate significant incremental sales. But for the next couple of years it will disrupt the market at the margins rather than transforming it. ■

More Information

- What will an IBM and Cisco Security Partnership 3.0 look like? (June 2017)
- The December 2018 HardenStance Network Security Sales Index (NSSI)
- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- HardenStance received no payment for publishing this Briefing.
- Register for **free email notifications** when HardenStance publishes new content.
- www.hardenstance.com

HardenStance Disclaimer