VansonBourne

PRODUCTIVITY

Best tool or best vendor?

How organisations are building their IT security stack

David Gallichan
Account Manager

The lack of a fully defined IT security strategy is complicating how organisations go about selecting tools and vendors to support their IT security needs.

Part two of our six-part ProductivITy series is exploring cybersecurity. As evidenced by **our previous article** in this edition, IT and business decision makers are highly concerned about the persistent and proliferating external threats that their organisation is up against. However, they're also very aware of the internal challenges that are contributing to their security struggles.

Given the regular stream of high-profile cyberattacks in the media, it's clear that these external threats are increasing the pressure on senior ITDMs when it comes to making the "right" decisions around which IT security tools they choose to deploy and the vendors that provide them. But, within this decision making process, they must also account for their stretched internal resources and the often tricky process of integrating new tools into an already crowded technology stack.

In this article, we will take a look at the way in which organisations are approaching tool and vendor selection, and what difficulties they are encountering with their IT security stack, while also posing the question as to whether their current approaches are as effective as they could be.

Fully defined IT security strategies – not as common as you might think

There's little doubt in our minds that IT security is currently more important than it has ever been – and this will only increase further as the complexity of IT environments also continue to rise, along with the constant evolution of the cyber threat landscape.

As such, it's a concern that fewer than four in ten (38%) respondents report that their organisation has a fully defined IT security strategy in place. This proportion drops as low as 13% among the smallest surveyed organisations, which immediately starts to indicate a headcount and/or knowledge deficit considering that 61% of the largest organisations have a full strategy in place. And while 37% overall have some form of loose framework, it seems as though organisations are leaving themselves exposed to a range of potential issues by not fully mapping out all aspects of their IT security.

Presence of a fully defined IT security strategy in organisations

Split by employee size	Fully defined IT security strategy	Loose IT security framework	In process of creating	Planning to create	No plans to create/ don't know
Total	38%	37%	6%	7%	13%
1-49	13%	42%	0%	22%	22%
50-249	15%	49%	5%	13%	18%
250-999	29%	39%	26%	0%	6%
1,000-4,999	56%	34%	6%	0%	3%
5,000+	61%	26%	1%	0%	12%

What's being covered by IT security strategies?

When it comes to what organisations are incorporating into their IT security strategy – whether it be fully defined, a loose framework, or in creation – the key focus areas are much what you'd expect them to be, with incident response, hybrid/remote working guidance, and training all commonly reported.

But only 20% say that a vendor roadmap features within this strategy. And while technology investment plans are cited by a substantially larger proportion (52%), this does suggest that organisations could be doing more to refine the way in which they approach selecting their IT security tools and vendors.

From an IT security vendor perspective, this lack of a clear roadmap within prospect organisations presents the opportunity to position themselves as a strategic partner, who can work alongside these businesses, not only in the provision of security tools, but also to help resolve some of the other challenges they face. Remember, from **our first article in this mini-series**, just 6% of respondents cited the tools/solutions in use as the current biggest problem with their organisation's IT security, with 51% pointing towards external threats, and 22% highlighting resources.

While this may appear fairly clear cut in terms of the biggest challenges at play, it also serves to reinforce the depth and breadth of the difficulties that organisations are facing. Not only that, but it further helps to illustrate the need for a deeper relationship between end user businesses, IT security vendors, and managed service providers (MSPs) as they aim to implement and maintain robust security defences.

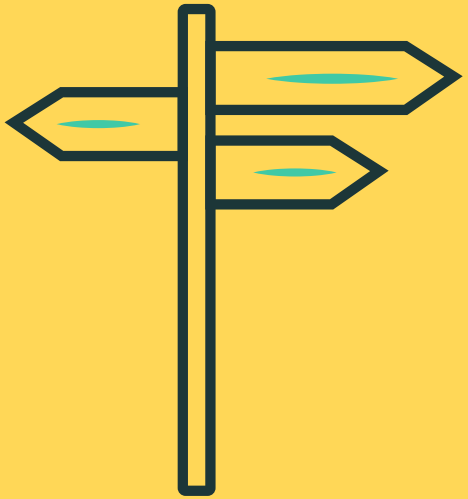
Best tools or best vendors?

In terms of the approaches that organisations have available to them regarding their IT security stack, generally these can be grouped into two camps – consolidating behind a preferred vendor or pursuing "best of breed" solutions. Both can have their benefits, but equally both can have their drawbacks as well.

With a consolidated approach, aligning behind a single vendor or very small group of vendors can improve the quality of the relationship while also helping to avoid the pitfalls of having a raft of incompatible technologies from different vendors that were never designed to integrate with one another. Ultimately, if left unchecked, these integration issues can undermine the efficacy of each tool, and, as a result, the overall security posture of the organisation. But, on the flipside of this strategy, aligning with just one vendor could lead to becoming locked into contracts that mean companies are governed by the roadmap of their provider rather than being able to follow their own path.

A "best of breed" strategy on the other hand helps to ensure that organisations have the best tool/solution for a specific purpose such as guarding against a certain type of threat. But, as alluded to, integration and management challenges can become an unintended consequence, potentially leaving the door ajar for opportunistic cyber criminals scanning for vulnerabilities that they can exploit.

So, really it would appear to be a case of pick your poison and commit to it, and as it turns out, there are plenty of respondents' organisations on each side of the fence - 54% are going after the "best" tools for them, regardless of vendor, with 31% going down the route of vendor consolidation and using as many of that vendor's tools as possible.



54%

use the "best" tools/ solutions, regardless of vendor

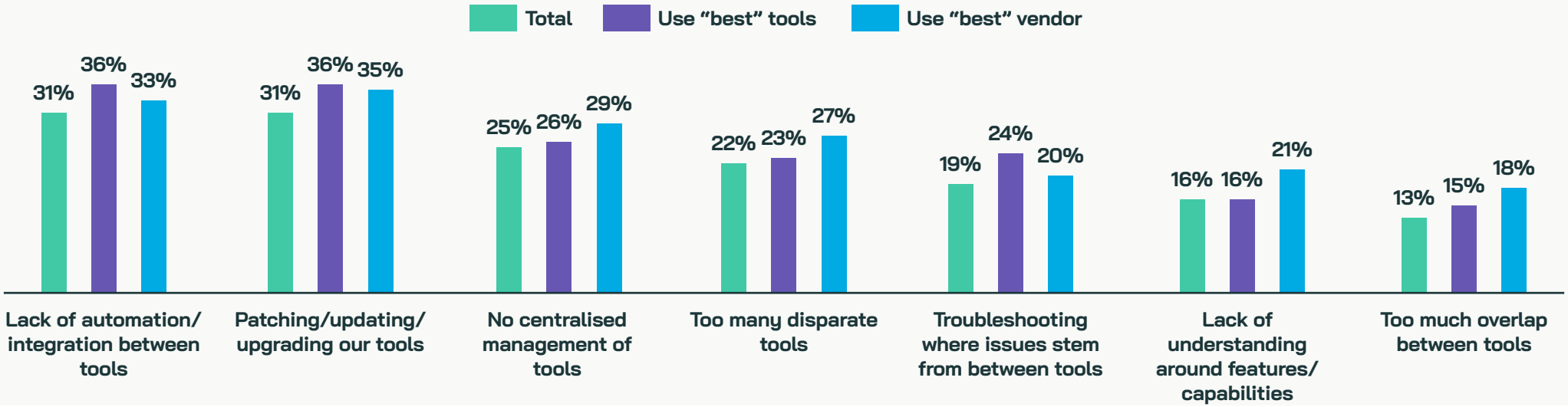
31%

consolidate behind the "best" vendor, utilising as many of their tools/ solutions as possible

Have solutions become part of the problem?

These differing approaches raise the question of what challenges are being encountered by those pursuing each strategy. Well, given that the largest proportion of respondents' organisations are utilising a "best in class" approach, it's perhaps unsurprising to see that a lack of integration between tools (31%), no centralised management of tools (25%), and too many disparate tools (22%) are among the key challenges overall with the IT security solutions that they have in place.

Most common challenges faced with IT security tools and solutions in place



However, the theory underpinning those percentages doesn't tell the full story, with the challenges not being exclusively driven by those adopting a "best in class" approach. In fact, issues with centralised management and too many disparate tools, as well as difficulties such as a lack of understanding around features/capabilities of tools and too much overlap between tools, are more likely to be reported by those from organisations who have consolidated behind a "best" vendor for them.

Comparing approaches: "Best" tools vs. "Best" vendor

	Use "best" tools	Use "best" vendor
Number of IT security tools in use	7	11
Number of specialist IT security vendors relied upon	6	5
Percentage who say a vendor roadmap is part of their IT security strategy	26%	12%

Although this might seem counterintuitive, when digging a little deeper the reason becomes clear – on average, those consolidating behind a best vendor (or vendors) are utilising 11 different IT security tools, while those using the best solutions for them, report a notably lower average of seven tools.

In terms of the number of different specialist vendors that they rely on for their IT security needs, the differing approaches between these companies leads to much the same outcome – six vendors for those with a best tools approach, and five for those who are more vendor driven, perhaps suggesting that any consolidation plans are in their infancy. Regardless, it would appear that those who are choosing the best tools have enabled themselves to maintain a slightly greater level of control over their security stack when it comes to decision making and solution selection.

This brings us back to the absence of a well thought out IT security strategy, and for organisations where a strategy is in place, the lack of a clear vendor roadmap within this. Just over a quarter (26%) of respondents, from organisations who tend to use the best tools for them, regardless of vendor, cite that a vendor roadmap is part of their IT security strategy. While this isn't a huge proportion, it does compare favourably to the 12% from organisations trying to consolidate behind a "best" vendor for them.

Strategic security partnerships
- limiting risk to maximise reward

Evidently, something needs to change if organisations are to better avoid the bear traps of either too many tools or too many vendors...or both. Consolidation attempts don't appear to have been all that fruitful and without the presence of a well thought out vendor roadmap within their IT security strategy, it is easy to see how end user organisations could find themselves being dictated to by their vendors' roadmaps, rather than implementing a plan based on their own IT security needs.

This apparent lack of direction means that the onus falls upon IT security vendors to become more of a strategic leaning post for end user organisations. However, this doesn't mean simply trying to cram more and more tools into already overcomplicated security stacks, but rather working alongside their prospects and clients to better understand the full extent of their challenges and assisting them in finding the right answers – whatever form that may take.

External threat actors are too advanced for organisations and security vendors not to be working effectively together, potentially leaving holes for cyber attacks to exploit. Ultimately, IT security is a team sport, and the good guys need to align their respective visions if they're to keep the bad guys out, as the repercussions are damaging for all parties involved in security failures.

But more on the teamwork side of things in our third and final article on cybersecurity, coming soon...

These survey findings are based on qualitative and quantitative interviews with 216 members of the Vanson Bourne Community, our insight network of IT and business professionals at the forefront of their industries. We regularly engage with our members to tap into their expertise and perspectives on the latest technology-driven trends facing their organisations today.

Whether you're looking for deeper market understanding or data to drive your strategy, insights from our expert community can help inform your thinking and test your hypotheses.

Our Productivity database and insight series harnesses Community insights to take a forensic look into the IT department, investigating the issues faced by tech teams in ever-changing times. You've just read the latest in our ongoing series, exploring the cybersecurity issues in tech today.

Get in touch to learn more about these findings or to discover how the insights in our Productivity database can support your goals today:

Let's talk about research