Next Generation
Security Distribution

Bitdefender

Blue Solutions Opinion Paper

The Signs That Show It's Time To Switch Security Vendor

How MSPs and Partners can Spot the Need for Change

0118 9898 222 | info@bluesolutions.co.uk | www.bluesolutions.co.uk

Introduction

For MSPs and other channel partners that deliver security solutions to end-user organisations, the market opportunity is huge and growing. According to insight from Allied Market Research, the global market for managed security services is expected to reach $29.9 billion (c. £22.6 billion) by 2020 – a compound annual growth rate of 16% from 2015[1].

Enterprise customers are, according to industry analyst Forrester, "turning in droves to managed security service providers,"[2] but there are strong signs that small and medium businesses are heading firmly in the same managed services direction too, with the total world MSP spend projected to represent nearly 20% of all IT services by 2019[3].

All in all, it's a burgeoning opportunity that should put MSPs and others in prime position to build and grow a profitable security business – but there's a downside.

Security, as a sector and as a discipline, moves so fast that a wide disparity has opened up between those security vendors who are able to offer compelling solutions that cover new bases as they emerge, without adding profit-eroding complexity, and those who are basically entrenched in outdated scope, practice, and expectations that serve neither customers' evolving need nor the partner's bottom line.

On the surface, many security vendors appear to deliver similar benefits in similar ways, yet when the devil in the detail is exposed, a very different picture is painted – and it is in this picture that partners will find the clues as to whether their current security vendor relationships are ripe for a rethink.

This paper explores the solution shortcomings that indicate it may be time for partners to jump ship on their current security vendor – and raises the prospect of what a better choice of vessel might look like!

How partners know they need to change security vendor, 1 - *The margin-killers*

More than anything else, this is the issue on which any partner's choice of vendor – security or otherwise – must turn. Managed service provision is not a viable business if it cannot operate profitably, yet shortcomings in many security vendors' solutions *actively erode the margins that the partner should be making out of them.*

Take the most obvious example of this: the tools that enable the partner and their end-user to manage the security services being delivered.

The plain fact here is that the partners' business cannot succeed unless they can monitor and maintain customer systems, and manage their billing, with the absolute minimum of costly manual intervention. The bigger the partners' customers get, and the more of them they bring on board, the more of a challenge this becomes.

Yet how many security vendors actually offer a **single console** that is not only powerful enough to unite all the management functions in one dashboard, but do so in a way that is simple enough for all levels of staff (in both the partner and the end-user organisation) to use, in a way that is reliably defined and controlled by role, without expensive and time-consuming training? And – critically - at *scale*?

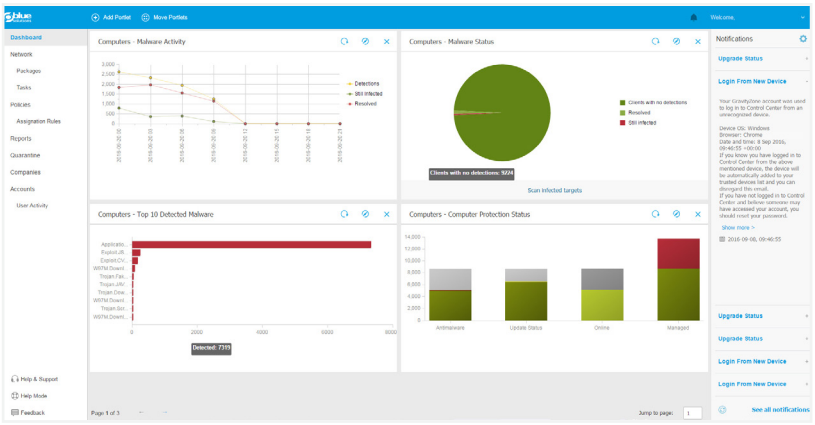
Even assuming vendors can overcome these hurdles, how many of them can confidently state that such a dashboard **integrates with the full range of RMM and PSA tools** (Kaseya, LabTech, ConnectWise, Autotask) that have become the *de facto* standard for most partners' managed service business, and that often represent significant existing investment that must demonstrate a return?

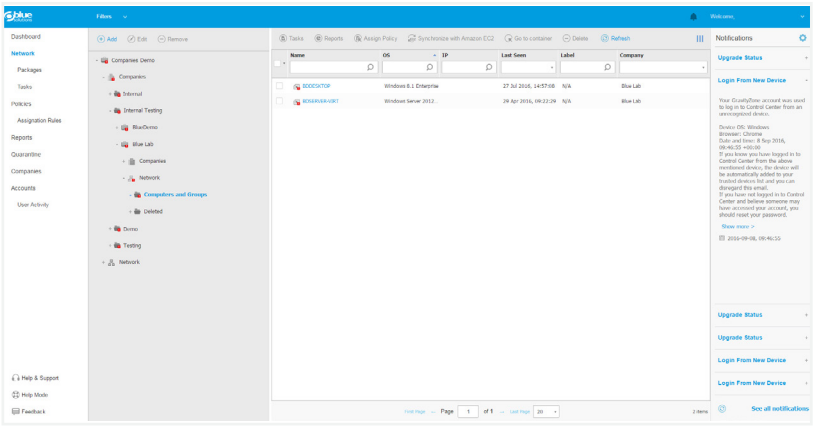
The reality is that many security vendors simply do not offer this unified management capability, or the integrations and interface simplicity that enable it to deliver maximised efficiency.

[1] http://www.alliedmarketresearch.com/managed-security-services-market
[2] http://mspmentor.net/managed-security-services/enterprise-customers-turning-droves-managed-security-service-providers-mss; download infographic at http://bit.ly/2bkJjcf
[3] http://mspalliance.com/managed-services-spending-rise/

Just to put into perspective how hazardous this is for the viability of, for example, an MSP business, the MSPAlliance Unified Certification Standard (UCS), the world's oldest and most respected certification audit for the cloud computing and managed service industry, regards any MSP business with gross margins of below 30% as having "risky corporate health"[4] – and a gross margin of 50% is generally viewed as the desirable minimum.

It begs the question how many security vendors' solutions are genuinely enabling MSPs to get anywhere near that figure.





All security and account features easily manageable, in one single console: a boost to service quality and margins that many vendors are nonetheless still unable to truly deliver.

Consider this example: a customer has performed an acquisition and now has many more users that need to be secured, but the device security policies of the acquired company are lax and operating non-conformant security software.

Their service provider now must work out the least operationally intrusive way of effecting what is essentially a "software heart transplant", to ensure the correct solution is in place, before starting to apply correct security profiles to each of the devices and their users.

Typically, this would result in the partner having to undertake, separately:

- Deployment of remote monitoring and management (RMM) agents to carry out a site survey
- Removal of the incumbent security console and all its device agent software
- A manual management and billing process (potentially a different one for each vendor chosen!), to ensure access to and constant control over licences for each of the modules required
- Implementation of a product management console, all the while navigating another set of CRM and quote/proposal management consoles until the additional product management technology is both proposed, ordered, deployed, configured and paid for.

Further, in cases like this, the solution being displaced will often still bear a valid licence, so introducing a replacement mid-term is financially unwelcome, but unavoidable, since it is necessary in order to ensure supportability by the service provider and compliance with security standards the customer already takes for granted!

Result: it costs more time and money to onboard and service customers (because it cannot all be done simply from one place), and more time and money to support them (because the lack of simplicity at the customer end generates more incoming support tickets). Ergo, the partner's profitability takes a nosedive.

How partners know they need to change security vendor, 2 – *Feature fails*

Clearly, economic viability is not the only potential indicator that the time has come for a partner to part company with its current security vendor. As we mentioned in the introduction, the security domain moves fast – and a simple tick-box exercise to establish if the current vendor is delivering against the most urgent threat vectors and up-to-date operating environments, to meet customers' ever-evolving use cases, can be very revealing.

Virtualisation, for example, as we explored in a previous paper, is a critical security consideration.

This is where many security vendors are simply not delivering the protection that their customers need, because their "virtualisation security solutions" have in fact not been designed from the ground up to operate in virtualised environments.

Instead, they are aftermarket bolt-ons for pre-virtualisation, pre-cloud architectures – a technical compromise that has a knock-on impact on both performance and economy.

[4] http://mspalliance.com/thought-managed-services-margins/

The hallmarks of such a fudge are numerous, and include:

- **Disparate architectures** for different cloud and data centre environments
- **Multiple agents** that drag down system response time (often to the point where it effectively stops the security functioning properly, thus opening up vulnerabilities)
- **Lack of uniform integration** across all virtualisation platforms, hypervisors and operating systems (VMware, Citrix, Microsoft Hyper-V, KVM, Oracle, Windows, Linux)
- **Non-optimised scanning** that burdens the virtual machine with management of the anti-malware processes on large numbers (typically 90%) of files that present no genuine danger

The potential feature fails do not end there, however. Consider one of the hottest topics in the security landscape – Data Loss Prevention (DLP). With IBM putting the cost of data breaches in 2015 at 23% higher than in 2013,[5] and with Gartner predicting that DLP adoption will rise to 90% by 2018,[6] DLP is a wake-up call for end-users and partners alike.

Yet only a handful of vendors offer it as an integral part of a wider security offering, with most DLP solutions being separate solutions, implying, as industry commentators have observed, that they can prove "expensive to install and maintain"[7] – hardly a recommendation for partners to keep these kinds of standalone DLP solutions on board.

Further, too many DLP vendors tie partners and end-users into reliance on an Exchange module and expose them to the costs associated with acquiring the corresponding licences, since this is the only way they are able to scan the outbound (SMTP) email traffic that is the principal carrier of sensitive data.

Partners must ask themselves whether a vendor's strategy to rack up add-on licence fees, which in turn erode the partners' margins or inflate their pricing to end-users, is a sustainable basis for a continuing commercial relationship.

And **on the device front**, too, there are plenty of reasons why a current security vendor's offerings might not be up to speed.

Device **peripherals** like external storage media (SD cards, USB thumb drives) and even the increasingly ubiquitous Thunderbolt hardware connector, if unrestrained) can support the growth of shadow IT and also present a significant security risk.

Yet few vendors see fit to make it easy for partners and end-users to manage and monitor these connections, or easily block or allow apps (peripheral-related or otherwise) that device users choose to download and use.

There are surely only so many feature fails a partner can tolerate before deciding to take their security business elsewhere!

How partners know they need to change security vendor, 3 – *Out-of-the-box vs. premium play*

But any discussion of the richness of security vendors' solutions feature must inevitably lead us to ask how many of those features are actually delivered in ready-to-go, out-of-the-box form – and how many of them are either heavily dependent on costly expert fine-tuning, or are only available as premium extras.

When this balance is too heavily stacked in the vendor's favour, it is time for the partner to start looking elsewhere for their security offering.

Exactly the same logic applies to support and service. It's not just a question of the *extent* and *quality* of the support – whether it's 24-hour, how intensively it can be called on in the deployment and roll-out processes, whether the support staff are product-certified engineers, and so on – but whether it is subject to product family restrictions (e.g. SMB customers get less support than enterprise), or indeed minimum purchase quantities.

[5] In https://securityintelligence.com/cost-of-a-data-breach-2015/
[6] In http://www.computerweekly.com/news/450302219/Global-infosec-spending-to-reach-63bn-in-2016-says-Gartner
[7] http://searchitchannel.techtarget.com/feature/Data-security-Alternatives-to-data-leak-prevention

The brake on business growth that a partner may experience by taking on customers that are rendered expensive to manage and support by the security vendor's product marketing and support policies is, once again, an excellent reason for partners to now be re-examining those vendor relationships.

Performance and savings uplift from truly virtualised security

Security solutions that have been built from the ground up for virtualised environments can deliver significant performance and savings benefits, as this table shows.

The data in the table came from testing physical-heritage security vendors' endpoint products against incompletely virtualised solutions, and then against purpose-built virtualisation security from Bitdefender.

The results speak for themselves!

Endpoint Security - Virtualisation Performance Estimator		Unit of Measure	Bitdefender	Next-best Preformer	Worst Preformer	Results	
						Bitdefender performance superiority/ saving relative to Next-best Performer	Bitdefender performance superiority/ saving relative to Worst Performer
Infrastructure Requirements[1]	RAM	GB	132.37	182.87	313.95	28%	58%
	Disk	GB	126.33	495.75	351.00	75%	64%
	CPU Load	GhZ	152.30	266.69	254.18	43%	40%
Training/Up-skilling[2]	Initial	Hours	18.00	15.00	24.00	-20%	25%
	On-going[3]	Hours	8.00	13.00	8.00	38%	0%
Deployment	Planning & Implementation	Hours	6.00	6.00	11.00	0%	45%
	Customisation and/or Consulting	Hours	1.00	4.00	5.00	75%	80%
Administration[4]	Daily[3]	Hours	316.25	442.75	506.00	29%	38%
	Periodic S/W Up-grades, Hotfixes etc.[5]	Hours	9.00	11.00	18.00	18%	50%

1 - Results shown represent average cumulative system resource requirements imposed by certain endpoint security products when deployed onto 150 individual machines, with management server and security server overheads included, and have been based on observations of software carrying out a full system scan with vendor's default settings.
2 - Estimate assumes two administrators
3 - Estimate assumes three year view
4 - Inclusive of estimated end user billing, system monitoring, management and reporting
5 - Three year view which assumes estimated quarterly involvement

How partners know they need to change security vendor, 4 – *Profile vs. proliferation*

Security is the most reputationally sensitive of all services, as far as customers are concerned – and partners providing security solutions are deeply implicated in that sensitivity. Nowhere is this thrown into sharper relief than in the EU GDPR regulations that are set to take effect in less than two years, under which **any MSP providing or provisioning services will be liable, as the incumbent "data processor", for any security breaches sustained.**[8]

Now, more than ever, then, it behoves partners to look again at their security vendors' stability, credibility, credentials, and expertise – and to make an honest decision on whether they are genuinely trustworthy in an environment that is on its way to becoming dangerously litigious.

Slick marketing and a high profile on media and social networks are not necessarily the most accurate barometer of this trust.

Instead, partners need to look at "adoption fundamentals" – in other words, how many big-name corporations are embedding the vendor solutions within their own technology (OEM)? How many endpoints worldwide do the vendor's solutions currently protect? How many nodes are the vendor's solutions running on, and how does that compare to the vendor's competitors?

In the final analysis, implementation is more telling than image – and it is on the basis of this criterion that partners must now judge whether it is appropriate to continue with their current security vendor, or seek a more reputationally reassuring relationship elsewhere.

How partners know they need to change security vendor, 5 – *Cloud/hybrid rigidity*

Cloud and security are coming together to potentially create a "perfect storm" of customer demand, with tech budgets focusing heavily on both these domains in 2016, according to industry analysts IDG.[9]

But there is a vital intermediate stage through which many customers will have to pass before they achieve either cloud or security nirvana. And the reality, regrettably, is that most security vendors simply do not offer the flexibility that enables partners to deliver to their customers a security solution that covers off both the cloud and non-cloud bases implicit in this phase *economically*.

To explain this, consider, for example, a typical security vendor's security scanning process. It may, if it is a more advanced solution, offload security scanning to a centralised scanning resource to reduce the processing burden on each endpoint. But this offloading is invariably confined to *either* on-premise or *same-network* scenarios.

This works fine with local data centres, private cloud, and some kinds of public cloud integrations, but if the customer has *distinct* networks, connected to via the internet, that *each* need protecting, most security vendors' solutions currently cannot deliver.

Another reason, therefore, for the partner to consider alternative security solution suppliers.

Conclusion: What price vendor change?

Fear of disruption, and of the costs that inevitably accompany it, dog the prospect of vendor change for partners.

Yet the fact is that in an era where ever more flexible MSP programs are becoming the dominant business and billing model, and cloud the dominant delivery mechanism, switching from one vendor to another no longer implies this degree of upheaval. The barriers to vendor change, in fact, are lower than ever.

[8] http://searchcloudsecurity.techtarget.com/news/450300226/Cloud-apps-failing-EU-GDPR-privacy-regulation-compliance-so-far
[9] http://www.idgenterprise.com/news/press-release/tech-budgets-focusing-on-security-and-cloud-computing-in-2016/

Yet change for change's sake is rarely productive, and partners must ask themselves honestly whether there are clear signals from their vendors that the latter are genuinely continuing to deliver on their inevitable promises of a profitable security business that comes with rock-solid credentials, latest-and-greatest threat vector protection, and efficiency tools that swell partners' margins.

The argument advanced in this paper is that many indicators from many vendors show precisely the opposite, and only one conclusion can possibly be drawn from this: that it is high time their partners sought their security vendors elsewhere.

Failing to do so could cost partners their reputation, their credibility – and, ultimately, their business.

About Blue Solutions

Since 2000, Blue Solutions (www.bluesolutions.co.uk) has enabled IT channel partners to market managed services software that boosts recurring revenues, strengthens margins, and clearly differentiates partners' offerings in a crowded market.

Key vendor relationships (Bitdefender, CensorNet, DataFortress, Malwarebytes, Microsoft, Phish5, Redstor, Symantec, TrendMicro and others) enable Blue Solutions to take the profit-sapping pain out of partners' processes, as well as deliver ready-assembled MSP solutions.

Uniquely, the company focuses 100% on partners' services revenues - not low-margin hardware – across security, Cloud, data protection, and more.

Blue Solutions enables partners to build profitable, regular revenues, delivering what competitors can't – scalable, economical managed services that delight end-users.

Next Generation Security Distribution

0118 9898 222 | info@bluesolutions.co.uk | www.bluesolutions.co.uk

FOLLOW US