Next Generation Security Distribution

Blue Solutions Opinion Paper

# Layered Security v. One-Stop-Shop:

## What You and Your Customers Need To Know

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

## Introduction

Malware is skyrocketing – and the numbers are shocking. Antivirus vendors are detecting some 200,000 new malware strains every day.

Loss of the precious data that is usually the target of these attacks - plus the operational disruption that inevitably accompanies them - sends hundreds of businesses under yearly. In fact, Lloyds of London has publicly stated that from 2015 they "fully expect a business to fail due to the financial consequences of a cyber attack"[1].

But It's not just the sheer volume of malware that is alarming – it's also the bewildering variety in the malefactors' armoury, and where, when, how, and who these weapons are programmed to strike.

The delivery channels overlap and feed off each other terrifyingly; according to the Verizon Data Breach Incident Report[2] (DBIR), for example, 54% of malware infections are due to interaction with the web, and 77% of malware infections are due to users receiving a malicious email with a web link or attachment.

Zero-day exploits, viruses, Trojans, malicious websites, phishing, spear-phishing, social engineering attacks - against this backdrop of unchecked proliferation, we surely have to ask ourselves whether the "one-stop-shop" solutions sold by some security vendors are seriously capable of doing the job they claim to do for customers – particularly SMBs.

Is it really possible for one solution to protect against every strain of malware? At every point at which it may strike? For every kind of exploit that it executes?

But what of the alternative – the so-called "layered" security approach? Does combining multiple solutions really give "belt and braces" protection, or does it simply offer more opportunities to accidentally expose the gaps in the wrapping?

## One-stop-shop security: years behind?

Recent attacks on high-profile brands and companies like Jamie Oliver, Carphone Warehouse, Ashley Madison and Talk Talk have demonstrated that, in contrast to the confident rhetoric of protection and containment that the industry likes to deliver, even larger organisations' IT security is seriously behind the curve. **It can neither spot the warning signs that malware is on the way, nor offer comprehensive enough protection against threats when they strike.**

The embarrassing proof for this claim is that, according to Verizon, in one year alone, 99.99% of exploits took advantage of vulnerabilities that had been identified as known risks **a year previously.**

And, breathtakingly, a number of the exploits **made use of security flaws that had been documented since 1999 – when many of today's security developers and engineers (and hackers!) were still at school!**

Firms do not publicly reveal the details of the IT security solutions and service providers that they use – for good reason – but to critical eyes, the shortcomings described above bear all the hallmarks either of one-stop solutions that have simply been oversold, or multiple disparate solutions that simply do not work together effectively.

[1] http:// www.businessinsurance.com/article/20150409/NEWS09/150409853/business-failure-from-cyber-attack-likely-in-2015-official
[2] http://www.verizonenterprise.com/DBIR/

## What are "layers" – and what benefit do they deliver?

Layered security's central philosophy is, at root, a logical one - that no one solution can cover every base.[3] Customers need layers of solutions, to address every evolving malware eventuality.

So, for example, an anti-malware suite might have four distinct functional layers, which will not displace the layers of functionality delivered by other solutions in the same customer. These might look like this:

- **Application hardening,** to make outdated or unpatched applications less susceptible to attack
- **Operating System security,** to stop exploit shellcode executing
- **Malicious memory protection,** to prevent the execution of payloads
- **Application behaviour protection,** for specific applications like Word, PowerPoint and others

But layered protection takes on two further dimensions of significance, too – an **economic** one, that will appeal instinctively to resellers, MSPs and other channel partners who supply security solutions to end-users, and a **predictive** one, that will appeal to end-users directly.

Firstly, **the economic.** If customers need layers of solutions to address every malware eventuality, that presupposes that the layers will not conflict with or displace each other. If the layers do not displace each other, then resellers and MSPs can potentially sell multiple security solutions into each customer, creating several revenue streams where previously there was only one.

Secondly, **the predictive.** Layering, despite what is said above, does not simply mean combining multiple security solutions and functions harmoniously (and profitably) within one customer, to protect against different kinds of malware.

In fact, in its most effective sense, layering means combining solutions that protect *against different kinds of malware across all the stages of evolution through which that malware passes, and by which it signals its presence.*

This is a *crucial* distinction. No security solution, layered or otherwise, delivers maximum value to customers and users if it only reacts to mature threats, because by this point the threats' ability to sow damage is already established.

Far better to detect *burgeoning* threats, across the *entire threat landscape*, so that the threat has already been mitigated by the time it becomes a "known" risk.

This philosophy is rooted in the idea that malware is a product like any other – it goes through a process of development, testing, and deployment, which translates into an infection timeline.

Effective layering of solutions means ensuring that your layers, whatever kind of malware they focus on, start to spot and remediate threats along this timeline long in advance of the threats hitting their stride, providing a carapace of protection - before, during and after.

Catch an infection early and it will do little or no damage.

[3] https://en.wikipedia.org/wiki/Layered_security#Philosophy

## What of the "one-stop-shop" approach?

Fundamentally, the idea of a one-stop security approach for customers simply militates against practical reality.

As with most things in engineering, one solution that is designed to address every conceivable problem tends to deliver mediocre performance across the piece. When malware is developing and mutating at such a stellar rate on a daily basis, this "one size fits all, always" approach simply lacks credibility.

Here are just a few examples of the challenges - both malware-borne and in-house - that security has to protect customers against if it is to do its job properly. How many of these is a one-stop solution credibly able to simultaneously defend against?

- Phishing email
- Spear phishing attacks (accounting for 55% of malware attacks experienced by IT networks in the last year)
- Drive-by download
- Malicious attachment
- Trojan
- Ransomware payload delivered by email
- Unpatched software
- SQL injection attack
- Web-borne malware attacks (accounting for 80% of malware attacks experienced by IT networks in the last year)
- APTs (accounting for 65% of malware attacks experienced by IT networks in the last year)
- Rootkits (accounting for 65% of malware attacks experienced by IT networks in the last year)
- Missing or poorly implemented encryption
- Weak wireless configuration
- Legacy and other unsupported applications
- Insecure vendors and business partners

Moreover, in an effort to fudge this inherent mismatch between the reality of the threat landscape and the functional capabilities of their products, many one-stop-shop vendors have resorted to deliberate opacity in how they assemble and describe their solutions.

For example, they often apply terminology borrowed from the enterprise and "point" versions of their products to the cut-down versions designed for one-stop SMB use, when the functional scope of each (and the extent to which they are supported) is in fact very different.

Does "web content filtering" mean the same thing in a separate-but-ever-more-closely-integrated enterprise solution as it does in a one-stop SMB sticking-plaster offering? Unlikely.

Likewise, vendors often combine SMB and enterprise offerings into one, giving the impression that the same high-capability technology is theoretically available to both audiences. But no vendor can truly offer champagne-level protection modules at beer-level prices; somewhere, functions are being rationalised, but vendors are often reluctant to clarify this.

Once again, the statistics speak for themselves: if one-stop software is the dominant approach in the market (which it is), and can comfortably handle all the threats ranged against it, then why, according to Verizon[4], do 60% of attacks manage to compromise organisations **within minutes?**

[4] As previously cited

And with a majority of IT admins and security practitioners stating, in recent research[5], that current working practices are only going to drive this risk skyward, (73% of respondents cited the use of commercial cloud applications, 63% home and offsite working, and 68% employee-owned mobile devices), does the one-stop approach really have *any* security credibility left at all?

## One-stop security v. layered – the commercial view

Of course, at some point in the sales cycle, the basic human need for convenience and the basic business need for cost-effective simplicity assert themselves, and this is where one-stop security solutions – particularly those delivered through the MSP model, where the customer is totally "hands off" – *can* prove attractive.

Customers value the solutions because their apparent all-inclusiveness gets a huge headache off the IT security manager's desk in one drop. Partners value the solutions because their very inclusiveness often means they come with centralised consoles for licensing, servicing, reporting, and technical management, plus integrations to automated RMM and PSA solutions.

This is a degree of low-maintenance manageability that the powerful layered players are, for the moment, perhaps not able to deliver in quite the same seamless way.

In addition, some non-layered security vendors do benefit from an established reputation and enviable brand trust, simply because they have been developing and marketing for so long. Some have even produced multiple award-winning solutions that, consequently, have a fiercely loyal reseller, MSP and end-user following worldwide.

## Conclusions

But partners are in this business to make a profit, and it stands to reason that if they can provide multiple layers of protection that cover off every conceivable malware instance, and charge for each of them - particularly within customer installations that can continue to use solutions the partner has previously supplied - the financials look compelling.

In contrast, the one-stop-shop offers little flexibility to tackle specific and emerging threats, little opportunity to easily multiply revenue streams, and, because it will often displace other solutions already installed, **little commercial potential within the multi-layered threat landscape that commentators are already predicting[6] will predominate in 2016 – and beyond.**

[5] See infographic at https://www.malwarebytes.org/articles/why-layered-security-is-important/
[6] http://www.securitynewsdesk.com/physical-security-and-cyber-security-predictions-for-2016/

## 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.

Learn more about layered versus one-stop-shop security opportunities in the IT channel.

Next Generation Security Distribution

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

FOLLOW US