Next Generation
Security Distribution

Blue Solutions Opinion Paper

LET'S GET PHYSICAL? SERIOUSLY?

The "Virtualised" Security Solutions

That Dance To Yesterday's Tune

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

Introduction

The meteoric rise of virtualisation technologies has exposed an embarrassing weakness at the heart of many vendors’ supposedly virtualised security offerings: namely, that they were not conceived, designed, or built for the challenges of virtualised environments at all.

Instead, the virtualisation capability has often been retro-fitted onto existing solutions designed for a physical age where servers were made of tin, kept on-premise, and maintained by large and expensive teams of IT personnel.

Like the car whose evolution has propelled it at higher speeds than its braking system could ever realistically keep step with, virtualisation is all too often a cutting-edge technology undermined by yesteryear’s security tools.

For today’s businesses – and the security vendors, partners and distributors that supply them – this is a challenge that is simply not going to go away. According to industry analyst Gartner, the virtualised server market “has matured rapidly over the last few years, with many organizations having server virtualization rates that exceed 75 percent, illustrating the high level of penetration.”[1]

And though this on-premise market is set to peak in 2016, the need for economical, on-demand, instantly extensible compute capacity is fuelling businesses’ use of both private and public cloud, both of which depend heavily on virtualisation for their operating model.

Public cloud provider AWS, for example, saw its AWS revenues rise almost 70% in 2015. Public cloud prices have also fallen 66% in three years, according to some estimates, further stoking demand for the benefits of virtualisation.[2]

Yet peel away the public cloud euphoria and the underlying trend is one of deep concern over the security of virtualised environments. The Jericho Forum, a think-tank devoted to information security matters that works closely with the Cloud Security Alliance (CSA), has stated that “A lot of companies are going into the private cloud because they cannot guarantee the security of the public cloud.”[3]

The implication is clear: when it comes to businesses’ perception of virtualised security, the existing raft of physical-heritage virtualised security solutions fail to inspire confidence. This paper explores why, and points to the specific features that *true* virtualisation security must offer.

Virtualised performance: traditional security’s Achilles heel?

Safeguarding system performance in virtualised environments requires a security approach that has been built from the ground up *for* those virtualised environments.

The real danger is that a traditional security approach, built on an underlying architecture that relies on the physical tenets of security on each machine, multiple agents, and indiscriminate scanning (even of files that are incapable of execution that can harbour malicious code) simply becomes one huge drain on the system’s core business processes.

This flies in the face of everything that virtualised environments stand for – a high degree of scalability, underpinning a high degree of performance, at much-reduced cost to the business.

Instead, what passes for virtualised security often in fact bogs down the entire business infrastructure, creating a productivity killer that wipes out the notional benefits of virtualisation and hits businesses where it hurts most – their bottom line.

[1] http://www.gartner.com/newsroom/id/3315817
[2] http://www.computing.co.uk/ctg/analysis/2445923/public-cloud-poised-for-a-huge-upswing-this-year (both references)
[3] http://www.computerweekly.com/feature/Cloud-computing-UK-companies-adopt-eagerly-but-often-insecurely

As one virtualisation security user put it, the acid test of suitability for a virtualised security solution is "the product's performance in our virtualization environment, how much the product would or wouldn't interfere with users' productivity..."[4]

A compromise architecture that has added virtualisation as an after-market security is unlikely to perform well in this respect; after all, seamless compatibility with all things virtual is a difficult thing to achieve if a product was originally architected to run on *no* things virtual!

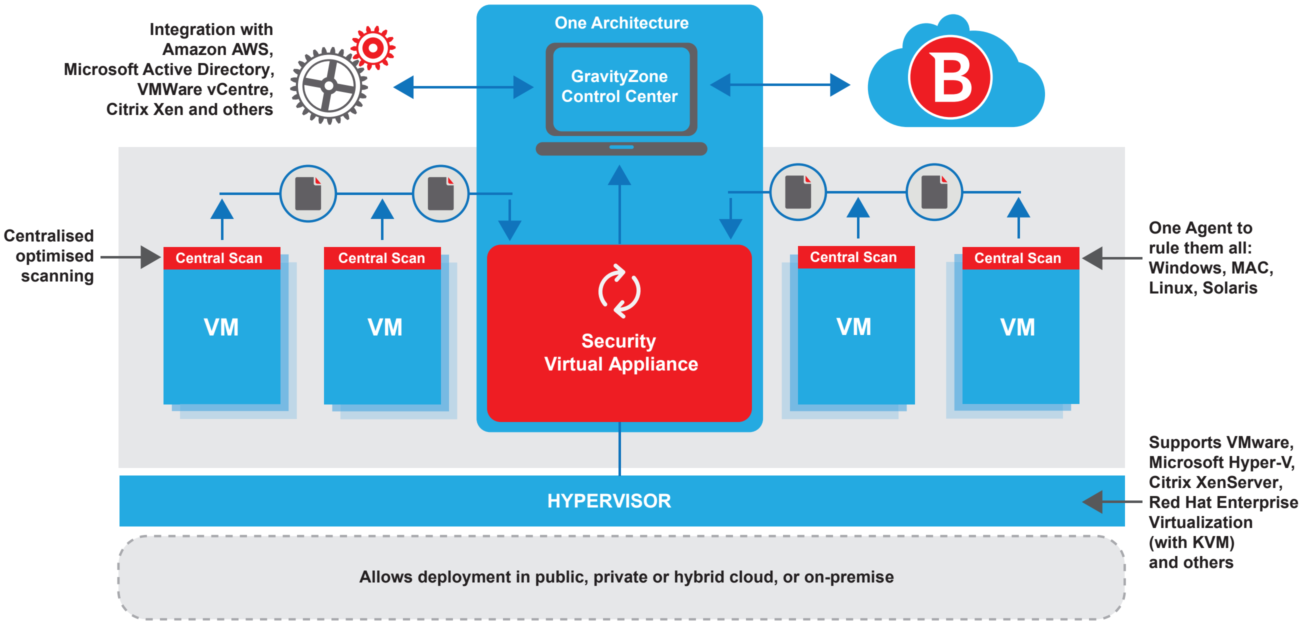
The situation is made even more unsatisfactory by the proliferation not only of virtualisation platforms but also the types of hypervisor that manage and run them - and *their* inherent strengths and weaknesses[5] - creating a huge hurdle for the performance of many security solutions.

Virtualisation security: defining features and must-haves (1)

To this end, we believe that the following features are the *minimum* a security product must offer if it is to operate effectively in a virtualised environment, without compromising overall system performance:

1. **One architecture**, enabling efficient, inbuilt (not add-on) visibility and control across data centre and cloud
2. **One agent**, covering any combination of virtualisation platforms, private and public cloud providers (not multiple agents dragging down system response times)
3. **Integration** with *all* leading virtualisation platforms, hypervisors, and operating systems (VMware, Citrix, Microsoft Hyper-V, KVM, Oracle, Windows, Linux)
4. **Centralised, optimised scanning**, to free each individual virtual machine from the burden of managing the anti-malware processes, and to focus on the c. 10% of files that are capable of presenting a ***genuine*** danger

Fig. 1



A security architecture built from the ground up for optimal performance in virtualised environments.

[4] http://download.bitdefender.com/resources/media/materials/virtualized-environments/en/Bitdefender-2015-NGZ-SecurityForVirtualEnviro-DS-70574-A4-en_EN-web.pdf
[5] http://searchservervirtualization.techtarget.com/feature/Three-hypervisor-and-virtual-environment-security-concerns

Managing the virtual security estate: a challenge too far for traditional vendors?

Perhaps the greatest operational weakness in security approaches that were not designed with virtualisation in mind is that they were never intended to manage and control the huge numbers of endpoints, servers, processes, devices and users that virtualised environments enable to be rapidly brought on board and, more importantly, added to.

Consequently, many of them have no integrated means to do so, meaning that deployment, implementation and ongoing provision swell the vendor’s or channel provider’s administration overheads and eat into their margins, whilst the customer experience is much diminished.

Again, this adds insult to injury because it effectively negates one of virtualisation’s proudest boasts; minimised hardware needs and energy consumption mean nothing if those savings evaporate because the security is so costly and time-consuming to manage!

But it would be a mistake to think that the absence of effective, easy security management and control is merely a financial inefficiency to be absorbed somewhere in the company accounts. The point here is that a security service or solution that cannot be easily managed runs the risk of being *mis*managed – and that potentially opens the door to an incident.

Multiply that risk by a generous factor (because virtual environments are so highly populated with both processes and users, and therefore present such a broad attack surface) and it is hardly surprising that recent research claims that **when a security incident involves virtual machines, the recovery costs double compared to that of a traditional environment!**[6]

Ultimately, traditional security solutions that have not been developed with virtualised environments in mind simply do not offer a “single pane of glass” onto the entire provisioning and management process, across the entire architecture.

The result, potentially, is that what starts off as provider pain and customer disenchantment eventually becomes the security solution *failing to do the one thing it was put in place for.*

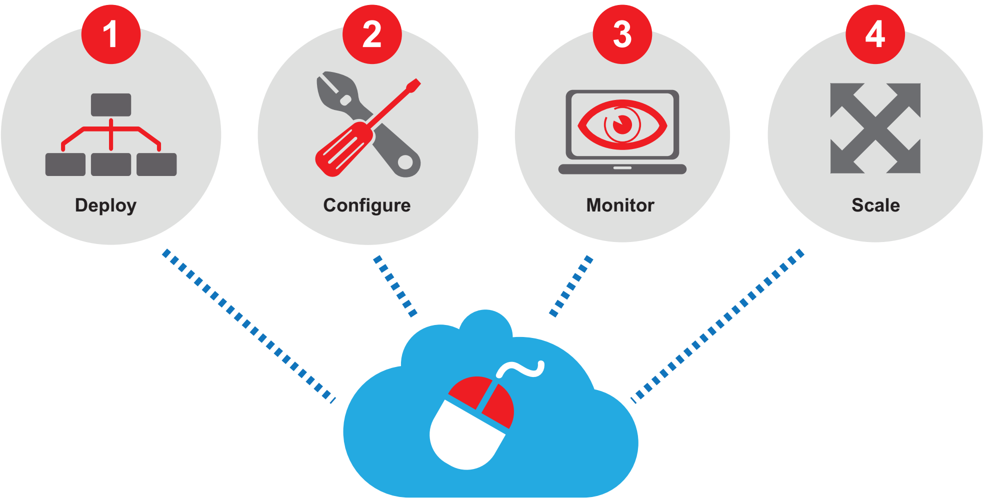
Virtualisation security: defining features and must-haves (2)

Inevitably, then, this leads us to consider how a security solution for virtualised environments can avoid the above shortcomings. We believe that the following features are indispensable:

1. **Simple and easy deployment** – Getting up and running quickly is part and parcel of delivering security in a virtualised environment. A self-configuring, hardened virtual appliance is an effective deployment mechanism to this end, but it must be intuitive for largely Windows-trained administrators to use!
2. **One single console** – Centralised management, deployment and enforcement of security policies to *any* number of endpoints, on any hypervisor, in *any* cloud, is critical to effective virtualisation security management, for end-users and service providers alike
3. **Instantly scalable** – A friendly console is useless if it does not offer the capability to easily scale security to protect proliferating endpoints, servers and users. Security scalability should ideally be a matter of simply cloning virtual appliances, at the click of a mouse, or relying on the elasticity of a cloud security service provider to achieve the same end result.

[6] http://www.csoonline.com/article/2974712/disaster-recovery/report-virtualization-doubles-cost-of-security-breach.html

Fig. 2



1. Simple and easy deployment to get up and running quickly
2. Configure enforcement of security policies to any number of endpoints, on any hypervisor, in any cloud
3. One single console for Centralised monitoring and management
4. Instantly scale security to protect proliferating endpoints, servers and users

Virtualised security made simple: a single console controls all monitoring and management.

Why virtualised security demands more of its anti-malware

The debate about whether physical servers or virtual servers are more secure rages on, but what is absolutely clear is that virtual machines have their own set of *additional* vulnerabilities that are distinct from, but potentially just as devastating as, those that apply to physical machines – with some additional potential for cross-propagation between them.

These range from hypervisor attacks (which could potentially compromise every virtual server controlled by that hypervisor), targeted malware that focuses on older VM server snapshots that have been generated as part of a disaster recovery process and are now defenceless, and attacks on unprotected physical servers to which virtual machines have been relocated.[7]

The question must of course immediately be asked, how likely is it that security solutions not originally conceived and built for virtualised environments can even *detect* these threats, still less *stop* them?

This virtualised inadequacy in many traditional security solutions is exposed further when we consider that existing endpoint security will often not only fail to *protect* virtualised environments, it can actually *disable* virtual security completely, as a result of slowing down the network![8]

It seems that many traditional security solutions built for non-virtualised environments are unlikely to offer either the specialist protection that virtualised environments require, or the confident defence against established threats that are common to both virtualised and non-virtualised environments.

In short, virtualisation demands better!

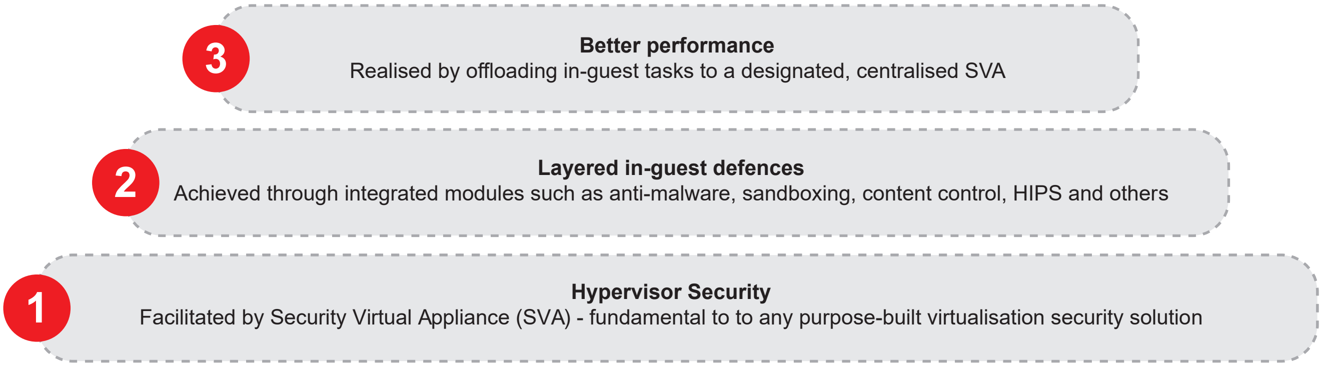
[7] http://www.zdnet.com/article/virtual-servers-no-safer-than-any-other-kind/
[8] http://www.ecommercetimes.com/story/80573.html

Virtualisation security: defining features and must-haves (3)

In our view, the vulnerabilities exposed above mean that true malware protection for virtualised environments cannot be achieved unless the following features are available:

1. **Hypervisor security** – The prospect of a hypervisor being compromised and taking unlimited numbers of virtual machines with it is chilling, but true hypervisor security must operate at a level *below* the OS, so that attackers cannot disrupt it or evade detection
2. **Multiple security layers** – Virtualised environments are designed to run software efficiently – and malware is software! This makes virtualised environments no safer than any other, so the same multi-layered security philosophy must apply, including anti-malware, anti-virus, zero-day threat protection, content control, device control, etc.
3. **Measurably optimised performance** – Performance issues are not only a productivity issue, they can also compromise security applications’ ability to do their job, as we have seen above. Virtualised security products *must be able to demonstrate independently-tested low levels of performance impact* in virtualised environments, as well as *proven levels of server consolidation* (an excellent indicator of both performance and economy)

Fig. 3



3 **Better performance**
Realised by offloading in-guest tasks to a designated, centralised SVA

2 **Layered in-guest defences**
Achieved through integrated modules such as anti-malware, sandboxing, content control, HIPS and others

1 **Hypervisor Security**
Facilitated by Security Virtual Appliance (SVA) - fundamental to to any purpose-built virtualisation security solution

The three touchstones of a trusted virtuallsed security solution.

Conclusion - Are you singing the right security song?

Physical server infrastructure is not dead – far from it – but it’s shrinking fast, and where it does still exist, it’s increasingly simply the chassis in which a much more powerful virtualisation strategy is now the engine.

One CIO went from 150 servers in his corporate data centre to just three, joking that he could use the space saved as a basketball court, and citing virtualisation as a driving factor in that downsizing. In his words, “Combining disparate applications in a shared virtualized server environment allows us to efficiently apply the resources of the physical server.”[9]

This sends a clear message – if one were needed – to end-users, channel partners, and distributors everywhere. The music of the market has matured. Virtualisation is the star, and the security songsheet of an earlier generation no longer has the tunes to match our times.

Let a new chorus begin.

[9] http://www.fiercecio.com/story/broadviews-cio-weve-gone-150-servers-3-our-corporate-data-center/2016-03-14

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