vmware®

IDG CONNECT

VIRTUALIZATION'S HIDDEN GEM:

APPLICATION SECURITY

How network virtualization and micro-segmentation can secure your application infrastructure

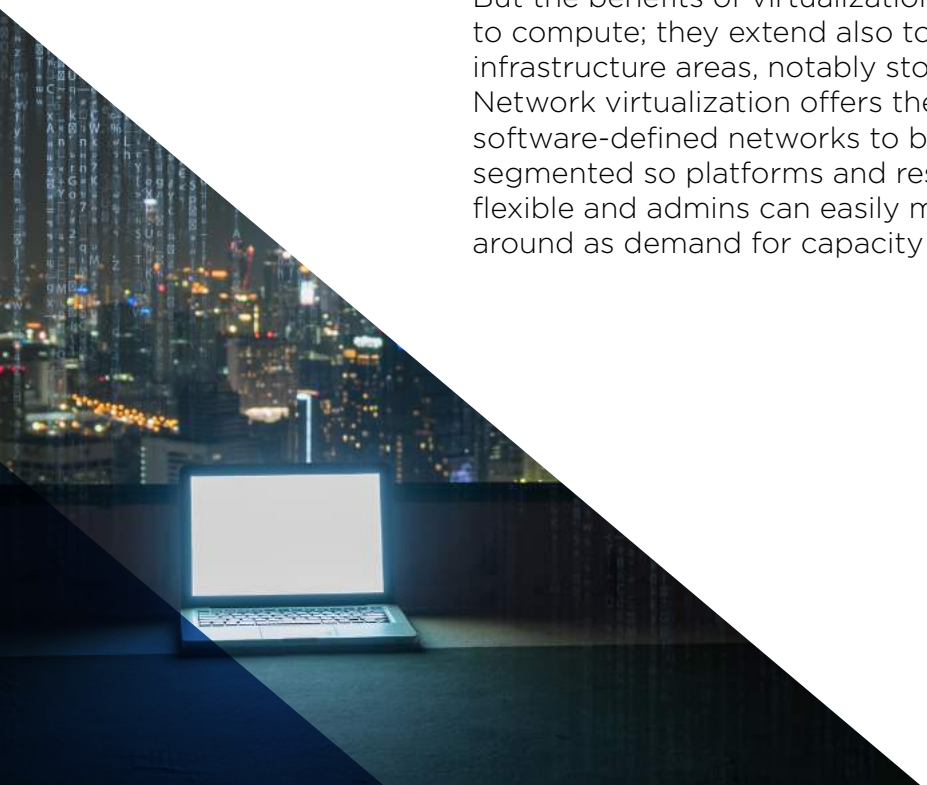
WHITE PAPER

INTRODUCTION : application infrastructure security is the ‘ace in the hole’ of network virtualization

The advent of x86 server virtualization in 2001 revolutionized data centers by providing a way to aggregate compute workloads on virtual machines, move those workloads across physical servers, gain unheard of levels of hardware utilization, reduce server room power consumption, and more.

But the benefits of virtualization are not limited to compute; they extend also to other core infrastructure areas, notably storage and networking. Network virtualization offers the chance too for software-defined networks to become micro-segmented so platforms and resources become flexible and admins can easily move workloads around as demand for capacity changes.

But the core qualities of network virtualization also offer another hidden gem: the chance to rethink the fundamentals of how application infrastructure, from database servers to email and web servers, is secured. And this opportunity comes at a serendipitous time as the old monolithic applications and reliance on tightly limited controlled platforms is being replaced by distributed microservices running across multiple on-premise and cloud platforms.



vmware®

IDG CONNECT

SECURITY: the pain that never goes away

The inexorable drive to move more business processes and activities to the digital sphere has changed the world. Startups will overwhelmingly tap the internet and IT to create low-touch/zero-touch environments that dispense with the cost and slowness of manual activities, and veterans and incumbents are faced with a binary choice - to adapt to the new world or die.

Moving physical products to software code (for example, CDs to MP3s, DVDs to digital streams or books to audio downloads) changes the face of production, distribution, logistics, and much more. Minimizing the need for physical outlets creates enormous operational efficiencies for Amazon and other online sellers. Little wonder that there is a never-ending race to digitize more; as Marc Andreessen has famously written, software is eating the world.

We've all seen how companies such as Uber can transform business categories through digitization. But the flipside of that dramatic change is that, as processes, goods and services grow in value, more attackers want to disrupt those processes and steal or compromise the valuable data and intellectual property therein.

Most companies today admit to having experienced data breaches (and most of the rest are misinformed or fibbing). Data breaches occur every day and can last for years without being detected. Those breaches can have traumatic effects on finances and bigger ones on corporate reputation. Even as enterprises and governments have invested more and more and hired specialist CISOs, the waves keep on coming. At the same time, regulations get tighter and tougher. With the General Data Protection Regulation (GDPR) legislation that impacts companies trading in the European Union beginning in May 2018, penalties imposed extend to four per cent of global revenue – potentially billions of dollars.

SECURITY: the pain that never goes away

After being constantly buffeted by threats, organizations have attempted to shore up their defenses, ploughing huge upfront capex sums into protecting their digital assets. For information security vendors this is a boom age and the boom shows no signs of stopping: from ransomware to industrial espionage and state-sponsored attacks, threats grow and morph. Depending on how you measure it, cybersecurity today is perhaps a $120 billion industry, outpacing even the broader technology industry while many of the hottest startups and IPOs come from the cybersecurity space. As Box CEO Aaron Levie has tweeted,

"Dear kids, if you want a job in 5 years, study computer science. If you want a job forever, study computer security."

Break down the information security industry a little and you discover that application security is the fastest growing sizeable internal category, perhaps tripling in scale over the next five years as organizations seek to protect the core business software and as attackers seek out loopholes that will give them access to the crown jewels – data.

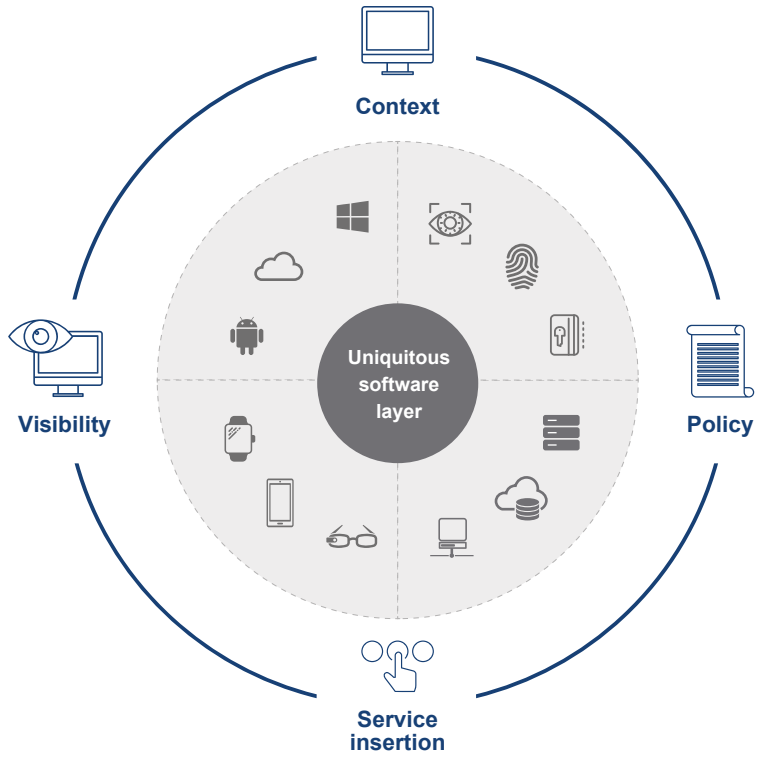
Adding to security woes is the trend towards a more fragmented infrastructure as Bring Your Own Device schemes, the rise of the Internet of Things, increased use of mobile devices, more federated, multiplatform environments and other movements threaten to create vectors for attackers to rend the fabric of defenses again and again.

ABSTRACT ART: it's not just about the perimeter anymore

Just as medieval kings and lords built castles with fortifications, strong walls, turrets and moats, defended by men with bows, arrows and boiling oil, the response of the information security industry has historically been about defending the perimeter, often with firewalls and server appliances for intrusion detection, blocking malware, viruses, identifying suspect behavior and other forms of threat management. But as threats have multiplied, morphed and blended, this is a tactic that no longer works on its own.

Today, we need other, complementary ways to protect assets. In particular, with borders being so porous and challenging to plug, there has been a shift towards protecting at the application infrastructure level. And one approach that protects application infrastructure arrives pre-packaged with network virtualization software. Virtualization hypervisors work by creating an abstraction layer that sits between application and underlying infrastructure and this layer can be tapped to create a far more effective form of defense than was previously possible, at a lower cost and with a lower requirement for administrative chores.

A UBIQUITOUS SOFTWARE LAYER MEANS SECURITY IS EVERYWHERE



Network virtualization bakes in and enables a way to create a more granular form of security known as micro-segmentation. This is where network activity is broken up into component workload services and where security measures can follow those workloads wherever they go, and regardless of what infrastructure they sit on or move to.

MICRO-SEGMENTATION : a cause for celebration

Micro-segmentation has several benefits:

• Risks are mitigated because malware, rogue code, an infiltration, vulnerability or compromise can be isolated and the attack surface is effectively shrunk.

• Provisioning secure services is fast with no procurement hoops to jump through or time-consuming sandboxing to check on performance impacts. Mistakes are avoided and organizations can achieve what they have always wanted from IT – a way to quickly react to market opportunities and risks.

• Micro-segmentation also allows for faster traffic as it doesn't require the diversions of the old perimeter model where data would be directed to security appliances on the network edge for scrutiny and approval.

• Compliance with regulations can be demonstrated and steps audited and recorded.

• Finally, micro-segmentation involves no 'rip and replace' mandate. Existing security infrastructure, network routers, switches and appliances can sit side by side with the new world.

A PANORAMIC VISTA

The result is a policy-driven security model that is fast, lightweight and effective. Admins gain a bird's eye view of what is going on in the network and potential threats from an abstraction layer that can act as a medium for additional security controls from a wide choice of vendors and tools, including for data-at-rest encryption. That view provides not just visibility but context too, preventing the lateral movement of threats that have pierced the perimeter and entered the datacenter.

This approach also has the benefit of being more pliable than the perimeter model. By using the abstraction layer to protect at the application workload level, data is no longer being shuttled to appliances that sit on the edge of networks and only provide a sideways view into network activity. The abstraction layer effectively offers a view up (to the application) and down (to the infrastructure) and across the networks. There is no need to create switchbacks that 'hairpin' traffic to suit the perimeter, appliance-based model.

It's also an approach that suits the modern demand towards hybrid IT deployment models, for example connecting public clouds to private clouds or creating dynamic virtual workspaces accessible by a wide variety of endpoint devices.

The abstraction layer can be used to protect, regardless of the infrastructure being used, whether IT is on-premises, in a private cloud, a public cloud, or mixture of any or all of the above.

By moving protection to the application workload and providing a holistic and granular view of what's going on in the network, organizations can move towards a security scenario where protection is strong, but that protection does not come at the price of agility or require huge budgets or vast operational complexity. Workloads gain their own private 'bubbles' and there is no requirement for rules to be constantly rewritten, and there is little to no impact on performance. Workload services effectively gain their own automation and policy-based security envelopes with near real-time provisioning.

Context is just as important as visibility. The abstraction layer provides a grandstand view of data traffic movement, allowing IT to apply security to the paths and access points that are busiest or most vulnerable. That layer is also a critical indicator that goes beyond the 'needle in a haystack' offered by point solutions such as log collectors and CIM-based information databases that can leave admins drowning in data but snow blind as to what all that data means.

CONCLUSION : a new take on security

Who should be looking at network virtualization as a source of application infrastructure security? Almost every enterprise. It's counterintuitive to wait for a data breach at a rival or in house before acting. Network virtualization should be in the minds of any CIO transforming IT operations and any CISOs who spend their lives fire-fighting.

Using the power of the abstraction layer as a way to insulate the corporate body from attack is likely to be a popular choice that complements traditional defenses and provides the insights and visibility to demonstrate compliance, provide an in-depth audit, and gain a deeper understanding of threats. Just as with server virtualization, early adopters of network virtualization stand to benefit and differentiate from their peers. Those who take the view of 'Nobody ever got fired by buying [insert your choice of large security vendor here]' and stick with approaches developed over 10 years ago will not.

Network virtualization, like server virtualization earlier, stands to deliver clear benefits to IT and the inside track it provides will give CIOs the chance to lead and drive innovation via a new position of strength.

READ ON

To find out more about how network virtualization can provide a panoramic view of what's happening to your data, and potential threats, visit
http://www.vmware.com/go/secure-app

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with VMware Cross-Cloud Architecture™ and solutions for the data center, mobility, and security. With 2016 revenue of $7.09 billion, VMware is headquartered in Palo Alto, CA and has over 500,000 customers and 75,000 partners worldwide.

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 44 million business decision makers' details to unite technology marketers with relevant targets from any country in the world Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.