VIRTUAL LOCK DOWN

Virtualisation has made the data centre a more flexible and agile place. However, the trade-off in this software-defined shift is a measure of complexity when it comes to protecting our data. Enterprises must reconsider their protection strategy to reflect the new, virtualised world.

Virtualisation of infrastructure certainly allows for an easy in building and deploying patches, new releases and other changes. For more than a decade, businesses and enterprises have leveraged virtualisation to reduce costs and streamline systems. Service providers are able to provide instant provisioning and offer the manageability of dedicated hosting without the need to invest in expensive hardware. While virtualisation at one point was considered a cutting-edge, and perhaps risky move, today virtualisation is becoming a prerequisite to achieve the agility needed to keep up in the modern business landscape.

There are obvious advantages to virtualisation, most notably the freeing of the infrastructure from bare-metal hardware while achieving power and cost savings. As aspects such as multi-core processors advance, it is fast becoming the logical choice to virtualise. "According to recent figures released by the IDC, Middle East and Africa witnessed growth of 10.3 percent in virtual server unit shipments, year over year. This reflects growing maturity in virtualisation adoption, with the aim to consolidate the infrastructure by using a few servers to deploy more virtual machines and exploit existing hardware capacities to a greater extent," explains Ray Kafity, Regional Sales Director, FireEye.

Virtualised networks and devices are vulnerable to a variety of malicious attacks. Security breaches of virtualised environments have included social networking sites, false scam websites, viruses, phishing and malware. These breaches have occasionally been so large and devastating to a business that the business itself was brought to ruin.

Prior to the advent of virtualisation technologies, servers were static and, once created, did not move around the network. This made for a simple security situation with easy to implement policies and monitoring processes. Virtualisation changed the game drastically. The benefits of flexibility, scalability and ease of deployment created a new level of agility, however, along with this flexibility, some would say, has come reduced protection for virtual servers. "Virtual machines are susceptible to Distributed Denial of Service Attacks as well as malware outbreaks," warns Tareque Choudhury, British Telecom, "Virtual machines in a production environment are the active live systems on the network. They should be treated just like any production system."

However, all of this agility brings with it some serious questions about security. "It would be fair to say that the main driver for companies today when looking at virtualisation is cost savings—simply less hardware to procure. However the investment on the security side is not always calculated as part of the overall analysis," says Nicolai Solling, Director of Technology Services, Help AG. The question of how virtualised environments should be treated and protected is a hotly debated topic. "One of the most critical aspects of security virtualisation is the ability to manage the environment," says Phillipe Ortodoro, Vice President of EMEA, WatchGuard, "However, policies must be assigned by VM, zone, or both, rather than by the traditional location or network connection."

10.3 %
growth in virtual service unit shipments in the Middle East this year

It would be fair to say that the main driver for companies today when looking at virtualisation is cost savings—simply less hardware to procure. However the investment on the security side is not always calculated as part of the overall analysis."

Nicolai Solling, Director of Technology Services, Help AG

According to recent figures released by the IDC, Middle East and Africa witnessed growth of 10.3 percent in virtual server unit shipments, year over year."

Ray Kafity, Regional Sales Director, FireEye

Some argue that there will always be an additional vulnerability to virtualised environments due to the hypervisor and virtualisation management layer. "So in theory some will argue that virtualisation will always be less secure. However, in practice, virtualisation and cloud have given us an opportunity to apply security and operation controls differently that could result in a significantly improved security posture when properly leveraged," says Sebastien Pavie, Regional Sales Director, MEA, SafeNet.

A major target for potential attackers in virtualised machines is, of course, the host. An attack on the hypervisor could provide access to all virtual machines running on that host and result in the compromise of an entire infrastructure. As such it is vitally important that they hypervisor is equipped with firewalls, IPS, endpoint security and encryption of all hard drives. "The general rule," advises Matvey Voytov, Senior Product Marketing Manager, Kaspersky Labs, "is that security should be implemented in all infrastructures, not only virtual. Large companies have different security solutions for very different environment —virtual, mobile and physical. It can be difficult to manage them simultaneously."

In addition to threats unique to a virtualised infrastructure, virtualised machines are also vulnerable to the same attacks as their bare-metal counterparts. "A disgruntled technician could plant a logic bomb on your network, create sabotage, or steal customer information, and cause irreparable damage to your business and reputation. In fact, analysis of many cyber incidents reported in the past has revealed that misuse of privileged access had been the root cause," warns V. Balasubramanian, Marketing Manager, ManageEngine.

This speaks to the traditional security threat of access. As virtualised machines can be created with just a few moves, this gaps is compounded. As access is parsed out to administrators and virtualisation sprawl grows, the element of human error becomes a larger issue. If there is unrestricted administrator access to all of the systems and data in a virtualised environment, this presents a clear vulnerability to the system. Virtualisation has given use improved agility when it comes to deploying systems, but it also creates a larger and more accessible data trail. "Any deployed hosts should have endpoint security enabled. In a physical network separate appliances are deployed to handle the network IPS, firewall and anti-virus," says Kalle Björn, Director, Systems Engineering – Middle East, at Fortinet.

In addition to these traditional gap in security, there are also unique challenges with managing virtualised security requirements such as logging, specific anti-virus applications and patching in a virtualised environment. As virtualisation becomes the norm, the industry is beginning to respond with original innovations and software to combat the specialised threats to virtualised machines.

Currently the market is flush with choices when it comes to virtual machine security, however, until recently many of the solutions can still leave virtualised machines vulnerable. Traditional security is not optomised for virtual environments and ends up consuming resources that should otherwise be conserved. Conversely, security products that are integrated into virtualised platforms fail to provide complete protection due to host platform limitations. The challenge in virtualised security is to find a solution with low resource consumption and high-level protection.

In light of both the traditional and unique security threats of a virtualised infrastructure, security should be at the forefront of the IT department's priorities. "It is essential that It departments of corporations recognise emerging security threats in order to adopt this new innovation without exposing their data. By mitigating the risks of VM, companies can achieve better protection and privacy than possible with older, stand alone servers," says Anas Ali Al Naqbi, Senior Security Consultant, eHosting DataFort.

Security providers are beginning to close the gaps in virtualised protection with specialised products for virtual environments. These strive to provide equivalent levels of security combined with minimised memory, processing and networking resource consumption. "In a cloud computing environment, an assortment of virtual applications with different risk classifications and trust levels now reside on the same virtualised server, and can communicate with other applications within this server. Much of the network traffic move East-West , from virtual machine to virtual machine, and the communications must be inspected and segmented. Traditional physical security appliances deployed in the data centre are looking at North-South traffic coming in and out of a virtualised server, and therefore may not see this traffic, at least not without painful network provisioning," says Saeed Agha, General Manager, Middle East, Palo Alto Networks.

The conflicts in providing full security in a virtualised environment can be a pain point for those managing such environments. "Before implementing a virtualised server solution, IT managers need to assess the potential risks and vulnerabilities their networks may face," advises Sean Newman, Field Product Manager, EMEA, Sourcefire. The network security solutions can be implemented as guest hosts, but this still leaves the system vulnerable. Security solutions can be implemented on the hypervisor level, but this would require both a security vendor and a virtualisation vendor to coordinate and integrate the solutions. Vanja Svajcer, Principal Research, Sophos puts it succinctly, "A virtual machine will only ever be as secure as the sum of the security of the hypervisor." ■

> A disgruntled technician could plant a logic bomb on your network, create sabotage, or steal customer information, and cause irreparable damage to your business and reputation. In fact, analysis of many cyber incidents reported in the past has revealed that misuse of privileged access had been the root cause."

V. Balasubramanian, Marketing Manager, ManageEngine