Five security trends to watch in virtualisation in 2017

By Vitaly Mzokov

22 May 2017

While virtualisation can improve IT agility and efficiency for a business, it also adds more layers of technology. Maintaining full visibility for each layer- and how they interact - can be a difficult task.

© bluebay via 123RF

What is critical to remember is that more layers generally mean more 'attack surfaces', increasing the ways in which cybercriminals can attack your business. As virtualisation grows in popularity, what are some of the security trends expected this year that businesses should note?

1. Virtualisation security is focusing on integration

Considering security solutions for virtual desktop infrastructure (VDI) and virtualised servers, enterprises will likely start paying more attention to the smooth integration between various systems instead of the thorough examination of product features under a microscope. Security solutions that can be integrated into the virtualisation infrastructure at a sufficient level to detect cyber attacks in their early stages, as well as those that deliver malicious activity information to the components of the corporate environment to make quick decisions that isolate and analyse the threat, will be those that businesses opt for going forward.

Through the integration between the infrastructure and security solution, enterprise-level customers are aiming to increase their reaction speed in response to security incidents, with the infrastructure and its automation platform executing management decisions and applying the changes. Enterprises will look for security solutions that can integrate with such infrastructure virtualisation solutions.

Last but not least, in constantly changing enterprise-level environments, there is always a risk of missing some virtual machines, especially offline ones, when executing an on-demand scan. Enterprises are looking at finding the easiest ways to make sure that powered off machines are not infected without powering them on.

2. Corporations to invest more in hybrid cloud protection

An emerging trend that will gain more importance in the next five years is the transition from private to hybrid clouds. Corporate environments will be composed of private IT infrastructure and public cloud infrastructure. Both parts will be

connected through protected communication channels – with the use of encryption among other tools – and managed from a unified console (or the control centre).

Moving forward, corporations will have more systems that can and should be taken outside the corporate perimeter and placed closer to the customer. Public cloud environments make it easy to do this.

By 2020, the growth of public cloud infrastructure, and the resulting costs of the infrastructure and security solutions for it, are likely to increase by 2.5 to 3 times, compared to what the industry analysts demonstrated in 2016.

Bringing a combination of on premise and off-premise environments under a single architecture and unified management results in specific security requirements where traditional security solutions are a ‘no go’. This is because they do not provide a full set of security capabilities for elastic corporate hybrid clouds, nor can they immediately and effectively follow infrastructure changes and support business growth.

3. More attacks and more damage

The number of attacks on corporate players will continue to grow. It is not only that global companies use or do not use virtualisation (at the moment more than 75% of businesses have been virtualised), but the question is whether they are able to watch all the processes occurring in the infrastructure with regard to the information security. Due to the complexity of large corporate infrastructures and complicated relationships among different systems within this, attack detection time will increase, along with the damage. This means that more and more systems will be in the high-risk zone.

In a large corporation, everything is communicating with everything. It is like an organism - a very complex and sophisticated one. And, like an organism, if one of the interconnected systems is infected, then the infection is rapidly transported across the whole infrastructure. One can identify the symptoms and understand that something’s wrong, but to identify all the infected areas to find the source in order to eliminate it can be difficult. Especially if one does not get to monitor everything that is going on inside the systems. In such cases, an organisation might not even know it is under attack for months or more. A breach can be damaging, but a breach that no one has noticed is much more dangerous.

4. Ransomware continues impact on VDI

Speaking about the growing importance of particular threats, it is worth mentioning ransomware, as crypto-locker and crypto-malware threats will become a headache for virtualised desktops.

Ransomware can hit a virtual desktop as well as a physical workstation, but when it comes to VDI, the risks are significantly higher. An infected virtual machine is linked to a data centre, which means that localisation and neutralisation of the malware in virtual workspace might have an impact on all infrastructure and business processes. If malware makes its way to the golden image — a template used for the creation of new virtual desktops — hundreds of the infected ones will be appearing every day.

Therefore, VDI protection task will go beyond the perimeter security to the level of each virtual machine where traditional endpoint protection solutions cannot help. Organisations will have to find efficient solutions, designed specifically for virtualised environments.

5. Mobility challenges call for unified security

The larger the enterprise, the more control it needs to achieve in order to make sure everything is safe and secure in how users interact with different business systems. Considering the fact that users are becoming more and more mobile and require seamless access to business services and applications from wherever they are, many corporations will find themselves implementing enterprise mobility management software (for example, VMware AirWatch and other solutions available in the mobility industry) for thousands of endpoints. This will require powerful yet resource-efficient security solutions to be tightly integrated with those enterprise mobility systems.

Problems with mobile devices fall into two major categories - data loss and possible hacks through a variety of malicious applications. While implementing VDI does reduce the risk of data loss and the prevention of unwanted intrusions, there are still challenges for unified security management to ensure the same high level of protection is available and efficient across various operating systems and devices for mobile productivity.

It is clear that cybersecurity is not about just one aspect of IT – rather, it is the some of the parts combined together. And while they are many challenges to face, businesses looking to benefit and receive improved IT agility and efficiency must have the right approach to IT security, along with the combination of experienced external and internal people, and a high level of trust, to ensure that there are no loopholes within the departments that make the organisation.

ABOUT THE AUTHOR

Vitaly Mzokov is solution business lead, data centre & virtualisation security at Kaspersky Lab.