CASE STUDY

THE CHALLENGES OF TRADITIONAL SECURITY IN **VIRTUALISED ENVIRONMENTS**

The virtualised environment has provisioned a more dynamic and flexible IT infrastructure for IT professionals. Virtual machines (VMs) can be delivered as a service and virtual desktop infrastructure (VDI) delivers desktops as a managed service, giving users access to their desktops, applications, and data anywhere, any time, on any device. The benefits of virtualisation reduce both capital and operational expenditures and promote business innovation and growth.

However, understanding the challenges of traditional security in virtualised environments is critical to ensuring the required security is in place and the organisation's business objectives are being met, minimising downtime and security risks that can result in loss of investment, resources and data.

Understanding the challenges of traditional security in virtualised environments can ensure long-term sustainability of the organisation's operation as a whole.

"Understanding the challenges of traditional security in virtualised environments can ensure long-term sustainability of the organisation's operation as a whole."

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

THE CHALLENGE:

Handling resource-intensive tasks and steering clear of "security storms" is a major challenge when using security that is not designed for virtual environments. Traditional security unfortunately does not recognise a shared resource environment.

On a physical host scans or scheduled updates initiate simultaneously across all VMs causing extreme load on the system resulting in a "Security Storm" negatively impacting performance and, often, production. Although these "storms" can occur with other types of security scans and updates they are particularly common if using traditional antivirus solutions.

Because of this, organisations need security solutions that address concerns and risks specific to virtualisation environments. The advantages of traditional agent-based security do not apply to the virtualised environment. In addition to "security storms", there are other key challenges created by applying traditional agent-based security to virtual environments:

- Instant-on gaps
- Compliance / Lack of audit trail
- Instant-On Gaps

There is a challenge to consistently and with significant speed provision security to VMs that are activated and inactivated in short bursts or during varying time periods. VMs that have been left dormant are in an unprotected state and run the risk of deviating so far from the baseline that the simple action of powering them on can mean inviting a massive security risk. Likewise, new VMs, even when built from a template that includes security, cannot immediately protect the guest without configuration of the agent and conducting security updates.

By provisioning and decommissioning them as needed for test environments, scheduled maintenance, disaster recovery, and to support "task workers" who need computational resources on-demand, enterprises can take advantage of the dynamic nature of VMs.

IT COMPLIANCE CHALLENGES

It is paramount that enterprise security policies and industry regulations are in line with the development of virtualisation technologies. Virtualisation, while creating new opportunities, comes with its own compliance challenges. Visibility and control of system and network activity are much more complex in virtual environments, since traditional host-based security software and network security appliances are not integrated into the introspection layer. It can be difficult to maintain an auditable record of the security state of a virtual machine at any given point in time, and, as VMs can be easily cloned and moved between physical servers, vulnerabilities or configuration errors may be unknowingly propagated.

The most effective way to address the issue comes by integrating the virtual machine security capabilities directly into the virtualisation platform, using hypervisor introspection – the ability to monitor and control what goes in and out of the hypervisor layer.

IMPLEMENTING THE SOLUTION:

Implementing an agentless architecture for VMware virtual machines, on all hosts and virtual server/desktops, and handing over resource-intensive tasks like AV, and other security scans, to a dedicated, security-hardened virtual appliance is a solution to consider.

AV solutions can often be identified as the root cause of sluggish servers that are failing to respond at critical times of operation. Server scans can eat up resources, causing huge CPU spikes which lead to unusably slow network speeds. This means virtual machines are in danger of losing connectivity during crucial periods, creating new security and operational issues which, at a minimum, impacts on an organisation's business objectives through loss of time and investment of resources and has more serious implications regarding data and the longer-term sustainability of the operation as a whole.

A case in point is one client's IT department who installed Trend Micro Deep Security.

The team is currently in the process of upgrading its infrastructure to ESX 5.1 on VCenter 5.5 servers, including upgrades to the fibre switching, and operates a VMware environment of VCenter servers and ESX hypervisors, running 260 virtual machines.

This infrastructure enables the IT team to deliver virtual servers and desktops to senior staff off-site in a highly efficient manner, with all the attendant benefits of VDI including rapid deployment of updates, ease of management, lower power usage, lower hardware expenditure and a unified desktop environment.

After running a demo the team set-up a proof of concept, replacing their existing provider with Trend Micro Deep Security, and saw an immediate improvement. It also improved troubleshooting, allowing the team to rule out their AV product if any future performance problems occur. They have also been impressed with the customisable dashboard interface of Deep Security, which allows admins to manage the entire virtual security environment from a single pane of glass.

"The most effective way to address issues comes by integrating virtual machine security capabilities directly into the virtualisation platform."

THE SOLUTION

Traditional agent-based security clearly does not offer the required security in a virtualised environment. The solution is to opt for an agentless architecture.

Virtualisation and cloud computing have changed the face of today's data center. Yet as organisations move from physical environments to a mix of physical and virtual, and private and public clouds, many continue to address the prevailing threat landscape with legacy security. In virtual

environments, this can increase operational complexity and decrease host performance and VM density. In cloud environments, legacy security leaves gaps in protection undermining the confidence to move mission-critical workloads to agile, lowcost cloud environments. Ultimately, this hinders the ability to fully invest in virtualisation and cloud computing and maximise the return on investment in these technologies.

THE PRODUCT:

As well as an agentless architecture for VMware virtual machines, Trend Micro Deep Security also offers virtual patching, integrity monitoring, log inspection, firewalling, web security, plus it also deploys policy and scans any new VMs automatically to address instant-on gaps and inter-VM attacks. Deep Security delivers comprehensive, adaptive, highly efficient agentless and agent-based protection, including anti-malware, intrusion detection and prevention, firewall, web application protection, integrity monitoring, and log inspection.

WHY TREND MICRO DEEP SECURITY? AT-A-GLANCE

- Accelerate virtualisation investments
- Minimise security impact
- Ensure cost-effective compliance
- Move safely to the cloud

WHY ANNODATA? AT-A-GLANCE

- Expertise and trust – your business needs the best IT solutions on the market and a dependable, trusted business partner.
- Technical know-how – you need access to IT excellence across a range of services.

Annodata is one of the UK's longest standing providers of Managed Services, covering Document Management, Unified Communications and IT.

For more information on how Annodata can help you become a more efficient enterprise, please contact:
marketing@annodata.co.uk or Tel: 01923 333 333

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

v1 – Sept17