Trend Micro™ and VMware® Horizon™ Suite

Securing the journey to the device independent workspace

EXEC SUMMARY

Today’s organisations operate in a post-recession world where competition is as strong as ever, but budgets remain tight and change is ever present. CIOs need to make IT investments which support enterprise agility but at low cost and in a way that adequately manages risk and ensures compliance. In this tough business environment, users are increasingly demanding more flexible ways to work in order to boost productivity, with BYOD leading the charge.

In end user computing, one response to these pressures is to implement a device independent workspace which helps IT to reduce operational costs and maintain control over the computing environment, whilst meeting end user and business demands for greater agility, innovation and value. The VMware Horizon Suite provides users with access to corporate resources such as applications, data and Windows desktops from any device, allowing IT to overcome BYOD and OS upgrade challenges in a simple, secure, compliant and low cost manner.

Trend Micro provides the final piece of the puzzle by securing VMware Horizon Suite with its Trend Micro Deep Security, OfficeScan and Mobile Security products. This comes from a lasting partnership developed over many years to offer a deeply integrated set of solutions, enabling comprehensive protection across physical and virtual environments. Read on to find out how Trend Micro can offer superior performance, maximum security, and simplified management for your transformative VMware Horizon Suite deployments.

SETTING THE SCENE

Organisations may have finally emerged from the dark days of a global economic recession but for most the business environment they face is as challenging as ever. To remain competitive they must be agile, they must keep costs down and they must respond to user demands for more flexible and productive ways to work – all in a secure, compliant manner.

Nowhere is this more true than in end user computing, where CXO demands for greater agility and value for money are combining with changing user expectations around BYOD, and challenges around OS upgrades as Windows XP comes to the end of its life.

CXO demands:
• Want to drive growth through business agility and reduced costs
• Recognise benefits of BYOD in productivity/staff retention
• Need to manage risk and stay compliant
• Need IT to lower operating costs; be more strategic; to support, not stifle business change

IT is under pressure
• Users now expect to access corporate networks regardless of OS, device or location
• They know traditional approaches to IT aren’t able to support changing business requirements
• IT budgets are under greater pressure thanks to recession
• Penalties for security and compliance failures are greater than ever before

BYOD
• The key driver for end user computing over the next decade: users want the flexibility and productivity it can bring.
• Gartner: half of employees already using own smartphone or tablet in UK workplace
• Users will use insecure workarounds if BYOD isn’t formally supported/acknowledged
• Users also want to mix personal and business on one device, single sign on, and personalised desktops
• Must be seamless, secure and user-friendly: corporate data to be centrally backed-up; any security, app and OS updates applied without affecting user experience

The big XP upgrade
• Microsoft will officially end Windows XP support in April 2014
• Today (December 2013), over 30% of all Windows XP licenses ever sold to business are still in production use
• Many organisations will be forced to upgrade to adhere to compliance requirements
• Upgrading the OS will accelerate hardware refresh, presenting opportunities and challenges
THE VMWARE ANSWER – THE DEVICE INDEPENDENT WORKSPACE

Essentially, the confluence of factors listed previously have left IT at a crossroads. It needs to find a way to provide employees with greater flexibility whilst retaining control over the end user computing environment. It also needs to securely manage BYOD and find a way of upgrading from Windows XP - all in a resilient and fully compliant manner which will reduce operating expenditure and position IT as a strategic driving force in the organisation.

It’s no easy task.

On the one hand IT could go for what is traditionally thought of as the low risk route: it could replace its Windows XP devices, upgrade to Windows 7 or 8 and restrict BYOD. It’s a well-rehearsed strategy with known CAPEX. However, it’s one which solves none of the key problems facing organisations today, adding no strategic value and failing to address the fact that two-thirds of budgets are tied up with OPEX, not CAPEX.

The answer is to begin the journey to a device independent workspace environment and to a brave new world of strategic agility, innovation and value.

VMWARE HORIZON SUITE

VMware Horizon Suite is VMware’s vision for the future of end user computing: the device independent workspace. There are three main elements: VMware Horizon Workspace™, VMware Horizon View™, and VMware Horizon Mirage™. Horizon Workspace is the foundational hub of the offering, acting as a management broker to provide centralised, single sign-on access to apps, files and desktop images. Users are able to access their desktop from any device, regardless of OS or format. Horizon View supports virtual desktops and Horizon Mirage is a better way to manage physical devices, whether on or offline.

With physical and virtual endpoints both supported, Horizon Suite is a fully integrated solution, delivering secure freedom - a device independent workspace for users which is still controlled and securely managed by IT. Users get access to a standardised workspace from which they can access data, apps and virtual Windows desktops - irrespective of device, OS or format - offering them the choice, flexibility and BYOD support they need. IT is able to deliver strategic innovation, enabling a happier and more productive workforce at lower cost and in a secure and compliant manner. With VMware Horizon Mirage, Windows XP migration is as simple as switching on and delivering a new OS layer with all user data and profiles saved.

TREND MICRO – SECURING THE HORIZON SUITE

The Horizon Suite is a radical departure from traditional approaches to end user computing so it requires a new approach to security. In this new environment there are new and different risks to manage. Shared computing resources and the multiplicity of devices means greater exposure to threats if they are not managed correctly. Traditional approaches to security in virtual environments require agents on each server and PC, which don’t fit into this new world of device independent workspaces environment creating severe performance, management and cost and security issues.

A new approach to security is therefore needed to deliver secure freedom, and it is one Trend Micro has been at the forefront of developing for years.

Benefits:

The benefits of choosing Trend Micro’s advanced security solution for VMware’s Horizon Suite revolve around the two companies’ long history of technical collaboration which provides a tightly integrated, complementary set of solutions to improve security, maintain compliance, lower costs and boost performance. Here’s how:

1) Trend Micro Deep Security integrates with VMware APIs to deliver agentless security tightly integrated into the hypervisor for virtual environments. A security hardened virtual appliance protects all virtual machines from network and file-based threats, eliminating problems associated with physical protection including:
   • Resource consumption, which can increase CAPEX and OPEX
   • AV storms, which can severely affect performance
   • Instant-on gaps, which can introduce severe security vulnerabilities
   • Operation overheads, with admins needing to provision and reconfigure security agents

(continued)
2) Deep Security’s VMware integration means it has full visibility of your dynamic virtual environment. In a non-persistent VDI setting this means it won’t lose track of your VMs once your users log-off and then count them as new endpoints the next day when staff log-on again.

3) Trend Micro OfficeScan provides security for physical endpoints including thin terminals. This industry leading product has reduced its full system scan time by 40 per cent and offers a 50 per cent boot up time improvement - maximising resources on low-cost, low power endpoints. This is useful on traditional desktops and laptops, but essential on thin terminals, where a RAM, CPU and disk space-devouring AV client would be impossible to run effectively.

4) Trend Micro Mobile Security is a highly efficient, low footprint solution to secure and manage mobile devices. It integrates mobile device management (MDM), mobile security, data protection, and application management—all within one easy-to-manage solution. By securing the mobile device, Trend Micro Mobile Security minimizes the risk of malware coming onto the network from end user BYOD devices.

5) Trend Micro Control Manager centralises threat and data protection policy management across multiple layers of your IT infrastructure, streamlining administration and providing more consistent enforcement. Customisable data displays provide the visibility and situational awareness needed to rapidly understand security posture, identify threats, and respond to incidents.

A NEW ARCHITECTURE FOR A NEW ERA IN END USER COMPUTING

The pressures facing business leaders, IT teams and corporate users today demand a new approach to end user computing. It requires a set of solutions which support the ideal of a device independent workspace, where all users can access their corporate resources from any device, regardless of OS, format or ownership. This is the promise held out by the VMware Horizon Suite, but it also opens up potential new threats to corporate data.

This is where Trend Micro comes in. Thanks to a long-running partnership with VMware spanning many years, a comprehensive and fully integrated set of products secure virtual and corporate resources, including thin clients and mobile devices, and offers simplified single console management. It simplifies IT, improves performance, lowers TCO, reduces risk and ensures compliance - satisfying the demands of CXOs, IT and business management alike.

Implementations needn’t be an all-or-nothing affair either. The flexibility offered by the VMware Horizon Suite with Trend Micro’s advanced security solutions means organisations can take smaller steps if they wish, managing and measuring risk and investment as they go. VMware Horizon Mirage and Trend Micro OfficeScan could be deployed on older PCs to begin with, for example. The lower security agent overhead frees up system resources to support migration from Windows XP to Windows 7, without the need for new hardware.

It’s just one of the ways VMware and Trend Micro together can help your organisation today.