

# Securing Your Journey to the Cloud



## Managing security across platforms today and for the future

### Table of Contents

Executive summary	1
Journey to the cloud varies, but challenges are shared	2
Security architectures must flex with the business	2
On the journey, all platforms must be secured	3
New security processes are required	4
Virtualised systems need virtualisation-aware security	5
The cloud needs security to address its unique risks	6
Security for the cloud depends on the cloud structure you deploy	6
Security from the cloud leverages the benefits of cloud deployment	7
Virtual and cloud platforms require trusted security	7

## Executive summary

Business drivers are changing the face of information technology. Virtualisation and cloud computing are optimising resources, saving costs, and offering new and exciting ways of delivering 24x7 services. Working practices are also evolving with the impact of consumerisation and the adoption of mobile devices, iPads, tablets, and smartphones, alongside laptops and desktops. Although providing significant business benefits, these changes are creating challenges as organisations secure and manage their diverse and dynamic system infrastructure, including physical servers and endpoints, virtualisation, and cloud services.

*Virtualisation and consumerisation are creating new demands to secure the system infrastructure*

Each company is on a unique journey to implement new IT services to support its business objectives. As businesses deploy new virtualisation, cloud computing, and endpoint architecture, security must be an integral part of the implementation. Threats to the IT infrastructure can impact businesses severely. Securing against these threats of virus attacks, inappropriate usage, and data loss is making all organisations review and upgrade their risk and security strategies. Also, meeting the regulatory and legal demands as they are embodied within the rules of corporate and information governance add yet one more dimension to securing these new infrastructures.

*Each company is on a unique journey to secure its systems and processes against threats and meet regulatory needs and rules of corporate and information governance*

Many companies may believe that they can deploy their current physical security solutions in their consumerised, virtualisation and cloud computing environments. However, migrating traditional security approaches to new system infrastructures creates real performance and service issues. In addition, traditional physical security does not address the security risks unique to virtual and cloud computing environments.

Organisations need a security solution that is designed to protect these new approaches to information technology. The solution must:

- ❑ Be fully virtual machine aware and integrated with leading virtualisation platforms.
- ❑ Secure against platform-specific threats and preserve performance.
- ❑ Deliver integrated security, for example, server security should include antimalware tools, encryption, event logging, secure system patching and upgrading and verifying the integrity of all information in files and databases.
- ❑ Address the unique aspects of physical servers, desktops and consumerised endpoints, virtualisation, and the cloud, provided in an integrated solution with one management console across all platforms.

*Solutions must be:*

- Fully virtual machine aware
- Secure against threats
- Preserve performance
- Integrate security across physical, virtual and cloud infrastructures

Wherever the business is on its journey to the cloud, it needs a security solution that will protect it today and as its data centre and endpoints continue to evolve in the future. System complexity is increasing and businesses need security they can trust. Businesses should look to a provider that has data centre, endpoint and cloud delivery options to support businesses as needs evolve. This will avoid costly retraining, allow for long-term planning, and lead to the foundation of a long term strategic business relationship.

## Journey to the cloud varies, but challenges are shared

Containing costs and improving utilisation of computing resources is driving new system architectures. Each business will embark on its own journey as its system infrastructure changes. The route adopted and timeframes will vary from business to business, but the challenges and imperatives are recognised by all.

Overlaid with high performance networks, the system infrastructure is evolving from physical servers and storage devices to virtualised resources located within the data centre, at a preferred partner, or resident in the cloud. In addition, users are now accessing systems from smartphones, tablet devices, physical and virtual desktops, and laptops. The demands on CIOs and system managers are ever increasing to deliver secure and trusted services.

All organisations have established a system infrastructure to support their business needs. Priorities are set by the business in order that customers can be serviced, suppliers can be supported and employees work effectively to meet the service, profit and revenue goals. Examples of how system infrastructures evolve include:

- An insurance company started to consolidate its server and storage resources, with server virtualisation and storage networks to reduce operational costs. In the process, the data protection practices needed to be enhanced. The backup and recovery was outsourced to a trusted cloud service, protecting the data centre infrastructure, the mobile sales force and insurance assessors.

To encompass a more flexible way of working, the company had to enable home working as well as link independent sales agents and insurance brokers. Desktop virtualisation is being deployed to support the extended enterprise, accessing standard, approved processes with a consistent set of security policies.

- A distribution company has to link its systems more tightly with the manufacturers and distributors with which it works. As the lead time to compile van and lorry manifests reduces from one month to 1-5 days, the business needs to be responsive as well as increase its overall service levels.
  - This was achieved by linking systems with suppliers which applied a new level of security. The company had to ensure the integrity of its own databases was not compromised. This led to a realignment of its physical and virtual servers. New security systems and practices were introduced to comply with its customers' ecosystems. These security processes had to support acceptance and confirmation of goods collected and goods delivered.
  - The company was already using a cloud service provider to track its vehicles internationally. It is now looking to extend this capability to speed up collections and deliveries by tracking pallets, crates and individual packages.

*As each organisation's system infrastructure evolves, the challenges, governance standards and operational practices, that have to be addressed, are recognised by all*

### Distribution Company Securing its Infrastructure



## Security architectures must flex with the business

Securing these new infrastructures and addressing the risk of how systems are managed is of increasing concern throughout all organisations, right to the boardroom. Personal details are being stolen, data centres and industrial plants are

being compromised and government and company documents are ending up in the wrong hands. Complexity of malware is an increasing challenge. Organisations are subject to internal as well as external threats. Security strategies and architectures need to be reinforced in order to protect organisations' hard won brand values and ensure business can operate continuously.

*Security solutions must respond dynamically, with threats emerging internally and externally for all businesses*

Furthermore, requirements and expectations for sound corporate, system and information governance continues to increase. Adoption of standards and regulations is determined by each business. These encompass audit standards, payment clearing processes, industry and government regulations set by regulators such as the SEC and FSA, the International Standards Organisations (ISO), with security standards set out in ISO 27001, and many more.

Securing all elements of the system architecture must be effective to minimise and manage risk. Elements of the system architecture that need to be secured include:

- ❑ Physical servers – are the basic platforms on which applications operate
- ❑ Endpoints - include access devices such as desktops, laptops, mobile devices, smartphones and tablets.
- ❑ Server virtualisation - enables multiple applications to run on a physical server host as if each application had full access to all resources. Virtual machines are created to support each application; each virtual machine looks like a physical machine.
- ❑ Desktop virtualisation - uses virtual machines to let network users maintain their own desktops on centrally located computers or servers.
- ❑ Cloud computing - enables on-demand access to a shared pool of computing resources, including networks, servers, storage, applications and services. Resources are made available so that they can be rapidly and easily provisioned with minimal management effort or interaction. Cloud computing can be deployed as a:
  - Private cloud - where the cloud is operated solely for one organisation.
  - Public cloud - where the cloud infrastructure is made generally available to the public or to businesses. Such services are owned by organisations selling cloud services.
  - Hybrid cloud - is a cloud infrastructure composed of private and public clouds.

*System architectures must be secured at all levels*

- Physical servers in the data centre
- Endpoints, through to mobile users
- Server virtualisation
- Desktop virtualisation
- Private, public and hybrid clouds

Threats emerge from outside and within each and every organisation. As the system infrastructure evolves to support the needs of all users and business units, security procedures must be agile, flexible and trusted to address the changes.

## On the journey, all platforms must be secured

Regardless of the exact journey, companies will use three different platforms.

- ❑ Physical - businesses will always keep some dedicated physical servers in their data centre. This will be required to deliver specific applications and services.
- ❑ Virtual - system resources, such as servers, storage and desktops are consolidated to deliver cost savings and provide the underlying foundation for cloud computing.

*All system platforms must be trusted and secured, including physical, virtual and cloud*

- Cloud – companies leverage the cloud to provide business change, introducing new ways of doing business flexibly, responsively, and more cost effectively. Whether organisations deploy private, public, or hybrid clouds will depend on their needs.

Securing these platforms against malware, inappropriate usage, and data loss is of increasing concern. In addition, all activities must comply with the principles and guidelines set out by the business. Each platform has its benefits, but also introduces unique security concerns.

Threats to physical servers and endpoints have been recognised and, in general, have been addressed with antimalware, firewall, intrusion prevention, web application protection and integrity monitoring. Identity management systems are used to verify users. However, as the system infrastructure evolves to handle mobile users and extend the supply chain to include approved customers and suppliers, the traditional view of a single secure firewall comes under threat. The proliferation of virtual servers, offering the ability to transfer applications to appropriate resources, is yet another example of the new model. Cloud computing can be used to facilitate this migration with computing resources within or external to the organisation. These new paradigms must be secured as they encompass new ways of doing business.

*The traditional single secure firewall needs to evolve to support endpoints, virtualisation and cloud services and address potential performance and service issues*

## New security processes are required

Applying traditional security approaches to new system infrastructures creates real performance and service issues. Worst of all, it will not address the needs to secure all systems in a very dynamic environment. It is important to recognise this, since as the system infrastructure develops, security must be managed and risks mitigated.

*Security solutions must be aware of virtual systems and be self-defending, moving with users and workloads across the system infrastructure*

New security approaches can address the concerns of physical, virtual and cloud platforms. Systems must be aware of the virtualised environments and be self-defending in external cloud environments. These new security approaches must also optimise platform performance. As the data centre evolves, businesses need security solutions that span across all three platforms while also addressing the threats unique to each.

Security must move with the users, applications and the workload on the system infrastructure. Host-based security controls reflect the virtualisation of security. It must address the instant provisioning offered by virtualisation and cloud. Establishing clear policies for each new virtual instance will ensure compliance to accepted security standards for all. This will mean avoiding unnecessary downtime due to infection or security breaches, delivering a better service to the business.

An example of what needs to be included with integrated security across physical, virtual, and cloud servers is a firewall, antivirus, protection against both known and zero-day attacks and collecting and analysing operating system events and application logs for suspicious behavior. Server security needs to support patching of applications operating in virtual machines, to protect vulnerabilities in critical systems until a patch is available and deployed. Encryption and file integrity monitoring are additional features required. This protection should create self-defending servers whether physical servers, on-site virtual machines, or virtual machines traveling into cloud environments.

*Example of what must be included:*

- Firewall
- Antivirus protection
- Analysing operating system events
- Application logs
- Patching applications
- Encryption
- File integrity monitoring

To simplify the management process and contain operational costs, the solution needs to have one management console that can be used across all three platforms, physical, virtual and cloud. In all, the controls used in the traditional physical world are also required in the new virtual and cloud environment. The way they are delivered needs to be responsive to the agile business and adapt to the changing shape of the system infrastructure.

## Virtualised systems need virtualisation-aware security

Virtualisation has delivered exciting gains, whilst making organisations realise that they have wittingly, or otherwise, embarked on a journey. Securing system operations from the data centre outwards needs to be carefully managed. Deploying traditional physical security across virtual machines is problematic. Automatic scans or updates are processed simultaneously across all of the virtual machines on the same host. This can cause debilitating performance degradation on the underlying host machine.

*Virtual-aware security solutions have access to the hypervisor and will stagger scans across virtual machines on the same physical host*

The solution is to harness access to the hypervisor so that a dedicated security virtual machine can stagger scans across all virtual machines on the same physical host. Using agentless security, virtual machine resources can be conserved and performance preserved. With a security solution that is fully virtual aware and tied in with the underlying hypervisor, greater benefits can be realised, such as more virtual machines running on each host. Security can be enhanced as each virtual machine will be automatically approved when it is moved and initiated on a server.

There are threats, specific to virtualisation, that are not addressed with traditional security. When a virtual machine is attacked, other virtual machines on the same host can become vulnerable. Protection needs to be applied on the virtual machine, not the host machine, to prevent inter-virtual machine attacks. Also, dormant, reactivated, or cloned virtual machines can wind up with out-of-date security. A dedicated scanning virtual machine can ensure that all virtual machines have up-to-date security. Virtual machine aware security can defend against these threats.

*Inter-virtual machine attacks need to be considered. Protection is required for each virtual machine, wherever it may be executed. Protection must be up to date for all virtual machines*

Desktop virtualisation is leading to the desktop being disassembled. Intrusion detection and prevention, applications, and user personas are discretely managed and stored, only to be recomposed via the network into the familiar workspace for each user at log-in. Applications appear to be local, but they can be streamed into the workspace, running on another virtual machine or as a service in the cloud.

This workspace is accessed by a physical client that is increasingly remote and mobile, such as home PCs, laptops, tablets and smartphones. The accessibility of the virtual desktop from multiple locations and devices has expanded the user workspace to be everywhere and anywhere. The user session now defines the desktop and spans multiple network locations within the data centre and remotely. Hence, an agent can no longer reside in a single location and provide coverage of the desktop; endpoint security must now span multiple network locations.

*Desktop virtualisation assembles various data streams, each of which must be managed and secured as it delivers the impression of local application support*

A host-based security agent on each of the servers dynamically senses and changes the security policy as the computing workload moves, for example, from inside the corporate network, to roaming outside the corporate network, or to another data centre or to the cloud. When organisations implement virtualisation, security must be

extended to each logical host node. Also, agentless antivirus, as discussed above, can be applied to virtual desktop instances, providing higher consolidation ratios than the resource intensive traditional agent-based antivirus approach.

In addition to securing virtual servers and endpoints, protection can be deployed as a virtual appliance to further support business virtualisation efforts. This enables security to be offered as a virtual appliance to secure the DMZ, for email and Web applications, for example.

## The cloud needs security to address its unique risks

Security and privacy are key concerns when using cloud services. Some of these often relate to complying with internal governance requirements. However, there is a difference between security *for* the cloud and security *from* the cloud.

### *Security for the cloud depends on the cloud structure you deploy*

In a private cloud, the business controls the hypervisor. Consequently, it can adopt the same approach to securing a virtual environment in the data centre as it does in the cloud. This will include a consistent level of virtual machine security, deployed across the system infrastructure.

In a public cloud, the business does not control the host machines, resources are leased or rented.

Public cloud service deployment models and security are:

- ❑ Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS). These are versions of cloud deployment which rely largely on the security provided by the service provider.
- ❑ Infrastructure-as-a-Service (IaaS) which provides more flexibility for security to be delivered by the organisation itself.

Because of the multitenant nature of IaaS architecture, securing this environment does not allow for dedicated virtual machine scanning or an agentless option. So security is best deployed on an individual virtual machine basis. Each self-defending virtual machine should have the same protection in a cloud environment as outlined above for a virtual infrastructure.

In addition, businesses can deploy data encryption for both the private and public clouds. This should be an automatic option for best practice in many cases. Using policy-based key management, encryption enables data to stay secure:

- ❑ Protection is needed against non-approved users who will not be able to access or use the data without access to the encryption keys.
- ❑ Data can be mobile, moving with the application, in both private and public cloud implementations. This must be secured against data loss or inappropriate access.
- ❑ When data is moved in the private or public cloud, any residual data should be digitally shredded. However, in the event that residual data remains after data is moved, the encrypted data is secure from inappropriate use.

*Security for the cloud must understand the infrastructure being used. The strategy deployed must also consider data encryption to deliver trusted operations, especially as data can move across private and public clouds*

*Each virtual machine should have the same level of protection in the cloud as it would have in a virtualised data centre*

## Security from the cloud leverages the benefits of cloud deployment

Examples of security from the cloud include:

- ❑ Hosted endpoint and email security
  - Security is managed in the cloud with all emails being filtered in and out of the email servers. Spam is prevented from reaching the network and email borne malware is managed, ensuring only virus free email is delivered to the mail servers. Encryption can safeguard the complete confidentiality of email communications and all the contained information. This takes away the need for security servers to be installed and managed within the data centre.
  - Security can be provided for users, regardless of their location, whether travelling away from their base or located in branch offices.
  - To include content filtering, routing or filing based on defined corporate policies, the cloud solution can work in a hybrid environment with a local virtual appliance providing this additional functionality.
- ❑ Cloud-client security
  - Threat intelligence can be delivered from the cloud to support lightweight clients.
  - Email, Web, and file reputation services can be correlated in the cloud and used to block threats before they reach the network.
  - The cloud can be used to issue security features such as mobile device locators or remote device wipes.

*Managed security services, from the cloud, delivers endpoint and email security. Content filtering, routing and filing can be added to meet with corporate policies*

Whether deploying a full hosted security solution or implementing protection that encompasses elements of cloud computing, security in the cloud can deliver faster threat protection and reduce the impact on client resources.

*Cloud-based security can be used to manage threats to all users, wherever they are located and if they are travelling*

## Virtual and cloud platforms require trusted security

As all companies look to gain more from their IT investments, virtualisation will be implemented increasingly across the systems. For faster IT service development and deployment, businesses will turn to the cloud. Working practices will evolve as employees, customers and suppliers leverage new devices. Businesses will benefit from the consumerisation of the endpoints, including iPads, smartphones, tablets, laptops, entertainment devices, and more. But this also means new ways of maintaining secure operations have to be deployed to contain costs and maintain a competitive position in today's global village.

All organisations will have a mix of physical and virtualised IT assets linking with cloud services. And they all need to be managed and secured cost effectively and consistently. They must meet regulatory and legal requirements and adhere to corporate governance rules. This means a consistent security strategy and security architecture must address the recognised risks to business.

*Security architectures must define new ways of delivering a trusted system environment whilst containing costs as IT services are deployed rapidly, responding to the business dynamics*

Physical assets, including servers through to the endpoints, need antimalware tools, encryption, event logging, secure system patching and upgrading and trust in the integrity of all information in files and databases. These physical devices will continue to support legacy applications or as required.

To harness the returns on investment offered by virtualisation, physical servers and endpoints will be virtualised. The virtual instances of each and every application and workplace must be secured without creating new system overheads. As a result, the security systems must be virtual machine aware. Self-defending virtual machines must be able to travel between private and public cloud environments with the added protection of policy-based encryption.

*As servers and desktops are virtualised and supported across a dynamic physical-virtual-cloud architecture, security systems must be fully virtual aware to support trusted solutions*

Planning for the future means accommodating choice. These choices will include:

- Implementing the most cost-effective solutions, whether harnessing physical, virtual or cloud infrastructures.
- Providing virtual appliance and hosted security deployment options to support business virtualisation and cloud implementations.
- Enabling users to interface with their preferred devices. Desktop virtualisation, evolving to workspace virtualisation, will be the first step towards offering secure choices. This will support today's and new, yet to be announced, endpoints.
- Adopting risk mitigation and business continuity options.

Wherever the business is on the journey to the cloud, security must be trusted and business and operational risk alleviated. System complexity is increasing, even if tools look to mask this. It is best to partner with a security solutions supplier that will provide protection for all server platforms as the data centre and endpoints evolve. The solution must:

*System complexity is increasing. The threat landscape is getting more aggressive. The best option is to work with a single provider that offers security solutions with data centre, endpoint, and cloud delivery options*

- Address the unique aspects of physical servers and endpoints, virtualisation, and the cloud, provided in an integrated solution with one management console.
- Secure against platform specific threats and preserve performance.
- Come from a provider that has data centre, endpoint, and cloud delivery options to support businesses as needs evolve. This will avoid costly retraining, allow for long-term planning, and build a strategic business relationship.

## Trend Micro

Trend Micro is a global leader in Internet content security and threat management. It aims to create a world safe for the exchange of digital information for businesses and consumers. A pioneer in server-based antivirus with over 20 years experience, Trend Micro delivers top-ranked security that fits customers' needs, stops new threats faster, and protects data in physical, virtualised, and cloud environments.

*A single provider will deliver security consistently from the data centre to endpoints and the cloud – building a strategic business partnership*

Trend Micro provides security solutions that can smooth the journey to the cloud, a transitional journey that will experience high points and challenges. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, its industry-leading cloud computing security technology and products stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com).