



IBM Italy S.p.A.

Security and Cloud Computing

- Security impacts, best practices and solutions -

Andrea Carmignani
Senior IT Architect

What is Cloud Security – It's about business and data behind it

The ability to maintain confidentiality, integrity, availability of business-critical IT assets
Stored or processed on a cloud computing platform

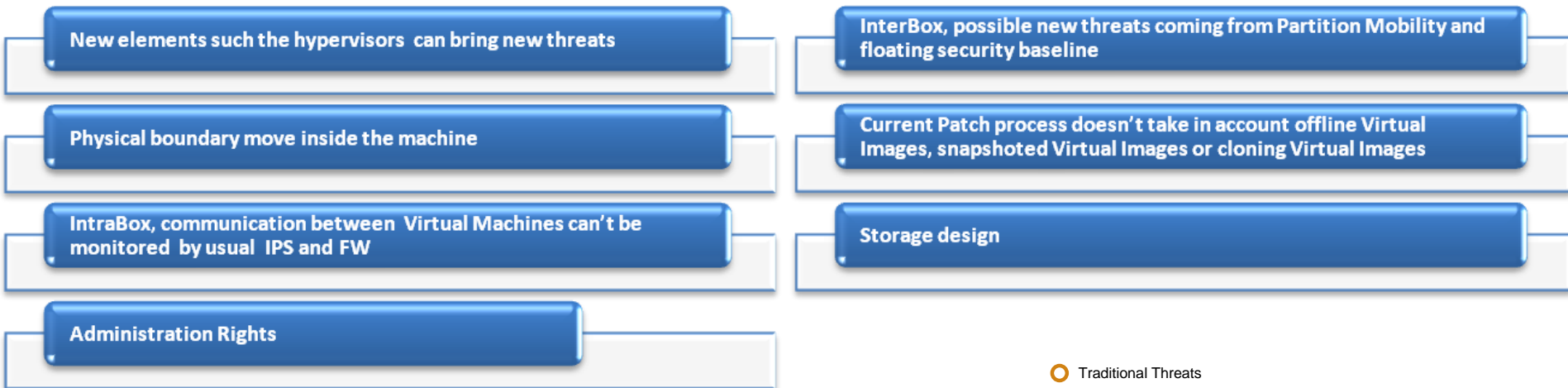
Some customer quotes...

"I Like the Idea of a new generation data center based on cloud but I'm concerned about security and network impacts"

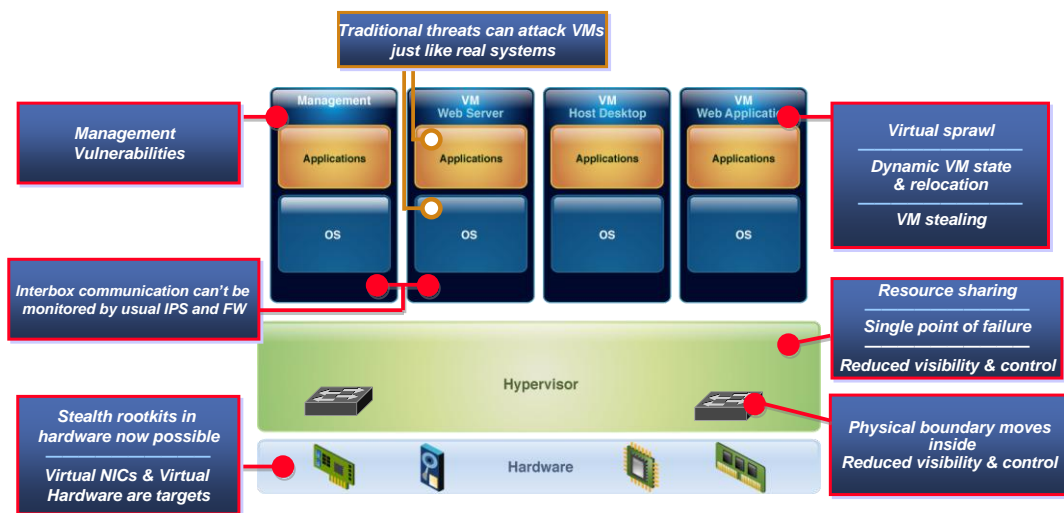
"How can you guarantee the same security level in a virtualized environment as well as a distributed one?..."

"What about identity propagation, audit & workflow segregation? What about impact on the existing infrastructure?"

Some security measures could lose part of their effectiveness while moving toward a dynamic infrastructure ...



- Traditional Threats
- New threats to virtual environments



New Elements bring new threats: the Hypervisor

The Hypervisor, the Golden Gate to the Virtual Images and the Host Resources, it's the director granting resources sharing among Virtual Images

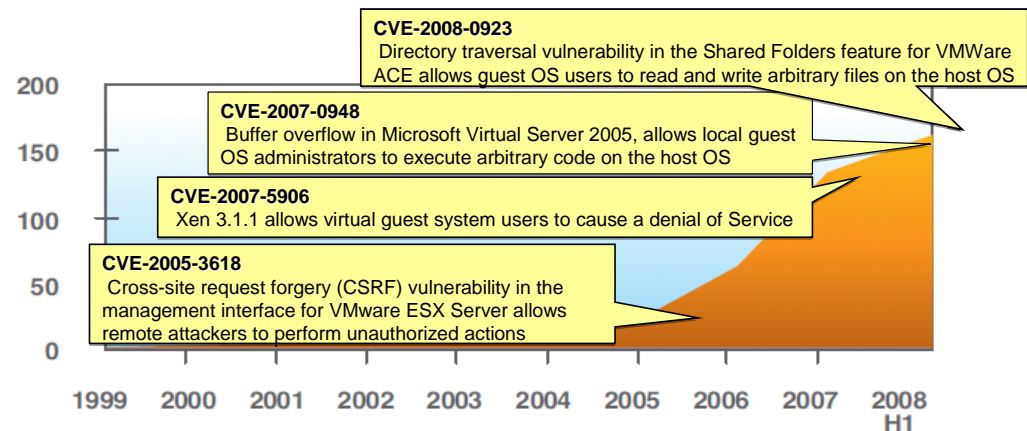
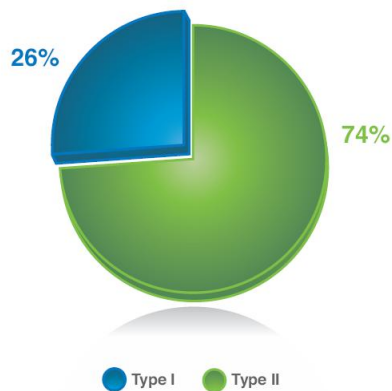
As a new layer in the usual software stack it is the new target for emerging threats
It's mandatory its ability to grant Virtual Image isolation avoiding resource sharing or data stealing

Nowadays we're living with these assumptions:

- All Hypervisors have vulnerability (by design)
- There's no publicly know Hypervisor attack (except the one for Xbox)

Percentage of Type I and Type II Virtualization Vulnerabilities

(Does Not Include Vulnerabilities in Third-Party Software)



Hypervisor, the first real attacks could be a question of time

Today vulnerabilities are detected before there are exploited from an attacker. Just because:

- till 2007 virtualization was a niche market, lack of adoption meant lack of interest from attackers
- poor initial knowledge about virtualization technology and its background

We expect the more virtualization will take place the more interest it'll have from the hackers

So the first real Hypervisor attack is a question of time

We must extend out existing patch, configuration and vulnerability management process to this platform

X86 Virtualization	Age	Vulnerabilities Report		Analysis
		NVD	Microsoft bulletin	
Xen	5 Y, since 2003	Total: 2 High: 2 Moderate: 0	N/A	Based on Linux Opens Source project
VMware ESX	8 Y, since 2001	Total: 23 High: 33 Moderate: 13	N/A	Based on RHEL
Hyper-V	2 Y since 2008	Total: 37 High: 33 Moderate: 4	Total: 34 Critical: 12 Important: 13	Based on Windows 2008 Most vulnerabilities reported are about IE and SMB

NVD: Nation Vulnerability database

<http://nvd.nist.gov/>

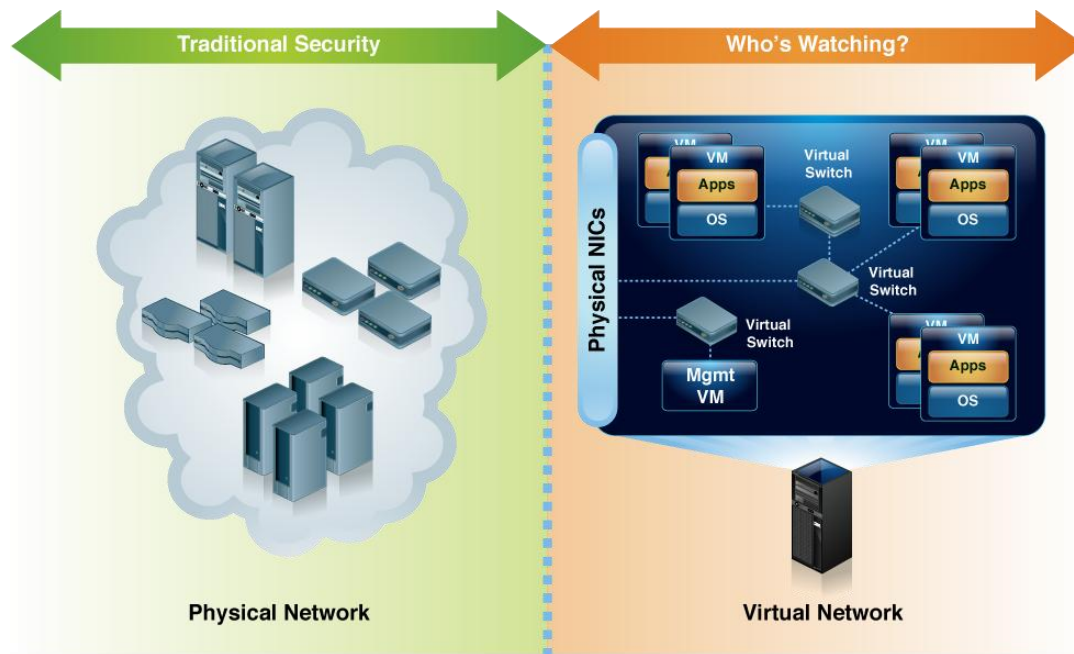
**No IBM PowerVM
vulnerability reported so far**

Physical Boundary and IntraBox Communication Issues, an example

Server & Network Convergence, physical perimeters move inside the machine:

- Network extends through the Virtual Switch or the Virtual I/O Server
- Network Administration boundary moves into the Box:
 - Could have some impacts on the network and server Management Process
 - Could have some impacts on Roles & Responsibilities

Communications between IntraBox Virtual Images cannot be monitored by external FW, IPS, or IDS therefore, attacks among Virtual Images are hard to detect via traditional methods.



Interbox communication, Virtual Images Mobility, a good flight it's a question of route and landing

Partition mobility makes it possible to move running partitions from one physical server to another. This provides:

- considerable systems management flexibility
- improved availability
- applications no longer have to be shut down to move them from one server to another

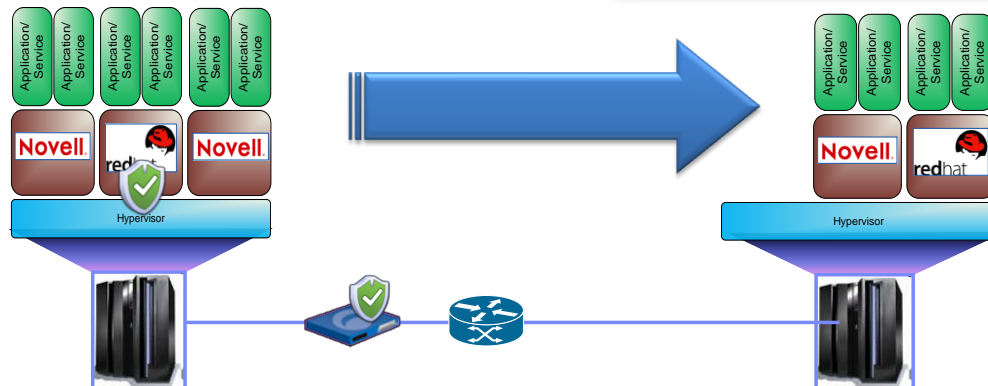
...but some security issues are awaiting through the journey from one host to another....

Data in memory is copied from one system to another to create a clone of a running partition

- Today data are transferred without being encrypted;
- This means possible threats like VI stealing, VI tampering, VI replacing

...as well as on the target physical host

- Is the VI security compliant with the target host security baseline?
- Does the destination “fulfill” origins’ security policy and regulation?
- can I move a back end VI to a system hosting front end VMs?
 - What about Firewall rules protecting the new system?
 - Are they exposing the VI to some threat?
 - Are they too strict preventing the VI to work properly?

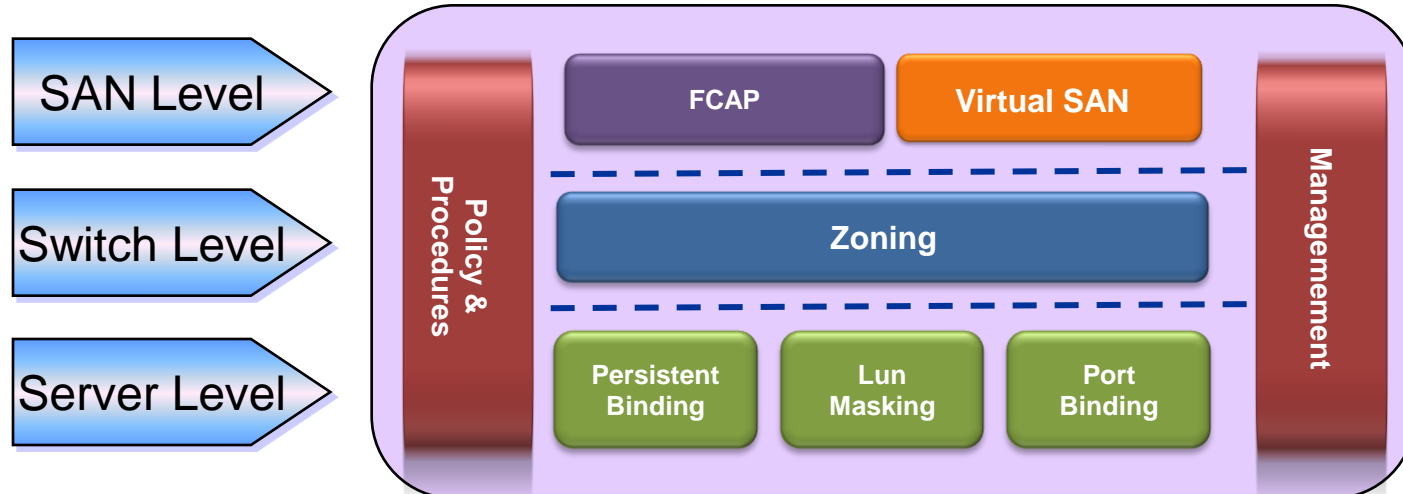


Storage Security – Last but not least security concerns

- Storage ecosystem have emerged in isolation with a focus on data availability and resiliency
- Data traceability is a challenge and rarely done
- Auditors and security professionals frequently treat the storage infrastructure as nothing more than “attached storage”
- It’s possible to act on several levels, balancing trade-off among deployed infrastructure, regulatory requirements, business expectation

- Storage System Security (SSS)** –external authentication services, centralized logging, and firewalls.
- Storage Resource Management (SRM)** – Secure provisioning, monitoring, tuning, reallocation of the storage resources.
- Data In-Flight (DIF)** –Confidentiality, integrity and/or availability of data as they are transferred across the storage network, the LAN, and the WAN.
- Data At-Rest (DAR)** –Confidentiality, integrity and/or availability of data residing on servers, storage arrays, NAS appliances

(according to **SNIA**)



we need an interdisciplinary approach based on the following steps...



Develop a strategy

Based on Business Requirements

Security Best practices

... think holistically



Design and Implement

Take a risk-based approach to security

- **Virtual/Physical Network Security Design**
- **Virtual/Physical Host Security Design**
- **Provisioning of virtual resources enforcing security domains and location constraints**
- **Secure Communication**
- **Identity Access and Management**
- **Audit/Log Infrastructure**



Technology and Services

Select Cloud technology and services

... modularity and standards are key

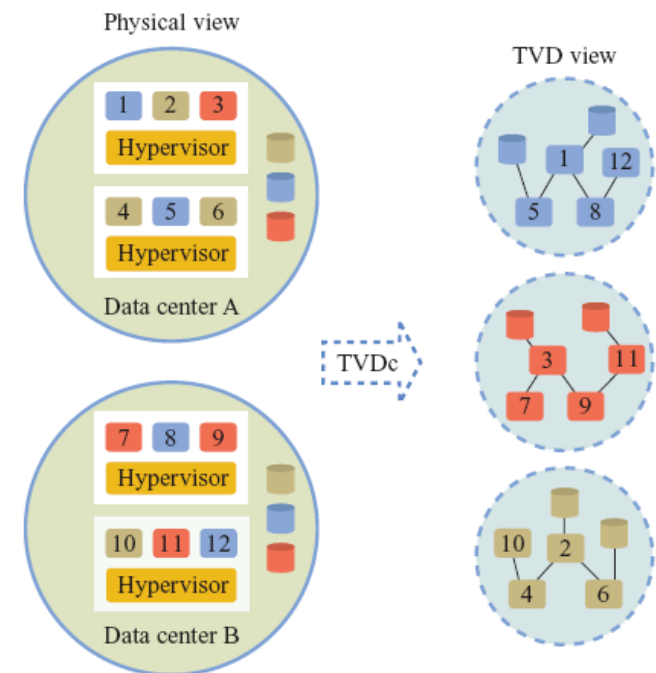
- **SOA Security (es: WS-Security, WS-Federation)**
- **Identity Federation (es: SAML, OpendID)**
- **IEEE 802.1q Vlan**
- **Hypervisor Certifications (es: Common Criteria)**

Trusted Virtual Data Center – The IBM model

The trusted virtual data center (TVDC) is a set of technologies and processes to address the need for strong isolation and integrity guarantees in virtualized, cloud computing environments. VMs and associated resources are grouped into trusted virtual domains (TVDs)

The goal of TVDC is to isolate workloads from each other. In particular, the TVDC aims to:

- 1) prevent data from leaking from one customer workload to another, even when a VM running the workloads malfunctions;
- 2) ensure that viruses and other malicious code cannot spread from one customer workload to another and that break-ins in one workload do not threaten the workloads active within the same physical resource;
- 3) prevent or reduce the incidence of failed configuration management tasks (i.e., misconfiguration)



IBM Security Solutions for Cloud Computing are composed by three main pillars

1 Cloud Security Consulting

Offer IBM ISS professional security services to clients engaging in cloud initiatives.

Examples:

- Security Design leveraging standards, best practices, IBM products (TIVOLI, ISS, Websphere)
- Information security assessment
- Protection policy and standards development
- Cloud assessment services
- Penetration testing for the Cloud

2 Cloud Security Products

Technologies in support of cloud computing

Develop products and technologies to protect cloud infrastructures and their tenants.

Examples:

- Proventia Network IPS and Virtual IPS appliances
- Virtual Server Security for VMware
- Identity and access management
- Security event and information management

3 Cloud-based Security Services

Smart business Security Services

Leverage the cloud as a delivery mechanism for IBM security services.

Examples:

- Vuln management service
- Email scrubbing service
- Web content filtering service
- Security event log management



Security For the Cloud – Existing Professional Security Services matching Cloud security needs

IBM Cloud Security Consulting

- **Security Governance & Strategy**
 - *Business Impact Analysis*
 - *Security Risk Assessment*
 - *Information Security assessment*
- **Security Design & Implementation**
 - *Policies, Standard & Guidelines development*
 - *Enterprise Security Architecture Design:*
 - *Auth, Authz, Accountability,*
 - *Confidentiality and Integrity,*
 - *Security Event Monitoring,*
 - *Regulatory Compliance and Privacy design and implementation*
 - *Solution Implementation*
 - *Network and virtualized server protection*
- **Security Awareness**
 - *Education and Training*

Focus

- Enterprise wide security assessment, design and implementation services to help build effective information security solutions
- Provides relevant security expertise in enabling organizations to define and implement a sound strategy for secure cloud computing.
- Services tailored to consider security implications of cloud computing.
- Services able to define roadmap for identifying which workloads could or have to be “clouded” first, respect to the strategic business needs
- Services able to design and implement a secure cloud enterprise infrastructure

Security from the Cloud - IBM Cloud Managed Security

IBM Cloud Based Managed Security Services

- **Security Enablement Services**
 - *Security Event & Log Management*
- **Content Security Services**
 - *E-mail content filtering*
 - *Web content filtering*
- **Vulnerability Assessment Services**
 - *Infrastructure Vulnerability Assessment*
 - *PCI ASV Vulnerability Assessment*
 - *Application Vulnerability Assessment*
- **Managed Security Services (for private Cloud)**
 - *Managed Firewall Services*
 - *Managed IPS/IDS Services*

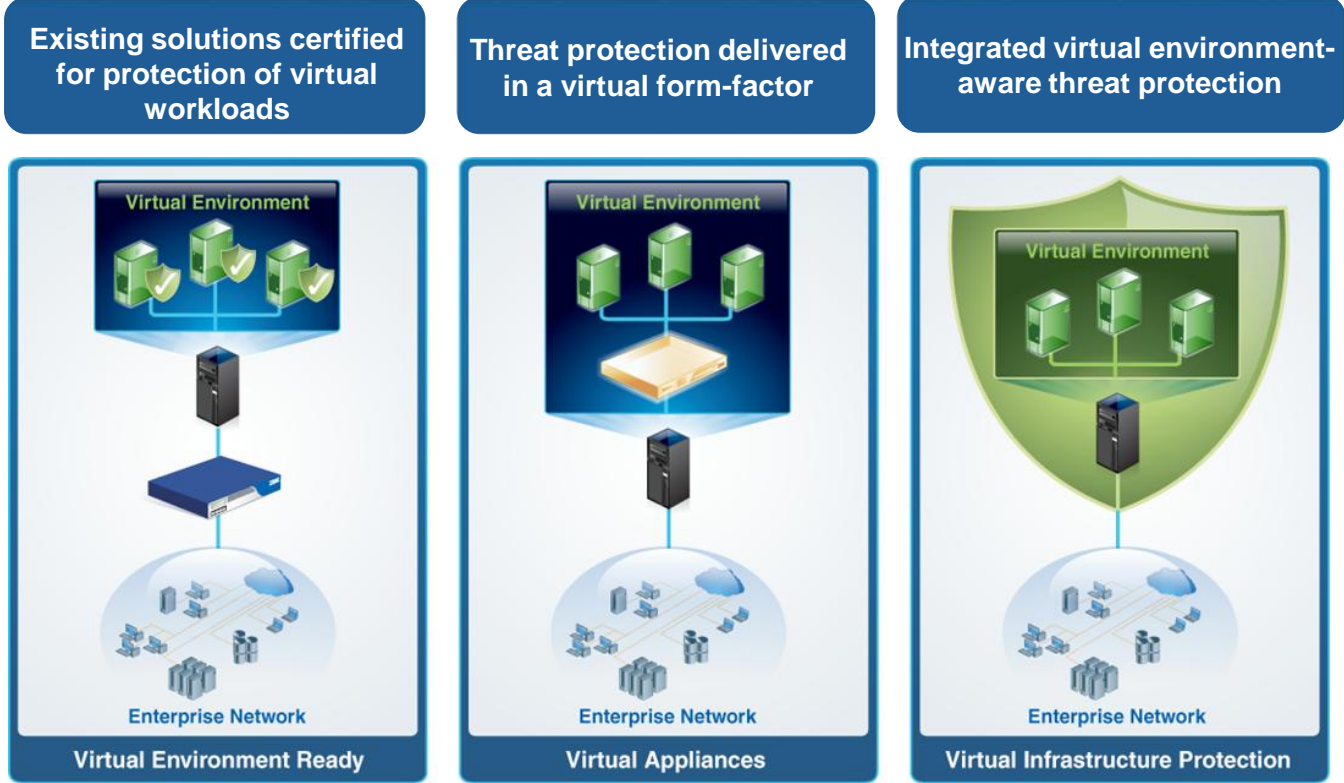


Focus

- Benefit from having in the “cloud” the expert tools, skills talent and processes
- Improve system uptime and performance
- Avoid large investment in technology and resources
- Reduce overall cost of doing business
- Focus in-house IT resources on core business functions
- Ensure business continuity by preventing attacks

IBM Virtualization Security Solutions deliver products and services, optimized for virtualization

This solution will enable customers to realize the benefits of virtualization while maintaining their security posture



- IBM Proventia® Server Intrusion Prevention System (IPS)
- IBM Proventia Network IPS
- IBM Proventia Network Mail Security Systems
- Data Loss Prevention
- IBM Managed Security Services
- Proventia Virtualized Network Security Platform
- Proventia Network Mail
- IBM Virtual Server Security for VMware®

Summarizing security countermeasures into a cloud infrastructure

A possible taxonomy

Domain	What	How
Network	<ul style="list-style-type: none"> ▪ Network Isolation ▪ Network Access ▪ DataFlows 	<ul style="list-style-type: none"> ▪ Vlan ▪ Firewall & IPS (virtual and physical) ▪ Specific Security solution for Virtual environment ▪ ACLs
Intra-box	<ul style="list-style-type: none"> ▪ Workload Isolation ▪ Granted Resource (CPU/IO/Mem) ▪ Inter Communication segregation & confidentiality ▪ Denial of Service 	<ul style="list-style-type: none"> ▪ Hardening ▪ Vlan ▪ Specific Security solution for Virtual environment ▪ Third party security Certifications ▪ Native or external solution (depending on the Hypervisor)
Storage	<ul style="list-style-type: none"> ▪ Data isolation ▪ Data integrity ▪ Data confidentiality at rest ▪ Data confidentiality in flight 	<ul style="list-style-type: none"> ▪ Encryption ▪ Fiber Channel security enabled ▪ Zoning ▪ LUN Masking
Inter-Box	<ul style="list-style-type: none"> ▪ Security posture ▪ Virtual Network Access Control ▪ Confidentiality 	<ul style="list-style-type: none"> ▪ Specific Security solution for Virtual environment ▪ Specific Solution for patch management ▪ Ad hoc network for Inter-Box Mobility
Infrastructure Management	<ul style="list-style-type: none"> ▪ Segregation of duties such as “Assign”, “Create”, “Deploy”, “Activate” 	<ul style="list-style-type: none"> ▪ Hardening ▪ Security Policy ▪ Specific Management solution with RBAC capabilities

In conclusion – some opinions

- *“Users will be challenged and served by these technology trends. Most will find a mix of onpremises application infrastructure and cloud application infrastructure services to be the best answer. However, the proportion of the two approaches will differ among users, industries and geographies. It will also change over time.” – Gartner*
http://www.gartner.com/it/content/1128400/1128412/key_issues_for_cloudenabled_app_inf.pdf
- *“You will be tempted to take a different path. Beware of this new path as it may lead to misfortune or danger. Business success. Good luck with money. You will be forced to make a very difficult decision which will pull you in many directions. This is a very stressful period. A trip taken now may result in a new friend. “ – On Line Fortuneteller*
www.greekboston.com/fortuneteller/

Cloud Security requires **change** the usual **security mindset** trying to **achieve** company **security** baseline **leveraging** a mixture of **technologies, standards, processes, trust models** and **best practices**