IBM Software

PCTY2010

Pulse Comes to You

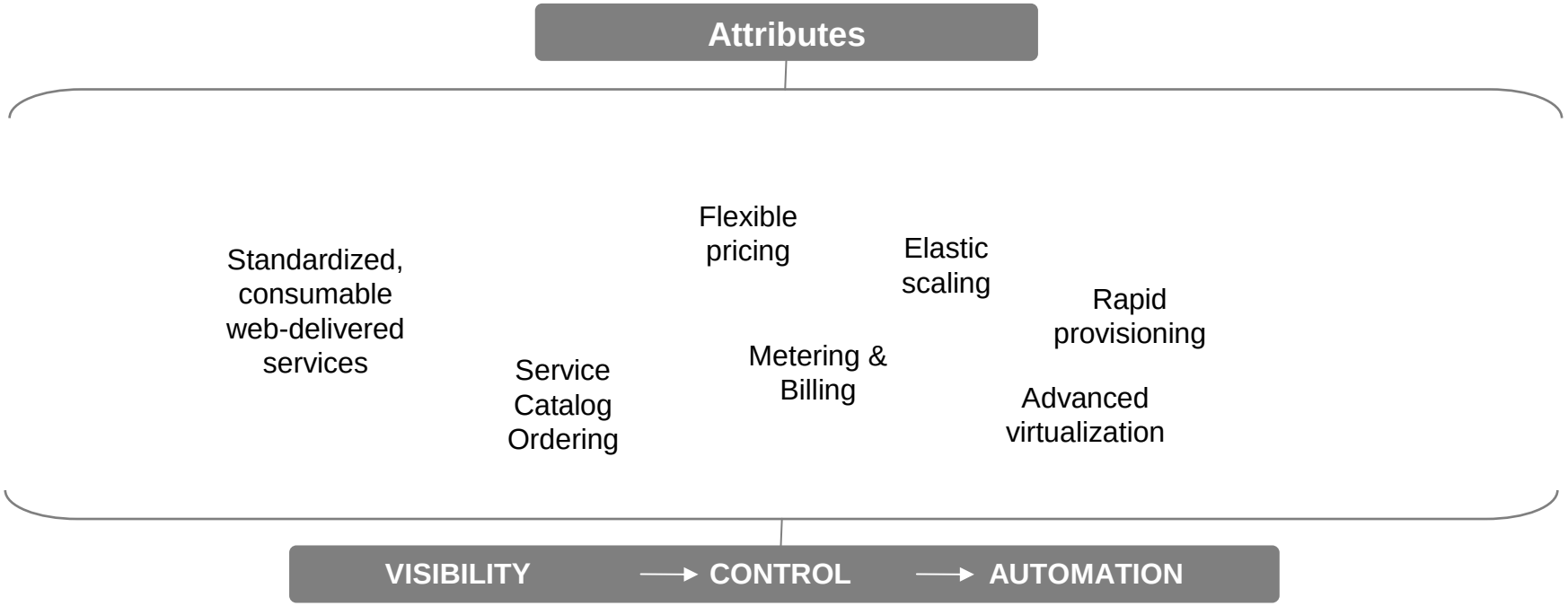
Cesare Radaelli

Security Tiger Team Leader, Italy
IBM Security Solutions

IBM Security in the Cloud

What is cloud computing ?

“Cloud” is an emerging consumption and delivery model for many IT-based services, in which the user sees only the service, and has no need to know anything about the technology or implementation



....service oriented and service managed
in a Secure environment


In the Cloud, a single web connection may control…
…an **entire data center**.

What is Cloud Security?

Confidentiality, integrity, availability
of business-critical IT assets

Stored or processed on a cloud computing platform

There is nothing new under the sun
but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary

Why is security important?

Security enables companies to pursue new, more efficient IT business models.

Strategic Outsourcing	Global Outsourcing	Grid Computing	Service Oriented Architecture	Web 2.0 Collaboration	Virtualization
Vendor Trust	Legislative Boundaries	Distributed Infrastructure	**Risks**	Web Threats	Data Leakage	Shared Infrastructure
SLAs	International Standards	Availability, Resiliency	**Security**	Web Security	Data Leakage Prevention	Isolation Technologies

Cloud Computing

Cloud Computing is a natural evolution of the evolving IT paradigms listed above.

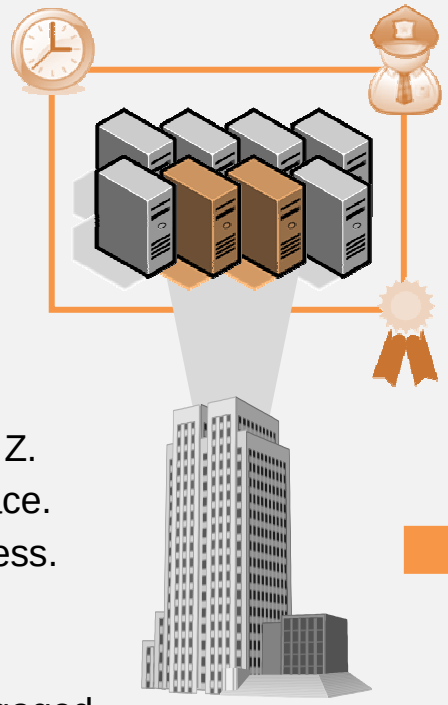
A variety of **security technologies**, **processes**, **procedures**, **laws**, and **trust models** are required to secure the cloud. **There is no silver bullet!**

Cloud Security 101: Simple Example

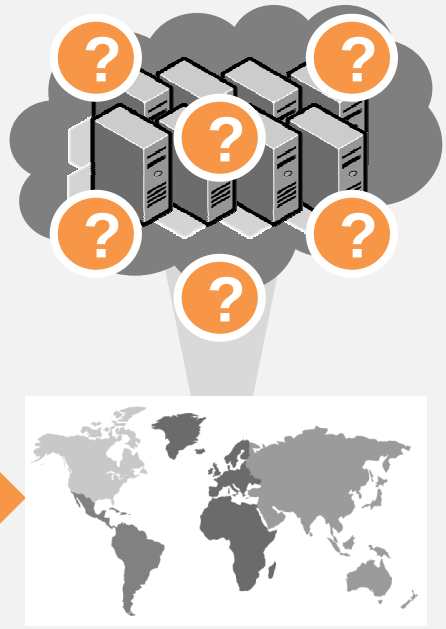
TODAY

We Have Control

It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.



TOMORROW



Who Has Control?

Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

Lesson Learned: We have responded to these questions before…
clouds demand **fast**, **responsive**, **agile** answers.

Recent Analyst Reports Confirm General Concerns – But also Highlight Security as a Potential Market Differentiator

- *"Securing your applications or data when they live in a cloud provider's infrastructure is a complicated issue because you **lack visibility and control** over how things are being done inside someone else's network."* Forrester, 5/09

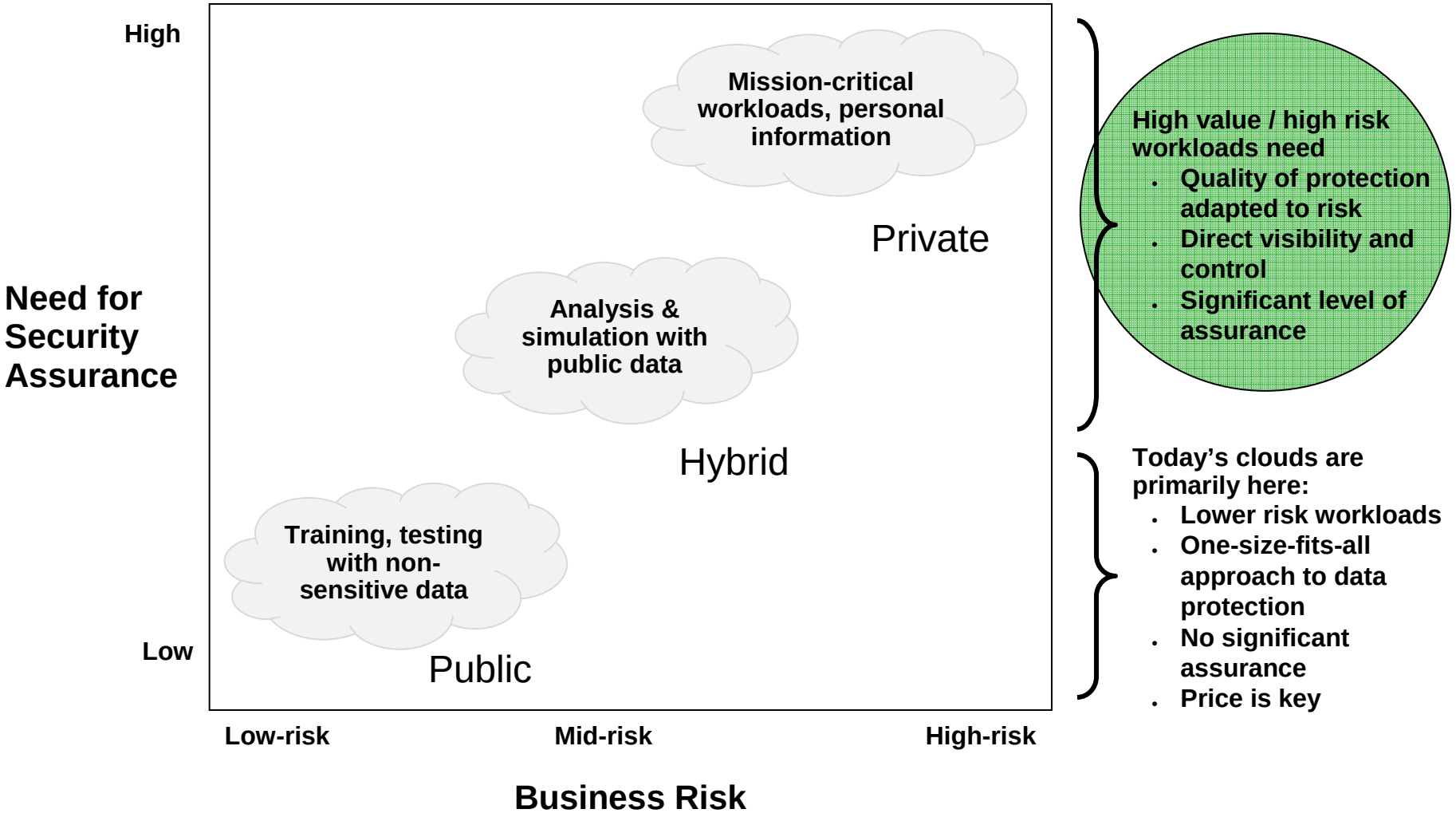
- *"Large enterprises should generally **avoid placing sensitive information in public clouds**, but **concentrate on building internal cloud and hybrid cloud** capabilities in the near term."* Burton, 7/09

- *"Cloud approaches offer a **unique opportunity to shift a substantial burden for keeping up with threats to a provider** for whom security may well be part of the value proposition."* EMA, 2/09

- Gartner's 7/09 *"Hype Curve for Cloud Computing"* positions Cloud Security Concerns into the ***early phase*** (technology trigger, will raise), and gives it a time horizon of ***5-10 years***

- ***"Highly regulated or sensitive proprietary information should not be stored or processed in an external public cloud-based service** without appropriate visibility into the provider's technology and processes and/or the use of encryption and other security mechanisms to ensure the appropriate level of information protection."* Gartner 7/09

Security as a Potential Market Differentiator:
Different Workloads have Different Risk Profiles



October 09 EDC Report:
Cloud Player Strenghts (Security)

Please pick the company that YOU THINK BEST fits the value - Security

	Valid Percent
IBM	21.7
Amazon	20.2
VMWare	9.9
Microsoft	9.1
Google	8.7
Sun	7.5
Citrix(Xen)	6.7
HP	5.5
Computer Associates	4.0
AT&T	3.2
Rackspace	2.8
Aptana	.8
Total	100.0

Market Alert - Perceptions of Cloud Service Providers © Evans Data Corp, 2009

IBM is ready to help in securing the cloud

The IBM Security Framework: Comprehensive Risk and Compliance Management

- **15,000** researchers, developers, and SMEs on security initiatives
- **3000+** security & risk management patents
- **200+** security customer references and **50+** published case studies
- **$1.5 Billion** security spend in 2008
- Managing more than **7 Billion** security events per day for clients

Gartner reports on security risks of cloud computing

…that map directly to the IBM Security Framework.

- Privileged User Access
- Data Segregation
- Data Recovery
- Investigative Support
- Regulatory Compliance
- Data Location
- Disaster Recovery

Gartner: Assessing the Security Risks of Cloud Computing, June 2008

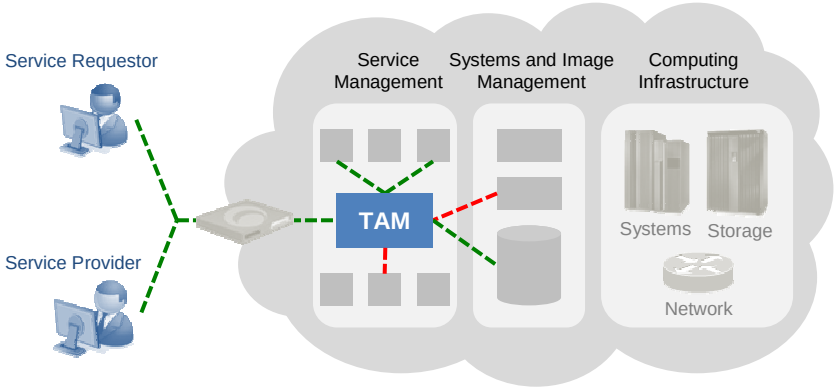
People and Identity

Privileged User Access

Separation of administrative and user roles in a cloud environment

Tivoli Access Manager (TAM)

Cloud Use Case: Provides validation and processing of user identity information. Addresses the need of authentication of users within the cloud ecosphere. Defines and manages centralized authentication, access and audit policy with access management.

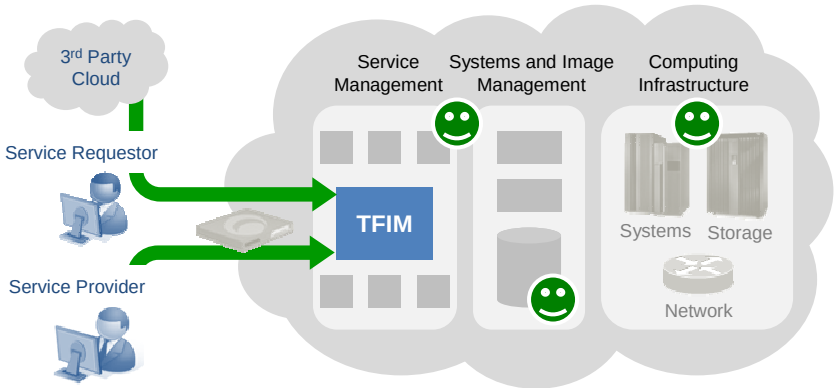


Cloud Identity Federation

Single access method for users into cloud and traditional applications

Tivoli Federated Identity Manager (TFIM)

Cloud Use Case: In massively parallel, cloud-computing infrastructures, TFIM enables trust between SOA-based initiatives by connecting users to services across business domains and helps enterprises strengthen and automate user access rights.



Application and Process

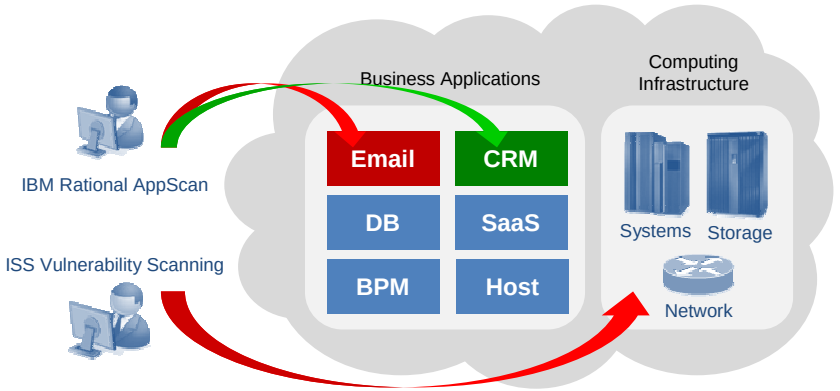
Compliance and Auditing

Vulnerability and compliance checking of cloud applications

IBM Rational AppScan & IBM ISS Vulnerability Assessment Services

Summary: IBM Rational AppScan scans and tests for common Web application vulnerabilities including SQL-Injection, Cross-Site Scripting and Buffer Overflow. IBM ISS Professional Security Services performs automated scans to identify operating systems, apps, and their respective vulnerabilities.

Cloud Use Case: External or internal testing of cloud applications and their hosted infrastructure. Delivered as components for integration into the cloud or as a hosted service via-the-cloud.



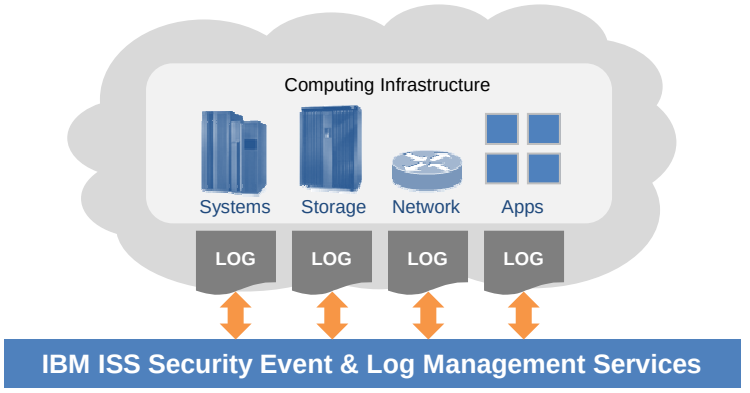
Investigative Support

Ability to inspect and audit a cloud provider's logs and records

IBM ISS Security Event and Log Management Service (SELM)

Summary: The IBM ISS Security Event and Log Management Service enables corporations to compile event and log files from network applications and operating systems, as well as security technologies, into one seamless platform – administered from an easy-to-use Web portal.

Cloud Use Case: Improves the speed of conducting security investigation and archives forensically-sound data, admissible as evidence in a court of law, for a period up to seven years.



Network, Server and Endpoint

Enterprise Security

Security for existing IT infrastructure as it extends to the cloud

IBM Enterprise Security Solutions

Summary: IBM ISS security products and services driven by X-Force research, Tivoli Security Software to reduce cost and risk, and IBM Systems work together to create a highly secure computing environment that minimizes the potential risk posed by security threats.

Cloud Use Case: Our end-to-end solutions allow customers to build a strong security posture - positioning them to reap the rewards of emerging trends such as cloud computing.

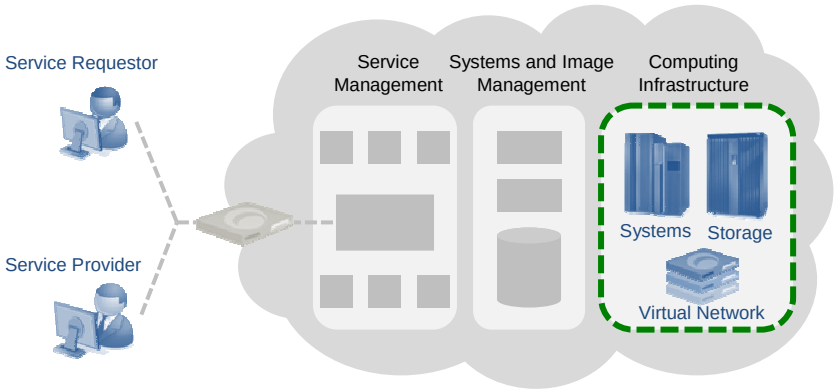
Virtualization Security

Security for pools of high performance virtualized resources

IBM Systems and IBM ISS Virtualization Security

Summary: IBM offers the industry's broadest set of virtualization capabilities. Relying on over 40 years of heritage and attention to security, IBM virtualization platforms are built with security as a requirement, not an afterthought. Solutions from IBM ISS, such as **Proventia Server and virtual appliances,** strengthen defenses by eliminating additional threats.

Cloud Use Case: Security of the virtualization stack - enabling flexible, rapid provisioning across heterogeneous servers and hypervisors.



IBM Security Solutions is positioned to help secure Cloud Computing in 3 areas

1 Cloud Security Consulting

IBM Strategy Mapping:

Define, invest in, and develop Cloud Consulting Services

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

Examples:

- Penetration testing
- Information security assessment
- Protection policy and standards development

2 Cloud Security Products

Technologies in support of cloud computing

IBM Strategy Mapping:

Develop a Standardized Cloud Implementation methodology with supporting technologies

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

Examples:

- Scalable chassis-based solutions
- Virtual appliances
- Integrated virtualization security
- Integrated server protection
- Proventia enhancements to better comprehend clouds (mobility, multi-tenancy)

3 Smart business Security Services

Smart business Security Services

IBM Strategy Mapping:

Develop and extend selected ITS Managed Services offerings

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
- X-Force threat analysis service
- Alliances with 3rd party services

Securing Cloud Infrastructures → **Security from an IBM ISS Cloud**

Inasset – case study

IBM Software

PCTY2010

Pulse Comes to You

INASSET

An integrated network protection system safeguards ISP customers

The Need:

A Neutral Business Datacenter, INASSET offers hosting, co-location, server-on-demand, private server farms and data protection. As a Neutral Business Datacenter, the company is subject to internal and external security regulations. To provide the best possible protection for its customers and ensure regulatory and risk management compliance, the company decided to look for a network traffic inspection solution to secure its service infrastructure.

The Solution:

INASSET implemented a multi-layer network intrusion solution. Firewalls offer the first layer of defense, and network traffic then passes through security appliances for a deep-packet inspection at layers two to seven. A site protection console aggregates information to help the company detect and resolve any security issues and prevent security incidents.

What Makes it Smarter:

- Intelligent technologies in the solution recognize malware based on the behavior of the malicious code. The solution provides protection not only from specific threats but also from all of a threat's variants.
- The instrumented appliances collect security data from the network, recognize threats and block them before they impact the business.
- The solution integrates the entire infrastructure, starting with network protection and reaching all of the servers installed at the company's data center.

"We're able to ensure business continuity for our customers through cost-effective processes while supporting regulatory requirements."

— Alessandro Gaspari, Director of Data Center Solutions & Services InAsset

Solution components:

- IBM® Proventia® MX firewall
- IBM Proventia GX appliance
- IBM Global Technology Services

inasset.
business datacenter


Thank
You