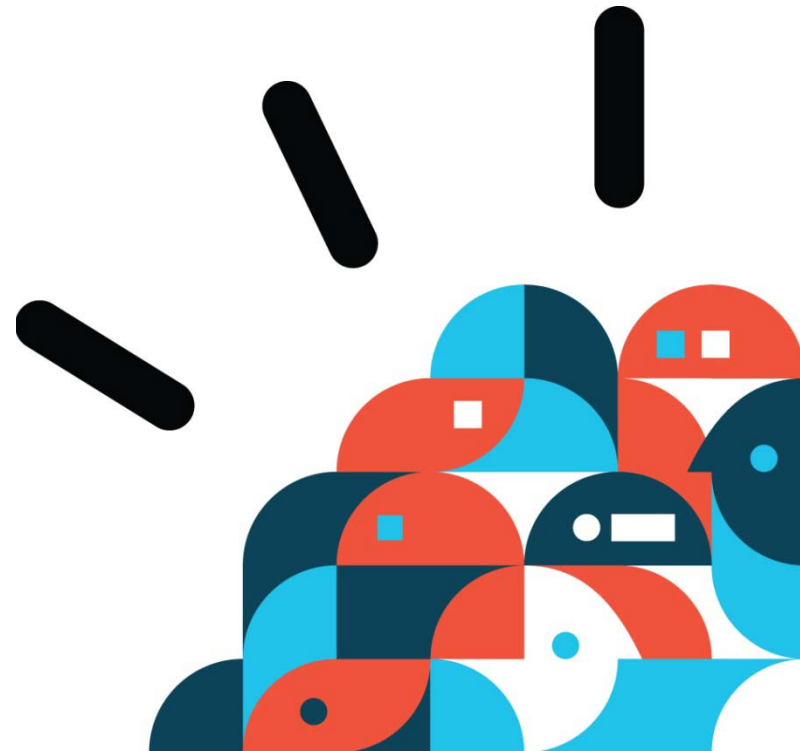


---

**Rethink IT.**  
**Reinvent Business.**  
Smart, Secure and Ready for Business

## **IBM Cloud Security**

Draft for Discussion  
September 12, 2011



## IBM Point of View: Cloud can be made secure for business

As with most new technology paradigms, **security concerns surrounding cloud computing** have become the most widely talked about inhibitor of widespread usage.

To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

The same way transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.

### Security and Privacy Expectations

Traditional IT

In the Cloud



**Trust**

# Cloud computing tests the limits of security operations and infrastructure



## Security and Privacy Domains

- People and Identity
- Data and Information
- Application and Process
- Network, Server and Endpoint
- Physical Infrastructure
- Governance, Risk and Compliance

## To cloud

- Multiple Logins, Onboarding Issues
- Multi-tenancy, Shared Resources
- External Facing, Quick Provisioning
- Virtualization, Reduced Access
- Provider Controlled, Lack of Visibility
- Audit Silos, Logging Difficulties

In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resources and applications increases - **greatly affecting all aspects of IT security.**

# Different cloud deployment models also change the way we think about security



## Private cloud

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party



## Hybrid IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability



## Public cloud

Available to the general public or a large industry group and owned by an organization selling cloud services.



## Changes in Security and Privacy

- Customer responsibility for infrastructure
- More customization of security controls
- Good visibility into day-to-day operations
- Easy to access to logs and policies

- Provider responsibility for infrastructure
- Less customization of security controls
- No visibility into day-to-day operations
- Difficult to access to logs and policies

To address these concerns, IBM is working with clients as both a cloud service provider and trusted advisor

## Secure IBM Clouds

IBMSmartCloud

Reduce costs.  
Improve service delivery.  
Enable business innovation.



Leveraging IBM's deep security skillset, hosting and strategic outsourcing experience, broad security portfolio, history of security innovation, and commitment to client trust as the foundation for building security into all cloud offerings.

**IBM Cloud Reference Model**  
(Foundational Security Controls)

## IBM Security Solutions

New Customer Initiatives Require Enhanced Security



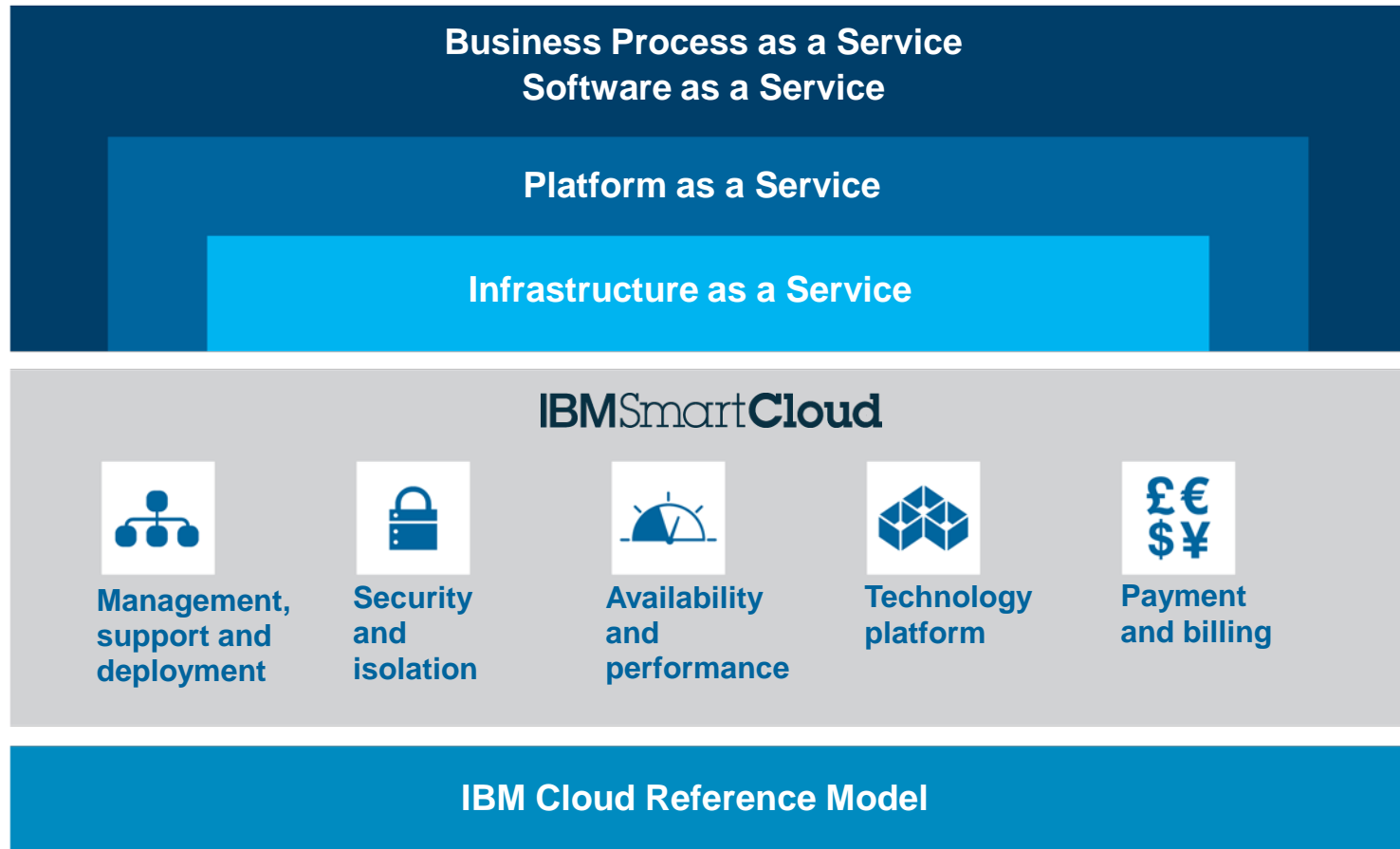
Leading portfolio of products and services to help secure cloud environments. Allows customers to address concerns when adopting private, public and hybrid cloud services by adopting security controls to match requirements of the workload.

**IBM Security Framework**  
(Cloud Security On Ramps)

Capabilities

Knowledge

# IBM SmartCloud provides a robust platform for the full IBM cloud portfolio, built on the IBM cloud reference model



# And is built against the following foundational security controls within the IBM cloud reference model



## Cloud Governance

Cloud specific security governance including directory synchronization and geo locational support



## Discover, Categorize, Protect Data & Information Assets

Strong focus on protection of data at rest or in transit



## Security Governance, Risk Management & Compliance

Security governance including maintaining security policy and audit and compliance measures



## Information Systems Acquisition, Development, and Maintenance

Management of application and virtual Machine deployment



## Problem & Information Security Incident Management

Management and responding to expected and unexpected events



## Secure Infrastructure Against Threats and Vulnerabilities

Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection



## Identity and Access Management

Strong focus on authentication of users and management of identity



## Physical and Personnel Security

Protection for physical assets and locations including networks and data centers, as well as employee security

## IBM Cloud Reference Model

# Our approach to delivering security aligns with each phase of a client's cloud project or initiative



## Design

Establish a cloud strategy and implementation plan to get there.



## Deploy

Build cloud services, in the enterprise and/or as a cloud services provider.



## Consume

Manage and optimize consumption of cloud services.

### IBM Cloud Security Approach

#### *Secure by Design*

*Focus on building security into the fabric of the cloud.*

#### *Workload Driven*

*Secure cloud resources with innovative features and products.*

#### *Service Enabled*

*Govern the cloud through ongoing security operations and workflow.*

### Example security capabilities

- Cloud security roadmap
- Network threat protection
- Server security
- Database security
- Application security
- Virtualization security
- Endpoint protection
- Configuration and patch management
- Identity and access management
- Secure cloud communications
- Managed security services

# Each pattern has its own set of key security concerns

**Infrastructure as a Service (IaaS): Cut IT expense and complexity** through cloud data centers

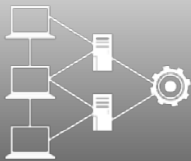
## Cloud Enabled Data Center

*Integrated service management, automation, provisioning, self service*

Key security focus:

### Infrastructure

- Manage datacenter identities
- Secure virtual machines
- Patch default images
- Monitor logs on all resources
- Defend network threats



**Platform-as-a-Service (PaaS): Accelerate time to market** with cloud platform services

## Cloud Platform Services

*Pre-built, pre-integrated IT infrastructures tuned to application-specific needs*

Key security focus:

### Data and Information

- Secure shared databases
- Encrypt private information
- Build secure applications
- Keep an audit trail
- Integrate existing security



**Innovate business models** by becoming a cloud service provider

## Cloud Service Provider

*Advanced platform for creating, managing, and monetizing cloud services*

Key security focus:

### Governance and Compliance

- Isolate cloud tenants
- Secure portals and APIs
- Manage security operations
- Build compliant data centers
- Offer backup and resiliency

**Software as a Service (SaaS): Gain immediate access** with business solutions on cloud

## Business Solutions on Cloud

*Capabilities provided to consumers for using a provider's applications*

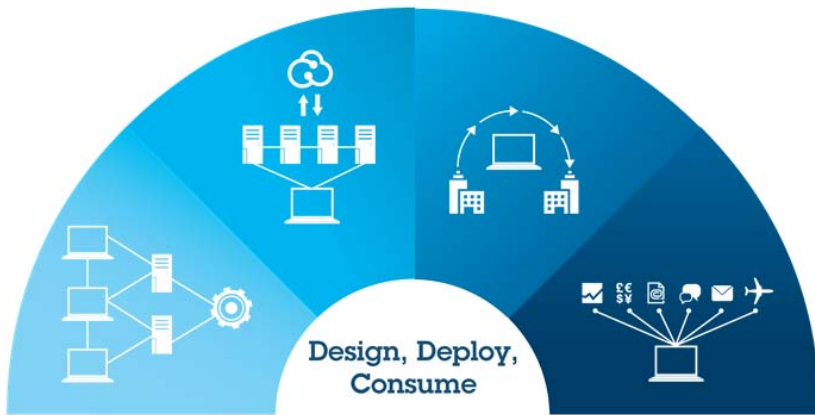
Key security focus:

### Applications and Identity

- Harden exposed web apps
- Securely federate identity
- Deploy access controls
- Encrypt communications
- Manage application policies

# IBM has a broad portfolio of products and services to help satisfy our customer's most pressing security requirements

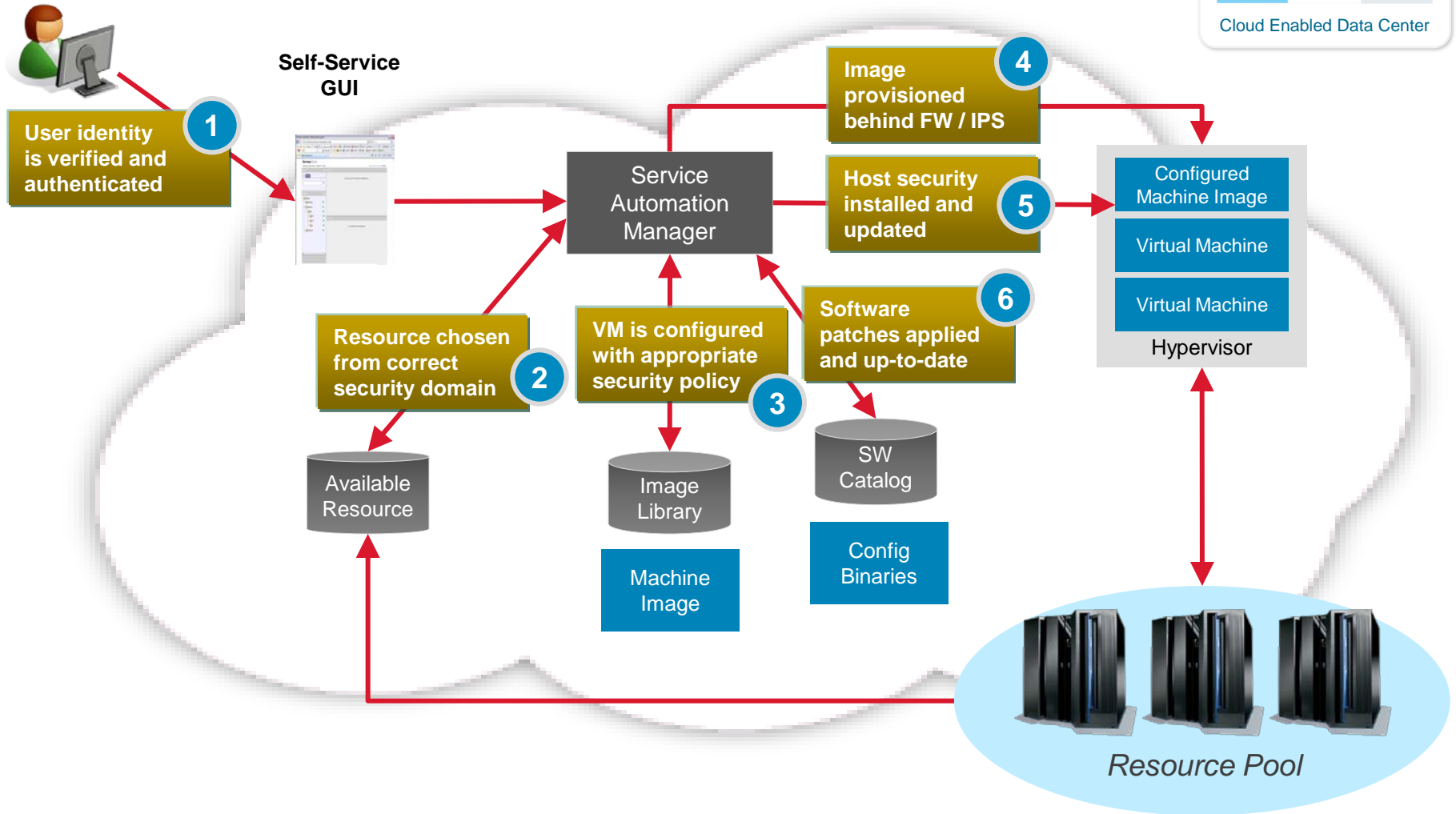
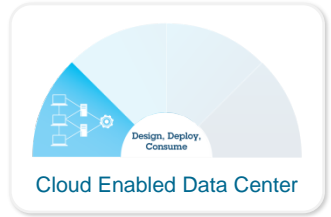
## IBM Cloud Security One Size Does Not Fit All



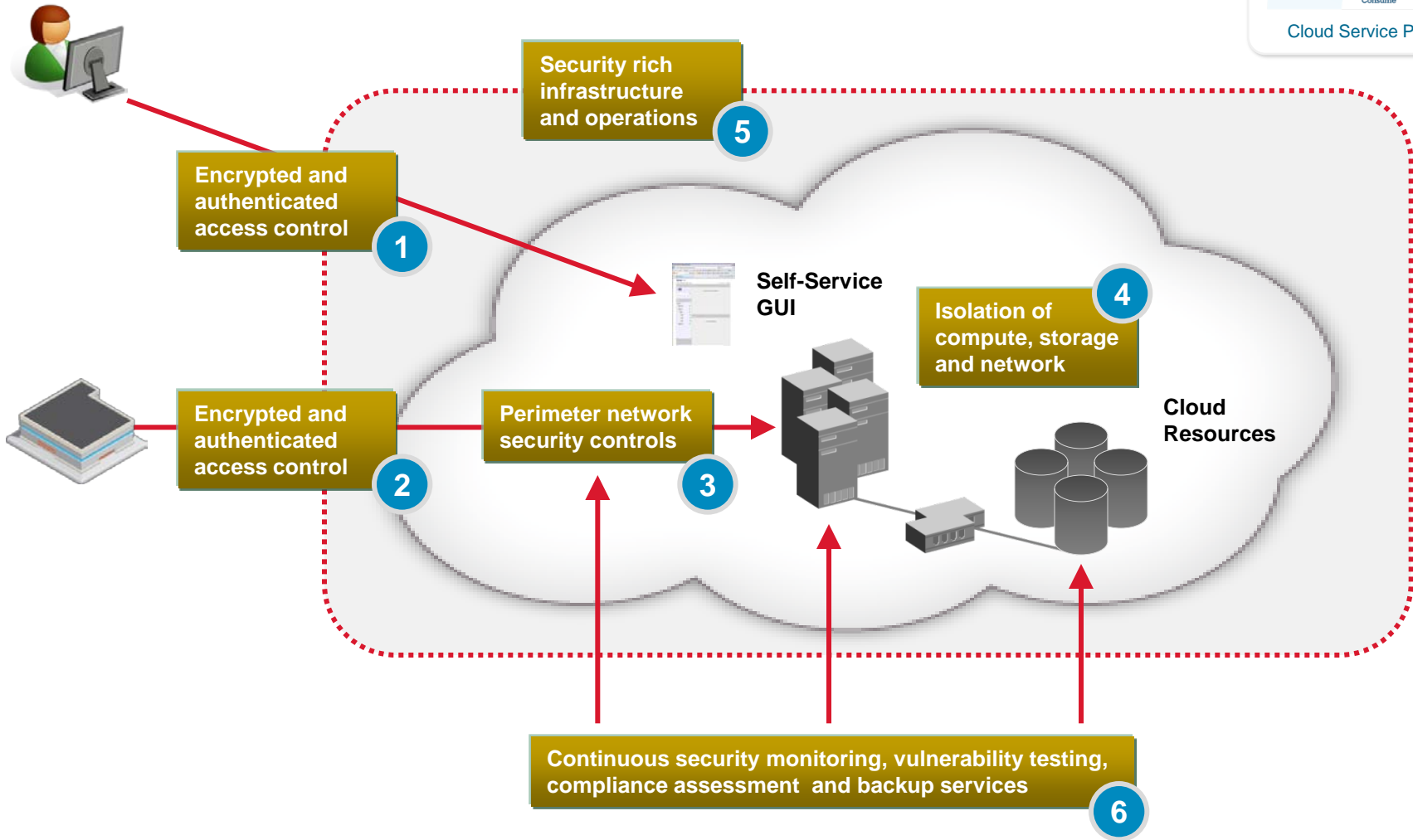
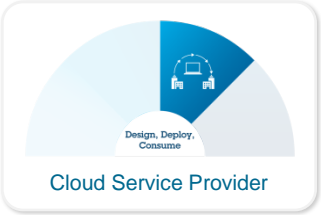
*Different security controls are appropriate for different cloud needs - the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.*



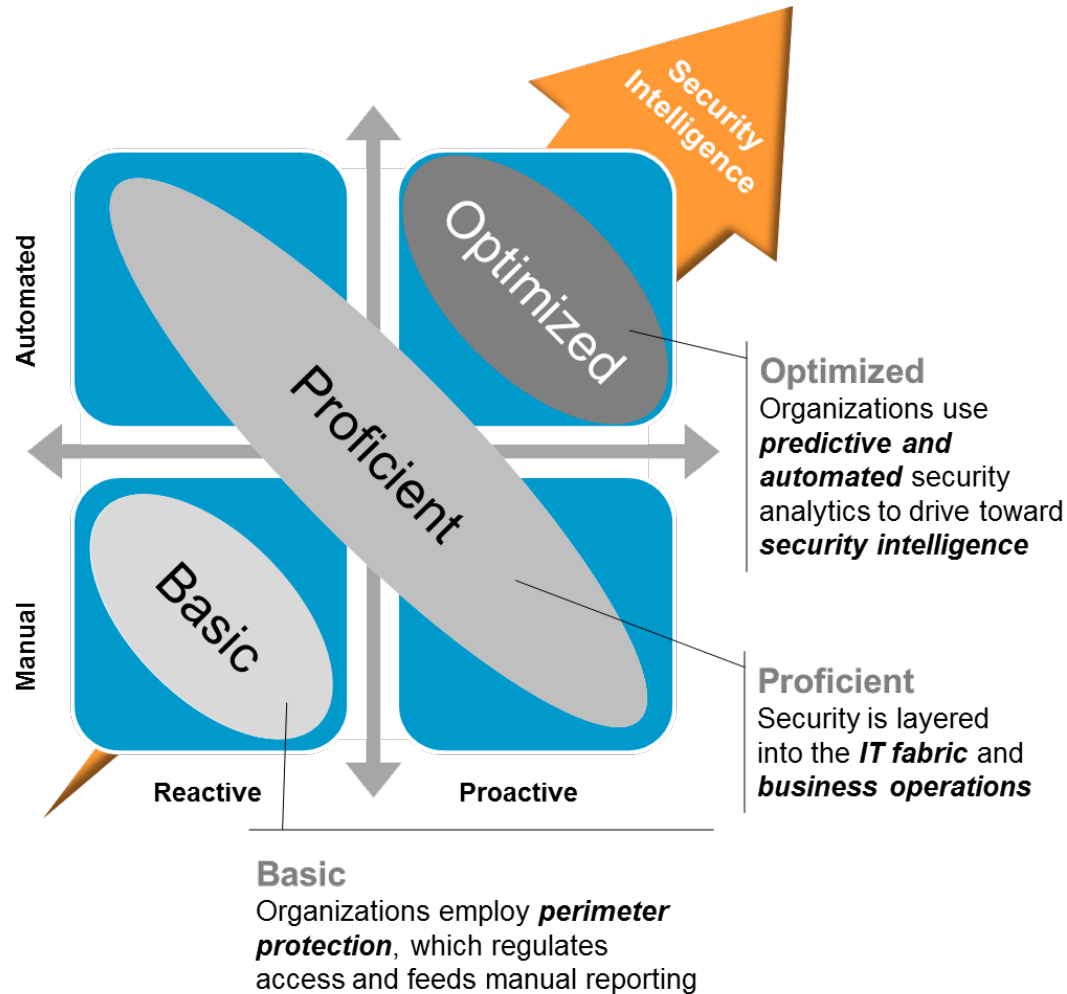
# Cloud Enabled Data Center - simple use case



# Cloud Service Provider - simple use case



In this “new normal”, organizations need an intelligent view into their security posture



# IBM has the largest, most complete IT security portfolio across the domains in the IBM Security Framework

