Safeguarding the cloud with IBM Security solutions

Maintain visibility and control with proven security solutions for public, private and hybrid clouds

Highlights

- Address cloud concerns with enterprise-class security solutions across all IT security domains
- Protect and manage internal and external users, data, applications and workloads as they move to and from the cloud
- Regain visibility and demonstrate compliance with activity monitoring and security intelligence

Cloud computing is transforming the way we think about IT. By treating IT as a true service, users can rapidly access the applications, business processes and infrastructure they need—resulting in greater operational efficiencies and lower costs than with many traditional IT deployments. However, as with any new technology, security is often seen as a major inhibitor to adoption. IT departments are concerned with reduced visibility into cloud data centers, less control over security policies, new threats facing shared environments and the complexity of demonstrating compliance. These concerns are especially magnified in public-cloud environments in which there is no physical access to the cloud infrastructure. As long as these concerns persist in the minds of those considering cloud, security issues will continue to hamper broad cloud adoption.

However, cloud security can be improved for business environments if it is designed into the underlying infrastructure, with layered defenses to protect workloads from attacks. Users also need solutions that can provide visibility into their overall security posture. It is important to understand the unique challenges that cloud introduces, while at the same time ensuring that the overall cloud security strategy can be integrated with existing IT security policies and procedures.

IBM has developed a portfolio of cloud security solutions that spans all security domains—people, data, applications and infrastructure. With an emphasis on visibility, control, isolation and automation, security solutions from IBM help create a cloud environment that drives down costs, increases security and meets the requirements of today's dynamic business climate.

Based on the IBM Security framework and informed by numerous client engagements, IBM provides products, services and expertise to secure every critical domain of the cloud environment.

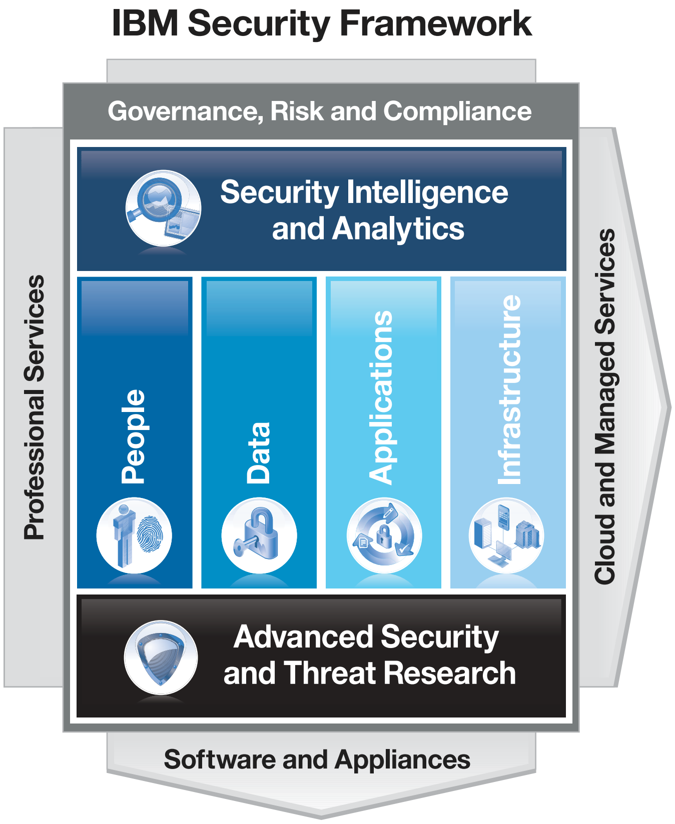
IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Figure 1: IBM has developed a portfolio of cloud security solutions that spans all security domains, as evidenced by our strong security framework.

Whether you are designing a new cloud service, deploying data and workloads to the cloud, or consuming information from cloud-based services, a holistic view of security and a strong understanding of risks associated with each domain are necessary to keep up with constantly-changing cloud infrastructures. Clearly, a responsive, integrated, end-to-end security approach is needed—like the approach offered by IBM.

The capabilities featured in IBM Security solutions enable IT departments to reduce and manage risks associated with cloud computing by:

- Managing identities and single sign-on access across multiple cloud services
- Protecting and monitoring access to shared databases
- Scanning cloud-deployed web applications for the latest vulnerabilities
- Defending cloud users and workloads from sophisticated network attacks
- Providing endpoint and patch management of virtualized machines for security compliance
- Increasing the visibility and auditing of cloud activity within multi-tenant environments

People: Simplifying identity and access management across cloud environments

Organizations need to ensure that authorized users across their enterprise and supply chain have access to the data and tools they need, when they need them, while also blocking unauthorized access.

As relationships extend outwards, enabled by the rapid and agile nature of cloud, organizations will need strong provisioning and auditing capabilities for service and application entitlements. Cloud environments often represent a large and diverse community of users, so these controls are even more critical. Cloud also introduces a new tier of privileged users: administrators and operating personnel working for the cloud provider.

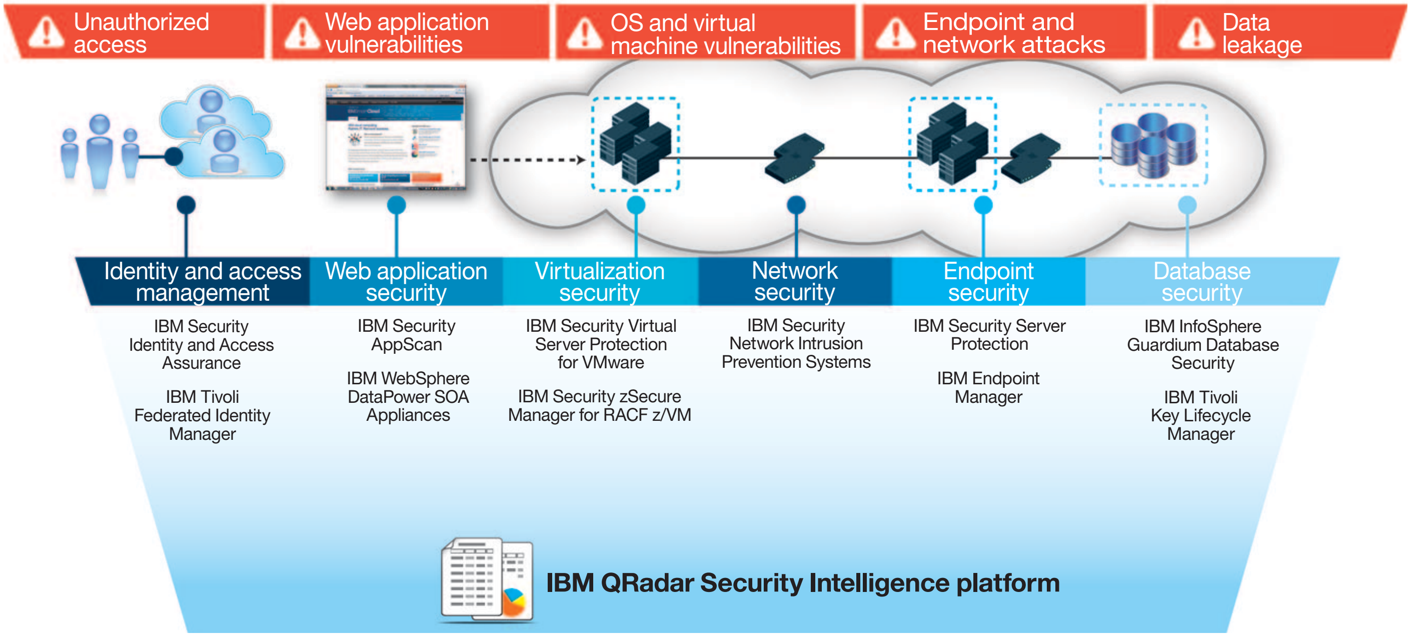
Unauthorized access
Web application vulnerabilities
OS and virtual machine vulnerabilities
Endpoint and network attacks
Data leakage
Identity and access management
IBM Security Identity and Access Assurance
IBM Tivoli Federated Identity Manager
Web application security
IBM Security AppScan
IBM WebSphere DataPower SOA Appliances
Virtualization security
IBM Security Virtual Server Protection for VMware
IBM Security zSecure Manager for RACF z/VM
Network security
IBM Security Network Intrusion Prevention Systems
Endpoint security
IBM Security Server Protection
IBM Endpoint Manager
Database security
IBM InfoSphere Guardium Database Security
IBM Tivoli Key Lifecycle Manager
IBM QRadar Security Intelligence platform

Figure 2: IBM protects against common cloud risks with a broad portfolio of flexible, layered security solutions.

To overcome these challenges, IBM Security Identity and Access Assurance helps users gain access to cloud resources, while also monitoring, controlling and reporting on the identities of the systems, database administrators and other privileged users. Users' roles are properly aligned to access capabilities and integration with the IBM QRadar Security Intelligence solutions, which enable compliance reports and cloud activity monitoring.

Identity federation and rapid onboarding capabilities help extend entitlements to applications and environments beyond the corporate firewall. IBM Tivoli® Federated Identity Manager provides authentication to multiple cloud applications with a single ID and password, providing self-service for identity creation and management. In addition, it enables administrators to leverage a virtual appliance deployment model to get started quickly. Built on a standards-based platform, this single sign-on solution also simplifies logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services. When securing private clouds running on IBM System z® mainframe platforms, the IBM Security zSecure™ suite helps simplify mainframe user administration and access controls.

Data: Securing access to sensitive information in shared environments

Data protection is another critical cloud security requirement, with concerns ranging from how data is stored and accessed to meeting compliance and audit requirements to the cost of data breaches. To be sure, sensitive or regulated data must be properly segregated within the cloud storage infrastructure, including run-time and archived data.

However, monitoring and managing data access in a cloud environment can be challenging. Clouds are multi-tenant, increasing the risk of inadvertent or malicious acts that may result in breaches. Database and system administrators may have access to multiple clients' data, and the location of stored data in a cloud may change rapidly. IBM helps assure data governance through database access management; monitoring and reporting of both cloud-based users and system and database administrators; and preventing access attempts by malicious users.

IBM InfoSphere® Guardium® Database Security solutions offer capabilities to help protect cloud-based customer information and intellectual property from both external and internal threats. These solutions help prevent unauthorized changes to sensitive cloud-based data by privileged users. They also reduce audit costs by providing a consistent approach for cloud- and non-cloud-based databases, including a centralized security console across different database platforms.

As data moves from the enterprise to an external cloud provider, securing the data both in motion and at rest is a primary concern. You must be able to encrypt data and securely share and manage the encryption keys between the cloud provider and the consumer. Proper encryption and key management can often be used to satisfy both corporate and government compliance standards when it comes to the security of private and sensitive information. IBM Tivoli Key Lifecycle Manager was one of the first solutions to fully support the Key Management Interoperability Protocol, an open protocol that enables the easy and secure exchange of encryption keys between key managers and encryption providers. This open standard enables organizations to maintain the integrity of their keys within their own operating environments while enabling the secure key exchange necessary to encrypt sensitive data stored in the cloud. Proper key management also facilitates secure destruction of cloud data by simply destroying or redacting the keys.

Applications: Fortifying cloud-deployed web applications

Today's headlines are dominated by application security failures. Poor coding practices and human error, combined with the relative ease of finding and exploiting these vulnerabilities, often makes application security a major point of weakness. Even more notable is the explosion of corporate web applications in the cloud. As cloud computing accelerates the pace of deploying application stacks, security must keep up.

The IBM Security AppScan® suite of products provides one of the industry's most comprehensive sets of tools to protect today's enterprise applications. The Security AppScan Standard Edition dynamic analysis platform enables you to take on the role of attacker so you can plan how to best protect your applications. The solution's automated update system allows you to continuously test and secure applications deployed to the cloud even as new threats are identified. You can also leverage Security AppScan Source Edition during the development of both new and existing applications to ensure that the development team is meeting the organization's security requirements and integrating security into their development practices.

With the explosion of Web 2.0-enabled services and devices leveraging cloud, it is important to ensure that these services have the same type of security that can be found in more traditional service-oriented architecture (SOA) and Simple Object Access Protocol (SOAP) services leveraging Web Services (WS)-Security and Security Assertion Markup Language (SAML). IBM WebSphere® DataPower® SOA appliances provide an industry-leading set of data security services for interfacing the new generation of cloud-based applications with the advanced security demands of an organization's internal backend systems.

Infrastructure: Protecting networks, servers and endpoints from attacks

Secure communications and help prevent intrusions with network threat protection

In a cloud environment, it is important to properly isolate all tenant domains and prevent data from leaking from one tenant domain into the next. To help achieve this, users need to manage their workloads and place them in separate security zones with a controllable policy. Cloud workloads are often Internet-facing, significantly increasing exposure to external threats and requiring an advanced level of protection for cloud workloads and their users. The IBM Security Network Intrusion Prevention System provides network-level protection against emerging threats and vulnerabilities. Backed by the IBM X-FORCE® research and development team, IBM network protection shields applications from exploitation, identifies personally identifiable information and other confidential data, and prevents users from opening up attack vectors to and from cloud resources such as instant messaging protocols and peer-to-peer file sharing.

Protect cloud resources with the latest patches, security settings and monitoring

Unpatched systems, unnecessary services and poor configurations settings are a high risk to cloud deployments. Moreover, the cloud's use of virtualization introduces additional security complexities, such as maintaining the security of offline or suspended images, as well as new classes of attacks targeting the hypervisor directly.

IBM Security Server Protection helps monitor cloud systems for suspicious activity while auditing important operating system and application objects, such as critical files and registry settings. This host-based intrusion prevention product inspects SSL-encrypted traffic to and from cloud-hosted web servers and decreases exposure to malicious activity with built-in firewall and intrusion prevention system capabilities to block network traffic at the host. Alternatively, cloud administrators and service providers can take advantage of IBM Security Virtual Server Protection for VMware, designed to provide VMware-based infrastructures with dynamic security capabilities without requiring host-based agents within each guest.

To deal with poorly configured systems in the cloud, IBM Endpoint Manager can help ensure that correct patches and security configurations are continuously assessed and remediated. This single approach supports multiple operating systems and third-party applications with thousands of out-of-the-box policies for assessing and ensuring security policy compliance. Built on BigFix® technology, this solution gives cloud administrators the confidence to deal with large and rapidly changing virtual server deployments without significantly increasing management overhead.

Secure virtualized environments and private clouds operating on mainframes

The Security zSecure suite provides cost-effective security administration, improves service by detecting threats and reduces risk with automated audit and compliance reporting. The following tools, in particular, can enhance mainframe cloud environments:

- **IBM Security zSecure Audit**—Compliance and audit solution enables users to automatically analyze and report on security events and detect security exposures
- **IBM Security zSecure Administration**—Enables more efficient and effective IBM Resource Access Control Facility (RACF®) administration, using significantly fewer resources
- **IBM zSecure Manager for RACF z/VM®**—Provides combined audit and administration for RACF in the virtual machine environment

Security intelligence: Visibility and insight into cloud activity and threats

By design, clouds hide underlying infrastructure from their tenants, which makes compliance with regulations difficult—especially those requiring comprehensive audits for sensitive workloads. In addition, many cloud providers must support third-party audits, and cloud customers are beginning to ask for forensic capabilities to support security investigations. Visibility and auditing are clearly critical capabilities.

IBM QRadar Security Intelligence solutions provide auditing capabilities and visibility into third-party software-as-a-service solutions by monitoring all traffic leaving the enterprise and going to third-party hosted solutions. By monitoring data at the application and network levels, QRadar can aggregate this information with other security technologies, such as IBM Security Identity and Access Assurance, to correlate not only what data is going to the cloud, but which user is sending it.

The QRadar VFlow virtual collector provides layer-seven monitoring for VMware ESX and ESXi virtual environments and provides application-profiling support for more than 1,000 applications out of the box. QRadar VFlow runs as a virtual host inside of the hypervisor and can monitor traffic from the virtual switch as well as port-mirrored traffic from a physical switch, providing complete visibility in both the traditional and virtual environments that comprise hybrid cloud environments.

Cloud security roadmap

As more organizations look to embrace cloud infrastructures, IBM has developed a roadmap toward cloud adoption, centered around three distinct phases: design, deploy and consume. These phases are very similar to those of a traditional application development lifecycle. In order to better enable and leverage the strategic and economic benefits of cloud infrastructures, applications and business solutions, it is critical to establish a clear cloud security roadmap up front, before embarking on your cloud journey.

	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 cloud fabric.	**Workload driven** Secure cloud resources with innovative features and products.	**Service enabled** Govern the cloud through ongoing security operations and workflow.
Examples of security capabilities	• Cloud security roadmap • Secure development • 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

Figure 3: The IBM approach to delivering cloud security aligns with each phase of a traditional application development lifecycle: design, deploy and consume.

IBM customer case study: EXA Corporation

An integrated set of IBM cloud solutions for automation, security and management is enabling EXA Corporation to create a secure, hybrid private cloud solution that combines proprietary and external data centers distributed across Japan. A solution—including IBM Tivoli Service Automation Manager, Security Virtual Server Protection for VMware and Tivoli Federated Identity Manager—has helped the company to reduce costs and improve disaster resiliency, offer secure cloud-based services to its customers, and improve the flexibility and scalability of its IT environment. For more information about this customer case study, please click here.

Why IBM?

Security is a journey, not a destination. When developing a cloud security strategy, make sure it aligns with your overall IT security strategy and treat it as an extension of your existing IT infrastructure. Security should be a part of the entire cloud lifecycle, from design to deployment to consumption. That's why IBM offers such a broad portfolio of security products and services—to help build cloud environments with fewer vulnerabilities, more intelligent security policies and incredible cost savings—for every tenant of the cloud.

IBM security solutions are supported by the world-renowned IBM X-FORCE team—one of the oldest commercial security research teams in the industry. X-FORCE helps organizations stay ahead of emerging threats by analyzing and maintaining one of the world's most comprehensive vulnerability databases. X-FORCE researches and evaluates the latest security threats and trends, and develops countermeasure technologies for IBM security solutions.

For more information

To learn more about IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2012

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated, or can result in misuse of your systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

♻ Please Recycle