Safeguarding the cloud with IBM Dynamic Cloud Security

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

Highlights

- Extend enterprise-class security from the data center to the cloud
- Gain visibility across the data center to the cloud with security intelligence
- Tailor the security-to-the-cloud use case

Cloud computing is transforming IT, resulting in greater operational efficiencies and lower costs than with many traditional IT deployments. However, cloud computing requires consistent protection against threats—whether the threats originate on-premises or from an outside source.

The IBM® Dynamic Cloud Security portfolio was created specifically to help enterprises leverage existing security investments and bridge a mix of traditional IT, private, public and hybrid cloud models. Deployed in private and hybrid cloud environments, Dynamic Cloud Security provides layered protection, deep insight across the infrastructure and a flexible approach to tailor the security-to-the-cloud use case.

To safeguard the cloud, enterprises must focus on the following key areas:

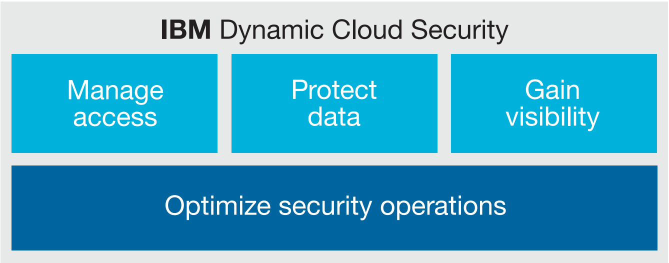
- **Manage access:** Safely connect people, applications and devices to the cloud—with easy-to-use identity and access management tools built for the cloud
- **Protect data:** Identify vulnerabilities and prevent attacks targeting sensitive data—using hardened underlying cloud infrastructure and applications
- **Gain visibility:** Monitor the cloud for security breaches and compliance violations—through advanced security analytics and threat intelligence from the cloud
- **Optimize security operations:** Deploy intelligence-driven security maturity across all environments by assessing and optimizing security practices

IBM delivers cloud security solutions including software, appliances and virtual appliances deployed in the enterprise data center on SoftLayer,[1] on IBM Bluemix™, and on other cloud platforms. SoftLayer provides integrated and automated high-performing cloud infrastructure and a wide range of cloud computing options. Bluemix is an open-standards, cloud-based platform for building, managing, and running applications of all types, including those for web, mobile, big data and smart devices.

Manage access: Control access across cloud environments

Organizations need to provide context-aware access to data and applications to authorized users when they need them, while also blocking unauthorized access. As relationships extend outward to diverse communities of users, organizations also need strong provisioning and auditing capabilities for service and application entitlements.

Cloud identity management: 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. Identity federation and rapid onboarding helps extend users to applications beyond the corporate firewall. IBM Federated Identity Manager provides authentication to multiple cloud applications with a single credential, providing self-service for identity creation and management. Built on a standards-based platform, this single sign-on solution helps simplify logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services. In addition, the IBM Single Sign-On solution allows developers to easily add similar user authentication and single sign-on functionality to applications running on the Bluemix platform.



Cloud access management: IBM Security Access Manager provides a gateway solution to deliver user-level security for workloads deployed on the cloud. A virtual appliance deployment model, available on SoftLayer as well as other cloud platforms, helps administrators get started quickly and scale to thousands of users, maintaining the same level of protection when applications are moved to the cloud by moving access management with them. This allows enterprises to have a singular and consistent policy enforcement point across the data center, private and public clouds.

Cloud privileged identity management: In addition to database administrators and system administrators, cloud computing introduces a new tier of privileged users: operating personnel working for cloud providers. IBM Security Privileged Identity Manager helps manage and control access to critical cloud resources by the organization's employees as well as personnel who work for cloud providers and have high-level privileged access.

Cloud identity services: For organizations with capital and staff limitations that still want the benefits of an enterprise-class identity and access solution, IBM Cloud Identity Services provides robust, cloud-based identity and access built on best-in-class IBM software and global delivery capabilities. IBM services use the cloud to deploy identity solutions quickly, at lower ownership costs and with simplified administration. With IBM services, there is no infrastructure for clients to build, and solutions can accommodate the changing needs of dynamic organizations.

Protect data: Reduce vulnerabilities, help prevent exploits

Sensitive or regulated data—including run-time and archived data in the cloud—must be protected from unauthorized access. IBM helps improve data governance through data discovery, access management, monitoring and reporting, and by blocking unauthorized access.

Cloud data activity monitoring: IBM InfoSphere® Guardium® Data Security solutions extend protection from the data center to cloud-based structured and unstructured data, sensitive information and intellectual property on SoftLayer. InfoSphere Guardium solutions also provide an efficient and protected audit architecture for cloud- and non-cloud-based data sources, including a centralized security console across different database platforms.

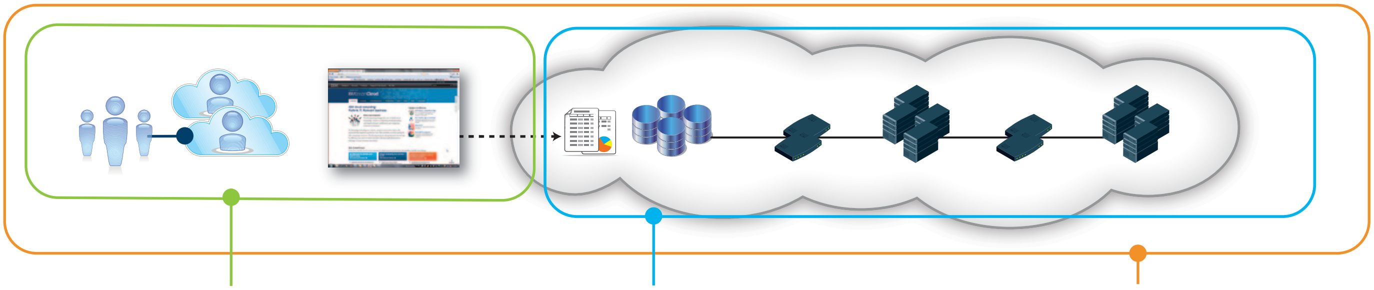
Cloud application security: Today's headlines are filled with news of data breaches that result from application security failures. Insecure coding practices and human error, combined with the relative ease of finding and exploiting application-based vulnerabilities, often make application security a major point of weakness. IBM Security AppScan® provides one of the industry's most comprehensive sets of tools to protect today's enterprise applications. The dynamic analysis platform included in IBM Security AppScan Standard Edition allows continuous testing of production applications that are deployed to the cloud. IBM Security AppScan Source Edition provides source code-scanning capabilities that help development teams discover and remediate security issues in new and existing applications—before placing the applications into production.

Today's DevOps environment requires agile application development. Developers who are unfamiliar with secure coding practices can gain application programming interface (API)-based access to security scanning services on Bluemix. IBM AppScan Mobile Analyzer and IBM AppScan Dynamic Analyzer produce vulnerability and remediation reports without the developer having to leave the Bluemix environment.

Cloud network protection: Internet-facing cloud workloads require an advanced level of protection on the network and at endpoints. Powered by IBM X-Force® research and development, IBM Security Network Protection helps shield applications and network infrastructure from exploitation, including zero-day attacks, provides visibility into network traffic, identifies personally identifiable information (PII) and other confidential data, and provides granular application control that prevents users from opening up multiple attack vectors such as malicious URLs, instant messaging protocols and peer-to-peer file sharing to and from cloud resources.

Cloud endpoint security: Unpatched systems, unnecessary services and poor configurations settings are a high risk to cloud deployments. IBM Endpoint Manager for Datacenters optimizes IT efficiency through higher levels of automation and enables users to find and fix problems in minutes across all endpoints (including physical and virtual servers), regardless of operating system—helping ensure continuous configuration compliance with security and regulatory policies.

IBM Dynamic Cloud Security



Manage access

Securely connect people, applications and devices to the cloud–with easy-to-use identity and access management built for the cloud

- Cloud identity management
- Cloud access management
- Cloud privileged identity management
- Cloud identity services

Protect data

Identify vulnerabilities and prevent attacks targeting sensitive data–with hardened underlying cloud infrastructure and applications

- Cloud data activity monitoring
- Cloud application security
- Cloud network protection
- Cloud endpoint security

Gain visibility

Monitor the cloud for security breaches and compliance violations–through advanced security analytics and threat intelligence from the cloud

- Cloud security intelligence

Optimize security operations

Deploy intelligence-driven security maturity across all environments by assessing and optimizing security practices

Cloud security managed services

Intelligent threat protection cloud

Security intelligence and operations consulting services

Gain visibility: Security intelligence and insight into cloud activity and threats

By design, clouds obscure underlying application traffic and user activity from their tenants, but this complicates activity monitoring and regulatory compliance reporting. Concerns about visibility and auditing can be roadblocks for many would-be adopters. Before making outsourcing commitments, organizations are also increasingly seeking advanced security incident search capabilities to support forensic investigations.

Cloud security intelligence: IBM QRadar® Security Intelligence, anchored by IBM Security QRadar SIEM, answers these concerns by monitoring all traffic going into and out of the cloud using a variety of hardware, software or virtualized software appliances. Cloud activity can be collected and analyzed within the cloud, or it can simply be collected and exported to an on-premises security intelligence resource. Suspect events and high-probability incidents can then be aggregated with complementary security technologies, such as IBM Security Identity and Access Assurance, to correlate not only what's occurring in the cloud, but also who's responsible for the actions.

QRadar solutions integrate with a growing list of cloud services and applications including SoftLayer, Amazon Web Services, CloudTrail, Salesforce, CloudPassage, Zscaler, Qualys and IBM Security Trusteer® Apex™. This allows organizations to embrace infrastructure as a service (IaaS), software as a service (SaaS) and hybrid cloud IT deployments with a combination of on-premises and in-the-cloud security intelligence appliances. QRadar solutions provide an audit trail for cloud-based applications when event and flow collectors are put into the cloud to forward security data to event and flow processors running within the client's data center. Organizations can also choose to implement a fully cloud-based security intelligence solution by collecting and forwarding on-premises data to a cloud-based instance of QRadar.

For VMware ESX and ESXi virtual environments, IBM Security QRadar VFlow Collector appliances provide Layer-7 monitoring and out-of-the-box profiling support for more than 1,000 applications. The solution runs as a virtual host inside the hypervisor and can monitor traffic from the virtual switch as well as port-mirrored traffic from a physical switch, providing visibility in both the traditional and virtual environments that comprise hybrid cloud environments.

Optimize security operations: Expertise to monitor, detect and act upon intrusions

IBM Cloud Security Managed Services help clients address the security challenges posed by a cloud environment without the costs involved in acquiring, configuring and managing new protection devices on premises. The offering addresses firewall, email and web security, as well as intrusion protection and event and log management. The service uses integrated security technologies, global threat intelligence and vulnerability research to meet customers' unique demands. Security professionals monitor cloud security around the clock, 365 days a year. Other offerings include emergency response services to help address suspected breaches in a cloud environment and a host-based intrusion detection system for servers.

IBM Security Intelligence and Operations Consulting Services help organizations develop security maturity in intelligence-driven operations across all environments. The IBM Security Intelligence and Operations Consulting Services team can help an organization assess, build and/or optimize its security intelligence and operations capabilities as it evolves its security organization to safely migrate its business to the cloud.

IBM Managed Security Services, powered by intelligent threat protection for cloud environments, provides "big data" insights, next-generation intelligence tools and powerful visualization of threats across hybrid cloud and on-premises environments.

Why IBM?

Security is a journey, not a destination. An enterprise cloud security strategy should align with the organization's overall IT security strategy as an extension of the existing IT infrastructure. IBM has 30,000 cloud clients and 6,000 security professionals, along with 10 Security Operations Centers worldwide to help customers adopt and secure the cloud. IBM Security solutions protect more than 270 million endpoints and monitor 20 billion security events each day. IBM Security solutions benefit from countermeasure technologies developed by X-Force as a direct result of analysis of the latest security threats and trends and one of the world's most comprehensive vulnerability databases. In addition, IBM Security Cloud Services can help plan, deploy and manage an organization's cloud security operations, reducing the requirement to have in-house skills and resources to do so.

For more information

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

For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2014

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.

Statement of Good Security Practices: 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 damage to or misuse of your systems, including to attack others. 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.

[1] SoftLayer Technologies was acquired by IBM in July of 2013.