IBM Security

IBM

Deploying unified security in a hybrid cloud world

Complex, distributed resources call for unified simplicity for hybrid cloud security

What if securing your cloud could accelerate your business growth?

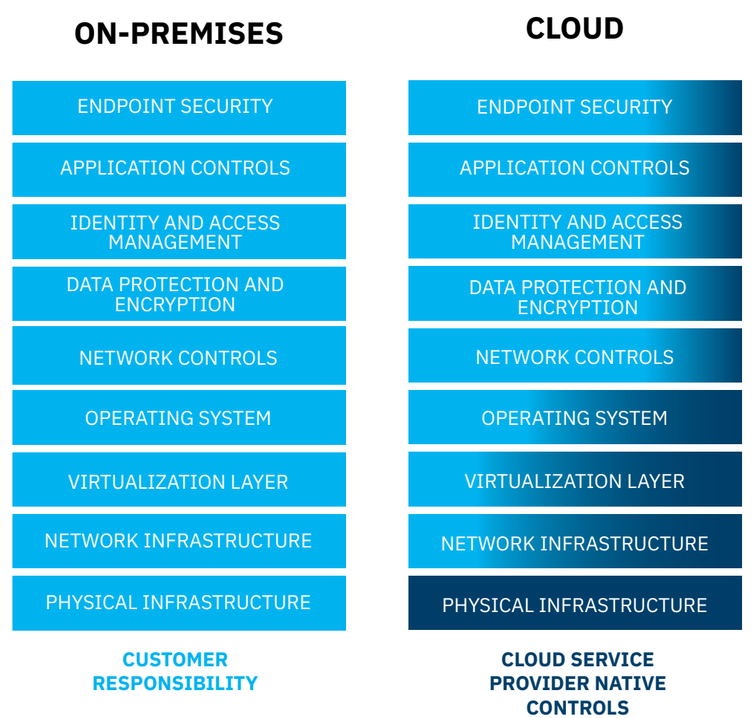
Everyone seems to have gotten the memo about the cloud. To achieve performance, reliability and cost-savings goals, enterprises are increasingly embracing the cloud for both software reliability and scalability. The move to the cloud alleviates the need to physically maintain servers and the network infrastructure surrounding them; however, it's important to note that with cloud environments, organizations won't be alleviated when it comes to security, rather they will need to continue to carry the responsibility of securing data and workloads both in the cloud and on-premises.

Even though a cloud service provider (CSP) may provide some level of security, hybrid cloud architecture can be complex and requires continuous management from enterprise security teams to ensure that data and workloads are kept safe and secure.

With increasing compliance requirements such as General Data Protection Regulation (GDPR), the growing number of advanced threats and the need to move at the speed of business, security teams need to provide a comprehensive security framework to protect cloud and on-premises environments.

An essential step for a hybrid cloud security framework is to put security first. By enabling secure-by-design and integrating security controls into DevOps processes and cloud migration initiatives from the beginning, security can accelerate your business by not having to use valuable time and resources on reactive responses to threats and compliance issues.

The shift toward cloud and hybrid cloud environments has changed the mix of responsibilities that administrators of on-premises and cloud systems must address.



The IBM Security approach to securing your hybrid cloud

While offering certain protections from zero-day exploits and insider attacks, the cloud alone does not provide the enterprise security controls you'd expect and need for a business leveraging the cloud. In one 2017 study, 42 percent of organizations reported an attack in their hybrid cloud environments.[1] Another recent study observed that more than half of organizations surveyed, including many in the healthcare sector, had easily-remediable network vulnerabilities from using outdated browsers and legacy or unpatched operating systems.[2]

Much like on-premises IT environments, a hybrid cloud environment has similar security concerns and requirements such as protecting data, securing systems and ensuring regulatory compliance. However, a hybrid cloud environment carries an additional challenge, which is to apply the same speed and attention to securing data on both cloud as well as on-premises environments.

The IBM® Security approach to securing hybrid cloud environments addresses the critical needs of enterprise-wide security with a focus to protect data, enhance productivity, and ensure compliance.

Protect Data

Data is one of the most valuable and critical assets entrusted to or created by a company. In a hybrid cloud environment, data lives both on-premises and in the cloud as well as moves between where it's stored and the endpoints and devices where it's accessed. For a hybrid cloud environment, you need to bring your own security controls to complement the security of your cloud service provider to keep your data safe and secure.

Enhance Productivity

For any business, productive time and resources are essential to maintaining success. Therefore, time and resources used in attending to preventable security incidents may not be the most efficient path for continued business growth. However, by working closely with DevOps to provide a security framework and the necessary tools to incorporate security controls from the beginning, productivity is not lost in having to go back and incorporate it later.

Ensure Compliance

Achieving and maintaining compliance can be complex, especially in a hybrid cloud environment where there are unique compliance challenges across heterogeneous environments. Therefore, in order to meet and maintain compliance in a hybrid cloud environment, it is essential to have visibility and reporting into both the cloud and on-premises systems.

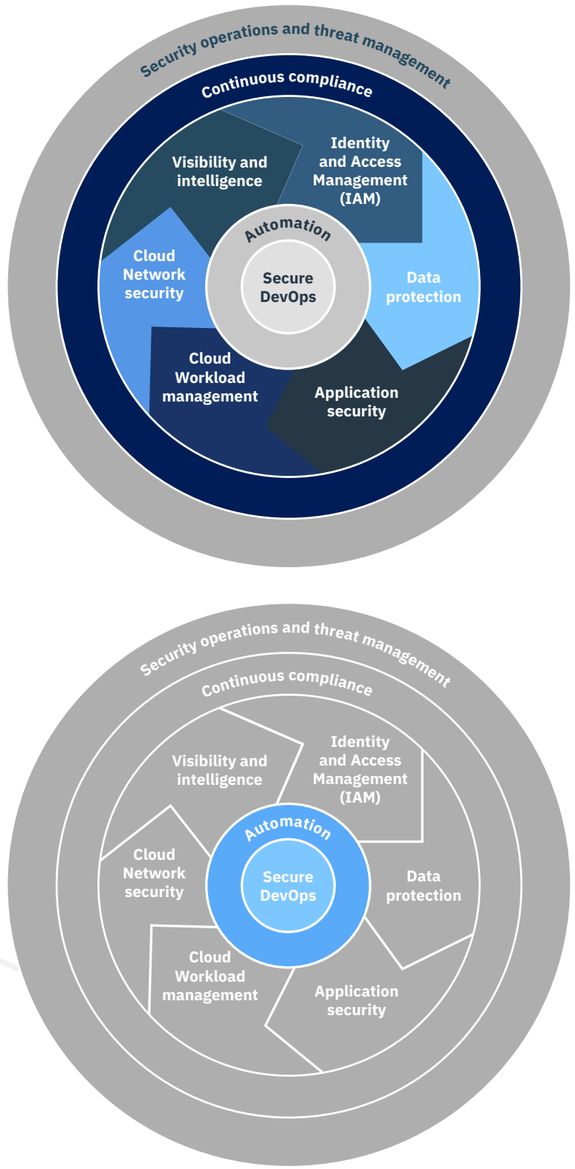
1 "Zero-Day Exploits Are Most Prevalent Attack in Hybrid Cloud Environments, according to Capsule8-Sponsored Study," *Capsule8*, February 28, 2018.

2 Heather Landi, "Report: 15 Percent of Healthcare Organizations Running Outdated Operating Systems," *Healthcare Informatics*, June 8, 2017.

IBM Security: Areas of focus and capabilities

For a more detailed look at what's needed to make sure you're safe and secure on both your cloud and on-premises environments, the wheel graphic organizes the 10 areas of focus and capabilities for establishing a comprehensive security framework.

Click the wheel to learn more →



Secure DevOps

It all starts with a focus on Secure DevOps. Line-of-business leaders apply pressure on DevOps teams to deliver value to cloud initiatives at speed and scale. These teams need to be supported by being given security policies and architectures to develop applications and workloads on the cloud with security in mind from the beginning, not as an afterthought.

Automation

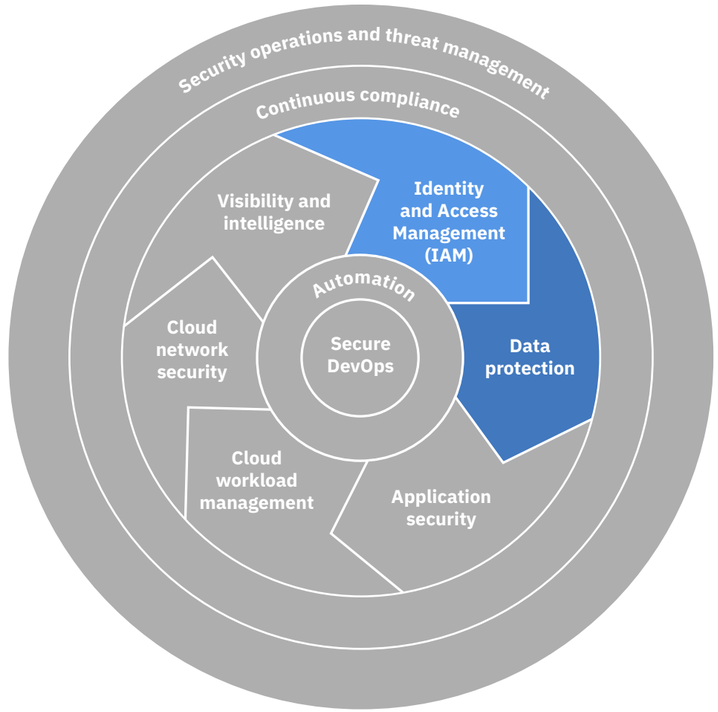
By integrating automated provisioning of security policies, security technologies and vulnerability scanning in your hybrid cloud environments and workloads, you are able to save valuable time and resources otherwise spent on reactive responses to threats.

Identity and Access Management (IAM)

Hybrid cloud architectures inherently multiply the places where an attacker might seek valuable data. With security software that can span multiple systems, administrators can apply uniform identity and access policies, view access logs and other records while delivering a seamless user experience.

Data protection

In a hybrid cloud environment, security controls must be consistent across multiple systems so that data is protected against internal and external threats. Protect your data inside or outside your on-premises perimeter—including across multiple clouds.



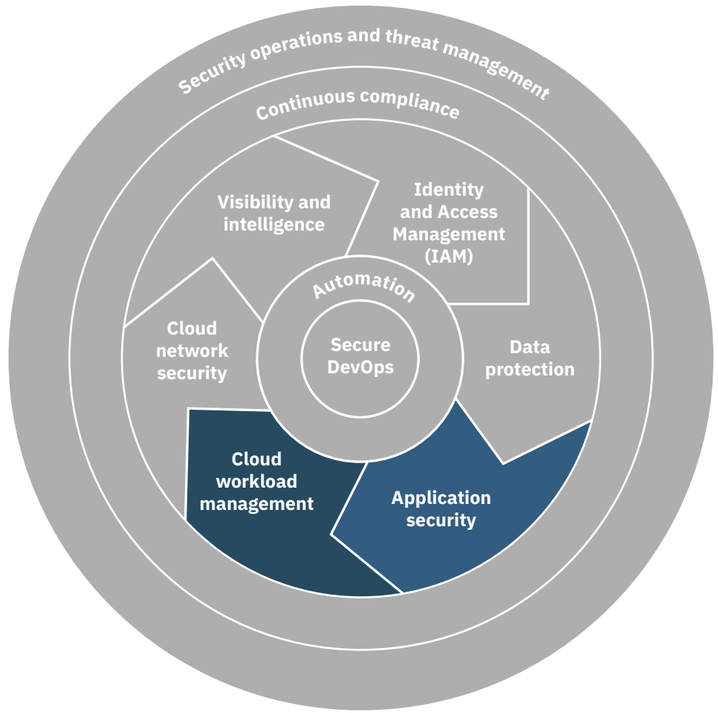
Click the wheel to learn more

Application security

The future of applications is cloud-based. To maximize your enterprise-security value, developers need tools that automatically address application security risk and intelligently report vulnerabilities in code before it is put into production. For open-source components, cloud security depends on automated security testing that reviews adopted code.

Cloud workload management

Administrators'' time to deal with security issues in a hybrid environment is limited. With constrained resources, they must prioritize. Security software and service solutions that leverage automation to efficiently scan for vulnerabilities and apply policies and security fixes across hybrid cloud ecosystems are ultimately a necessity at scale.



Click the wheel to learn more

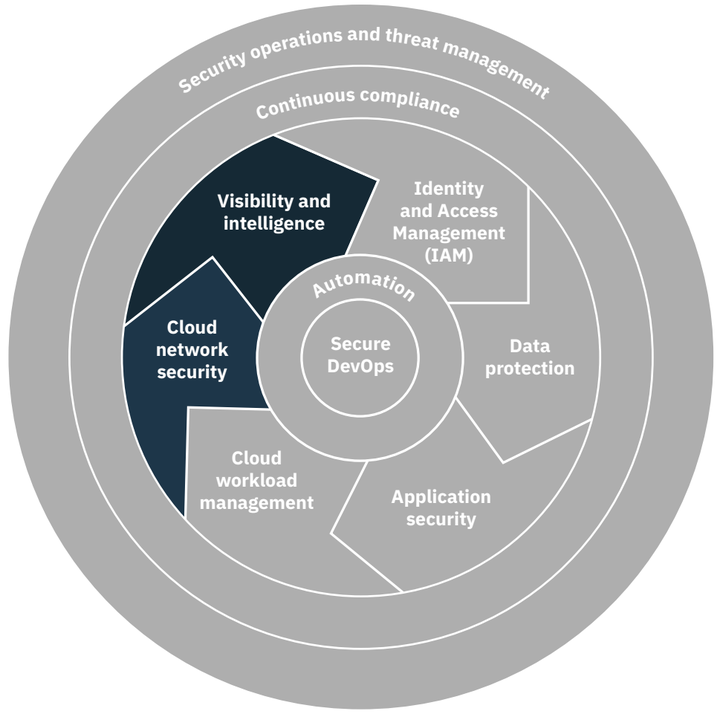
Attackers rely on the inattention and time lag that can plague security administrators. Effectively securing hybrid cloud systems requires an emphasis on consolidated, up-to-date views of logs and other security data so IT staffers and security analysts can quickly spot anomalies and react to them with a consistent approach for each CSP.

Visibility and intelligence

Hybrid cloud environments can be diverse and complex. Therefore, it is essential to have visibility into threats and vulnerabilities within your organization, so that any security incidents are responded to quickly and accurately.

Cloud network security

Because cloud systems may be challenging, securing them requires flexibility, speed, automation, and alignment with on-premises systems. An ideal system should ensure that applications work securely across multiple CSPs' cloud environments and on-premises systems.



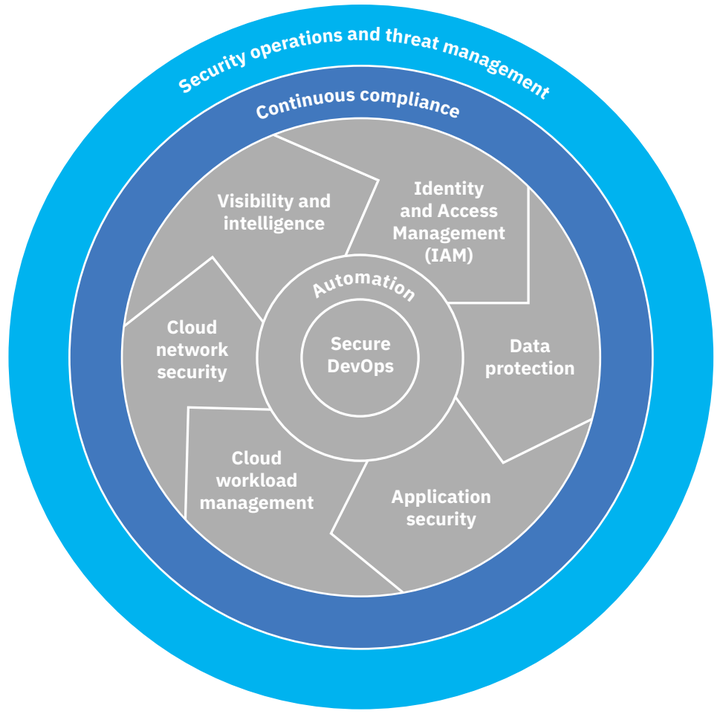
Click the wheel to learn more

Security operations and threat management

To be effective with security operations and threat management, it is essential to have central policy management and visibility across both your on-premises and cloud workloads, enabled through a single unified security framework. Your security operations center (SOC) and team will need to continue to detect known and unknown threats, go beyond individual alerts to identify and prioritize potential incidents, and apply AI to accelerate investigation processes.

Continuous compliance

Achieving and maintaining continuous compliance across regulatory and industry mandates is a tough task for most organizations—and especially so for DevOps teams. Your business can get ahead of compliance with AI-based software to stay on top of regulatory trends, dynamic monitoring tools to track compliance risk across your organizations, automation to streamline auditing and reporting, and services to deliver invaluable expertise and insight.



Click the wheel to learn more

Hybrid cloud security solutions from IBM

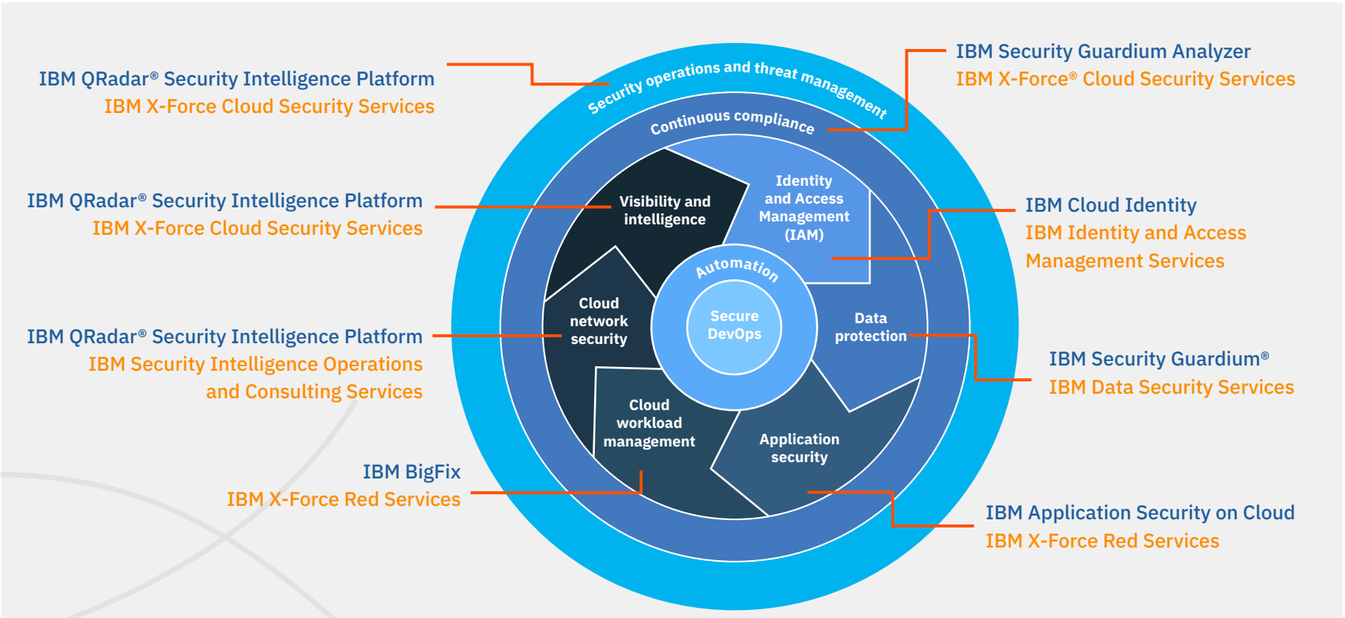
No matter where you are on the cloud spectrum, products and services from IBM can help address all areas of focus and capabilities for a comprehensive hybrid cloud security framework.

Leading IBM Security products

- IBM Security Guardium®
- IBM Security Guardium Analyzer
- IBM Application Security on Cloud
- IBM Cloud Identity
- IBM QRadar® Security Intelligence Platform
- IBM BigFix

Expert IBM Security services

- IBM X-Force® Cloud Security Services
- IBM Data Security Services
- IBM Identity and Access Management Services
- IBM X-Force Red Services
- IBM Security Intelligence Operations and Consulting Services



LEGEND
IBM Security product IBM Security service

For more information

To learn more about securing the hybrid cloud, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security software and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than one trillion security events per month in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2019

54015454-USEN-01