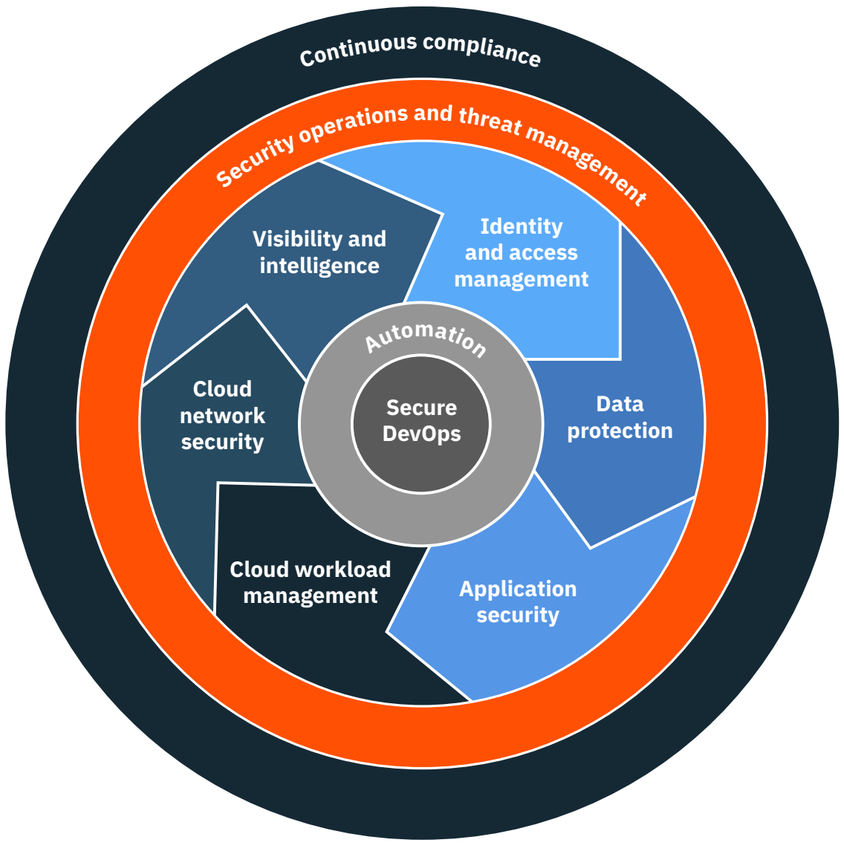
# Secure your hybrid cloud environments

## Protect your distributed mission-critical data and tap into expert assistance




Click the wheel to learn more

## HIGHLIGHTS

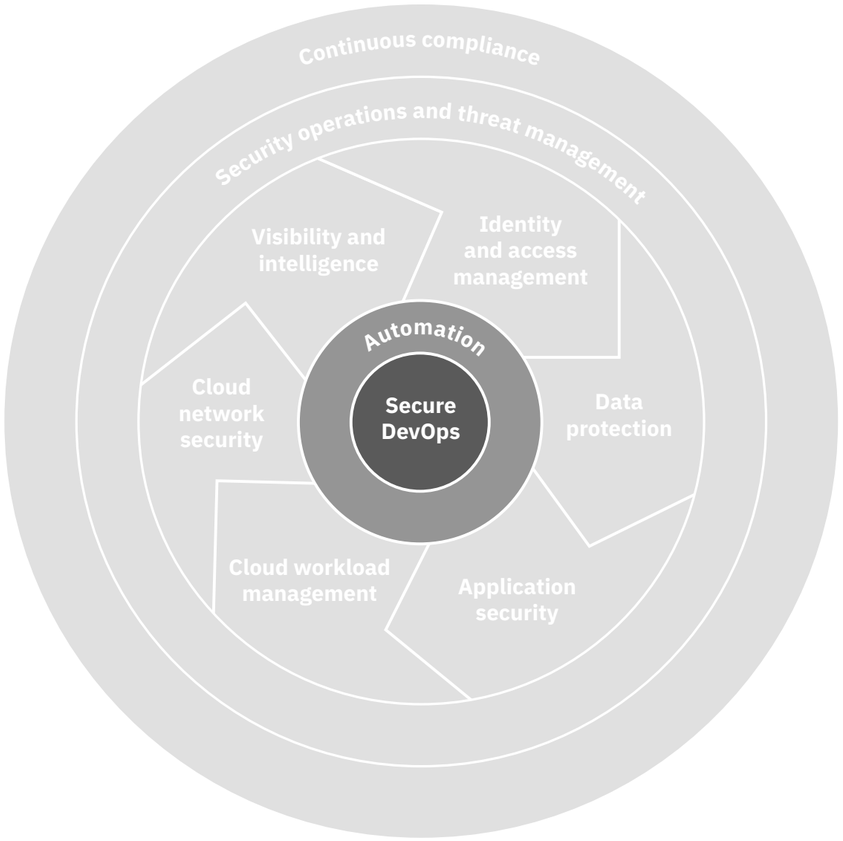
- **Secure DevOps:** Enable security policies and reference architectures to develop applications and projects with security in mind, and not as an afterthought.
- **Automation:** Integrate the automated provisioning of security policies and technologies for hybrid cloud.
- **Data Protection:** Protect data inside or outside your on-premises perimeter—including across multiple clouds.
- **Application Security:** Help ensure application security from test to deployment.
- **Identity and Access Management (IAM):** Extend IAM policies from on-premises to the cloud.
- **Visibility and Intelligence:** Gain visibility and intelligence to detect and stop advanced threats.
- **Cloud Workload Management:** Secure your workloads to protect against risks with endpoints, policies and more.
- **Cloud Network Security:** Protect your company against debilitating attacks with network security for the cloud.
- **Security Operations and Threat Management:** Detect and defend against threats with visibility across log events and network data from endpoints and apps.
- **Continuous Compliance:** Assess your organization's controls framework, and identify new regulations and continuously evolve your controls to stay compliant.

As business demands require accelerated delivery of new applications and services, companies both big and small are increasingly moving to the cloud. As a result, IT teams must now oversee and manage resources in multi- and hybrid-cloud environments, including Amazon Web Services (AWS), Microsoft Azure and IBM® Cloud™.

While cloud environments may offer basic security features, security and compliance for these environments continue to remain a responsibility of the company's IT department. Cloud service providers (CSPs) offer widely-varying levels of basic security, however this basic security may fall short of your requirements and may lead to vulnerabilities that can be exploited. Additionally, effectively securing hybrid IT environments is complex and requires specialized skills that may be hard to find or costly to adopt.

IBM Security offers a portfolio of products and services that can protect your data by complementing your own security with the security provided by your CSP, enhance productivity by establishing a security framework and tools to incorporate security from the beginning with your DevOps team, and ensure you're compliant by delivering visibility and reporting into your cloud and on-premises environments.

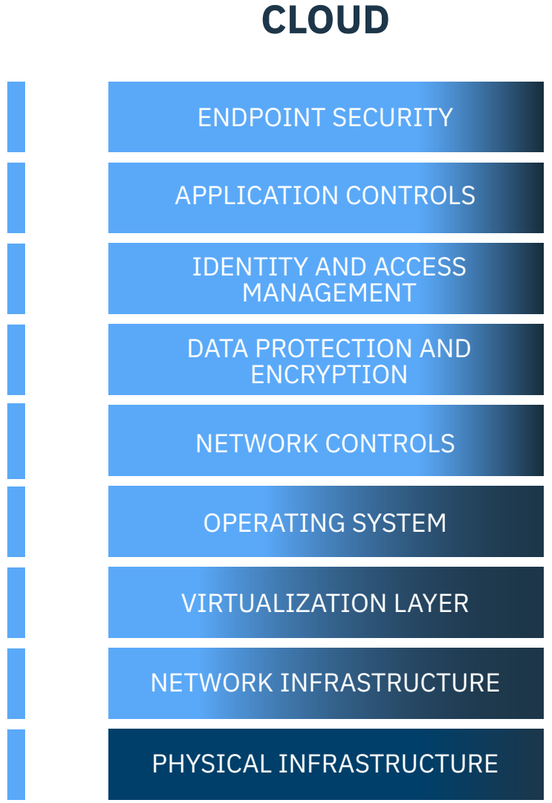
# When moving to cloud, put security first




Click the wheel to learn more

Hybrid cloud architectures can deliver the best of both worlds when it comes to cloud adoption. While on-premises resources may still be a necessity, a hybrid cloud approach allows enterprises to leverage both public and private cloud architectures to provide flexibility[1] and meet the needs of the business.

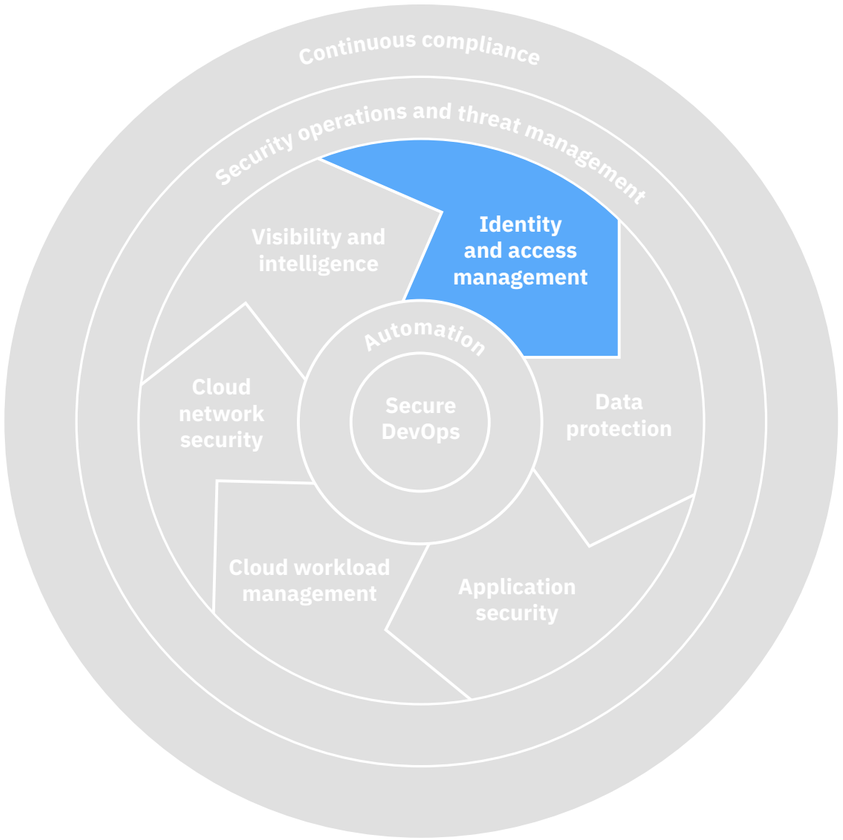
A critical step for any migration to the cloud or when building native cloud apps is to put security first by incorporating security controls in the design and development phase. Building security into cloud initiatives and working closely with DevOps teams, businesses can save crucial time and resources that would otherwise be spent on reactively addressing potential vulnerabilities and data breaches when they occur. Additionally, it is important to remember with a hybrid cloud environment that securing the hybrid cloud is a shared responsibility between the CSP and the company's security team. In hybrid cloud environments, your security controls and people continue to play a critical role in securing data and workloads in the cloud as well as on premises




*In cloud environments, security is a shared responsibility between your organization and the CSP.*

1 Nathan Crawford, "Comparing public, private and hybrid clouds," *RCR Wireless,* April 20, 2018.

# Use strong IAM to keep bad actors out




Click the wheel to learn more

A recent report found that 26 percent of companies had experienced attacks related to an insider's misuse of a privileged account.[1] Of course, whether threats originate from within or outside your network, the importance of strong IAM cannot be overstated. To protect critical assets wherever they are, IT professionals need the ability to bridge IAM from on-premises environments to cloud-based resources and endpoints that may extend beyond the reach of the traditional network perimeter.

IBM Cloud Identity, an identity-as-a-service (IDaaS) solution, enables you to extend local IAM policies to cloud-based applications, and to rapidly deploy new cloud applications. Additionally, it provides the ability to offer single sign-on (SSO) access directly from an application, so users can quickly access the applications they need once they successfully log in to the network.

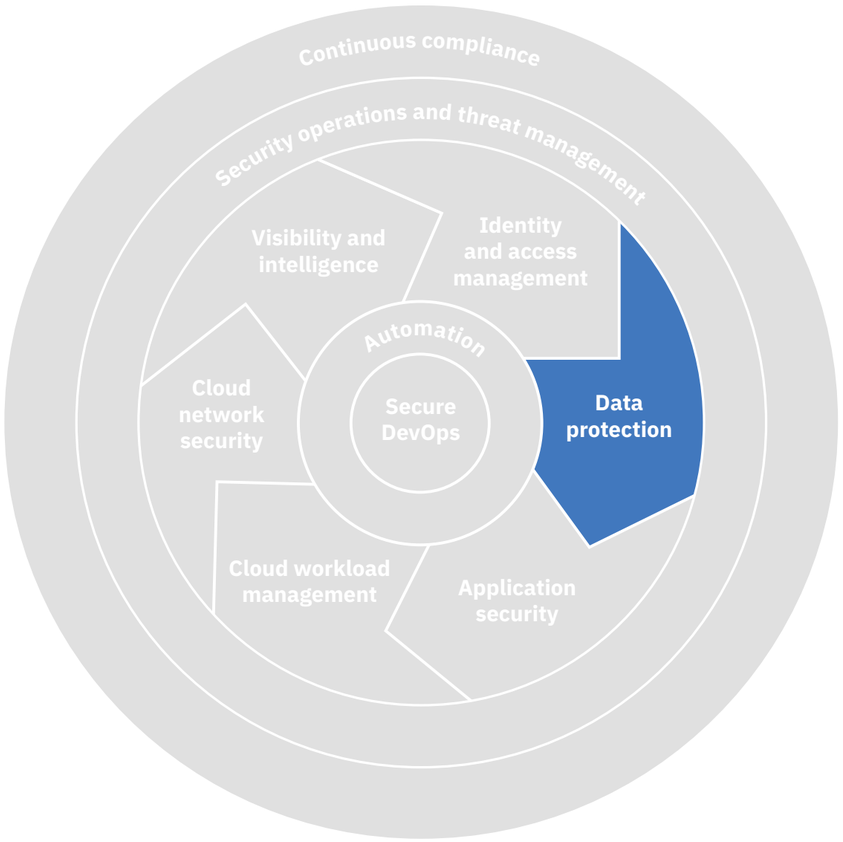
In addition to the IBM Cloud Identity software solution, IBM Security offers IBM Identity and Access Management Services where identity and access management security specialists work with you to design solutions tailored to your business and security objectives across your entire enterprise, including user provisioning, enterprise single sign-on, multifactor authentication and user activity compliance.

**More than**
**2 billion records**

***were unintentionally exposed in 2017 due to misconfigured cloud servers and networked backup incidents alone.[2]***

1 "Zero-Day Exploits Are Most Prevalent Attack in Hybrid Cloud Environments, according to Capsule8-Sponsored Study" Capsule8, February 28, 2018.
2 "IBM X-Force Threat Intelligence Index 2018," ***IBM Corp.,*** March 2018.

# Protect data across your hybrid cloud environment




Click the wheel to learn more

A lack of robust security controls in any IT environment can leave an organization with exposed data, declining productivity, and compliance risks. In a hybrid cloud environment, security controls must be consistent across multiple systems and data centers so that data is protected against internal and external threats.

IBM Security Guardium® gives you intelligent visibility into your entire data protection journey and granular access controls to sensitive data elements, whether they are stored on premises or in the cloud. You can discover and classify sensitive data, uncover usage patterns and assess compliance risks.

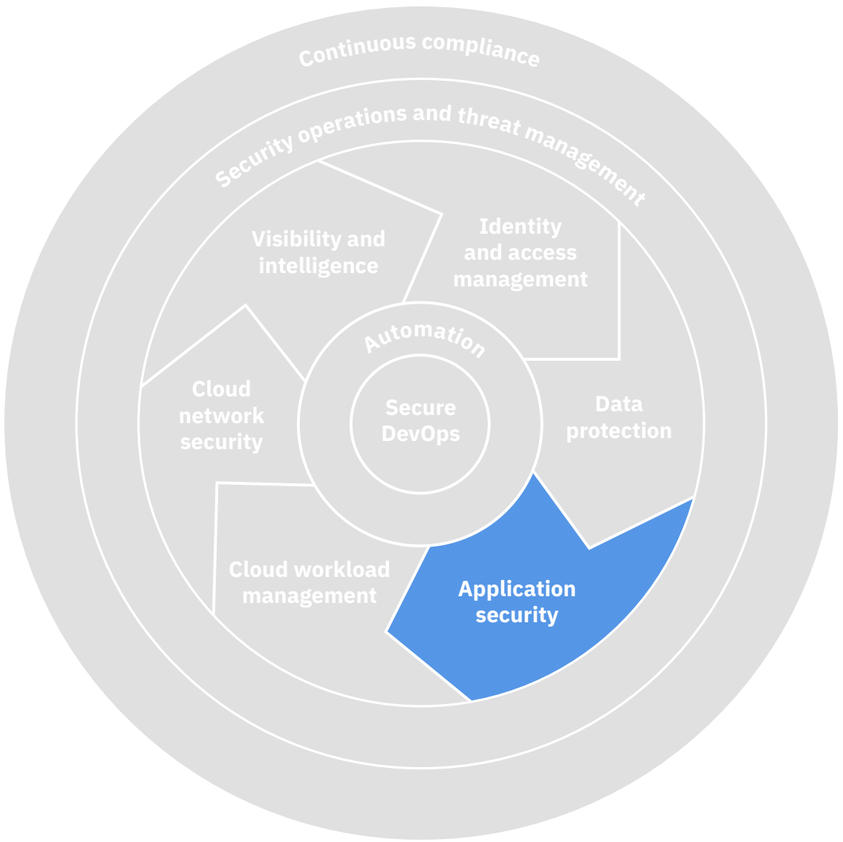
IBM Data Security Services can help you incorporate a risk-balanced strategy with leading data protection technology to safeguard your organization's critical data. With both consulting and integration services, data security specialists can help you optimize control over data using market-leading loss prevention and encryption technology.

**USD148**

***Average cost per stolen record in a data breach.[1]***

1 "2018 Cost of a Data Breach Study: Global Overview," ***Ponemon Institute,*** July 2018.

# Secure cloud-based applications from development through deployment



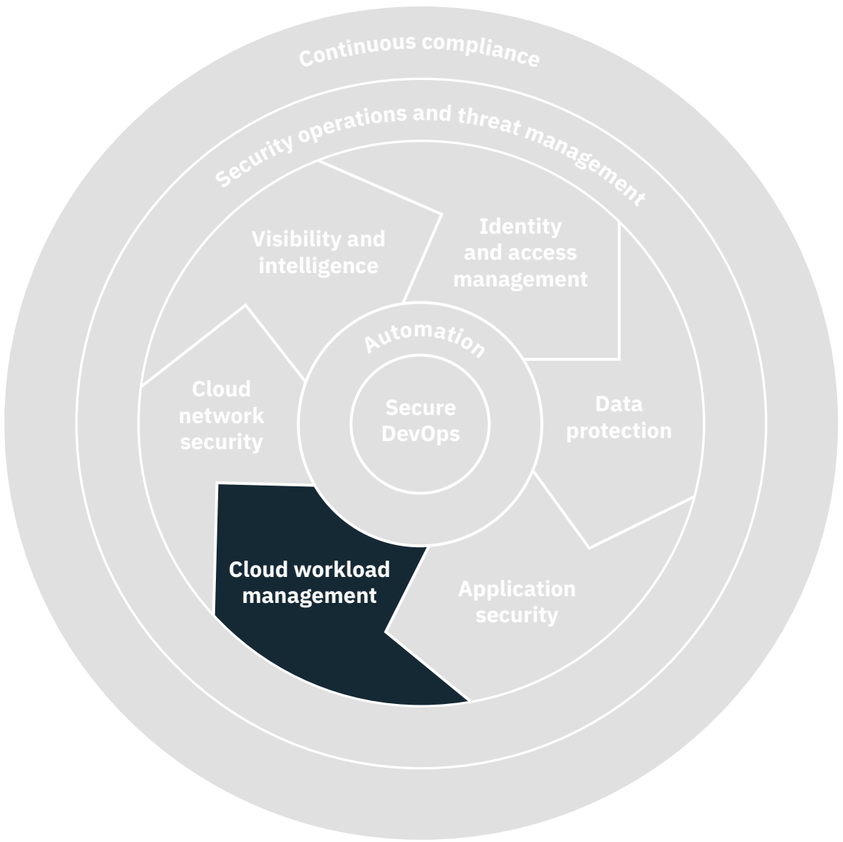

Click the wheel to learn more

When building applications on the cloud, DevOps teams can accelerate development testing and the delivery of applications. However, maintaining security and compliance of critical assets outside the confines of the traditional network infrastructure can be challenging.

IBM Application Security on Cloud is a powerful solution that allows developers and IT managers to perform static, dynamic and mobile application security testing in the cloud. This can accelerate migration, deployment and scaling by making applications cloud-ready while detecting and fixing vulnerabilities in real time.

IBM X-Force Red Services offers penetration testing and vulnerability management programs to help security leaders identify and remediate security flaws covering their applications as well as their entire digital and physical ecosystem.

# Remove the complexity of managing hybrid cloud workloads




Click the wheel to learn more

The move to the cloud can accelerate your workloads from development to deployment. However, for cloud-based workloads, management and maintenance can be challenging. IBM Security can help you manage workloads on the cloud so they continues to stay reliable and secure.

With IBM BigFix®, IT departments can cut operational costs, compress endpoint management cycles and enforce compliance in real time.

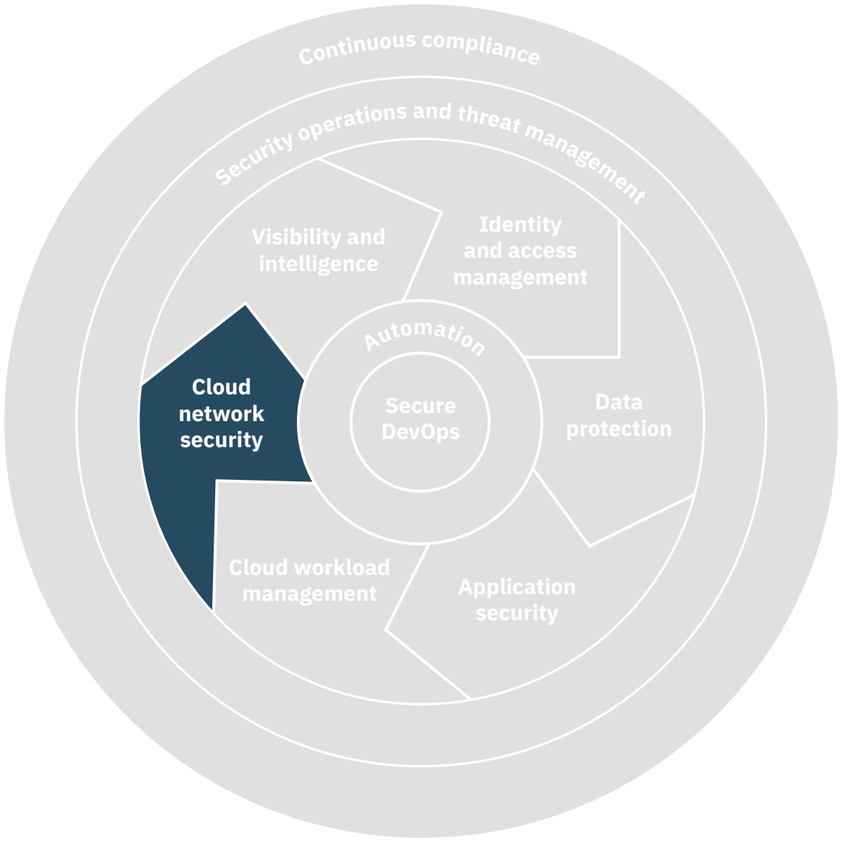
IBM X-Force Cloud Security Services helps to close critical security gaps by delivering advisory and managed security in your cloud environments, including AWS, Azure and IBM Cloud, as well as on- premises clouds, helping you gain visibility and control of all aspects of your hybrid cloud security.

**42%**

***of organizations with hybrid cloud environments have experienced a security attack in 2017.[1]***

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

# Strengthen security in your networks




Click the wheel to learn more

It takes organizations an average of 197 days from the time a data breach occurs until it can be identified.[1] IBM QRadar® Security Intelligence Platform can help shorten this critical lag by empowering security analysts to detect anomalies, uncover advanced threats and remove false positives in real time. The solution centrally collects and analyzes log and network flow data throughout even the most highly distributed environments to provide actionable insights into threats.

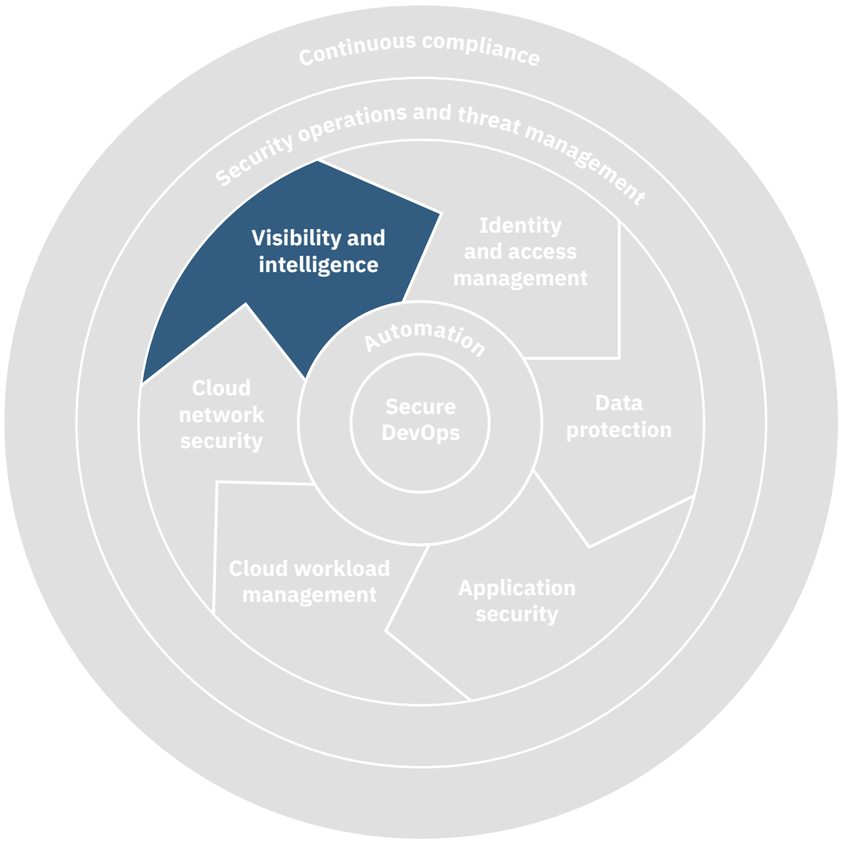
IBM Security Intelligence Operations and Consulting Services can help your organization develop more maturity in intelligence-driven operations across all your network environments. Security intelligence operations specialists can assess your security capabilities and maturity against best practices in security. If you want to create or improve your security operations center, IBM will plan, design and build it out.

**61%**

***of organizations store personal information in public cloud services.[2]***

1 "2018 Cost of a Data Breach Study: Global Overview," *Ponemon Institute,* July 2018.
2 "Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security," *McAfee,* April 2018.

# Filter out the noise with security information and event management




Click the wheel to learn more

Security teams are inundated with notifications and event data on potential security incidents. Filtering out the noise to avoid false positives can be challenging without a way to quickly identify and tag credible incidents. IBM Security solutions leverage artificial intelligence to label suspicious behavior, obtain a precise analysis of threat data, and gain comprehensive real-time visibility into user activities across both on-premises and cloud environments.

IBM QRadar Security Intelligence Platform is a powerful security intelligence solution that can help uncover hard-to-find advanced threats, detect anomalies and remove false positives in hybrid-cloud IT environments.

With IBM X-Force Cloud Security Services, the X-Force Team can identity the false positives that can sap the effectiveness of your Security Operations Center (SOC). Tests for gaps and weaknesses with precision and provides expert remediation, beginning with your most critical vulnerabilities first.

***By some estimates, ransomware payments doubled in 2017 to at least USD 2 billion, while global losses from compromised email scams are expected to top USD 9 billion in 2018.[1]***

1 Selena Larson, "The hacks that left us exposed in 2017," *CNN Money,* December 20, 2017.

# Extend your security operations and threat management to the cloud

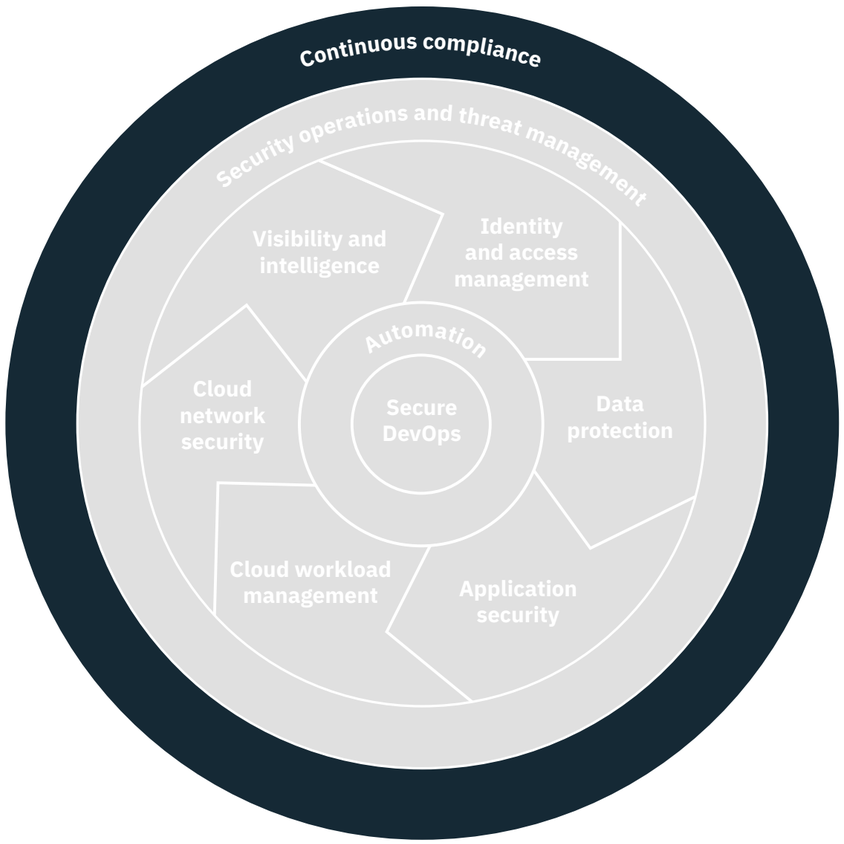

Click the wheel to learn more

After addressing the core capabilities needed to secure a hybrid cloud environment, they need to be supported by security operations and threat management processes. IBM Security can extend your security controls and monitoring to help prevent, detect and respond to threats in your cloud environment.

IBM QRadar Security Intelligence Platform can help you gain actionable insights, quickly identify the top threats and reduce the total alert volume. Additionally, QRadar can help you gain closed-loop feedback to continuously improve detection, and use the time savings from automated security intelligence to proactively hunt threats and automate containment processes.

IBM X-Force Cloud Security Services can help you automate provisioning by applying a base security policy in minutes. Centralize security protections and visibility across cloud and on-premise environments and simplify security management and monitoring with a single provider and portal.

# Ensure continuous compliance in your hybrid cloud environments




Click the wheel to learn more

Achieving and maintaining compliance across regulatory and industry mandates is a tough task for most organizations—and especially so for DevOps teams. In a hybrid cloud environment, compliance grows more complex as you expand your business to multiple clouds, making it more difficult to track, achieve, and maintain compliance.

IBM Security Guardium Analyzer can help you efficiently find regulated data, understand data and database exposures, and act to address issues and minimize risk. It also identifies risk associated with personal and sensitive personal data that falls under privacy regulations and mandates. By streamlining compliance activities it helps compliance managers, data managers and IT managers get the information they need, at the right level of detail, to collaborate efficiently.

IBM X-Force Cloud Security Services can help give you visibility and enforce policies across multiple clouds and on-premises environments to enable continuous compliance. IBM cloud security specialists provide the strategy needed to enable continuous compliance for your business.

# Why IBM?

Managing hybrid cloud security can be complex, but you don’t have to go it alone. IBM is a global cloud provider with innovative cross-cloud environment security products, a security services specialization and managed offerings. IBM offers leading hybrid cloud security technology. Artificial intelligence capabilities delivered through IBM Watson™ can augment your security analysts’ skills by providing highly-scalable and detailed threat analytics.

## For more information

To learn more about IBM products and services for hybrid cloud security, 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 products 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 one trillion security events per month in more than 130 countries, and holds more than 3,000 security patents.



IBM Security

New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2018



54022054-USEN-02