Address six essential concerns of cloud security to build your business

From key questions to next steps, necessary considerations for enabling secure cloud deployments
Building a secure cloud infrastructure

In a recent survey, nearly half of IT respondents said concerns over security create critical roadblocks to considering a move to public or hybrid cloud infrastructure. But while security in the cloud should be a priority, it does not have to be an inhibitor. In fact, while an essential concern, the need for security has not stopped many organizations from proceeding with cloud deployments.

For many, cloud deployments are no longer just a priority; they are a mandate driven by the business—but a mandate where security often is not initially considered. With mounting pressure to tap into cloud benefits, migrations often proceed with little or no consideration of how data is protected or threats are mitigated. The move to cloud, on the other hand, can actually provide even higher levels of protection than the organization has in its on-premises deployments.

When considering cloud security, organizations often believe they are strong in a few areas but lacking in others. And many organizations face a cloud security skills gap. They also face challenges around providing cloud resources as quickly as the business demands. Nevertheless, security is a shared responsibility between you and your cloud provider—whether that means a third-party service in a public cloud, your own IT department’s cloud experts for a private cloud, or a combination of teams for a public or hybrid cloud.

No matter where your organization stands in the journey to cloud, or which areas you may need to strengthen, IBM can provide you with the technology, services and guidance to help you securely deliver cloud-based applications.

This white paper introduces the six key areas that organizations should consider in securing their cloud infrastructure and the capabilities that are available across each:

1. Identity and access management
2. Cloud network security
3. Protection for data in the cloud
4. Application security
5. Visibility and intelligence
6. Workload security management

Robert Mahowald, Randy Perry, Brad Casemore and Ben McGrath, *Cloud Going Mainstream: All Are Trying, Some Are Benefiting; Few Are Maximizing Value,* IDC, September 2016.
For a secure cloud infrastructure, examine six areas of concern

1. Managing identity and access
   - What is being done to ensure that employees who leave your company are deprovisioned from accessing your cloud applications?
   - Are you protecting the infrastructure-as-a-service (IaaS) cloud platform management console appropriately?
   - How are you regularly assuring that you verify the identities of all users accessing your data and applications?
   - Who is using unsanctioned software-as-a-service (SaaS) applications? What is the risk?
   - What steps have been taken to enforce access policies across disparate directories and access methods?
   - How are access compliance policies applied across your IT infrastructure?

2. Analyzing network management
   - What tools are in place to automatically detect and block exploits, suspicious behavior and other unwanted activities in cloud deployments?
   - What measures have been taken to prevent and respond to distributed-denial-of-service (DDoS) attacks?
   - Do you have a virtual private network (VPN) connecting workloads on diverse identity-as-a-service (IaaS) platforms?
   - Do you monitor application programming interface (API)-based communications to and from your cloud workloads?

3. Protecting cloud networks
   - Is sensitive data shared inappropriately?
   - Are you encrypting storage in IaaS, platform-as-a-service (PaaS) and database-as-a-service (DBaaS) workloads?
   - Is personally identifiable information (PII) masked?
   - Do you monitor cloud workload configuration files?
   - How are structured and unstructured data monitored?
   - What steps have you taken to discover and classify data?
   - How are you ensuring compliance for critical data that's stored in the cloud?
   - How is audit data being created and stored to support compliance mandates?
   - Have you assessed security controls mandated by industry and government regulations?
   - Could a managed security service provider help expand your operations?

4. Uncovering vulnerable cloud applications
   - Do you have tools in place to find vulnerabilities in applications developed for cloud and mobile users?
   - How often are you analyzing applications deployed in the cloud for vulnerability to exploits?
   - How are you gaining access to recommendations for remediating vulnerabilities in cloud and on-premises applications?

5. Gaining visibility into activity and threats
   - How are you obtaining visibility of your security posture across cloud and on-premises infrastructures?
   - What tools are in place to trace suspicious login activities to external cloud resources such as Salesforce?
   - Are you seeing which new resources are being deployed?
   - Are you monitoring system calls and processes?
   - What steps have been taken to monitor potential insider threats?

6. Managing cloud workload security
   - How do you ensure security in your development operations (DevOps)?
   - What solutions are being used to prioritize and patch your most important asset vulnerabilities?
   - How are unplanned and unauthorized changes to workloads' configuration files being detected?
Get identity and access under control

The first line of defense in the cloud against data compromise, theft or cyber attack is to control user access to resources. Understanding who is accessing resources and how they are doing it is key in avoiding both security and compliance pitfalls. Whether organizations are building their own cloud workloads, leveraging commercial cloud solutions such as Box and Salesforce, or using a public cloud service, identity and access management (IAM) must be a top priority.

But IAM in the cloud does not have to be a reinvention of your security approach. In fact, the strategies for managing access to cloud deployments are similar to managing access in on-premises deployments, from provisioning and password management to identity governance and privileged user management.

What is different in the cloud is often the diversity of directories and access methods. An effective strategy for cloud IAM must take those diversities into account while enabling organizations to enforce enterprise-wide policies.

Solutions for identity and access management

IBM is an industry leader in IAM, offering solutions that include:

- **IBM® Cloud Identity Service**, a scalable IAM solution that is fully integrated, from the data center to the software running in the cloud
- **IBM Security Access Manager**, helping simplify user access management for employees and consumers
- **IBM Security Identity Governance and Intelligence**, providing management across the user lifecycle

60% of IT professionals say strong authentication is the most important capability for controlling access in the cloud.

Read what the analysts say about IBM leadership in IAM.

Learn why IBM Cloud Identity Service was named a market leader by analyst firm Ovum.

1 Based on an IBM-commissioned survey conducted by TechValidate, March 2017.
Network security is fundamental to any IT security deployment, whether in the cloud or on-premises. Poorly managed networks can create vulnerabilities that attackers will try to exploit.

The key approach is to focus not only on protecting the network perimeter, but also on stopping threats from moving between workloads. Attackers are adept at overtaking a workload and using it to carry an attack to another point inside your cloud infrastructure.

Any cloud deployments can create new attack surfaces, based on anomalies in technologies or user behavior, threats or breach attempts. Effective network management strategies should acknowledge new attack surfaces and manage them appropriately.

The rapidly expanding universe of Internet of Things (IoT) devices, from cash registers to security cameras, shows how new cloud-based endpoints can mean new vulnerabilities. Even so, only 36 percent of organizations are concerned about protecting sensitive data generated by IoT devices. Strong monitoring and threat protection tools are essential, no matter what part of your infrastructure is at risk.

Solutions for network management

IBM offers solutions that enable effective network security measures for cloud deployments. They include:

- **Managed security services for cloud workloads**, helping secure assets on workloads with capabilities including firewall management, and intrusion detection and prevention deployed on commercial clouds including IBM Cloud, Amazon Web Services and Microsoft Azure
- **IBM vulnerability management service**, combining managed scanning services with expert workflow and case management to protect your network infrastructure
- **IBM managed web defense**, helping safeguard assets from DDoS attacks and massive outages by helping you plan for, respond to and correlate data during an attack

78% of survey respondents say traditional network security solutions either don’t work or have limited functionality in the cloud.²

Learn the latest findings on the impact of vulnerabilities on organizations around the world.

Safeguard your critical cloud-based data

Organizations worldwide recognize the importance of protecting the repositories of mission-critical data that reside in cloud deployments. In fact, Forrester has reported that more than half of all IT spending in cloud security soon will go to protecting data in the cloud.¹

A strategy for data protection in the cloud, however, has essentially the same elements as the strategies most organizations use for their on-premises deployments. Some classes of data should be encrypted, while access to other classes of data should be monitored. Databases should be regularly analyzed for vulnerabilities, and solutions for encryption, access monitoring, and vulnerability analysis should provide security for new data hosts in the cloud.

Solutions for data protection

IBM offers tools to support your data protection efforts in both on-premises and cloud deployments. They include:

- **IBM Security Guardium®** data protection, helping ensure the security, privacy and integrity of critical data across a full range of environments, including databases, big data, cloud, file systems and more
- **IBM Multi-Cloud Data Encryption** for data stored in files and folders, along with key lifecycle management, which centralizes and automates the encryption key management process and provides encryption key storage
- **Penetration Testing Services from IBM X-Force® Red,** providing analytics that helps transform massive quantities of vulnerability reports into action plans

---

Uncover vulnerable cloud-based applications

Whether you're using commercial applications to access data in the cloud or building and deploying your own applications for the cloud, vulnerabilities in the software code can open the door to security breaches. Attackers can and will exploit those vulnerabilities to access mission-critical data in the cloud—just as they do for mobile or on-premises applications. But the complexity of cloud application deployments makes these vulnerabilities especially challenging to manage.

Effective application security requires regular security analysis and remediation of applications. In addition, cloud deployments often exploit the latest development tools, so application security tools must enable organizations to analyze a broad range of tools. The ability to develop secure applications, assess for vulnerabilities—and swiftly remediate them—is key.

Solutions for application security

IBM offers powerful solutions to enable secure application development and ongoing vulnerability assessments. They include:

- **IBM Application Security on Cloud**, helping secure web and mobile applications by detecting security vulnerabilities
- **IBM Security AppScan®,** helping minimize web application attacks and data breaches by automating testing of application security vulnerabilities
- **IBM hosted vulnerability management,** providing cloud-based services that scan your internal and external network infrastructure to identify and classify vulnerabilities and offer steps to remediate threats
- **Penetration Testing Services from IBM X-Force Red,** providing a single, interactive view into your asset vulnerabilities across your enterprise

[Watch a webinar to learn how to accelerate your security testing expertise.](#)
Gain visibility into activity and threats

End users who access web applications that have not been authorized by the IT department present an ongoing cloud security threat. It's not uncommon for their unauthorized activities to result in damaging vulnerabilities.

What's more, unauthorized access is difficult to manage because any cloud provider—whether yourself or a third party—naturally seeks to make applications easy to access and use. To guard your organization from the damage these activities can cause, it's necessary to have tools that can help you understand where employees are going in the cloud, where traffic to outside sites is originating, and where that traffic is going.

An effective cloud security strategy provides visibility to all end users' access to cloud solutions, as this helps enforce access policies. Your strategy should incorporate tools for 24x7 monitoring and intelligence and event correlation and alerting.

Solutions for visibility and intelligence

IBM Security solutions deliver the visibility and intelligence organizations need to thwart security threats brought on by the cloud. They include:

- **IBM QRadar® SIEM**, consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network
- **IBM QRadar on Cloud**, providing IBM Security professionals to deploy and manage infrastructure, while your staff performs threat management tasks
- **IBM QRadar Advisor with Watson™**, helping identify and understand threats using cognitive capabilities that tap into unstructured and structured data and correlate this data with suspected offenses. Powered by IBM Watson for Cyber Security, the solution augments the intelligence security teams can access, enabling them to tap into vast amounts of security knowledge and obtain insights relevant to specific security incidents
- **IBM Security Information and Event Management (SIEM) Services** (including information lifecycle management, integrated service management and managed SIEM)

Learn more about how cognitive technology is revolutionizing cybersecurity.

---

Manage the security of cloud-based workloads

If enterprises struggle to manage workloads within and across IDaaS environments, it's even more of a challenge to ensure that their cloud workloads are secure. Administrators and developers must ensure that installation and setup occur with the right security and network configurations. Then they must carefully manage access to workloads and to various management consoles in order to maintain file and configuration integrity as well as intrusion prevention and endpoint protection. Today’s enterprise solutions create multiple management systems and require frequent manual intervention. As a result, organizations must either automate security hardening for a large number of workloads or risk falling victim to a breach.

Cloud workload security management solutions typically install a small agent on endpoints, connect these agents to a central service (available in security-as-a-service platforms or as on-premises products), then offer centralized management of key cloud workload security aspects.

Solutions for workload security

IBM offers a range of solutions to support your efforts to maintain security across your workloads. They include:

- **Managed security services for cloud workloads**, helping secure workloads deployed on commercial clouds, including IBM Cloud, Amazon Web Services and Microsoft Azure
- **Managed Protection Services for Servers**, offering protection using Trend Micro Deep Security, a market leader in protecting physical, virtual and cloud servers around the world
- **IBM BigFix®**, helping you gain visibility into the constantly changing endpoint landscape while bridging the gap between threat detection and remediation

51% of security professionals say security is their greatest concern in migrating workloads and/or IT services to the cloud.1

Learn how BigFix is transforming endpoint security.

1 Based on an IBM-commissioned survey conducted by TechValidate, March 2017.
**Next steps**

**What steps should you take next?**

With today’s explosion in security issues, and multiple options for addressing them, many enterprises struggle to understand how to achieve cloud security. IBM can help you along the path to an effective cloud security strategy with assessments in which IBM experts work with you to determine the tools and assets you have, collect your requirements and create a personalized cloud security roadmap.

### Cloud security strategy – Method summary

<table>
<thead>
<tr>
<th>Delivery phases</th>
<th>Key activities</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1: Project initiation</td>
<td>Initiate project and collect and review data</td>
<td>• Data collection checkpoint&lt;br&gt;• Project work plan</td>
</tr>
<tr>
<td></td>
<td>Prepare team and assets</td>
<td></td>
</tr>
<tr>
<td>Phase 2: Assess</td>
<td>Identify current IT security posture</td>
<td>• Current state assessment&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Catalog enterprise cloud usage</td>
<td></td>
</tr>
<tr>
<td>Phase 3: Analyze</td>
<td>Define target state</td>
<td>• Populated cloud security maturity framework&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Perform gap analysis</td>
<td>• Strategic assessment with gap analysis&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Prepare executive report</td>
<td>• Executive summary report&lt;br&gt;</td>
</tr>
<tr>
<td>Phase 4: Recommend</td>
<td>Develop project definitions and prioritization</td>
<td>• Roadmap&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Create roadmap</td>
<td>• High-level plan&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Develop business case*</td>
<td>• Business case (optional client request)</td>
</tr>
</tbody>
</table>

* Capability Maturity Model Integration (CMMI)
Why IBM?

With a comprehensive portfolio of cloud security solutions, including recognized leadership in IAM, IDaaS offerings as a cloud vendor, and strong consulting and managed services, IBM can help you securely deploy applications and services in the cloud. No matter where your organization is on the cloud security continuum, IBM can provide the guidance and the tools you need to strengthen your security posture.

A note about compliance

Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the European Union’s General Data Protection Regulation (GDPR) force many to place their focus squarely on keeping up with new requirements. While it’s important to remember that being in compliance does not guarantee security, compliance is a key driver for organizations that are examining their overall cloud security. The security pillars outlined in this paper can support your goals for compliance as well.
For more information

To learn more about IBM MaaS360, 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 IBM X-Force® research, provides security intelligence to help organizations holistically protect their 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 15 billion security events per day 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