bmc

Solution White Paper

Protect Your Hybrid Cloud Environment with a Policy-Based Approach to Security

Table of Contents

Executive Summary

The need to ensure a secure hybrid cloud environment, also known as a multi-cloud environment, has never been greater. Why? The demands of the digital economy are driving more business users to the cloud and that growth generates more opportunities for threats to emerge. The rush to the cloud has escalated to such a level that according to Gartner, the worldwide public cloud services market is expected to have grown by more than 17 percent in 2016 to a total of $208.6 billion. A big component of that growth has been Infrastructure as a Service (IaaS), which leaped by about 42 percent in 2016, and Software as a Service (SaaS), which grew more than 21 percent over 2015.[1]

The need for speed is a big motivation to move to the cloud as business users and developers demand faster access to infrastructure services and application environments. If IT can't support these people fast enough, business users and developers may go outside the organization and source infrastructure from the public cloud. While this approach may make sense for certain services, it may give rise to "Shadow IT," which increases business risk due to inadequate visibility and governance.

Cost is another big driver, but ironically, even though some organizations choose to use public cloud services to reduce costs, lack of oversight can cause it to be considerably more expensive than a private cloud by enabling unrestrained service acquisition. Even when purchasing controls are employed, costs can spiral out of control when unused or underutilized resources remain active.

Public cloud environments are often outside the reach of IT's processes and best practices for service management, leading to potential security and compliance gaps. The public cloud needs to be governed, secured, and maintained just as well as on-premises infrastructure.

So, how can organizations ensure governance, security, and compliance across private and public cloud environments while still providing frictionless access to cloud resources? **This white paper explains how to achieve these objectives with best practice processes that enable consistent IT and regulatory compliance and change management policies across a multi-cloud environment**. The paper will review unique security considerations for on- and off-premises cloud environments and how to centralize governance and access to services—no matter where they are located.

1 Gartner Says Public Worldwide Services Market to Grow 17 Percent in 2016, September 15, 2016

> **"...if you use any cloud today, you already have a hybrid. 'Hybrid' is not a third type of cloud. It is the set of challenges you face when you use an increasing array of external cloud services and connect them to in-house resources."**
>
> **– Forrester, Cloud Powers the New Collected Economy: The Cloud Computing Playbook, by Liz Herbert and Dave Bartoletti, May 27, 2016**

INTRODUCTION

In general, IT has more control over on-premises resources because it provides the opportunity to establish firewalls, control networking, and align the infrastructure with corporate standards. For public IaaS resources, IT still has control of instances and some networking control, enabling them to operate and govern in a manner very similar to managing on-premises resources. However, for PaaS or SaaS services, the infrastructure is managed by the cloud service provider, thus removing some of the security levers one might have as compared to owned, on-premises resources.

It's important to note that not all cloud services are equal. Some may run critical applications or allow access to sensitive data, whereas others might be more innocuous, serving a temporary or non-critical role. A key tenet in protecting these complex, multi-cloud environments is to have a good understanding of where the risks are and how critical they are to the organization's success. Being able to automatically prioritize when and where to remediate vulnerabilities is critical to ensure that limited resources can address the highest risks the fastest. **Thus, a solution that helps identify and prioritize remediation actions enables security posture to improve while minimizing the impact on continuing business operations**.

Identifying vulnerabilities is often done by security personnel whereas IT operations are often responsible for remediation, including patching, configuration changes, etc., all while ensuring that appropriate processes are followed and changes are documented. A smooth handoff between these groups is necessary to ensure that security risk is properly addressed. This collaboration between security and operations is referred to as "SecOps."

"Organizations that embrace cloud without fully understanding the environment and associated risks may encounter a 'myriad of commercial, financial, technical, legal, and compliance risks," according to the Cloud Security Alliance.[2] The CSA also points out that organizations need to understand the risks they assume when they subscribe to each cloud service.[3] That's why IT needs to manage its cloud environment holistically across existing management systems with consistent process integration to leverage established approval, change management, and CMDB practices.

STANDARDIZATION

More variability in your environment not only increases the management challenge, but also increases the potential for security vulnerabilities. Standardization has long been touted as an important method for gaining cost efficiencies, but it's also important for security and compliance. This starts with deploying consistent, standardized, and approved cloud services that have been tested and meet the organization's requirements for security and compliance.

One proven method to ensure consistent deployment of standardized and approved software stacks is to use service blueprints, which help define the software and desired configuration of deployed cloud services. The desired configuration also includes critical security and compliance controls that are automatically deployed when cloud services are deployed. Using hardened network and software libraries in blueprints ensures that the network and software attack surfaces are minimized, resulting in increased security. Users can easily request cloud services through a cloud service catalog that can then be deployed consistently, following the blueprints to multiple staging environments such as development, test, and production, or across multiple domains including private cloud or public IaaS. **Done properly, the blueprint not only helps deploy approved, secure, and compliant stacks, it also provides a mechanism to update and change your stack definition as new patches are released and become part of your desired deployment**.

Deploying "security hardened" cloud services isn't the end game. These services continue to run and may drift from their desired configuration state, due to changes to improve performance, unauthorized changes, or new patch requirements. Standards change, new threats are identified, and remediation actions against those threats also change. Thus, once changes occur, either they need to be reset to the desired standard or the standard needs to be changed and pushed out to the environment.

2 The Dirty Dozen: 12 Cloud Security Threats, InfoWorld, Fahmida Y. Rashid, March 11, 2016

3 Ibid

A CLOSER LOOK AT BLUEPRINTS AND NETWORK DEFENSE

A server's blueprint should provide a comprehensive level of detail through firewall-like concepts, which are called network paths. With the cloud, network paths are logical representations of the access rules you choose to allow.

Your cloud management platform should defend your network effectively. When a service request or fulfillment request is made, it should be able to determine actual server instances that have been deployed and what roles they serve based on the blueprint components used to create them. It should also identify the right firewalls that need to be created and the specific firewall instances where those rules need to be added based on where those workloads have been deployed.

If you don't have these capabilities, then you have to depend more on perimeter firewalls, which increases risk. That's because if someone can compromise an outer perimeter, that person can gain more access to any of the resources inside the perimeter.

Case Study

Situation: A global bank needed to create a secure yet agile environment for the rapid creation and delivery of innovative digital financial services.

Complication: They needed to improve the time to market of new services, but approvals and application development were taking too long.

The Solution	Benefits
Uses automation and a cloud management platform to deploy standardized environments to minimize variability	Provides a secure, low cost, and more easily managed environment that can easily be scaled up or down to meet the agility needs of the bank.
Uses a consistent set of tools to manage performance, compliance, and change across both public and private cloud environments	Mitigates risk for managing multi-cloud while reducing administrative overhead.
Uses a single cloud management platform from BMC	Allows the bank to quickly provision new cloud services that meet security standards regardless of environment (public or private). Ultimately, this enables the bank to respond quickly to ongoing changes in the financial services industry and rapidly deliver new banking services such as e-wallets, one-click loans, and person-to-person payments.

GOVERNANCE

Cloud governance involves the integration of traditional IT governance best practices, such as compliance, service management, visibility, and chargeback into the cloud environment.

Governance extends four primary processes across cloud environments:

- **ITSM process integration** to ensure that corporate change and CMDB processes are fully integrated from on-premises to cloud environments.
- **Security and compliance** to ensure that internal and external policies are followed, regardless of environment, to maintain secure IT resources and a system that enables audit readiness and compliance with regulations. This includes managing entitlements with role-based access control to cloud resources.
- **Performance and availability** to monitor and identify real and potential trouble spots that can impact service availability or performance and take corrective action. This is becoming increasingly critical as cloud services may span on- and off-premises resources.
- **Financial management** to track the cost and benefits in the cloud by maintaining tight fiscal controls and transparency into usage and financial impact.

Controlling unauthorized access to cloud resources, also known as Shadow IT, is best accomplished through a combination of providing easy access to desired services and using only approved tools and processes. Users are less prone to go around the process if internal tools can accommodate their needs without undue process overhead. For example, governance through process adherence for securing proper approvals can be executed across different services using a cloud management platform with integration to the service desk. By integrating compliance with the service desk / IT service management (ITSM) solutions, you can ensure that all changes are documented and remediation efforts follow the same processes and capture full documentation with step-by-step audit trails.

Services should be managed through a single interface with a platform that can:

- Define pre-approved and manually approved request types
- Manage entitlements using roles and groups of users to control access to cloud resources
- Capture a complete history of all IT changes across the enterprise (audit)
- Define policy-based selection of target resource platforms

Here are some best practices to govern access control and check for compliance:

- **Implement Role-Based Access Control (RBAC)**: This type of control drives users to the appropriate service based on their role. With cloud computing, IT resources are shared, but sharing can introduce security risks. For example, one user (or tenant) may be able to access another user's resources or data. That's why it's important to control who has access to specific resources and isolate those resources to ensure that only those people who are entitled can actually gain access. This includes:
  - Isolating workloads and user access so that the engineering team, for example, doesn't access production applications or sensitive data such as HR records.
  - Establishing business rules so that while a developer might want to use 15 reserved instances of AWS®, they are limited by business rules that permit only 5 instances in the corporate private cloud.
- **Multi-Tenancy**: Organizations that broker cloud services for users, especially those involving public clouds or external users, should build in multi-tenancy from the start to reduce the risk of unauthorized security access or resource sharing. Breaking up a cloud into separate tenants provides the ability to isolate workloads and assign access to different network segments.

Case Study

Situation: Wipro, a leading global IT services firm, manages elite hybrid cloud environments with optimized ITSM and compliance.

Challenge: Wipro needed the ability to provision, configure, secure, monitor, and manage applications and cloud infrastructure to provide high performance, cost-effective services.

The Solution	Benefits
Implements ITIL®-compliant service management	Provides consistent processes for incident, problem, change, service request, and SLA management across physical and virtual environments.
Uses dashboards	Provides up-to-the minute visibility to incidents, change, and other activities for physical and cloud-based systems—greatly reducing risk.
Provides automated patching and configuration	Supports customer compliance with diverse legislative mandates and industry standards.

MICRO-SEGMENTATION

Micro-segmentation uses network virtualization to improve security by sharing intelligence between different security functions. This concept applies where individual workloads require specified access rules to other workloads within a logical service. This activity increases network isolation within the deployed components and supports the principle of granting the "least-access" privilege, rather than leaving network access completely wide open.

It means that you should be clearer on how to manage your database server by opening up the database port and specifying that a certain application server is the only one that can reach that port. There may be a particular port that is only accessible from the front-end web server, and it requires a non-standard https port for access. That's why it's critical to lock down micro-segments, define the level of granularity required for access, and block all others.

AUTOMATED REMEDIATION

Hackers are most likely to exploit known vulnerabilities that have not yet been patched. In fact, studies have shown that 80 percent of attacks target and exploit a known vulnerability.[4] To be more secure in the cloud, you must tie operations more closely to security so that identified vulnerabilities can be prioritized and remediated quickly. By connecting the technology that IT operations and security teams use, vulnerabilities can be discovered, prioritized, and patched quickly and automatically, thus reducing risk. Your vulnerability scanning tool, for example, should be able to connect and merge vulnerability scan results into an actionable set of server targets for operations to use. Further integration with configuration management and change tracking software allows vulnerabilities to be prioritized, tracked, and processed through change management approval and then automatically remediated, removing significant manual effort and potential for error.

An effective cloud management platform should enable enterprises to maintain continuous compliance by first driving compliance automatically when a service is provisioned. This is best accomplished through blueprints that specify the desired state of deployed services. Once deployed, the solution should provide ongoing automation of patching along with configuration management and remediation to keep resources in compliance. Maintaining continuous compliance can be an arduous task, especially as cloud environments grow quickly and change often. Therefore, it's important for organizations to use **a solution that helps create and prioritize actionable remediation plans to simplify the job for operators, allowing them to focus on the biggest threats and critical systems first**.

Due to the variability of cloud services, some resources may be under the control of the management platform while others may not. For instance, not all cloud IaaS vendors provide the same level of access to cloud infrastructure, sometimes limiting the ability of the customer to fix identified vulnerabilities. In these cases, it's important to understand the risk of the vulnerability, and the service level agreement of the cloud provider to fix the vulnerability. Even in these cases, having a cloud platform management solution that can extend to these services can help:

Better understand the exposure of identified security vulnerabilities

Restrict deployment of certain workloads to higher risk (and hopefully lower cost) clouds

Move workloads off of higher risk clouds until vulnerabilities can be remediated

Case Study

Situation: A global insurance company needed a way to manage security and vulnerabilities across its 7,000 server private cloud.

Challenge: Because they are in a regulated industry, they need to follow processes and prove adherence to those rules and regulations.

The Solution	Benefits
Integrates their server configuration software with their ITSM and scanning tools	The company now performs over 100 compliance validation checks per server without human intervention. If non-compliance events arise, they are able to remediate automatically, with full documentation in the change tracking software.
Uses their server configuration software to automate compliance checks and speed audit results	By automating compliance checks across their environment, they have increased audit readiness and reduced related labor costs by 95%.
Integrates their server configuration software with vulnerability lifecycle management system	By managing vulnerabilities and automating remediation through server configuration tools, the data center and cloud servers are more secure from threats and attacks.

COMPLIANCE

Enterprises must comply with a variety of regulations such as PCI-DSS, SOX, and HIPAA, depending on their industry and geographic region. However, providing an audit trail to demonstrate compliance can be completely manual and time consuming unless it is automated. Auditors expect organizations to have a verification function to produce evidence that demonstrates compliance and process integrity.

Enterprises need to be audit-ready and may struggle with manual processes that are time consuming and error-prone. They can address these challenges with automation that provides compliance with regulations and the ability to track changes for audit reporting in the cloud. This allows them to measure workloads for compliance against standards. Policies for regulatory and security compliance requirements should be automatically applied to the service at the time of provisioning, enable remediation of out of compliance issues, and provide the reporting necessary to prove compliance.

Case Study

Situation: An investment research firm needed to migrate to the cloud while maintaining control and complying with standards.

Challenge: The company was using a different set of tools for managing its heterogeneous environment and needed to take a consistent, integrated approach.

The Solution	Benefits
Introduces standards and automation to migrate workloads to the cloud	The company supported its move to the cloud with a single set of tools that manages IT services across private cloud and legacy systems, as well as hybrid and public cloud environments.
Maintains control and ensures regulatory compliance and alignment with ITIL best practices	Blueprint technology automates the design, management, and governance of compliant environments. Automated compliance checks for SOX and PCI DSS notify staff of compliance drift while integrated ITSM capabilities manage ITSM processes across legacy and cloud-based systems.
Uses a policy service to detect and remediate compliance issues	Automating data center regulatory compliance and cloud compliance helps improve security while reducing costs and the time required to prove compliance.

SECURITY PRINCIPLES

Automation of cloud security is extremely important due to the scale and frequency of resource changes. The table below lists a few core security principles and how they can be automated with BMC solutions, including Cloud Lifecycle Management (CLM), SecOps Policy Service, and SecOps Response Service.

Security Principles	Implications for Cloud	Using BMC Solutions
Minimize attack surface area	Attack surface for cloud includes network, software, and human areas that need to be minimized	Use CLM to define secure resources in service blueprint during provisioning Use SecOps Policy Service and SecOps Response Service to continuously monitor and reduce attack surface
Least-access privilege	Grant users only the minimum access to cloud resources that allows them to do their jobs	Use CLM for access control, tenancy, and entitlements to cloud workloads
Defense in depth	Use layered security controls to increase cloud security	Use CLM to define blueprints that allow security controls such as firewalls for different tiers of an application
Standardize with secure defaults	Use standard secure components	Use CLM service blueprints that use secure hardened resources and set up compliance policy checks
Zero trust	Use micro-segmentation to ensure application stacks are kept isolated	Use CLM service blueprints to define micro-segments in your network design
Automate security	Automate vulnerability detection and remediation	Use SecOps Policy Service to automatically detect and remediate security and compliance Use SecOps Response Service to prioritize, plan, and reduce vulnerabilities

ADDITIONAL GUIDANCE

As your hybrid environment grows and evolves, it's critical to look at security and governance holistically. This is especially important as you add more public cloud providers or shift to other types of cloud services (IaaS, PaaS, or SaaS). With a PaaS or SaaS services, customers have little to no control over the underlying infrastructure, instead relying on the vendor to identify and address vulnerabilities. Understanding their approach to dealing with these vulnerabilities or compliance issues will help you make better decisions about where to place your critical business services and data.

Here are some questions to consider when you engage with a public cloud provider or private cloud management platform vendor to help assess how well it is being governed. If the provider or platform vendor cannot answer these questions to your satisfication, consider a different provider or include an additional governance layer that might help minimize exposure.

Key Questions to Assess Governance Policies	Important Considerations
How do they perform multi-tenancy?	Does it meet your internal standards? If not, how will you limit access within your organization to these services?
What kind of access controls do they allow?	Can you control access to their services programmatically?
What kind of performance metrics and SLAs do they have?	Can you use your existing performance management tools to ingest this data to measure across an entire business service?
What kind of information do you get back from a public provider to help you determine security breaches?	Do they provide you with log files and access reports, and how will you analyze those reports against change records?
If it's a platform as a service (PaaS), how do they update for vulnerabilities?	Are there service levels that they agree to meet to update security? Do they inform you about potential vulnerabilities that might affect your services?
If there is a patch that has to be applied to an operating system, what's the turnaround time for the patch to be applied?	How does their service level commitment match your internal policies for remediation? Consider how this affects which workloads you will run on their cloud.
What type of dashboard do they use to provide you with governance metrics?	Consider metrics that measure performance, availability, security, and financial impacts.
How do they segregate data and users? How do they keep that environment up to date? If you need info about what's impacting their performance, can you get that info?	If not to your standards, consider which workloads are appropriate for that cloud service.
Do they offer automated vulnerability remediation to make sure patches are applied in sequence of importance in the most optimal timeline?	What is your internal SLA for applying critical patches post findings by the security team? Does the tool meet requirements?
Does the tool discover unknown/untracked servers and network devices and bring them into formal governance?	Unknown/untracked devices could be safe hosts for attackers. The tool should be able to bring all such entry points under governance.

SUMMARY

It's critical to take a holistic approach to cloud security and governance that is compatible with physical and virtual systems across both on- and off-premises environments. Start with a solution that lets you provision services across any platform from a single service catalog. According to Forrester, "Your main goal here is to balance low friction business adoption of cloud services with the right level of governance over cloud usage in your enterprise. Cloud undeniably enables adaptation by orders of magnitude, but don't expose the enterprise to excessive risk. Continually reassess your governance using feedback from the business key performance indicators (KPIs) that are important to your CEO and board of directors."[5]

With a governance model and access controls that depend upon the profile of the user, cloud services can deliver the level of security that gives people access to only what they need to see. This model should provide the visibility and transparency to make sure that the organization knows what materials are being distributed across specific public cloud services. It must include determining factors related to access and control, such as where their intellectual property is and where they put their customer data and sensitive materials.

With proper governance, you can create a necessary partnership between IT and lines of businesses (LOBs), where IT delivers more flexible access to cloud services yet still maintains control to minimize risk and financial impact. The platform interface should make it easy for business users to request configurable services across the infrastructure, platforms, and applications without having to go through IT.

Cloud Lifecycle Management accelerates innovation and continuous delivery of digital services. It coordinates, controls, and secures application and infrastructure services across hybrid environments, with integrations to essential IT management processes to control risk and reduce cost.

The solution consolidates operations and provides a single place to govern and give access to services. It determines who has access to which cloud based on their level of authority so that only designated people can make changes on systems. It utilizes automation that helps prevent organizations from overstepping their authority and creating "Shadow IT" resources. Furthermore, the solution provides users a service catalog for standard access to different cloud services—on-premises and other services such as AWS or Azure®. With this catalog, users can track cloud services costs from an authorization and budgeting perspective, while feeling confident that their resources are also secure.

Cloud Lifecycle Management, when combined with BMC ITSM, Discovery, SecOps Policy Service, and SecOps Response Service, has been helping enterprises worldwide address the challenges of maintaining security in multi-cloud environments while meeting the demands of digital business.

5 Cloud Powers the New Connected Economy – Vision: The Cloud Computing Playbook, Liz Herbert and Dave Bartoletti, Forrester, May 27, 2016

FOR MORE INFORMATION

For more information on Cloud Lifecycle Management, watch this **demo video**.

489341