bmc helix

App-Centric Cloud Security Posture Management

Table of Contents

03 Executive Summary

04 The Problem / Negative Impact

05 The Case for App-Centric Security

07 Asset Discovery and Dependency Mapping

08 App-Centric Security Posture Management

10 Closed-Loop Security Incident Management

12 Conclusion

Executive Summary

Cloud-native and cloud migration projects can stall if multi-cloud security and compliance methods are not carefully reexamined. Agility and security are not mutually exclusive. By linking security and compliance management with asset discovery and ITSM, scrum teams can more easily visualize, triage, and remediate the security posture of the microservices they develop. In this way, cloud security posture management is embedded within the SDLC, resource dependencies are understood, and security incidents and change smoothly managed. Business agility accelerates without compromising security and compliance.

The Problem / Negative Impact

The cloud is no longer a hyped-up future state, but a present-day reality as 91% of enterprises use public cloud. Gartner projects $90 billion will be spent in 2020 on IaaS and PaaS services. While the growth continues unabated – 24% YOY – organizations are vexed about securing their public cloud footprint. To punctuate that point, 93% are worried, so much so that 55% expect to deploy a new cloud security solution within the next year[1]. Clearly, current tools and methods for cloud security are not good enough for the majority of enterprises.

Despite those concerns, our appetite for cloud IaaS and PaaS shows no sign of waning. An organization's cloud footprint is constantly changing and ever-growing. An army of developers are using CI/CD pipelines to continuously push updates for their microservices that live in the cloud. Those cloud-native apps[2] are composed of cloud IaaS and PaaS resources, every instance of which must be appropriately configured if they are to be secure, and therein lies the problem. The misconfiguration of cloud resources remains the leading cause of cloud security failures.

Microservices are not static, and there can be hundreds of them. With each update to a microservice comes the risk of a single misconfigured resource inadvertently exposing intellectual property or customer data. This challenge is complicated by several factors:

Impaired visibility. In a 2019 report from EMA, 73% of security professionals cite struggles with visibility into cloud infrastructure due to provider limitations.

New services. Cloud service providers (CSPs) are constantly innovating, releasing new services which are similar, but not identical, and which must be configured so that they are secure.

Accelerating agility. Agility is good for business, and yet it brings its own security challenges. Scrum teams are self-organizing and asynchronous. Under intense pressure to meet delivery schedules, security considerations can create friction, potentially creating improper incentives for unseemly behavior like pushing security to the side.

This is a volatile mix, especially when one considers that a data breach costs nearly $4M on average[3]. That number goes up for highly regulated industries such as healthcare, for certain countries, and as the size of the organization increases. Then there is the potential of damaged trust, which impairs current and future business prospects, as well as regulatory penalties. The stakes are high, and the challenge of securing the enterprise's public cloud footprint a daunting task.

[1]Cybersecurity-Insiders, 2019 Cloud Security Report. The 93% breaks down as follows: 38% are extremely concerned, 37% very concerned, 18% moderately concerned.

[2]Throughout the paper, the words "apps, microservices, and business services" will be used interchangeably.

[3]Ponemon Institute, 2019 Cost of a Data Breach Report

The Case for App-Centric Security

Enable Agility, Don't Hinder It

While the **concept** of app-centric security itself is straight-forward – simplify security for the developers, so that they can own and manage the security posture of their cloud applications – the implementation is much more intricate. Simplifying security for the developers is a multi-layered challenge, so it is important to understand why we should undertake this mission.

According to SiriusDecisions, a full 78% of organizations use agile methods in R&D[4]. This means the cloud footprint is constantly evolving as developers relentlessly innovate. While innovation is imperative to competitive advantage, so is information security. Yet, security methods all too often remain manual or ad-hoc, which is completely incongruent with the scale and rate of change that the cloud delivers. The inevitable bottlenecks then grind the gears of agility. The enterprise needs fewer vulnerabilities to be promoted from development (hereafter, "DEV") into production ("PROD"), but they also need to innovate faster. And this means shifting security left into the software development lifecycle (SDLC).

The pervasive challenge is that, for developers, security is not their first thought. It is *not* that they don't care, but in all but the most mature organizations, the tools and methods given them create stumbling blocks. Force-feeding a laundry list of point-specific, cloud-specific security tools on the scrum teams is not a recipe for buy-in or success. It complicates security unnecessarily. So then, how do we equip the developers to own and manage their cloud security, without impeding agility?

Requirements

Automated asset discovery and dependency mapping. First, developers need a means to automate asset discovery and application mapping across multiple cloud environments. This will reveal dependencies between the multi-cloud IaaS and PaaS resources which the app/microservice use and allows for the logical grouping of these assets within a "business service." This information is then available to a cloud security solution which presents the security posture of the logical grouping of those resources. As such, asset discovery and dependency mapping are foundational to the job of app-centric security posture management.

Automated security checks and remediation. Next, a developer needs an automated means of checking the secure configuration of their multi-cloud resources. Developers should have complete autonomy and accountability to manage their multi-cloud security posture for their application. The security solution should ingest the logical "business service" groupings – created during automated asset discovery – which in turn allows the developer to quickly visualize their app's security posture and prioritize their security backlog. Then, automated remediation further simplifies security for the developer: simply click a button.

[4]SiriusDecisions Summit, May 2019

Integration of security incidents to ITSM processes. Where security and compliance violations are identified in STAGE or PROD, the cloud security solution should automatically trigger an incident ticket be opened, notifying the owner (in this case, the microservice developer or scrum team leader). When remediating the change, a change request should automatically be opened, and the organization's change control process initiated. Once the change request is approved, the CMDB can be updated.

Centralized governance. The Security and Compliance team benefits because fewer misconfigured resources will find their way from development environments ("DEV") and into TEST/STAGE. It should be noted that the Security and Compliance team retains ownership of the security and compliance policies against which the IaaS and PaaS resource configurations are tested, and remediated. In this way, S&C retains oversight and governance across the expanding multi-cloud footprint, while the complexity of security is abstracted away from the developer. Resources are securely and consistently configured across the public cloud by the developers who are using those resources, and within the guardrails defined and maintained by the Security team.

Multi-cloud support. As previously alluded, multi-cloud support is required because 81% of organizations use more than one CSP. The solution must also automate security checks, as well as their remediation, so that the thousands of cloud resources are consistently and securely configured.

Enterprise integration. A REST API allows discovery and security tooling to integrate to the CI/CD pipeline and to each other. Each specialized solution shares valuable context with the other. It also allows for integration to the incident and change management workflows, so that change is smoothly managed and an audit trail readily available.

In summary, a fundamental imperative of simplifying security for the developers requires:

- automated resource discovery and dependency mapping
- logical grouping of resources into a business service
- automated, policy-based security and compliance checks and remediation
- multi-cloud and REST API
- presenting security posture of a business service in a visually intuitive manner

These requirements simplify the security lift for developers, so that security is more readily embedded within the SDLC and fewer risky configurations are promoted to PROD. The Operations team can then continuously monitor PROD for configuration drift, with the same multi-cloud configuration solutions used in DEV. The Security team is then free to rise above manual or ad-hoc policing of the rapidly changing cloud footprint and deliver the higher value work which every Security team knows is out there, but rarely has time to execute.

Now that the case is clear – *enable agility, without compromising security and compliance* – as are the requirements, let's examine asset discovery in more depth.

Asset Discovery and Dependency Mapping

As data centers give way to public and private clouds, new flexible, cloud-native applications help drive the business forward. These cloud environments and cloud-native apps must coexist with legacy infrastructure and software. Not surprisingly, organizations which lack visibility into how their cloud-native services are implemented struggle with their digital transformation. Automated asset discovery and dependency mapping provides the trusted foundation that catalyze that digital transformation by enabling LOB stakeholders to monitor, secure, optimize, and service their hybrid cloud infrastructure in the way the business thinks of it – through an application-centric lens.

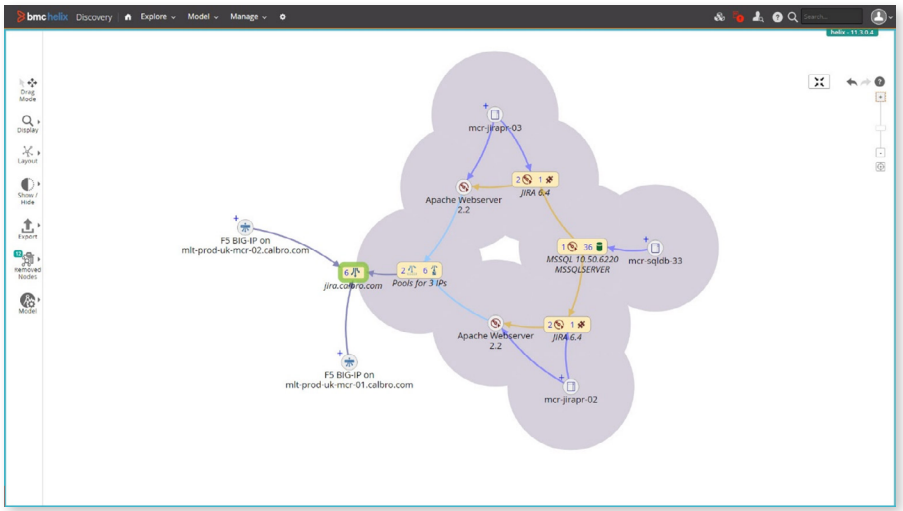

Figure 1: Logical Grouping of Resources in a Simple Business Service

Once the resource dependencies are mapped, the app's resources are logically grouped into a "business service." This logical group can then be leveraged by the business stakeholders in creative ways, such as managing resource allocation, optimizing cost, or continuously managing security and compliance of just that specific business service.

Automated, agentless discovery of multi-cloud infrastructure and applications keeps the dependency map updated as quickly as the scrum team can push updates. The ability to map discovered resources into a model of the business service from any point within the app reduces the need for application-specific expertise. This visually intuitive abstraction also simplifies configuration management of those resources, providing helpful context to the scrum team when they triage their security backlog.

BMC Helix Discovery is one such asset discovery solution. Agentless, lightweight, and scalable, it is a cloud-native SaaS solution that is ready-to-run and updated with new content monthly. BMC Helix Discovery seamlessly integrates with BMC Helix CMDB for continuous data synchronization. And BMC Helix Discovery can map assets and dependencies across data center, public cloud, and private cloud environments, leveraging APIs and agentless protocols.

App-Centric Security Posture Management

Once multi-cloud resources are found, dependencies mapped, and business services logically grouped, a cloud security solution can ingest this information and add security context. Automated checks of the business service's resource configurations against a library of security and compliance policies present a real-time view of the developer's security posture.

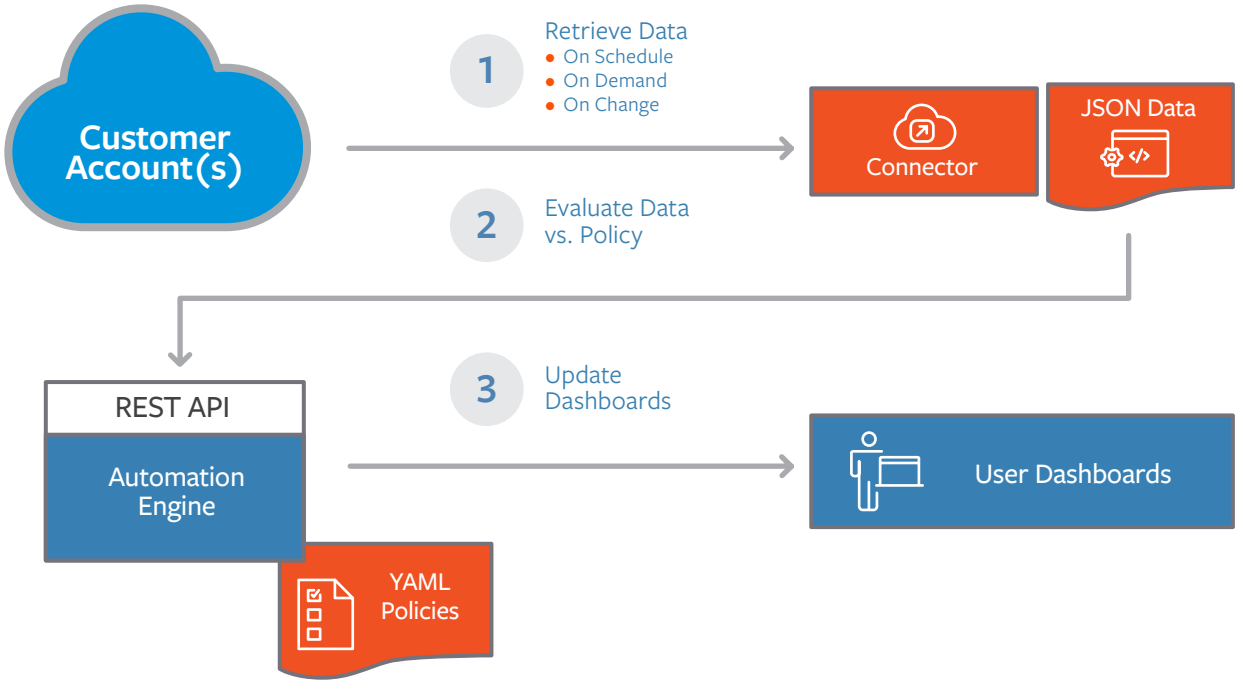

Figure 2: Automated Security Checks

By showing the developer only what she needs to manage the security posture of her application, and by cross-referencing this posture against the relationships shown in the application map, she can triage her security backlog.

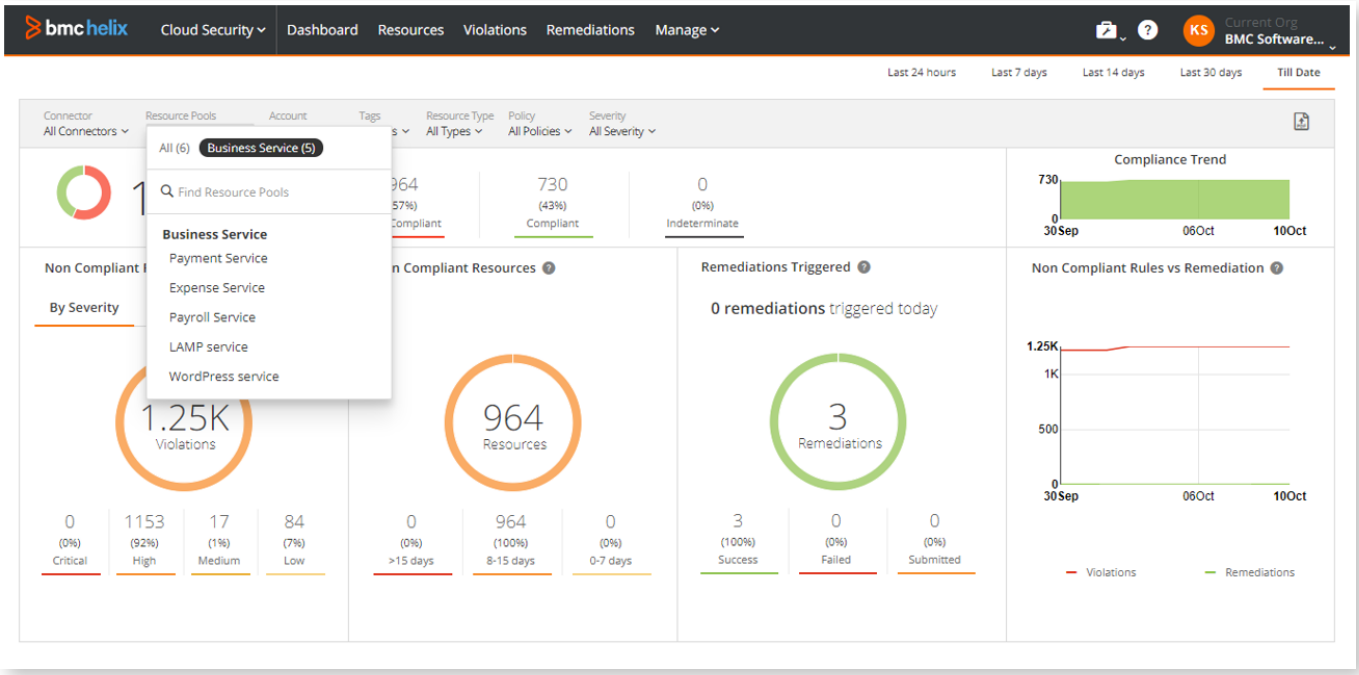

Figure 3: Security Posture Visualization for Business Services

Automated remediation to any security and compliance violations abstracts the complexity of security management away from the developer. The Security team retains complete control of the remediation details behind the scenes: the developer need only know "This is a violation, and I click this button to make it go away."

BMC Helix Cloud Security automates security and compliance checks and remediation – without any coding required – to ensure that IaaS and PaaS resources are securely configured. A ready-to-use library of policies, delivered as code as part of our SaaS service, simplifies security and compliance across AWS, Azure, and Google Cloud and includes remediation action. Native integration to BMC Helix Discovery equips the developers to manage their security posture within the context of their application, and single sign-on renders switching back-and-forth between the paired solutions seamless.

Closed-Loop Security Incident Management

Automating the "find and fix" makes security easy for the developers, so they can focus on "telling time instead of building a watch." Since most organizations use multiple clouds, and that cloud footprint is constantly changing, it is important to manage that change smoothly. Native integration to the service desk for incident and change management is key to having a fully documented audit trail.

Of course, your multi-cloud footprint not only includes (potentially hundreds of) DEV accounts, which the developers own, but also STAGE and PROD, which Operations monitors. To smoothly manage change here, such a security solution should also integrate with the service desk: when a violation is found in STAGE or in PROD, automatically open an incident ticket; when a remediate request is made, automatically submit a change request and launch your change management workflow. (Remember, DEV owns their DEV accounts, subject to the same security and compliance policies used throughout the organization.)

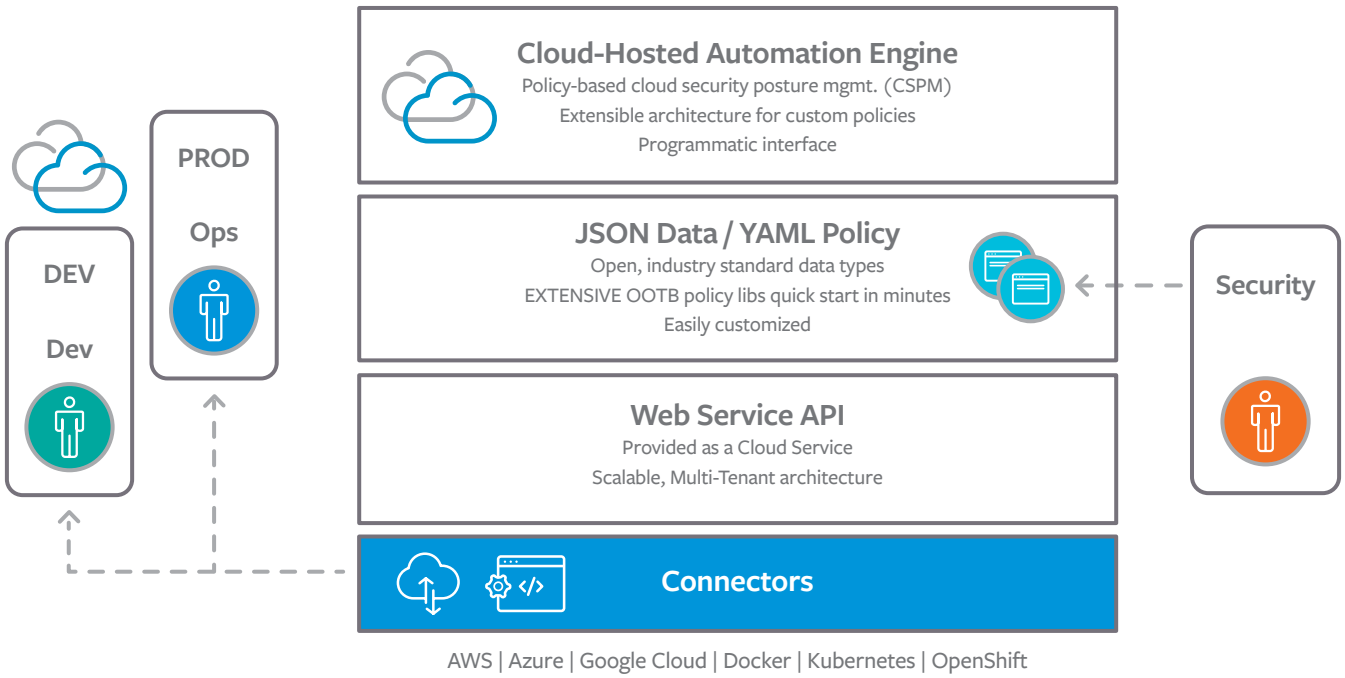

Figure 4: Multi-Cloud Security Posture Management

Such automated incident and change management provide a crystal-clear audit trail to the immutable production infrastructure.

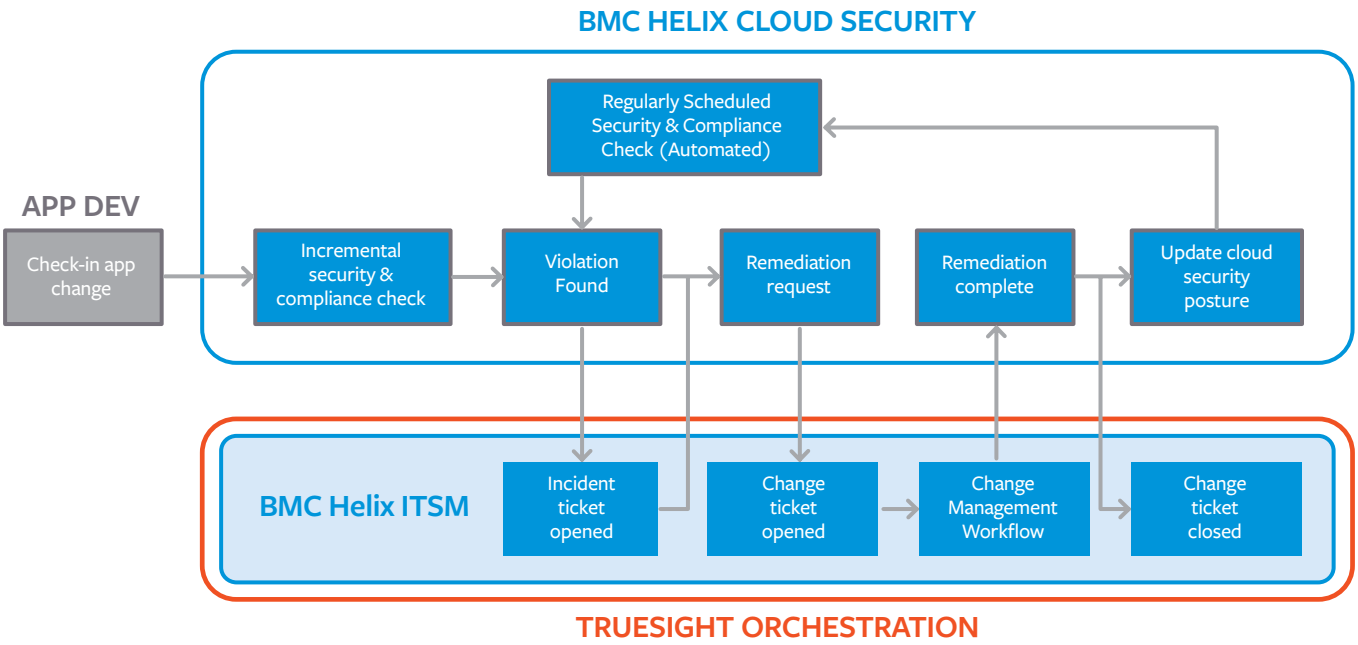

Figure 5: Closed-Loop Security Incident and Change Management

Conclusion

To maximize the agility benefits of the public cloud, organizations should implement a multi-cloud, policy-based, and automated security and compliance solution which not only finds violations in IaaS and PaaS configurations, but also fixes them. Integration to an asset discovery solution, as well as the ITSM service desk, keep the gears of agility running smoothly. Built upon the BMC Helix platform, the combination of BMC Helix Cloud Security, BMC Helix Discovery, and BMC Helix ITSM delivers a powerful means of transforming app-centric cloud security posture management (CSPM).

For more information

To learn more about how BMC can accelerate your business agility without compromising cloud security and compliance, please visit bmc.com/cloudsecurity.

About BMC

BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent **www.bmc.com**