

BMC Helix Cloud Security

Automated security and compliance of your multi-cloud resources and containers.



Business Challenge

The public cloud has reimagined the way we do business. Rapidly embracing change, iterating, learning. With this transformation, come hundreds, if not thousands, of accounts; similar, but not identical, cloud services across multiple platforms; and business apps and microservices updated at a dizzying frequency, consuming thousands of cloud resources, each one of which must be properly configured to be secure and remain compliant.



Secure



Compliant





Cloud Security Reaches Critical Mass

A lack of cybersecurity skills hampers many organizations. Tools intended for on-prem usage flounder in the cloud. Unable to keep pace with security and compliance demands, IT find it difficult or impossible to scale cloud operations with the speed the business demands.

Attacks are focused on the public cloud because the pickings are easy: misconfigured cloud resources unwittingly expose billions of records to prying eyes. Automation has changed the game for hackers, enabling them to find and attack vulnerabilities within minutes.

To accelerate cloud operations while managing risk, IT need a state-of-the-art means of making cloud security as agile as their development teams.



BMC Helix Cloud Security

Designed in the cloud, for the cloud, BMC Helix Cloud Security automates security testing and remediation of cloud resources and containers, so that they are consistently and securely configured, and stay that way.

Because it is SaaS, there is nothing to install: you can begin securing your AWS, Azure, and GCP environments in as little as 5 minutes. The intuitive interface provides “point, click, and fix” capability, automating remediation with the click of a button.

Four Simple Steps



Connect



Scan



Assess



Remediate



Solution Capabilities

BMC Helix Cloud Security is designed with the enterprise in mind:

- + Multi-cloud security of services from AWS, Azure, and GCP from a single dashboard
- + Automated security checks and remediation
- + Automatic event-driven compliance
- + Full-stack container configuration security (Docker, Kubernetes)
- + Extensive out-of-the-box library of standards-based policies from the Center for Internet Security (CIS)
- + Custom security policies, exception management, and alerts
- + RBAC (Role-Based Access Control)
- + Multi-tenancy, organizational views, and resource pools
- + REST API
- + Integration to incident and change management



Solution Highlights



Quickly Realize Value

SaaS delivery simplifies implementation and operation of BMC Helix Cloud Security. There is nothing to install. Connect, scan, assess, and fix. Data connectors are available for on-premises and major cloud technologies. The solution delivers a deep bench of out-of-the-box policies, as well as the flexibility for easy modification or creation of custom policies.



Multi-Tenancy, Organizational Views, and Resource Pools

Schedule automated scans, or run them on demand, to identify when production resources have fallen out of compliance or contain vulnerabilities that need remediation. Cloud Ops, IT Security, and Development gain instant visibility into current status, and automated remediation accelerates fixes.



Full-Stack Container Security

Short-lived resources break the traditional security and compliance model. BMC Helix Cloud Security is up to the task, securing the entire container stack, from Kubernetes clusters down to Docker images.



Use Case: Securing Multi-Cloud Resources

Challenge: Accelerating Change

Your multi-cloud footprint is in constant flux. The sheer volume of accounts, business services, and public cloud resources which those services consume, combined with the velocity of updates released by Dev teams spread across the enterprise, present a clear and present danger to your cloud security. Each update carries with it the risk that a cloud resource will be misconfigured and unsecured, silently exposing your business to nefarious actors who are probing your cloud defenses. This problem outstrips human capacity.

Solution: Automated Multi-Cloud Security Testing and Remediation

BMC Helix Cloud Security makes it simple to assess the security, compliance, and risk of the multi-cloud resources which your applications consume – and to quickly remediate configurations. Scheduled scans regularly monitor for multi-cloud compliance drift at a cadence of your choosing.



Solution Highlight: Cloud Control Plane

BMC Helix Cloud Security provides a single cloud control plane spanning all types of cloud services and technologies.

AWS Resources

- + User access & policies (IAM)
- + Network (SGs)
- + Compute (Lambda, EC2)
- + Storage (S3)
- + Blueprints (CFN)
- + PaaS services (CloudTrail, RDS, Elasticsearch, KMS)

Azure Resources

- + User access & policies (Azure Subscription)
- + Network (Azure Net, Connect, NSG)
- + Compute (VMs)
- + Storage
- + Blueprints (Azure RG)
- + PaaS services (Azure Logging)

GCP Resources

- + User access & policies (IAM)
- + Network
- + Compute Engine
- + Storage

Full-Stack Container Resources

- + Docker containers, images, daemon, and host
- + Kubernetes container orchestration



Use Case: Securing Containers

Challenge: Short-Lived Resources

Container usage within the enterprise is spreading like wildfire. The promise of “build once, deploy anywhere” appeals to distributed Dev teams and Cloud Operations alike. The trouble is that containers break the typical security and compliance model.

Containers are lightweight, spin up quickly, and are often killed when their job is finished. Their lives reside in the spaces between security scans, requiring a new approach to securing these short-lived assets.

Solution: Full-Stack Container Security

BMC Helix Cloud Security delivers container security top-to-bottom, from the Kubernetes cluster all the way down to run-time instances of Docker images. Here again, automated scans and built-in remediation make your security agile up and down the entire stack, from orchestration to run-time, including:

- + Kubernetes clusters
- + Docker image
- + Docker host
- + Docker container
- + Docker daemon

One tool secures your multi-cloud resources and full-stack containers.



Summary

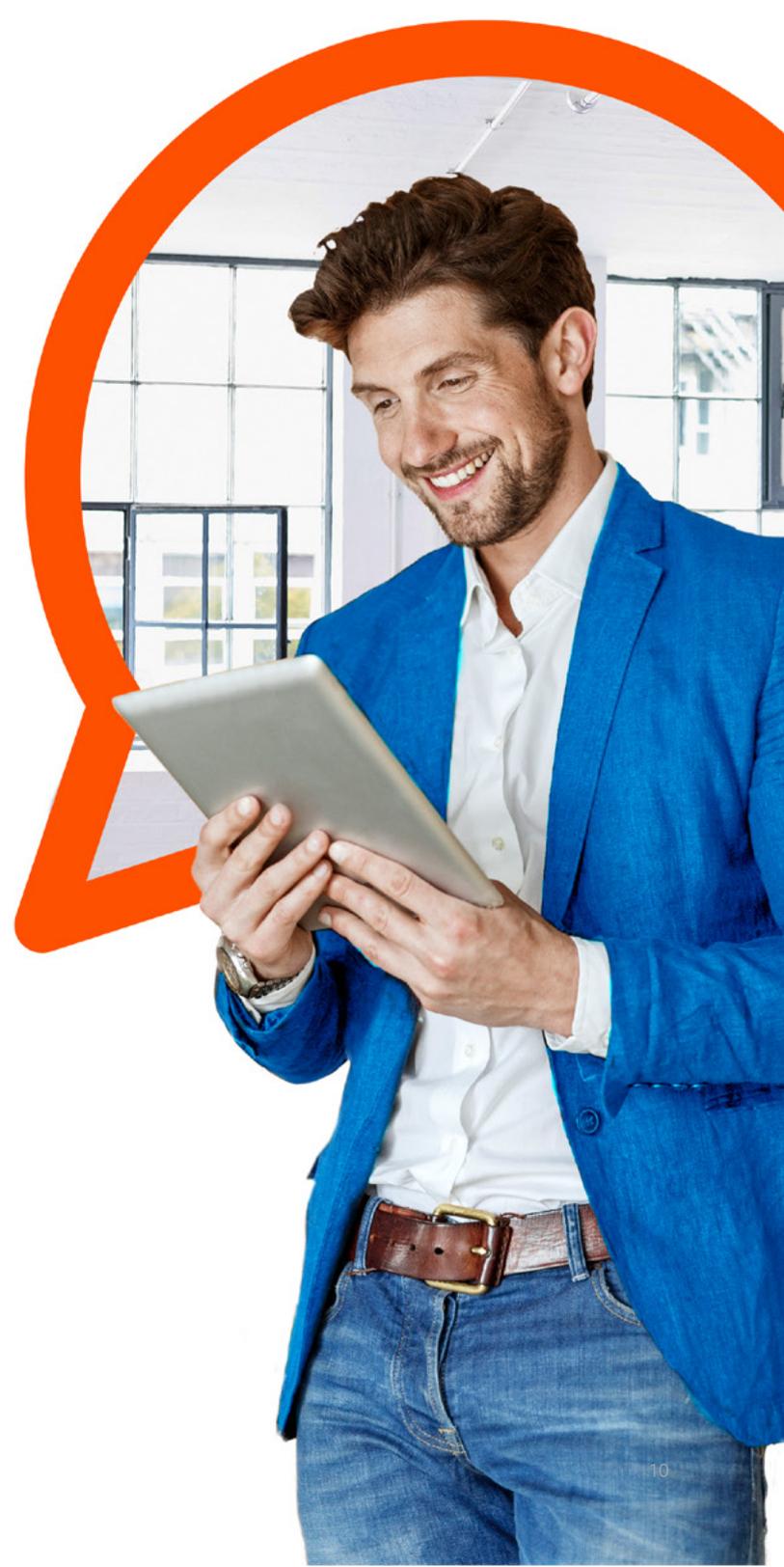
Just as the public cloud has reimagined how we do business, so too must the digital enterprise demand new approaches to cloud security and compliance. Cloud Operations and Security must reduce risk without sacrificing business agility.

BMC Helix Cloud Security automates security and compliance checks and remediation across multi-cloud platforms. Because it is SaaS, implementation is fast and easy. With pre-built connectors and a deep bench of standards-based security policies, value realization is even faster.

By scheduling compliance scans of multi-cloud resources and containers while streamlining remediation, organizations of any size and scale can improve security across their digital business infrastructure -- so you can run your business while you reinvent it.

For More Information

To learn more about BMC Helix Cloud Security, please visit:
www.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.

Run and Reinvent

www.bmc.com



BMC, BMC Software, the BMC logo, and the BMC Software logo are the exclusive properties of BMC Software Inc., are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. © Copyright 2019 BMC Software, Inc.

