Hybrid Cloud
Server Management
and Compliance

With BMC Helix Remediate
Summary

Businesses of all sizes use cloud servers to augment their on-prem IT capabilities. Whether on-prem or in the cloud, organizations need a single console from which they can manage security and compliance of their servers. BMC Helix Remediate provides that ability. This whitepaper explains how the solutions which comprise BMC Helix Remediate come together to simplify the job of server security and compliance.

Business Problem

Over 91% of organizations use public cloud, including server instances such as EC2 from Amazon Web Services (AWS). AWS dominates the global IaaS public cloud market, with $15.5 billion in 2018 revenue. But it is not just AWS cloud servers to be managed; businesses also have on-prem servers. To simplify the already Herculean task of managing server security and compliance across their hybrid cloud enterprise, organizations need a single context from which to do so, because simplifying security and compliance enables business agility.

Explanation

Consider an organization running EC2 instances in their AWS accounts. There may be any number of Virtual Private Clouds (VPCs) running, in any number of accounts. Under the Shared Responsibilities Model, the customer is solely responsible for patch, vulnerability, and compliance management (OS and EC2 configuration) of their EC2 virtual machines. An enterprise could easily spin up hundreds, if not thousands, of EC2s spanning DEV, QA, and PROD environments, every instance of which must be appropriately configured and maintained if it is to be both secure and compliant.

Someone might be tempted to do this manually. Trouble is, the cloud changes too quickly. Limitations of visibility and shadow cloud usage notwithstanding, even if one could locate all of the EC2s running in the enterprise’s public cloud estate, and then manually enroll them in an endpoint management solution, the list would be outdated the moment the tedious effort is completed, if not before. Developers are continuously innovating, and their CI/CD pipelines wait for no one.

---

1 Gartner, July 2019 press release, 2019-07-29, Nag et. al.
2 https://aws.amazon.com/compliance/shared-responsibility-model/
Fortunately, policy-based, automated “find and fix” is a forte of BMC Helix Cloud Security (Figure 2), which can **programmatically locate EC2 instances and automatically enroll** them in BMC’s TrueSight Server Automation, whose strength is patch, vulnerability, and compliance management of servers.
Solution

BMC Helix Remediate is a solution set which includes BMC Helix Cloud Security, BMC Helix Automation Console, and TrueSight Server Automation.

- **BMC Helix Cloud Security** (BHCS) automates policy-based security checks and remediation, so that cloud IaaS and PaaS services are securely configured.

- **BMC Helix Automation Console** helps IT Operations identify, prioritize, and remediate vulnerable servers (such as those missing patches), by enriching scan data from popular vulnerability scan tools. It is a single console to manage both on-prem and hybrid cloud servers.

- **TrueSight Server Automation** acts as the execution engine for OS compliance assessment, patch deployment, vulnerability remediation, deployments, and server management.

Our solution to set up cloud server management for any new public cloud server consists of 3 simple, automated steps.

**Automated Agent Installation.**

First, a BHCS policy searches your AWS environment for any EC2 instances which do not include a lightweight Smart Agent. This Smart Agent is part of the TrueSight Server Automation (TSSA) solution. Upon finding such an EC2 instance, BHCS flags it as a violation and uses its inherent automated remediation capabilities, in cooperation with SSM, to install the TSSA Smart Agent. This automated installation can happen with a simple mouse click (“on-demand”), or with fully automated Self-Driving Remediation. It can also happen consistent with your incident and change management process. The choice and control are yours.

**EC(2) Phone Home.**

Next, after having been installed on each of the flagged EC2 instances, each Smart Agent begins sending a heartbeat signal back to the Smart Hub, installed in a Management VPC within your AWS environment, as shown in Figure 3. This heartbeat requires no manual intervention to setup.

![Figure 3: Hybrid Cloud Server Mgmt. with BMC Helix Remediate](image-url)
Poll and Enroll.
TrueSight Server Automation (TSSA) polls the Smart Hub, recognizes the new heartbeat, and enrolls the newly identified EC2 instances with the Smart Agent in the TSSA managed service.

All 3 steps happened automatically, with no manual intervention. The security and compliance of each EC2 in the organization’s AWS environment(s) is now being managed by TSSA, in cooperation with BMC Helix Cloud Security.

Similarly, TSSA also manages the security and compliance of on-prem servers, installing Smart Agents, polling heartbeats, and so on. This is the power and simplicity which BMC Helix Remediate provides its customers: a single context from which to manage security and compliance of servers, whether they reside on-prem or in the cloud. This user experience, shown in Figures 4 and 5, together with automation, simplifies the complex job of server management.
The jobs, patch orchestration, and vulnerability management for all servers, physical or virtual, on-prem or in the cloud, are facilitated via the BMC Helix Automation Console and by using the battle-hardened capabilities of TrueSight Server Automation to execute tasks behind the scenes.

![Figure 6: Missing Patches on Servers Under Management](image)

![Figure 7: Vulnerabilities Listed Within the BMC Helix Automation Console](image)
Conclusion

The solutions within BMC Helix Remediate combine to simplify and automate the job of server management, whether those servers reside on-prem, in the cloud, or both. Using policy-based automation and remediation, we find cloud servers not being managed, install a lightweight smart agent, and enroll them in TrueSight Server Automation. OS patching, vulnerability management, and server compliance are all managed from a single GUI.

For more information
To learn more about BMC Helix Remediate, or its constituent solutions, please contact your local BMC Sales office, or visit us online at www.bmc.com/remediate.