Check Point
SOFTWARE TECHNOLOGIES LTD

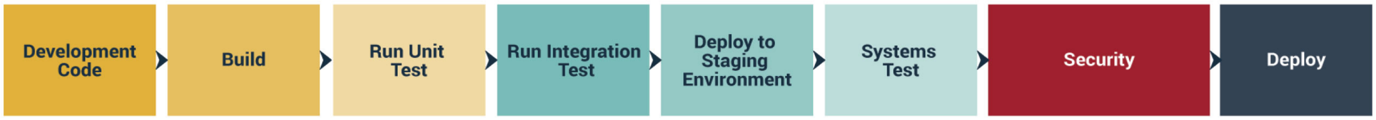
SOLUTION BRIEF

CLOUDGUARD DOME9 ACCELERATES RUGGED DEVOPS FROM DEVELOPMENT TO DEPLOYMENT AND BEYOND

DevOps and Continuous Delivery practices are being widely used by organizations that want agility and faster time-to-market to better respond to changing business needs. Development, QA and operations teams face the challenge of incorporating security into the software development lifecycle (SDLC) without slowing things down. Siloed approaches to security hardening that worked in the past are incompatible with the holistic, iterative model of software development and deployment underlying DevOps. Traditionally, security reviews involved mostly manual processes at the end of product development and QA. Any security risks or issues detected in the product, sent the code back to development, causing significant delays. Development teams spend 50 percent less time fixing security issues when they incorporate security throughout the SDLC rather than retrofitting security at the end[1].

CloudGuard Dome9 provides the security foundation for Rugged DevOps with tools that allow automated testing and enforcement of security and compliance into how you build, deploy and run applications in the public cloud without sacrificing agility. The CloudGuard Dome9 Compliance Engine, extends organizations the ability to automate security and compliance early into the DevOps process as Infrastructure as Code (IaC). Enterprises can test the security and compliance posture of their CloudFormation template (CFT) and proactively harden security before deploying software-defined infrastructure in live environments. Here are four ways in which DevOps teams can harden their applications with CloudGuard Dome9:

1. **Validation Before Deployment:** Test the security and compliance posture of application architectures (e.g., AWS CloudFormation templates) with a single click prior to deployment.

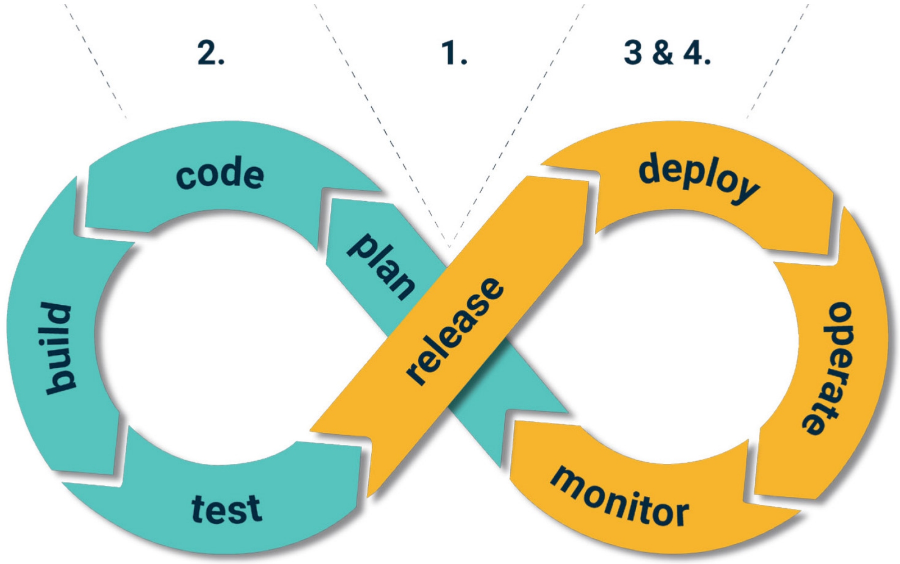


Traditional Manual Security Integration in the DevOps CI/CD Pipeline

WITHOUT CLOUDGUARD DOME9: Ops creates a CloudFormation template (CFT) that describes the application architecture to be deployed in detail. The security team translates the CFT, clarifying specifics with the Ops team, and then manually verifies that the design conforms to security and compliance requirements, a process that often takes weeks to complete.

WITH CLOUDGUARD DOME9: The CloudGuard Dome9 Compliance Engine allows security teams to visualize and validate security and compliance of a CFT with a single click in minutes prior to deployment. This removes manual security limitations and speeds up the process while eliminating friction between security and operations. Organizations can quickly check the pass/fail status of a CFT and use this to gate releases.

[1] 2016 State of DevOps Report presented by Puppet and DORA



The CloudGuard Dome9 Automated Security Integration Solution
for Rugged Dev Ops

1. Validation Before Deployment
2. Automated Testing During Development
3. Secure Deployments
4. Actionable Alerts

2. **Automated Testing During Development:** Use the CloudGuard Dome9 API to incorporate testing of security best practices and compliance into the continuous build processes early in the cycle.

   WITHOUT CLOUDGUARD DOME9: Security checks are typically run after development and functional testing is completed. Any security vulnerabilities detected later in the SDLC force costly redesign and slowing down the process.

   WITH CLOUDGUARD DOME9: Automation engineers can use the CloudGuard Dome9 API to programmatically run security and compliance checks on CFTs as part of the build and QA processes, incorporating this testing early into the build process. With security and compliance checks moving up the cycle, vulnerabilities and regressions can be detected and fixed early, drastically reducing the cost of fixing security issues.

3. **Secure Deployment:** Maintain a closed-by-default security posture in the cloud by locking down cloud environments except to allow authorized software deployment.

   WITHOUT CLOUDGUARD DOME9: Users or roles responsible for deploying an application to a production environment typically have complete access to the environment. These individuals can make changes to all security group policies at any time through scripts, automation, etc., creating security exposure.

   WITH CLOUDGUARD DOME9: With Tamper Protection and Region Lock from CloudGuard Dome9, cloud administrators can lockdown cloud environments and prevent any security configuration changes except when the application needs to be deployed. Tamper Protection continuously monitors managed cloud environments for any changes made through the public cloud console or via the API and automatically reverts unauthorizedmodifications. At the time of deployment, Tamper Protection can be turned off programmatically, and then reactivated once the application is deployed and security configuration is modified.

4. **Actionable Alerts:** Streamline alerts in highly dynamic cloud environments with machine intelligence, allowing operations teams to focus on alerts that require immediate attention.

   WITHOUT CLOUDGUARD DOME9: Infrastructure as code allows DevOps to spin up and tear down virtual machines programmatically. This makes dynamic cloud environments challenging to monitor and manage from a security perspective without automation. The constant notifications and alerts triggered by security group changes, new stack deployments, added and removed instances, and new networks can exacerbate the problem, making it difficult to figure out what to prioritize.

   WITH CLOUDGUARD DOME9: CloudGuard Dome9 uses machine intelligence to prioritize alerts and notifications and improve the signal to noise ratio of alerts by a factor of two. Real-time, actionable alerts and notifications are delivered in AWS environments through the Simple Notification Service (SNS), which can then be consumed by downstream applications such as, Splunk, Sumo Logic, Graylog and Loggly. This automated intelligent alert process allows an administrator to resolve issues quickly rather than spend cycles figuring out what is important.

CONCLUSION

The CloudGuard Dome9 Rugged DevOps solution is unique in that it enables security and compliance to be incorporated early in the SDLC as well as for validation of the live environment. With a cloud-native, API-based approach, CloudGuard Dome9 integrates with all IaaS public cloud providers to leverage continuous security and compliance monitoring and maintain the most current cloud providers rules enabling active protection. With security and compliance moving up the SDLC and now part of the continuous deployment pipeline, DevOps achieves a closed feedback loop and controlled system that continually improves, accelerating an organization’s time-to-market.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises’ cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

CONTACT US
Check Point Software Technologies Ltd.
959 Skyway Road, Suite 300
San Carlos, CA 94070
USA +1-800-429-4391
www.checkpoint.com

For a free security assessment or trial, please contact:
US Sales: +1-866-488-6691
International Sales: +44-203-608-7492