Check Point SOFTWARE TECHNOLOGIES LTD

ESSENTIAL CAPABILITIES FOR PUBLIC CLOUD SECURITY

As applications transition from datacenters to the public cloud, enterprises must rethink their security strategy. The public cloud requires a new breed of security solutions that offers **visibility, active protection, compliance management, and intrusion detection.** CloudGuard Dome9 delivers security and compliance automation to address the biggest challenges of enterprises as they scale in the public cloud.

1. Security Architecture Review

Security architects need to perform high level architecture reviews of application deployments and identify potential security risks across cloud-native services including S3 buckets and lambda functions.

CloudGuard Dome9 allows you to visualize your cloud security at the infrastructure level using a dedicated, purpose-built platform that allows you to interactively identify configuration drift, assess impact of new vulnerabilities and spot firewall rule misconfigurations quickly.

2. Continuous Compliance Assessment

Applying security controls to ensure nothing is broken in a dynamic cloud environment can be hard via traditional methods. Doing compliance checks on an ad hoc basis is no longer sufficient.

The Compliance Engine from CloudGuard Dome9 allows customers to automatically and continuously assess their cloud security configuration against regulatory standards and built-in security best practices. They can use pre-packaged test suites that check for compliance or they can easily create their own customized test suites that capture their organization's unique requirements.

3. Custom Cloud Governance For The Enterprise

Enterprises need the ability to translate policies into concrete checks that model their organizational requirements.

CloudGuard Dome9 offers an expressive yet concise language to define custom compliance rules that can be included in policies in the Compliance Engine from CloudGuard Dome9. The ability to create custom rules in a simple and intuitive manner, all in the size of a tweet, eliminates the need to write hundreds of lines of code for your specific compliance policy.

4. Unified Cloud Inventory Management

Asset detail is challenging to manage with accounts associated with the same public cloud, but when you factor in multi-account and multi-vendor scenarios (any mix of AWS, Azure, and/or GCP) that process becomes impossible to manage. Enterprises must have a single view to clearly understand the full state of any instances/asset in order to get complete context.

CloudGuard Dome9 synthesizes policy attributes from multiple cloud providers and multiple accounts/regions into one management pane to give you an inventory/asset management view of your entire environment. You can further analyze the security posture of any instance from multiple lenses (security policy view, IAM policy view, and GuardDuty findings view) to obtain a true holistic understanding of your network.

5. Mean Time Reduction For Incident Response

On average, it takes incident responders 200 days to detect breaches.

CloudGuard Dome9 allows you to quickly visualize and investigate network activity and traffic and generates intrusion alerts based on potentially unauthorized or malicious activity within your cloud environment. The visual exploration tool along with rich contextualized information are extremely useful to analyze short lived services like lambda functions and other cloud-native platform components.

6. Prevention Of Misuse Of Privilege

Enterprises need to ensure hackers don't obtain unauthorized privileges to launch unauthorized assets (ex. bitcoin mining).

CloudGuard Dome9 has full context of your account activity and the types of assets in your environment. Using CloudGuard Dome9 cloud security intelligence and the compliance engine, you have a baseline of assets that should be in use. If someone obtains unauthorized privileges to create blacklisted assets, CloudGuard Dome9 cloud security intelligence can detect such IAM changes and immediately provide detailed alerts.

7. Active Policy Enforcement

Enterprises need to ensure that only security admins are managing firewall rules/policies and prevent unauthorized changes to their environment.

CloudGuard Dome9 allows you to lock down security groups so unauthorized changes are tracked and configuration is reverted back to the gold standard config. This is especially valuable in environments when an unauthorized user, misconfiguration or buggy script by a developer that changes configuration and violates internal policy or compliance standards.

8. Non-Use Enforcement Of Foreign Regions

Customers have over 10 regions in the cloud that are typically not in use. Each region has its own management interface and configuration that is especially hard to manage consistently at scale.

CloudGuard Dome9 can ensure foreign and unused regions stay isolated and protect against attacks such as bitcoin mining, ensure data sovereignty, and mitigate shadow IT abuse.

9. Mitigation Against Compromised Credentials

Customers need to ensure compromised credentials of privileged users does not result in full account compromise, data hijacking, or large scale ransomware attacks.

CloudGuard Dome9 adds an extra layer of security to your most sensitive AWS services by providing just-in-time privilege elevation on an as-needed basis for select IAM actions. It's sudo for the cloud!

10. On-Demand Access To Cloud Servers/Services

Enterprises need to ensure to turn off port or IP access to services if they are not in use in order to prevent attacks (port-scanners, botnet etc).

CloudGuard Dome9 provides just-in-time access that let you lockdown servers and ports by default thereby reducing the overall attack surface of the service. Admins and Ops teams can get access to specific services for a pre-defined period of time, after which the ports are closed again.