Check Point
SOFTWARE TECHNOLOGIES LTD

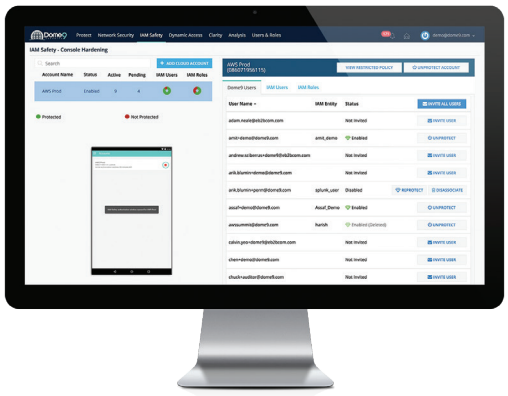
PRODUCT BRIEF

PRIVILEGED IDENTITY PROTECTION WITH CLOUDGUARD DOME9

PROTECTION AGAINST COMPROMISED CREDENTIALS AND IDENTITY THEFT IN THE CLOUD

In the software-defined world of the public cloud, it is critically important for businesses to protect cloud accounts and roles against compromised credentials and identity theft.

A compromised privileged user account can mean data theft, Domain Name System (DNS) hijacking, denied access for legitimate administrators, or worse. In the cloud, the traditional boundary of a network perimeter disappears, and Identity and Access Management (IAM) becomes the new security perimeter.



Businesses should follow best practices for effective IAM management, such as creating and using IAM users instead of the root account, enabling multi-factor authorization (MFA) for all users, and using IAM roles to share access for federated access scenarios. In addition, security teams need better tools to effectively manage IAM policy and protect against the worst-case scenario where a privileged user account gets compromised.

Privileged Identity Protection with CloudGuard Dome9 provides an additional layer of defense on top of native IAM in the cloud. Privileged Identity Protection offers offers better visibility and control over IAM users and roles, allowing administrators to easily manage granular permissions across their entire cloud environment. Privileged Identity Protection from CloudGuard Dome9 lets admin "lockdown" specific IAM actions in a cloud environment and requires privilege elevation to authorize these actions for a limited time. For example, a cloud administrator may disallow even privileged user accounts from deleting hosted zones in Amazon Route 53 without requesting just-in-time authorization via a mobile device. Think of Privileged Identity Protection from CloudGuard Dome9 as sudo for the cloud.

KEY FEATURES

- Granular control over IAM users, roles and actions
- Access management based on Principle of Least Privilege (POLP)
- Second level, out-of-band authorization from a mobile device for restricted actions
- Admin Support for ad-hoc IAM authorized permission elevation for users through the CloudGuard Dome9 web console
- Federated access management for enhanced security protection
- Audited tamper protection from suspicious user activity

DIFFERENTIATION

- Enhanced layer of defense to existing public cloud IAM services
- Access restriction of IAM users and roles to contain blast radius
- On-demand, time-based authorization to minimize risk of compromised accounts
- Active protection over both cloud control planes and API
- Balance between seamless access and practical security

KEY BENEFITS

Minimal Impact from Compromised Credentials and Identify Theft

By restricting access to actions that can have a catastrophic impact on a cloud environment and requiring additional just-in-time authorization, Privileged Identity Protection minimizes potential harm caused by compromised credentials. When privileged users need to perform risky operations such as setting up encryption keys or DNS entries, Privileged Identity Protection issues a temporary elevated permissions lease. So even with knowledge of a privileged user account's password, attackers cannot perform certain restricted actions without access to the legitimate user's mobile device for two-factor authorization. Privileged Identity Protection from CloudGuard Dome9 protects companies from a multitude of attacks, including "man-in-the-middle" or "man-in-the-browser" attacks.

Access Restriction and Tamper Protection

CloudGuard Dome9 provides a complete view of all of IAM users and roles, offering the ability to strip access to critical actions from all users and roles. Administrators will still be able to perform these actions through just-in-time privilege elevation. When tamper protection is enabled, Privileged Identity Protection analyzes IAM users and roles for suspicious activity and notifies you when an unauthorized IAM operation is attempted. In essence Tamper Protection ensures that IAM policies are not compromised.

Quick and Simple Onboarding for Instant Protection

CloudGuard Dome9 is a flexible and transparent SaaS solution that doesn't require any proxies. With Privileged Identity Protection, you can harden your public cloud console and protect it against theft, man-in-the-browser attacks, and more. Simply start by creating a policy and deciding which IAM actions are considered risky. Then connect your public cloud account to CloudGuard Dome9 by selecting the accounts you want to protect in your cloud console. Finally, invite users to join and install the CloudGuard Dome9 application on their mobile devices. With these three simple steps, you now have enhanced security and peace of mind.

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

DCISPB12102018