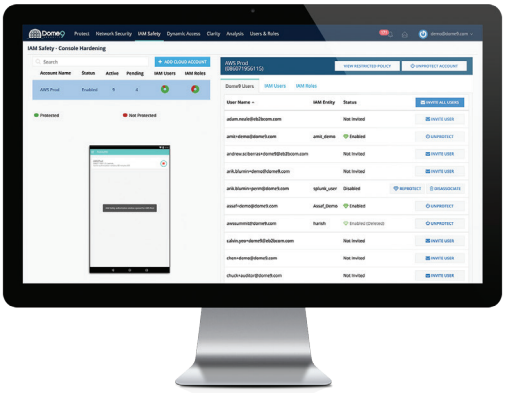
PRODUCT BRIEF

DOME9 IAM SAFETY

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 authentication (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.

Dome9 IAM Safety provides an additional layer of defense on top of native IAM in the cloud. IAM Safety offers better visibility and control over IAM users and roles, allowing administrators to easily manage granular permissions across their entire cloud environment. Dome9 IAM Safety lets administrators “lock down” 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 IAM Safety privilege elevation as *sudo* for cloud IAM accounts.

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
- 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, IAM Safety minimizes potential harm caused by compromised credentials. When privileged users need to perform risky operations such as setting up encryption keys or DNS entries, IAM Safety 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. Dome9 IAM Safety protects companies from a multitude of attacks, including "man-in-the-middle" or "man-in-the-browser" attacks.

Access Restriction and Tamper Protection

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, IAM Safety 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

Dome9 Arc is a flexible and transparent SaaS solution that doesn't require any proxies. With IAM Safety, 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 Dome9 Arc by selecting the accounts you want to protect in your cloud console. Finally invite users to join and install the Dome9 application on their mobile devices. With these three simple steps, you now have enhanced security and peace of mind.

ABOUT DOME9 SECURITY

Dome9 delivers verifiable cloud infrastructure security and compliance to all businesses at all times across all public clouds. The Dome9 Arc SaaS platform leverages cloud-native security controls and cloud-agnostic policy automation to bring comprehensive network security, advanced IAM protection and continuous compliance to every public cloud environment. Dome9 offers technologies to assess security posture, detect misconfigurations, model gold standard policies, protect against attacks and insider threats, and conform to security best practices in the cloud. Businesses use Dome9 Arc for faster and more effective cloud security operations, pain-free compliance and governance, and Rugged DevOps practices. Learn more at www.dome9.com

---

CONTACT US
Dome9 Security, Inc.
701 Villa Street
Mountain View, CA 94041 USA
+1–877-959-6889
www.dome9.com
contact@dome9.com

For a free security assessment or trail, please contact:
US Sales: +1-877-959-6889
International Sales: +44-20-8144-0620

DIAMSPB05052017