Cloud Infrastructure Entitlement Management

Zero-Trust Identity & Entitlement

There are numerous factors that determine the effective policy of an asset in the cloud. As the cloud environment expands and new users and workloads are added, it is complicated to follow best practices for defining the security properties of those assets. As a result, DevOps teams often erroneously grant excessive permissions for cloud assets—expanding the attack surface. Traditional IAM tools, preconfigured permissions in developer settings, and manually configuring permissions do not keep up with what is needed to secure the cloud at DevOps speed and scale.

Organizations need Cloud Infrastructure Entitlement Management (CIEM) to automate and deploy least privilege based privilege models in order to reduce the attack surface and ultimately achieve zero trust.

Visualize, Detect, Prioritize, and Remediate IAM Risks

With Check Point CloudGuard, optimize user and workload access and privilege management to ensure you have the perfect dose of permissions, and quickly implement recommendations for over permissive roles. CloudGuard provides you with visibility of effective permissions, and identify over permissive entitlements, suggest remediation.

Check Point CloudGuard CIEM Technology for Optimized User and Workload Access and Privilege Management:

With CloudGuard you will gain visibility into the effective permission of users and assets and gain recommendations on over permissions. You can then easily achieve a path to least privilege entitlement.

CloudGuard CIEM technology helps you identify manage permissions by:

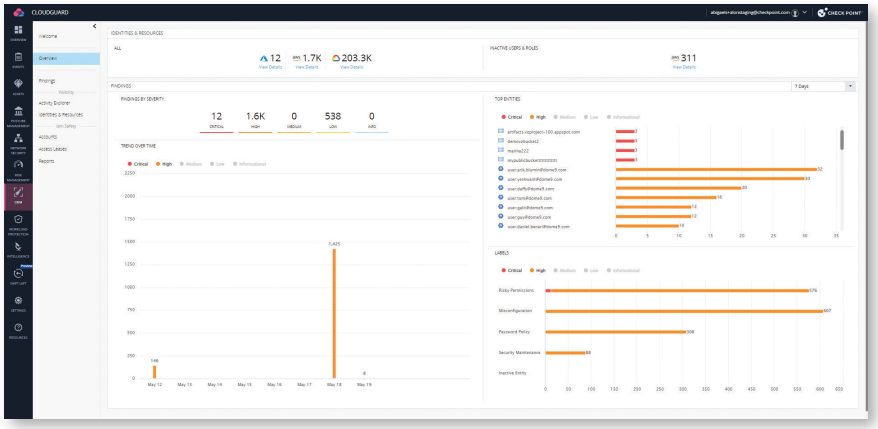
- Visualizing effective permissions of users and cloud services
- Detecting unused roles, over-permissions and risky entitlements that can put you at risk
- Automatically generating least privilege roles recommendations based on actual usage

Understand Your Permissions & Enforce Least Privilege Across Your Clouds

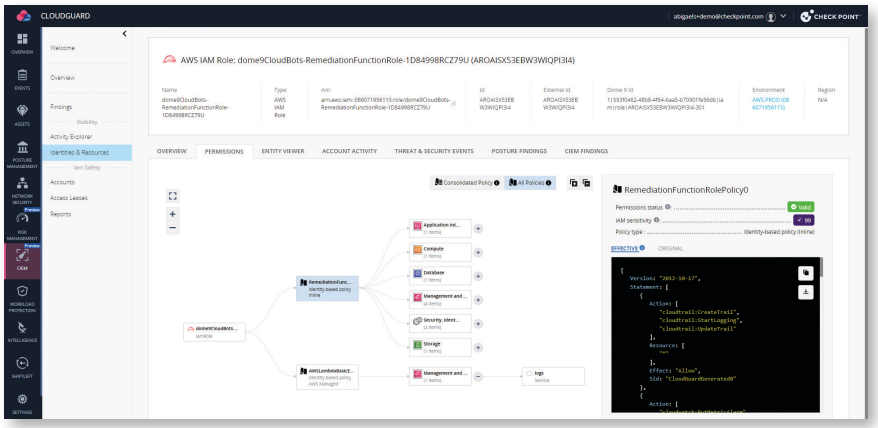
Understand the actual effective permissions of users & cloud services, identify exposure and risks and automatically generate explicit least privilege role recommendation to reduce access and revoke unused permissions.

Eliminate the Complexities of Entitlement Management to Reduce Risk

CloudGuard's CIEM capabilities remove the complexities involved in remediating misconfigured identities and entitlements. By automatically calculating the effective policy for any asset, and by automating the enforcement of least privilege access, CloudGuard reduces the attack surface for users.



CloudGuard's CIEM uses machine learning to analyze account activity logs to detect anomalies and suggest the correct policy settings to ensure least privilege access.



CloudGuard's CIEM Enables Organization To:

- Reduce TCO
- Automate remediation of identity risk
- Auto-enforce least privilege access
- Gain visibility into entitlements through machine learning analyzed permission paths
- Apply best practice least privilege politics that DO NOT impact functionality
- Eliminate the need to manually search for and remove redundant user accounts

Unified Security, Built to Reduce Risk in the Cloud

The CIEM capabilities are part of the unified cloud native security tools provided in CloudGaurd. Check Point understands that unification is a means to an end which is why our CIEM feeds into the Effective Risk Management engine, which combines all of the outputs from the posture management, vulnerability & malware scanning and CIEM, to provide each risk with a score based on the business's architecture and priorities. CloudGuard then produces business-centric risk remediation prioritization for security teams, to ensure security optimization.

More Context, Actionable Security, Smarter Prevention

From **code to cloud**, Check Point CloudGuard delivers **automated** cloud native security, unified across your applications, workloads, and network to **manage risk, maintain posture, and prevent threats**, in context, at cloud speed and scale. CloudGuards prevention-first approach protects applications and workloads throughout the software development lifecyle, and includes an effective risk management engine, with automated remediation prioritization, to allow users to focus on the security risks that matter. For more information on CloudGuard, visit **www.checkpoint.com/cloudguard**

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com