CHECK POINT

CloudGuard CNAPP

This Privacy Data Sheet explains how Check Point's Cloud Native Application Protection Platform ("CloudGuard CNAPP") processes personal data.

About CloudGuard CNAPP

CloudGuard CNAPP is an integral component of the CloudGuard Cloud Native Security platform, enabling you to prevent threats and prioritize risks across your cloud applications, networks, and workloads. CloudGuard CNAPP object-mapping algorithms integrate cloud inventory and configuration details with real-time monitoring data from multiple sources, such as VPC Flow Logs, CloudTrail, Amazon GuardDuty, AWS Inspector, and Check Point's Threat Cloud feeds. The result is contextualized information utilized within the CloudGuard platform to enhance visualization, querying, intrusion alerts, and policy violation notifications.

How Does Check Point Comply With Applicable Data Protection Regulations?

At Check Point, ensuring customer privacy and security remains our foremost concern, with the trust our customers place in our services being one of our most valued assets.

- **Security.** As a leading AI-powered, cloud-delivered cyber security platform provider over the past decades, we acknowledge the significance of implementing rigorous security measures to safeguard our customers' information. For more details, visit our Information Security Measures Policy.
- **Privacy by Design.** We operate under the principle of privacy by design. This means that we prioritize the protection of personal data and privacy throughout the entire lifecycle of our products and services. We treat personal data with the utmost care. Our commitment to privacy is reflected in our policies, procedures, and the way we do business. For more details, visit our Privacy Policy and our Trust Point.
- **Disaster Recovery.** We maintain comprehensive plans and procedures for disaster recovery and business continuity.

- **Transfers.** In order to regulate the transfer of personal data between the Check Point entities, Check Point has adopted an intercompany agreement for transfers of data between its various Check Point entities, including the EU Standard Contractual Clauses and UK International Data Transfer Addendum to the EU Standard Contractual Clauses. Check Point's U.S. subsidiary, Check Point Software Technologies, Inc. (and its subsidiaries) has self-certified its compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (DPF).

What Types Of Personal Data Does CloudGuard CNAPP Process?

CloudGuard CNAPP may process the following data:

- Basic personal data, including name, username and corporate email address.
- Metadata extracted from AWS/Azure CloudGuard Intelligence, including source IP, destination IP and the protocol used.
- Logs derived from API calls, including names, usernames, corporate email addresses, and records of actions performed by specific usernames.
- Audit logs and alerts (which may include personal information such as names, usernames, corporate email addresses, unique identifiers assigned to users within a system, IP addresses, login times, action details (Information on what specific actions users performed).
- Workload data for AWP SaaS scanning. Such data may include user's metadata (network traffic, events, system activity etc.), IP address, timestamps of access, etc. Such data is scanned for vulnerabilities and deleted immediately

Why Does CloudGuard CNAPP Process Data?

CloudGuard CNAPP processes data to deliver comprehensive cloud security and risk management across your cloud environments. By analyzing data from cloud applications, networks, and workloads, it can:

- Identify Vulnerabilities: Detect misconfigurations and security gaps in your cloud infrastructure.
- Prevent Threats: Monitor for malicious activities and potential threats in real-time.
- Prioritize Risks: Assess and rank risks to help you focus on the most critical security issues.
- Automate Security Policies: Enforce consistent security policies across all cloud assets.

- Processing data allows CloudGuard CNAPP to provide visibility and control over your cloud environment, ensuring that your applications and workloads remain secure from development through deployment.

For more information on the purposes for which we process personal data, please visit our Privacy Policy.

What is the Duration and Frequency of Processing?

Data is shared with CloudGuard CNAPP throughout the subscription term.

What are the Retention Periods?

Data Type	Retention Period
Basic personal data (name, username and corporate email address)	Subscription term. Additional retention periods vary based on the purchased license: 1 month, 3 months, 6 months, or 1 year.
Metadata extracted from AWS/Azure CloudGuard Intelligence	Retained for the subscription term. An extended retention period can be purchased as an optional paid add-on.
Logs derived from API calls	Retained for 1 year
Alerts	Retained for 1 year
Audit Logs	Retention duration varies per preference – 6 months or 1 year. For Microsoft Azure – 3 years.
Workload data for AWP SaaS scanning	Such data is scanned for vulnerabilities and deleted immediately

Where Is Personal Data Stored?

Personal information is stored on AWS Cloud Hosting Service. The hosting locations available are: United States, Europe, Australia, India, Canada, and Singapore. The location is selected per customer's choice during the onboarding process.

Sub-Processors

Check Point engages third-party Sub-processors in connection with the provision of the Check Point's products and services. The list of Sub-processors is available at our Sub-Processors Page.

Privacy Options

We provide the following tools, empowering our customers to select their data and privacy preferences:

- Control and customize user access to data across their cloud environments.
- Track logging and monitoring of user activities. This helps in auditing access patterns, detecting unauthorized access attempts, and demonstrating compliance with regulatory requirements.
- Create secure zones where only authorized users can access sensitive data.
- Grant temporary access controls to users for specific tasks or time frames, reducing the risk associated with long-term permissions.

Authorized Access To Personal Data

Customer Access

Access to data is controlled by customer's selected administrators. Only users authorized by the administrators can access data. All access and any action taken by administrators or by their authorized users are fully logged.

Check Point Access

Data contained within the customer's CloudGuard CNAPP environment may be accessed by Check Point's support and R&D teams for troubleshooting and security purposes. Such access is granted only to those authorized representatives for which the access is necessary to perform their intended functions. Any access to specific customer data by Check Point personnel requires prior approval.

Information contained in this data sheet is for awareness only, may be modified, and does not constitute legal or professional advice or warranty of fitness for a particular purpose. This Privacy Data Sheet is a supplement to Check Point's Privacy Policy. Please visit it for more information on how Check Point collects and uses personal data.

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

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com