THREATCLOUD AI

Privacy Data Sheet

This Privacy Data Sheet explains how Check Point's ThreatCloud AI solution ("ThreatCloud AI") processes personal data.

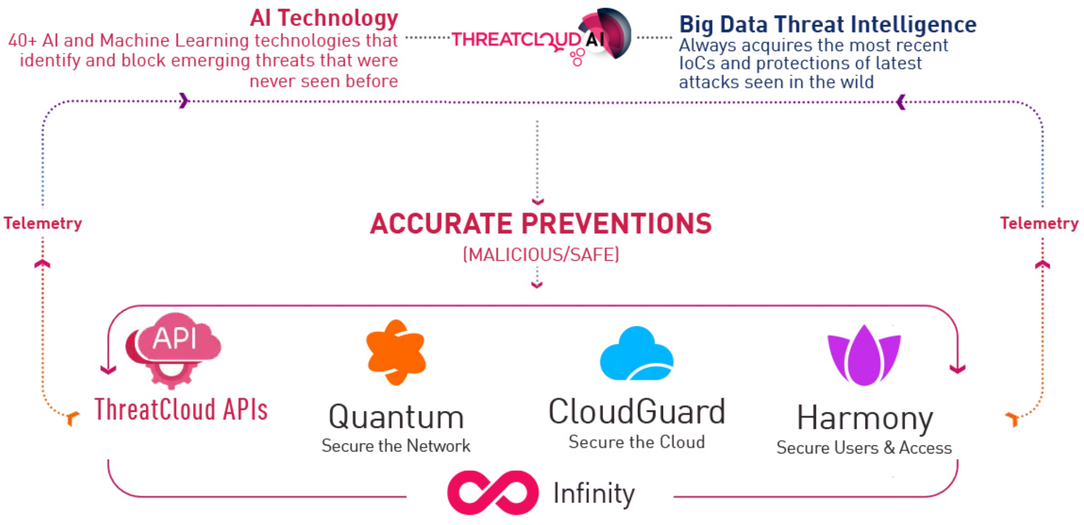
About ThreatCloud AI

ThreatCloud AI is a cybersecurity system based in the cloud, that leverages the latest AI technologies, big data threat intelligence and the industry's leading cyber researchers to prevent Zero-Day attacks.

ThreatCloud AI seamlessly connected to all IT environments via Check Point's Quantum, Harmony and CloudGuard product lines - covering network, endpoints, email mobile and cloud, ensuring comprehensive protection across organizational infrastructure. ThreatCloud AI analyzes billions of files, websites, URLs, and other resources per day, providing the security to over 100K customers globally.

ThreatCloud AI proliferates Threat Intelligence globally in milliseconds, so that attacks found in one location will immediately be blocked all over the world.

For more information visit our ThreatCloud AI site


AI Technology
40+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before
THREATCLOUD AI
Big Data Threat Intelligence
Always acquires the most recent IoCs and protections of latest attacks seen in the wild
Telemetry
ACCURATE PREVENTIONS
(MALICIOUS/SAFE)
Telemetry
API
ThreatCloud APIs
Quantum
Secure the Network
CloudGuard
Secure the Cloud
Harmony
Secure Users & Access
Infinity

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.

1. **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.
2. **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.
3. **Disaster Recovery.** We maintain comprehensive plans and procedures for disaster recovery and business continuity.
4. **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 the various Check Point entities, including the EU Standard Contractual Clauses and UK International Data Transfer Addendum to the EU Standard Contractual Clauses. 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 ThreatCloud AI Process?

ThreatCloud AI integrates within various Check Point's products, collecting and processing data that customers have previously shared and stored within these products.

This data may include:

- File content (in case file is uploaded to ThreatCloud for inspection via Threat Emulation or Threat Extraction)
- File metadata – for example file name, file type, source IP, file path
- URLs
- Domains
- IPs
- Partial web page content – for example, title, copyright, favicon, links, HTML code.
- Customer identifier (for example, Customer ID).
- Device identifier
- In cases where ThreatCloud AI processes email traffic data, specific email-related information may be captured to help detect, analyze, and respond to potential threats. This data may include, email subject, sender and recipients' data.

Why does ThreatCloud AI Process Data?

ThreatCloud AI processes and stores data for well-defined scenarios to provide customers with product functionality and to ensure a high level of service.

In the processing stage ThreatCloud AI will inspect content to classify it as benign or malicious in order to prevent malware, phishing and other cyber-attacks.

What is the Duration and Frequency of Processing?

Data is shared with ThreatCloud AI throughout the subscription term.

What are the Retention Periods?

DATA TYPE	RETENTION PERIOD
Files that are classified as benign	Approximately 5-6% of the files are randomly retained in an encrypted format for a period of five days, while all other files are deleted immediately.
Files that are sent for text extraction	10 minutes
URLs that are classified as benign	1 year
Domains classified as benign	1 year
IPs classified as benign	1 year
Files, URLs, Domains IPs and HTMLs classified as malicious	Data is retained for 10 years solely for cybersecurity purposes (files are stored in encrypted format). In specific instances, certain malicious data may be retained longer if deemed valuable for cybersecurity analysis.

**For partial web page content classified as benign or metadata, the processed data is not intended to contain personal data. However, in certain instances, personal data may be unintentionally included and retained for up to 2.5 years.

Where does ThreatCloud AI Store Personal Data?

ThreatCloud AI runs on Amazon Web Services in several sites. Data will be uploaded by Check Point's products configurations and policies and will be processed in the same region in which it was uploaded to.

After classification processing is finished, inspected files and file metadata will be retained in the same region to which it was uploaded and processed. Data may be copied to other regions for the purpose of security research and debugging – this is mostly a manual process done by authorized personnel only, normally for malicious content analysis.

Web security data such as URLs, domains and IP addresses may be transferred globally for the purposes of cyber-security defense, security enhancement, monitoring and providing service functionality.

Available regions are:

SERVICE	REGIONS
File Security/Threat Emulation/ Threat Extraction	EU, United States, Canada, UAE, India, Australia, and UK
Web, Domain, URL, and IP security	EU, United States, Canada, UAE and India
Metadata for all security services	EU

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.

Authorized Access to Personal Data

Data and metadata may be accessed by Check Point's support and R&D teams for security research, monitoring, and quality assurance. Such access is granted only to those authorized representatives for which the access is necessary to perform their intended functions.

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