CHECK POINT™

Quantum

Quantum Threat Prevention Privacy Data Sheet

This Privacy Data Sheet explains how Check Point's Quantum Threat Prevention solution process and storage personal data.

About Quantum Threat Prevention

Quantum Threat Prevention includes various software blades, each providing distinct network protections. Together, they deliver the industry's leading Threat Prevention solution. Powered by ThreatCloud AI — the intelligence core behind all of Check Point's products — this advanced cybersecurity solution uses AI and big data threat intelligence to prevent cyber-attacks.

Quantum Threat Prevention services are provided in three product packages:

1. NGFW package: This package includes the following Threat prevention blades:

   - IPS – Intrusion Prevention System, designed for robust defense against harmful and undesirable network traffic. This blade focuses on vulnerabilities in applications and servers, as well as attacks "in the wild" by exploit kits and malicious attackers.

2. NGTP package: This package includes all protections from the NGFW package, along with the following additional blades:

   - Anti-Virus – Provides prevention for malware at the gateway. This protection communicates with ThreatCloud AI and integrates several other prevention engines to analyze indicators.
   - Anti-Bot – Offers post-infection protection, primary scans outbound traffic to prevent evidence of compromises such as Command and Control (C&C) traffic. The Anti-Bot protection communicates with ThreatCloud AI to analyze indicators.
   - URL filtering – Allows granular control over which websites can be accessed by a given group of users, computers, or networks. URL Filtering can control access to entire websites or specific pages within a website.

3. SNBT package: This package includes all protections from the NGFW and NGTP packages, along with the following additional blades:

    - Threat Emulation – Analyzes files and executes them in a virtual sandbox to identify malicious behavior. The Emulation service leverages the power of Check Point's ThreatCloud AI that processes millions of parameters collected from runtime behaviors to detect the newest threats.
    - Threat Extraction – Delivers clean and reconstructed versions of potentially malicious files that are received by email or downloaded from the web. Maintaining uninterrupted business flow, while emulation continues in the background, Threat Extraction eliminates unacceptable delays created by traditional sandboxes, offering a practical prevention-first strategy that blocks malicious content, such as active content and embedded objects, from reaching users at all.
    - Zero Phishing – Blocks both unknown zero-day and known phishing attacks on websites in real-time, leveraging machine-learning algorithms and inspection technologies.

For the rest of the blade see this data sheet:

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).

How does Check Point Comply with Applicable Data Protection Regulations?

Package	Protection	Data Processed
NGTP	IPS	Data processing occurs locally on the gateway. Malicious incidents with IPs, domain, URL, ports and Metadata are sent for storage
	Anti-Bot	Domains and metadata are uploaded for processing to ThreatCloud AI
	Anti-Virus	File Hashs and metadata are uploaded for processing to ThreatCloud AI
	URL-Filtering	1 year
SNBT	Threat Emulation	Files and metadata are uploaded for processing to ThreatCloud AI for inspection 2 years
	Threat Extraction	
	Zero Phishing	URLs, website content and metadata are uploaded for processing to ThreatCloud AI

Metadata may include:

- File metadata – File name, File type, source, file hash
- URLs that can be extracted from files
- URLs
- IPs
- Domains
- Web page content – titles, copyright, favicon, links, HTML code, text
- Customer identifier
- Device identifier
- Email subject, sender and recipient (where applicable)
- Network traffic data (where applicable)

Why Does Quantum Threat Prevention Process Data?

Quantum Threat Prevention processes data to analyze and identify malicious content and to prevent attacks and zero-day threats. During processing some data may be sent to Check Point's ThreatCloud AI for inspection.

After classification data may be used for the purpose of security research, improving Check Point's security engines, providing product functionality such as logs and dashboards, system monitoring, debugging and product quality.

What is the Frequency and Duration of Processing?

Data is shared with Quantum Threat Prevention throughout the subscription term.

What are the Retention Periods?

Package	Protection	Retention Period
NGTP	IPS	Data of malicious events: IPs, domains, URLs, ports and Metadata are retained for 5 years
	Anti-Bot	Data is uploaded to ThreatCloud AI, see ThreatCloud AI Privacy Data Sheet for more information about the retention periods
	Anti-Virus	
	URL-Filtering	
SNBT	Threat Emulation	
	Threat Extraction	
	Zero Phishing	

Where does Quantum Threat Prevention Store Personal Data?

Personal information is stored on AWS Cloud Hosting Service. By default, the region is determined using geolocation logic, which is based on the customer's location, proximity and availability of data centers. However, there is an option to configure the gateways to use a specific region by customer's choice. See ThreatCloud AI for Privacy Data Sheet for more information about data that was uploaded to it.

The available regions are:

Protection	Available Regions
Anti-Bot	EU, United States, Canada, UAE, India and UK
Anti-Virus	EU, United States, Canada, UAE, India and UK
Threat Emulation	EU, United States, Canada, UAE, India, Australia and UK
Threat Extraction	EU, United States, Canada, UAE, India, Australia and UK
Zero Phishing	EU, United States, Canada, UAE, and India
URL-Filtering	EU, United States
IPS	EU

In the event of a data center failure, automatic failover is activated to an alternate data center, determined by proximity. (Note: Choosing a specific data center location (e.g., within the EU) will disable data center failover functionality.

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:

- Preferable region. Customers may choose the region to which data will be uploaded and processed by ThreatCloud AI
- Adjustable blades. Every blade may be turned off/on to allow full control of your organization's environment.
- Enabling statistical data. Customers may enable or disable sharing of their statistical data pf malicious events of the IPS blade

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