CHECK POINT

Quantum
Threat Prevention

This Privacy Data Sheet explains how Check Point's Quantum Threat Prevention solution processes 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 web-based protection, using machine learning technology. It 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 domain and URLs can be accessed by a given group of users, computers, or networks. Using machine learning technology and categories URL Filtering can control the access to entire websites or specific pages within a website.

© 2025 Check Point Software Technologies Ltd. All rights reserved.

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

- Threat Emulation – A comprehensive file security service that scan files statically and dynamically 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 web based attacks and techniques in real-time, leveraging Check Point's patented machine-learning algorithms and inspection technology.

The blades referenced in this privacy data sheet pertain specifically to Quantum Threat Prevention.

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).

© 2025 Check Point Software Technologies Ltd. All rights reserved.

What Types of Personal Data Does Quantum Threat Prevention Process?

Blade	Data processed
IPS	IPS data is processed locally, by the Customer, on the gateway, and no data is transmitted to Check Point. If a malicious event occurs, the following additional data will be uploaded to ThreatCloud AI: Domains, URL, Account ID, Source IP, Country, and Industry.*
Anti-Bot	The following data is uploaded to ThreatCloud AI for processing: Domains, and File Hash. If a malicious event occurs, the following additional data will be uploaded to ThreatCloud AI: URL, Account ID, Source IP, Country, and Industry.*
Anti-Virus	The following data is uploaded to ThreatCloud AI for processing: File hash. If a malicious event occurs, the following additional data will be uploaded to ThreatCloud AI: Domains, URL, Account ID, Source IP Country, and Industry *
URL-Filtering	The following data is uploaded to ThreatCloud AI for processing: Domains
Threat Emulation	The following data is uploaded to ThreatCloud AI for processing: File itself, File name, File type, File hash, URLs extracted from the file, Domains, Email Metadata, and Account ID
Zero Phishing	The following data is uploaded to ThreatCloud AI for processing: URLs, Website content (titles, copyright, favicon, links, HTML code, text), and Account ID.
Threat Extraction	Threat Extraction data is processed locally, by the Customer, on the gateway, and no data is transmitted to Check Point.

The information shown in the table above contains both personal and non-personal data.

* The information in the table above outlines the default data uploaded to ThreatCloud AI when a malicious event occurs. Customers may choose alternative settings for handling malicious event data, including:

- Disabling the upload of additional data
- Anonymizing any additional data that is uploaded

© 2025 Check Point Software Technologies Ltd. All rights reserved.

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.

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 Quantum Threat Prevention throughout the subscription term.

What are the Retention Periods?

Protection	Retention Period
IPS	Data of malicious events: Device ID, IPSIPs, Domains, URLs, Ports, File hash, Country, and Industry are retained for 5 years (local gateway).
Threat Extraction	Threat Extraction data is processed locally, by the Customer, on the gateway, and no data is transmitted to Check Point.
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	
Threat Emulation	
Zero Phishing	

Where does Quantum Threat Prevention Store Personal Data?

The data 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 Privacy Data Sheet for more information about data that was uploaded to it.

© 2025 Check Point Software Technologies Ltd. All rights reserved.

The available regions are:

Protection	Available Regions
IPS	EU
Anti-Bot	EU, U.S, Canada, UAE, India, Singapore, and UK
Anti-Virus	EU, U.S, Canada, UAE, India, Singapore, and UK
URL-Filtering	EU, U.S, and Singapore
Threat Emulation	EU, U.S, Canada, UAE, India, Singapore, Australia, and UK
Zero Phishing	EU, U.S, Canada, UAE, India, Singapore, Australia, and UK

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:

- Regional preferences. Customers can select the region where data is uploaded and processed by ThreatCloud AI.
- Configurable blades. Each blade can be activated or deactivated to provide control over an organization's environment.
- Statistical data sharing. Customers have the option to enable or disable sharing of statistical data regarding IPS blade malicious events.
- Threat Prevention can be used with local Sandblast or Private ThreatCloud appliances.
- Customers can configure how additional data is uploaded if a malicious event occurs; data may be uploaded, anonymized, or not uploaded at all.

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.

© 2025 Check Point Software Technologies Ltd. All rights reserved.