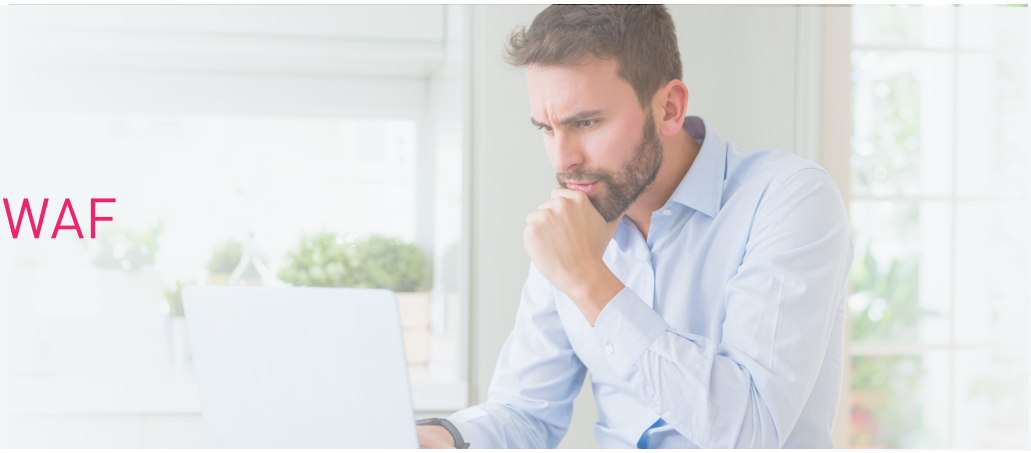
Check Point WAF



This Privacy Data Sheet explains how Check Point' Web Application Firewall ("WAF") processes personal data.

About Check Point WAF

Check Point WAF leverages artificial Intelligence (AI) to provide web application firewall and API Protection. By integrating AI with IPS signatures, it offers protection against both known threats and zero-day exploits. The AI engine continuously adapts to your application's behavior, monitoring adjustments across the application's lifecycle. This results in a low rate of false positives and reduces the need for frequent rule adjustments following each application update.

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

© 2024 Check Point Software Technologies Ltd. All rights reserved.

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 Check Point WAF Process?

- **Identifiers used to identify users' interactions with Check Point WAF:** Typically including: IP addresses, HTTP headers and HTTP custom fields (these can contain user agent strings, referring URLs, and other data). However, it is important to note that the state machine generated from this data does not contain any personally identifiable information.

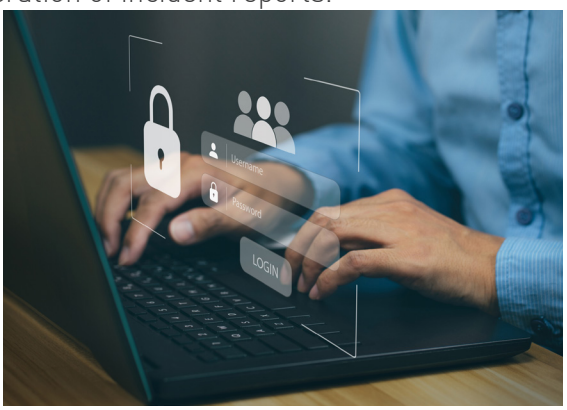
- **Personal data extracted from logs:** Check Point WAF analyzes log information about detected security events. If your web application processes personal information, these logs may also contain such data.

Important clarification: WAF inspects logs to detect security events. However, you have the option to configure local logging, ensuring that data remains within your infrastructure and is not shared with Check Point.

Why Does Check Point WAF Process Data?

Check Point WAF processes personal data to enhance the security and performance of web applications by:

- Detecting and mitigating threats: by analyzing incoming and outgoing traffic, Check Point WAF identifies and blocks potential threats.
- Continuous learning and adaptation: Check Point WAF use data to continuously learn and adapt to evolving user activity and threat landscapes, improving the ability to detect and prevent new and sophisticated attacks.
- Logging and monitoring: Logs produced and handled by Check Point WAF are utilized for tracking security events and incidents, including the generation of incident reports.
- Performance optimization: by understanding traffic patterns and user behavior, Check Point WAF can optimize the performance and availability of web applications, ensuring a better user experience.



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

© 2024 Check Point Software Technologies Ltd. All rights reserved.

What is the Duration and Frequency of Processing?

Data is shared with Check Point WAF throughout the subscription term.

What are the Retention Periods?

DATA TYPE	RETENTION PERIOD
Identifiers used to identify users' interactions with Check Point WAF	7 days
Personal data extracted from logs concerning detected security events	1 year*

*After your subscription ends, your data is retained for 30 days, during which you can retrieve it. After this period, the data will be deleted.

Where Is Personal Data Stored?

Personal data 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 your 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:

- Check Point WAF inspects logs to detect security incidents. However, you have the option to configure local logging, ensuring the data remains within your infrastructure and is not shared with Check Point.
- Check Point WAF can be configured to minimize the processing of information that could be directly linked to an individual. You have the option to configure traffic conditions to either suppress logs with the "Suppress Logs" action in custom rules or to disable logging altogether

© 2024 Check Point Software Technologies Ltd. All rights reserved.

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 Check Point WAF 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.

© 2024 Check Point Software Technologies Ltd. All rights reserved.