Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

Check Point Cloud Service Security Statement

Customer privacy and security is top priority at Check Point. Your trust in Check Point's services is our most important asset. This document outlines our policies and safeguards that we enforce in our cloud services and data centers, to ensure your organization's data is safe with us.

Check Point Cloud Services

Check Point provides the following cloud-based services:

ThreatCloud

In 2012, Check Point established ThreatCloud, the first collaborative security infrastructure to fight cybercrime. ThreatCloud dynamically reinforces Check Point Threat Prevention Software Blades with real-time threat intelligence derived from Check Point research, global sensor data, industry feeds and specialized intelligence feeds from the ThreatCloud IntelliStore.

SandBlast Cloud Service

The SandBlast Cloud Service enables subscribers to send files for threat inspection with the use of Check Point Threat Emulation sandbox, and for sanitizing with the use of Check Point Threat Extraction. The Service is available to Check Point Security Gateways, to Check Point SandBlast Agent, to SandBlast Cloud, and to any entity directly subscribing to the service via the SandBlast API. Under the Services, by default, files are sent for emulation based on data center proximity and availability. The Service allows the users to select data centers in specific locations, so that emulations will be performed only in those geographic locations.

Capsule Cloud

Check Point Capsule Cloud provides security continuity to organizations. Capsule Cloud provides constant, up-to-date protection to mobile users outside of the enterprise security perimeter. Check Point Capsule Cloud also provides real-time protection against web threats by directing all mobile device traffic through a tunnel or proxy directly to the Cloud, where the data is then scanned against the security policy. Capsule Cloud offers protection by using Check Point Software Blades (including the IPS, Anti-Bot, Anti-Virus, Application Control and URL Filtering Software Blades) as a cloud-based service. Capsule Cloud ensures that the corporate policy of the aforementioned Software Blades is always enforced.

Check Point Data Center Locations

Check Point SandBlast Cloud service data centers are located in:

- Frankfurt, Germany
- San Jose, California, USA
- Tel Aviv, Israel

These data centers serve the ***SandBlast Cloud Service***, ***ThreatCloud*** **Service** and **Capsule Cloud** management, logging and databases.

Check Point **Capsule Cloud** enforcement points are located in data centers distributed globally and based on third-party hosting services.

There is an additional distribution layer in the ThreatCloud service that is based on third-party CDN (Content Delivery Network), to globally facilitate short response times.

Check Point cloud services provide global availability and redundancy. Each connecting host dynamically selects the best data center based on proximity and availability, with full failover between the data centers.

Selecting a Specific Data Center Location

SandBlast Cloud Service

By default, files are sent to emulation based on data center proximity and availability. The service supports the option to define a data center in specific locations, so that emulations will be performed only in those geographic locations.

ThreatCloud

ThreatCloud is a query platform providing gateways with up-to-date threat information for policy enforcement. It does not provide the ability for customers to define a specific data center location. ThreatCloud does not store customer information, unless the gateway is configured to share sensitive data with authorization. This configuration is fully controlled by the customer in the management dashboard.

Capsule Cloud

In the Capsule Cloud management, customers may choose to be served by Capsule Cloud enforcement gateway in a specific data center location. Capsule Cloud traffic will not go through the excluded gateways. In this case, policy enforcement takes place only in the gateways chosen by the customer.

Data Center Security Controls

This section describes the security controls which Check Point enforces across its cloud-service data centers to protect customer data.

Network and Communication Protection

- All communications to Check Point cloud services are fully encrypted and authenticated using high standard cryptographic protocols.
- All service clients perform server validation to prevent man-in-the-middle attacks.
- Perimeter firewalls are deployed with strict policies to protect all hosts within the data center.
- Internal firewalls are deployed to segregate traffic between application and database tiers, and to enforce the principle of Least Privilege between hosts within the data center.

Access Control

- Access to Capsule Cloud Management and Logging, SandBlast Cloud and ThreatCloud data centers is restricted to a select group of authorized and fully vetted personnel.
- Two-factor personalized authentication is required for any administrative access.
- Role-based access control is enforced for access to all data center systems.
- Access control to all systems is centrally managed.
- Passwords of network equipment are managed through enterprise management tools.
- Access to systems and data is logged and monitored.
- Access rights and privileges to specific employees are closely monitored by Check Point security teams.

Service Availability Control

- Redundant systems and networks are deployed across servicing components.
- Load balancing ensures service availability in case of component failure.
- DRP: In case of data center failure, automatic failover is deployed to an alternate data center. (Note: Selecting a specific data center (for example, in EU) will cause the loss of data center failover functionality.)
- The customer account: policy, users, logs and configurations are stored in redundant locations.
- Check Point enforces internal policies to control the retention of backup data. All data is backed up at each data center, on a rotating schedule of incremental and full backups.

Education, Penetration Testing and Security Reviews

- Employees are trained in the corporate security policy.
- Routine security reviews and penetration tests are performed.
- Any findings or violations are handled promptly.

Physical Security

Check Point deploys an array of measures to ensure the physical safety of its Capsule Cloud Management, SandBlast Cloud and ThreatCloud data centers.

- 24x7 manned security, including foot patrols and perimeter inspections.
- CCTV surveillance cameras with motion detection are deployed throughout the data center facility.
- All facilities are equipped with an alarm system.
- Physical access to the data center facility is limited to a select group of authorized and fully vetted personnel. All access is logged and monitored.
- The data centers are located in dedicated rooms at purpose-built facilities.
- The data center buildings are engineered to withstand local seismic, storm, and flood risks, based on local regulations.
- Although we do not seek certification, we strive to replicate the standard of ISO/IEC 27001.

Environmental Controls

The data center facilities utilize the following environmental controls:

- Humidity and temperature control
- Back-up cooling system
- Smoke detection

Power Management

The data center facilities utilize the following redundant environmental controls:

- Uninterruptable Power Supply (UPS) system
- Power distribution units (PDUs)
- On-site generators

Information Collection and Usage

This section details which information may be sent to Check Point cloud servers and how it is used and stored by us.

ThreatCloud

The following information may be sent by Check Point gateways to ThreatCloud:

Signature Queries by Threat Prevention Software Blades

The Anti-Virus, Anti-Bot, URL-Filtering and Application-Control software blades send web domain-names and cryptographic hash digests of inspected files to ThreatCloud.

All information is sent anonymously without attribution to the customer's or the gateway's identity.

To maximize customer privacy, only domain names are sent to ThreatCloud and not full URLs. A query for a domain name retrieves the database portion relevant to that domain and sends it to the gateway. Subsequently, enforcement for full URLs is processed locally on the gateway, not in ThreatCloud.

Anti-Virus, Anti-Bot Enforcement Log Sharing

The Anti-Virus and Anti-Bot blades may share enforcement logs with ThreatCloud. The logs are shared anonymously and are used by Check Point for statistical analysis.

The shared logs do not contain private customer data such as internal IP addresses, gateway IP, etc.

Customers may enable or disable sharing of this statistical information with ThreatCloud through SmartConsole settings.

Threat Emulation Appliance Malicious Detection Sharing

Threat Emulation appliances may send anonymous cryptographic hash digests of detected malicious files to ThreatCloud.

Threat Emulation appliances may also send malicious files detected by Threat Emulation.

Customers can enable or disable sharing of Threat Emulation information with ThreatCloud through SmartConsole settings.

Sharing Statistics for IntelliStore Tracking

Customers using IntelliStore may opt-in to view statistics in their user-center account. If this option is selected by the customer, information shared with ThreatCloud is not anonymous and is associated with the customer account.

SandBlast Cloud Service

File Sending

Subscribers of the SandBlast Cloud Service are able to configure their gateways to send files for emulation to the cloud-based service.

Through the SmartConsole policy, customers can control which network traffic to be monitored and what file types to be sent to the service by their gateways.

Handling Non-Malicious Data Files and Documents (excluding Executable files)

Non-malicious data files and documentation are always deleted immediately after emulation is complete. Information about the files is never stored by Check Point.

Handling Malicious Files and All Executable Files

The following actions are performed on files that are detected by the Service as malicious and on non-malicious executable files:

- Malware Research
  Files may be stored by Check Point to enable vulnerability research. The files are made available to designated Check Point security researchers, for in-depth threat analysis of infected files. Files and customer information are not shared with anyone outside the select group of designated Check Point personnel, unless explicitly agreed to by the customer.

- Sharing File Hash with ThreatCloud
  A cryptographic hash signature of files that are detected as malicious and of non-malicious executable files may be shared with ThreatCloud. This feature facilitates the sharing of new emerging vulnerabilities in order to allow Check Point gateways that are connected to the ThreatCloud service to detect and block malicious files.

File Persistence

Non-malicious data files and documents received by the SandBlast service are deleted at the end of the emulation and are not stored by Check Point. In addition, virtual machines are reset every 5-10 minutes to facilitate complete data elimination.

Capsule Cloud

Logs

Logs are automated records of events, in a given scope, for audit trail and diagnostics. Through this service, we analyze information generated by a user's traffic. Logs are automatically generated by the service and are influenced by the specific security policy and user's activity (generated traffic). Every few seconds, all logs are gathered from all of the active gateways. The transition of logs between our cloud gateways is done by secured communication through an encrypted tunnel.

The log files are kept in a secured space segregated from other tenants, for at least 30 days. If the "log transport agent" is chosen when the copy is downloaded, the original log will not be deleted from Check Point servers.

User Identity

The Active Directory Synchronizer synchronizes users in an Active Directory environment with a database in the Check Point Cloud. Only the user's email is uploaded and kept in the Capsule Cloud database, as a part of the Management Gateways. We do not scan or save any other user entity attributes. Emails serve as unique identifiers. Check Point does not use or share these emails with any third parties. In certain scenarios, system messages can be sent to specific users from our system. The administrator has full control to enable or disable all email messages. If the user entity is either disabled or deleted from the Active Directory, the email address is removed from the cloud database.

Cookies

Check Point may have to use a limited number of cookies that are essential to our services. Without these cookies, the management portal would not work properly.

Analytic cookies

Analytic cookies help us understand how our management portal is used, to enable us to improve the user experience. For example, the anonymous information can tell us what interests our visitors the most, or if any errors are present on the site.

Check Point may also use cookies to save customer settings and to remember preferences (such as: language preference, order of lists, search filters).

Social networking cookies are never used.

Website Tracking

Third parties are not allowed to collect personally identifiable information directly from visitors of our website. Furthermore, we do not respond to 'do not track' signals or similar mechanisms.

Disclosure to Third Parties

Check Point may use third-party components or services as part of the Capsule Cloud product. We may share some information and traffic with a third party as part of this service, but it will never contain identifying information. Check Point does not rent, sell, or lease personal information to other companies or individuals.

Disclosure for Compliance

Check Point may disclose personal information if it has a good faith belief that such disclosure is required by law or necessary to (1) conform to legal requirements or comply with legal process served on Check Point or this website; (2) protect and defend the rights or property of Check Point and this website; (3) enforce its agreements with the customer, or (4) act in urgent circumstances to protect personal safety or the public.

Note: Check Point's privacy policy describes Check Point's treatment and control of personal information obtained from our website, user center and mobile apps. Check Point reserves the right to change the security features of this service from time to time at its sole discretion.