PRIVATE THREATCLOUD®

CHECK POINT PRIVATE THREATCLOUD

Up-to-date threat intelligence and product updates for isolated and/or highly regulated environments

Product Benefits

- Maintains the highest security posture on air-gapped networks by enforcing advanced Threat Prevention technologies fueled with real-time intelligence
- Implements efficient, flexible, and controlled distribution of intelligence based on organizational needs
- Controls delivery of product updates for networks of any size, including large networks and MSSPs
- Maintains absolute privacy with one-way data-syncing, ensuring no data or queries exiting the defined perimeter

Product Features

- Delivers real-time automatic security updates to offline gateways for SandBlast Network, SandBlast Agent, SandBlast Mobile and CloudGuard.
- Allows complete control and flexibility in accessing and fetching the real-time Threat Intelligence from Check Point ThreatCloud™
- Enables efficient distribution of updates across large distributed networks
- Unidirectional communication assuring data from the private network does not get exposed to the internet

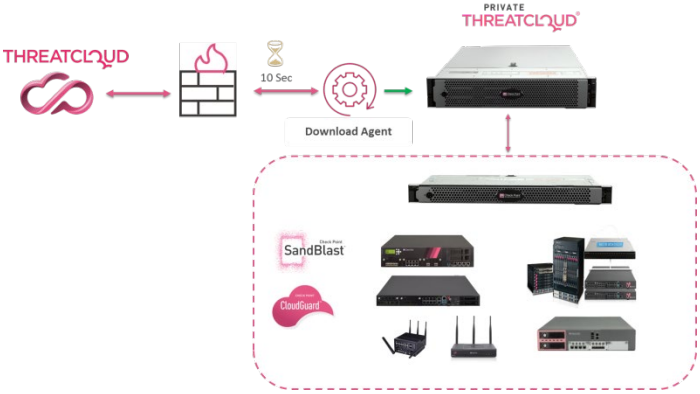
In today's constantly evolving threat landscape, keeping products up-to-date and obtaining intelligence to stay ahead of the latest emerging threats is critical to every organization. Industries that require organizations to abide by extremely stringent security regulations face a unique challenge. How do they remain isolated but also implement the most up-to-date protections against evolving threats?

While isolated environments are inherently harder to breach, malware can still successfully enter secluded ecosystems through the efforts of highly motivated hackers and the unintentional actions of users with authorized access. Thousands of new malware variants are created every hour, making manual protection update processes impractical. Given this pace of new malware development, offline environments are vulnerable to attacks without real-time threat intelligence and the most current versions of threat prevention products.

SOLUTION

Check Point Private ThreatCloud™ brings the best security to highly regulated, isolated and offline networks by bringing threat intelligence, software updates, and patches to offline environments, while ensuring that data stored and processed stays within the perimeter. Private ThreatCloud allows customers to host and fully control their own private node of ThreatCloud enabling full control and maximum privacy of intelligence delivery to gateways implementing Check Point threat prevention technologies.

For organizations that operate in industries with tight policy requirements, Private ThreatCloud is a key component in preventing attacks from known and unknown threats. With Private ThreatCloud, Check Point enables organizations to maintain the highest security posture in isolated environments by pushing regular and real-time product updates, even when running in air-gapped environments. The controlled delivery of intelligence and updates provides a flexible management infrastructure which enables MSSPs and organizations with large numbers of gateways to efficiently manage the process of updating these devices.



THE OFFLINE CHALLENGE

Offline environments harbor the most sensitive and strategic data and services, providing ample motivation to sophisticated attackers to find ways to inject infections in the isolated network. APT adversaries use novel techniques to penetrate these highly protected networks. Initial infection could occur through a process glitch, lax security control, an internal user, usage of an infected USB drive, etc. In a typical attack, malware is initially injected into an internal trusted system, and spreads laterally to its strategic destination. This kind of attack often takes advantage of both known and unknown vulnerabilities. Due to the very nature of being offline, these environments don't have access to up-to-date threat intelligence. Until now, it has been impractical to implement security controls such as IPS, AV and Anti-bot in these environments at the pace required to truly safeguard the established perimeter.

TIMELY INTELLIGENCE

Check Point ThreatCloud™ is a public cloud-based data repository that feeds security gateways, endpoints and mobile security agents, as well as mobile and cloud security platforms with real- time security intelligence. ThreatCloud analyzes more than 3 billion threat indicators every day, as well as the largest set of IPS signatures in the industry.

AUTOMATIC SECURITY UPDATES

To maintain robust protection, organizations must ensure that security software is updated with the latest releases and patches to maintain a defensive stance against attackers. Check Point Private ThreatCloud enables software update distribution through the Check Point Upgrade Service Engine (CPUSE) for offline environments, allowing organizations to efficiently maintain controlled delivery of updates to IPS, antivirus, anti-bot, URL Filtering, and application control.

EFFICIENT DISTRIBUTION

Through Private ThreatCloud, large organizations and MSSPs can plan and deploy product updates and patches in a controlled manner, allowing efficient distribution of new intelligence and software updates to best meet their needs.

UNIDIRECTIONAL DATA FLOW

The on-premises hardware appliance assures unidirectional updates such that information is only able to enter the protected environment, while not allowing data to leave the established perimeters.

FLEXIBLE DEPLOYMENT

Private ThreatCloud provides flexible deployment options to adapt to organizations' needs. The four main methods of deploying Private ThreatCloud include:

- On-board download agent
- Unidirectional DMZ
- Manual Sneaker net
- Unidirectional data diode

PRIVATE THREATCLOUD SPECIFICATIONS

Private Threat Cloud brings the powerful, robust resource of Threat Cloud to private networks and isolated customer networks.

SERVICES	
Service	**Description**
Site / URL Reputation Database	Real-time reputation queries from Check Point Antivirus, Anti-Bot, and URL Filtering
Package Updates	Update package requests for IPS, Application Control, Anti-Bot, and Local SandBlast appliances
Check Point Update Service Engine	Check Point gateway software update queries
Custom Threat Indicators	File hashes detected by local SandBlast appliances are added as custom threat indicators for serving Antivirus

DEPLOYMENT OPTIONS	
Load Balancing Options	**Description**
Single-Box	• Private ThreatCloud is installed on a dedicated appliance. • The download Agent is installed on the same appliance as the private ThreatCloud.
Unidirectional	• Private ThreatCloud is installed on a dedicated appliance. • The download Agent is installed on a different appliance or VM and sends unidirectional updates to the Private ThreatCloud appliance. • Select this deployment if you do not want the Private ThreatCloud appliance to access the Internet directly.
Clustering	• ClusterXL/VRRP with state synchronization disabled. • Layer 2 connectivity between appliances hosting private ThreatCloud. • Use high-availability (HA) configuration.

UPDATE OPTIONS
Download Agent on Private ThreatCloud or local network Download Agent deployed in DMZ, with enforced unidirectional communication using: • Check Point gateway • Commercial third party data diodes • Manual data transfer from DA to Private ThreatCloud

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com

