CHECK POINT CAPSULE CLOUD

FEATURES

- Includes IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, and Threat Emulation
- Data centers located across the globe
- Supported on iOS, Android, Windows, and MAC platforms
- Single Sign-On (SSO)
- Logs can be pushed and stored locally or viewed online
- Active Directory integration for identity awareness

BENEFITS

- Extend corporate security policy to mobile devices
- Prevent download of suspicious files, access to malicious websites, and bot damages on mobile devices.
- Protect mobile users outside the enterprise security perimeter
- Extend Check Point security to remote offices without security appliances
- Real-time protection against web threats
- Apply a single security policy for both on premise and mobile devices
- Deliver the protection of Check Point Software Blades via a cloud-based service
- Always up to date and fully tuned software

CHALLENGE

Historically, organizations enforced corporate security policies to protect all devices and data within the traditional corporate network from being exposed to threats. Over the last several years, the traditional network has disappeared. Organizations have evolved, and are confronting a situation where business data is accessed from everywhere, and travels outside the network. The increased need for business continuity and the associated risks posed by mobile devices create a huge challenge for security professionals.

As more and more workers access corporate and business data remotely, new gaps are opened within the organization's infrastructure. Mobile devices expose users and organizations to new sources of attacks. Without knowing it, you may have accessed a malicious site, or downloaded a virus unintentionally. Security "blind-spots" like these expand as employees use mobile devices to consume business data from anywhere and everywhere they go.

With as many as 11.6 million mobile devices infected[1], organizations need to have the ability to provide the same level of protection for mobile devices and remote offices as they provide for devices within the confines of the corporate network perimeter.

SOLUTION

Check Point Capsule enables organizations to provide security continuity across their business operations, providing always-on, always up-to-date protection for mobile users outside the organization's security perimeter.

With Check Point Capsule, organizations are able to leverage protections from all Check Point Software Blades as a cloud-based service, protecting the network and their users from threats everywhere they go; preventing suspicious file downloads, blocking malicious websites, and stopping bots before they have a chance to cause damage.

Check Point Capsule offers real-time protections by directing all traffic from mobile devices through a secure tunnel to the cloud where corporate policy is enforced. A single policy can be applied for both on premise and off premise devices that is centrally managed through SmartDashboard or remotely through an intuitive web user interface for pure cloud deployments.

With 24/7/365 coverage by Check Point experts, and datacenters located around the globe, organizations can truly provide always on and always up-to-date protection for their entire network and users. Whether on premise or outside the enterprise security perimeter, organizations can ensure their assets, data, and devices are protected.

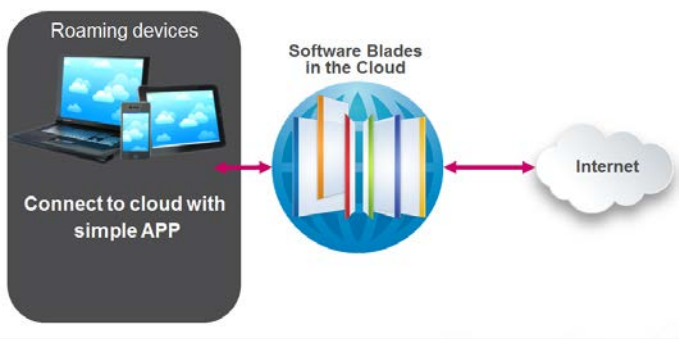
[1] Source: Kindsight Security Labs Malware Report 2014

Extend corporate security policy to mobile devices

Check Point Capsule enables organizations to extend the same policies from their corporate network to protect mobile devices and remote offices, wherever they are. With Check Point Security Management, organizations can manage mobile device policy in the cloud the same way they manage any other gateway, by simply adding a network object for the cloud to the relevant policy rule. Once the policy is implemented, it will automatically propagate to all on premise gateways and extend the corporate security policy to the cloud.

Protect mobile users outside the enterprise security perimeter

Check Point Capsule facilitates the use of devices on the go, whether they are iOS or Android tablets and smartphones, or laptops. All traffic from any roaming device is directed to the cloud service using a secure tunnel. No user data is sent in the clear. Each packet gets scanned for both inbound and outbound traffic to ensure it is safe for use.



Prevent access to malicious files, websites, and bot damages

With Check Point Capsule, organizations are able to leverage protections from all Check Point Software Blades as a cloud-based service, protecting the users and their network from threats everywhere they are. In addition to mobile users, remote offices can leverage the security service by connecting their local appliance to the cloud, extending corporate security without the need to deploy additional hardware.

Powered by Check Point ThreatCloud, up-to-date protections provided by IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, and Threat Emulation ensure that users and remote offices are protected from downloading malicious files, accessing risky websites, and stop bot communications before damage is caused.

Maintain full visibility with a single, integrated management platform

Check Point Capsule can be managed through Check Point Security Management, allowing for seamless integration into existing Check Point deployments.
Logs are sent from the cloud directly to Check Point Security Management, giving organizations centralized visibility of log activity.

Policies can also be managed from the intuitive web user interface. Available from any browser, the easy to use web user interface requires no extra license or installation. All logs are consolidated by the service and available from the web user interface, enabling full visibility and management of Check Point Capsule.

Seamless client installation and distribution

Check Point Capsule is easy to implement. Client installation supports Group Policy Object (GPO) distribution and Single Sign-On (SSO). Once installed, the client configures itself. There is no need for an administrator to configure it. Check Point Capsule integrates with active directory for identity awareness. In addition, the client is network aware, and able to disconnect itself when working within the corporate LAN.

Powered by Check Point ThreatCloud

Newly discovered threats are sent to ThreatCloud, which can then protect other Check Point connected gateways.
Each newly discovered threat signature is distributed to other Check Point connected gateways and the cloud to block the threat before it has a chance to spread. This constant collaboration makes the ThreatCloud ecosystem the most advanced and up-to-date threat network available.

SPECIFICATIONS

PROVIDED TECHNOLOGIES	
• IPS	• Anti-Bot
• Application Control	• Threat Emulation
• URL Filtering	• VPN (IPSec)
• Antivirus	

CLIENT PLATFORM SUPPORT	
• iOS	• Windows
• Android	• MAC

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim 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: 650-654-4233 | www.checkpoint.com