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 laptops 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. Laptops can 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 laptops to consume business data from anywhere and everywhere they go. Without knowing it, you may have accessed a malicious site, or downloaded a virus unintentionally.

Solution

Check Point Capsule enables organizations to provide security continuity across their business operations, providing always-on, always up-to-date protection for 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 laptops through a secure tunnel to the cloud where corporate policies are enforced. A single policy can be applied for both on premise and off premise laptops that is centrally managed through SmartConsole 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.
Extend corporate security policies to Windows and Mac laptops
Check Point Capsule enables organizations to extend the same policies from their corporate network to protect laptops and remote offices, wherever they are. With Check Point Security Management, organizations can manage policies 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 users outside the enterprise security perimeter
Check Point Capsule facilitates the use of Windows and Mac laptops on the go. All traffic 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.

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
- Application Control
- URL Filtering
- Antivirus
- Anti-Bot
- Threat Emulation
- VPN (IPsec)

CLIENT PLATFORM SUPPORT
- Windows
- Mac

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; 650-628-3000 | Fax: 650-628-2117 | www.checkpoint.com

© 2019 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March, 2019