Check Point* Capsule Cloud* Enhances Security for Mobile Users

Check Point's cloud-based cyber security services help organizations address increasing cyber risks resulting from increasing numbers of mobile users.

Overview

Over the last several years, the boundary lines around traditional networks have disappeared. The dramatic increase in the use of mobile technology has caused the network to evolve, and organizations are confronting a situation where business data is accessed from everywhere and is used and stored outside the network.

The increased need for business continuity and the associated risks posed by mobile users create a huge challenge for network security professionals. As more and more workers access corporate and business data remotely, new gaps are opened within the organization's infrastructure. These mobile users can expose organizations to new sources of attacks. Without knowing it, a user may have accessed a malicious site, or downloaded a virus unintentionally and then bring that into the organization when they next work at a company facility.

To help protect enterprise assets, Check Point Software Technology,* an Intel® Network Builders ecosystem member, has launched Capsule Cloud,* a cloud-based cyber security service, leveraging Intel architecture-based servers to help protect mobile users outside an enterprise security perimeter.

The Challenge

Companies are embracing smart, mobile devices (mobile phones, tablets, and laptops), leveraging the ubiquitous computing power and connectivity to dramatically increase employee efficiency and effectiveness. However, these new smart mobile devices also have the potential to give hackers many new opportunities to steal corporate or personal data or disrupt business, vital services, and infrastructure.

Corporations are facing this challenge today as the threat level has increased, exposing their laptop-using remote and traveling workers. In a 2017 survey of 1,900 IT professionals in large US companies conducted by Check Point,[1] data loss emerged as the main mobile security concern with 65% of those surveyed. Other concerns include lost or stolen devices (61%), users downloading unsafe apps or content (59%), and unauthorized access to corporate data and systems (56%).

The Solution

Check Point, leveraging Intel technology, has developed a cloud-based service called Capsule Cloud to provide comprehensive, multi-layer protection features to users working outside of the security-enabled enterprise perimeter.

Capsule Cloud leverages network functions virtualization (NFV) to offer Check Point's security protections as a virtual network function (VNF)-based cloud service running on Intel architecture-based servers. With Capsule Cloud, organizations can
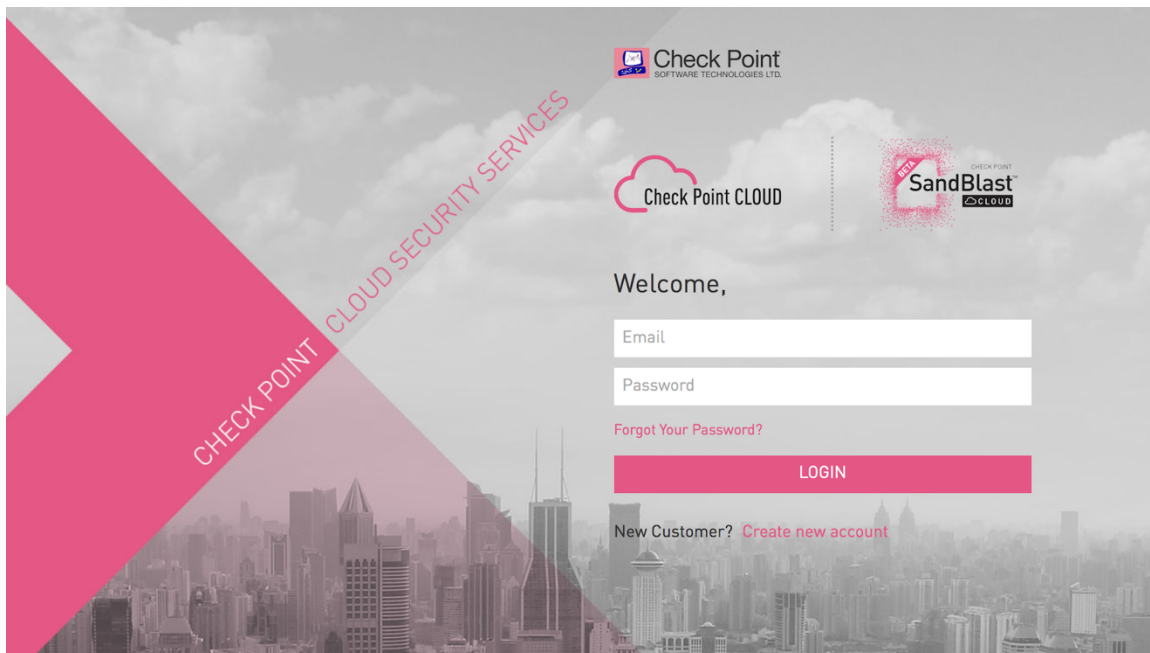
Figure 1. Capsule Cloud log in screen[2]

seamlessly extend advanced security policies to mobile employees to block downloads of suspicious files, deny access to malicious websites, and thwart bot damage.

Capsule Cloud is network security delivered as a service using apps on the mobile device to direct user traffic through purpose-built cloud servers via a security-enabled tunnel. These servers running Check Point virtual security gateway appliances inspect each data packet to ensure that advanced cyber security policies are enforced.

Capsule Cloud also benefits from Check Point's ThreatCloud centralized threat intelligence database and service. ThreatCloud continuously evaluates newly discovered threats and pushes out the latest threat signatures to all Check Point security gateways and cloud users to help prevent threats from spreading and propagating throughout the enterprise.

Capsule Cloud Features

- Multi-layer advanced threat prevention functions, including intrusion prevention system (IPS), application control, URL filtering, antivirus (A/V), anti-bot, and threat emulation and extraction (sandboxing technology)

- Data centers located across the globe providing worldwide access

- Logs can be pushed to the cloud for online viewing or stored locally

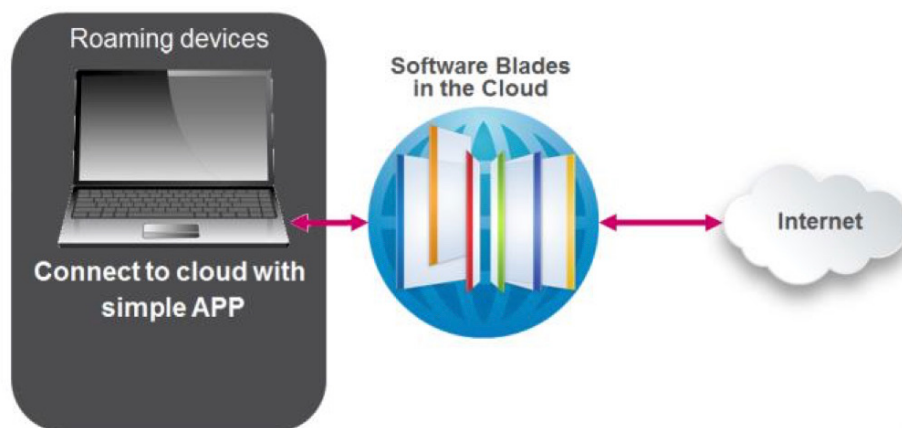- Active directory integration for identity awareness and single sign-on (SSO)

Figure 2. Check Point Threat Prevention Architecture

Capsule Cloud is deployed using Check Point's multi-layer Threat Prevention Architecture, which virtualizes Check Point's security gateway and management system, enabling it to run on an Intel architecture-based server located in the cloud. Each security layer runs independently as a layer with central management that allows a customer to customize protections by turning the protection layer on or off via a web-based interface based on the needs of the enterprise. In addition to powering cloud-based services, Check Point Threat Prevention Architecture can also be deployed on premises using physical Intel processor-based servers to bring additional security features to enterprise environments and applications.

A fundamental/basic component for Capsule Cloud is the use of industry standard servers that can run Linux* or Windows* operating systems. Thus, Check Point software is optimized for Intel architecture-based servers based on the Intel® Core™ i processor family and the Intel® Xeon® processor family. Some of the key CPU features that are critical to Capsule Cloud performance include:

- Receive side scaling: RSS (also called multi-queue distribution) shares all the receive data processing for a TCP connection across multiple processors or processor cores for efficient cache utilization.
- CPU-level threat detection: This feature facilitates the use of application programming interfaces to aid with threat emulation and extraction.
- Intel® Virtualization Technology (Intel® VT): Intel VT is a collection of Intel technologies and features that provide a hardware assist to the hypervisor virtualization software to eliminate virtualization performance overhead and improve security. Intel VT includes CPU, memory, I/O, graphics, security, and networking virtualization support.
- Multi-core architecture – The Capsule Cloud Threat Prevention/Security gateway software is designed to scale up in performance linearly with increased compute resources. Intel's multi-core CPUs, which range from 4 cores to 22 cores, provide the performance that allows Check Point to achieve outstanding performance and throughput in the cloud.

Check Point will soon introduce a version of Capsule Cloud for Internet of Things (IoT) sensors built into industrial, security, and enterprise systems that need cyber security protection.

Conclusion

Check Point Capsule Cloud provides a comprehensive advanced threat prevention-enabled solution for an enterprise's computing infrastructure that is increasingly mobile and located outside of the enterprise perimeter. With performance delivered by Intel architecture-based servers, Capsule Cloud enables organizations to extend and enforce their security policies everywhere without impacting network throughput or employee productivity.

About Check Point Software

Check Point Software Technologies Ltd. (www.checkpoint.com) provides industry-leading solutions and protecting customers from cyberattacks with a very high catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises— from networks to mobile devices—in addition to comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

About Intel Network Builders

Intel Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software-defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.