CHECK POINT CLOUDGUARD CONNECT

NETWORK SECURITY AS A SERVICE

Closing branch security gaps to protect against Gen V attacks

Benefits

- Latest and always up-to-date security
- Elastic and scalable
- Under 50 milliseconds latency with global presence
- Redundant links ensure 99.999% uptime
- APIs automate on-boarding new sites
- GRE or IPsec tunnels ensure privacy

As enterprises increasingly move their on-premises branch office workloads and applications to SaaS applications, they are adopting Software Defined Wide Area Networking (SD-WAN) to intelligently route traffic directly to cloud services using local broadband and to the datacenter using existing MPLS lines.

However, connecting branch offices directly to cloud services using a local Internet breakout significantly increases their security risk, as the branches are no longer protected by centralized data center security. This exposes branch offices and the enterprise WAN to sophisticated multi-vector Gen V attacks. A new approach to branch office security that is agile, cost-effective, easy to maintain and always up to date with the latest security is needed.

It's time to rethink how security is delivered to remote branch offices.

CLOUD-DELIVERED THREAT PREVENTION

Check Point CloudGuard Connect is a cloud-hosted network threat prevention service offering a maintenance-free, comprehensive, affordable security solution for remote sites and branch offices. CloudGuard Connect seamlessly delivers the latest and most comprehensive cyber security available, protecting branch offices from the latest generation of targeted and advanced cyber threats.

CloudGuard Connect doesn't burden IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments. With a simple and easy setup process, network traffic from existing SD-WAN edge devices are tunneled to a primary cloud-based network security service at a near-by location. A second connection provides redundancy. This ensures branch offices stay connected and removes the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

PREVENT ZERO-DAY THREATS

Check Point provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. Check Point protects SaaS, IaaS and now branch office assets from sophisticated threats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks.

Unlike other solutions that only detect threats, Check Point prevents threats. Check Point SandBlast Zero-Day Protection is a cloud-hosted sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters the network.

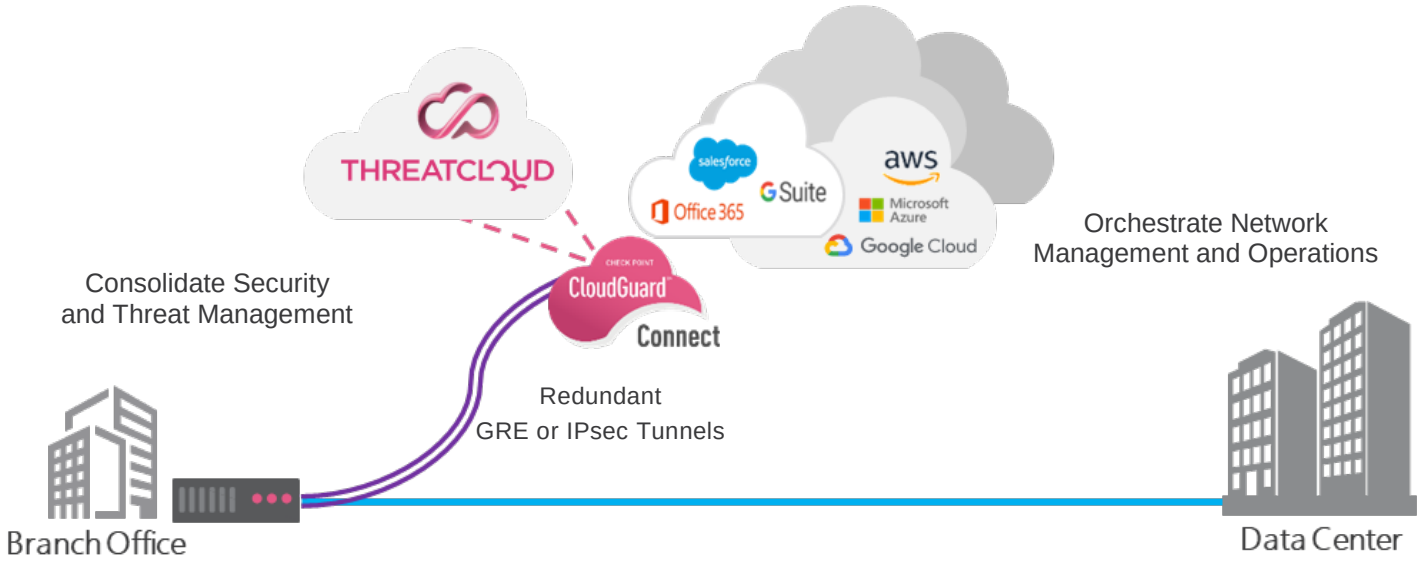
Malware is detected during the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. This innovative solution combines cloud-hosted CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

The Check Point solution also includes Application Control and URL Filtering to enforce safe web use. IPS, Anti-Bot and Antivirus protect customers from known threats. HTTPS inspection safeguards companies from threats trying to hide inside encrypted HTTPS channels.

Furthermore, Check Point is a fully consolidated and connected cyber security architecture protecting on premises, cloud and branch networks as well as endpoint and mobile devices from advanced persistent threats. Threats identified on one device can be automatically propagated as an IoC (Indicator of Compromise) to protect branch, mobile and cloud-hosted assets from the same zero-day threat.

CLOUD NATIVE ARCHITECTURE

Cloud Connectors: entry points for all IPsec or GRE tunnels into the cloud infrastructure, Cloud Connectors are grouped in clusters across different datacenters offering redundancy and elasticity. Connecting to a near-by location ensures low latency. **Cloud Gateways**: cloud delivered security enables separate policies for each subscribed tenant where capacity automatically expands as demand increases. Hardware or software updates are completely transparent, providing maintenance-free security. **Web Portal**: adding sites, setting site-wide security policy and viewing logs and reports is easy with the web portal. The Infinity cloud portal is also integrated with SaaS, a CASB solution protecting SaaS and other cloud-hosted assets.



SIMPLE AND INTUITIVE WEB MANAGEMENT

Simplified central management provides an intuitive, simple on-boarding process, security policy configuration and monitoring. Powered by Check Point SmartEvent see the most important threats with a single view across the entire infrastructure. Take control of security events with real-time forensic and event investigation, compliance and reporting. Respond to security incidents immediately, reducing the time spent remediating incidents.

OPTIMIZE WAN SECURITY

CloudGuard Connect has been fully tested and integrates with leading SD-WAN vendors. The solution enables flexible, automated service chaining from SD-WAN platforms to CloudGuard Connect to optimize traffic to the Internet and cloud applications. The initial configuration of automated service chaining can be centrally managed. Application security policies are defined once and programmed to all sites in contrast to the branch firewall security model requiring device-by-device management. Centralized management not only reduces the time to deploy and IT resource costs but also provides more consistent policies, reducing risk across the enterprise.

SPECIFICATIONS

Cloud Services	
Branch-to-Site connection	IPsec IKEv1, IPsec IKEv2 or GRE tunnels
Redundant availability zones	Yes
Availability regions	US South-East, US North-East, US South-West, US North-West, Canada, Italy, Germany, France, Sweden, Ireland, United Kingdom, Hong Kong, South Korea, Singapore, Japan, Australia, India, Brazil, Bahrain and South Africa
Multiple branch IP	Yes
Dynamic branch IP	Yes

Software	
Security	Outbound network firewall, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, and SandBlast Threat Emulation (sandboxing)
Latency	up to 50 milliseconds[1]

Performance	
Single IPsec tunnel	Up to 870 Mbps per tunnel

Management	
Cloud-host web-based management	Yes
On-premises R80 Security Management	Yes

Branch Edge Device	
SD-WAN	Aruba, Aryaka, Citrix, Silver Peak, VMware
Other	Generic, Microsoft Azure Firewall Manager

1. the expected additional latency for a branch in the same CloudGuard Connect region

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