CHECK POINT CLOUDGUARD EDGE

VIRTUAL SECURITY GATEWAY

Closing Branch Security Gaps to Protect against Gen V attacks

Benefits

- Lightweight VM designed for WAN Edge
- 1 GB of memory, 1 GB of disk, 1 CPU core
- Automated sites on-boarding
- Cloud and Enterprise management options
- Support inbound and outbound traffic inspection
- Maintain privacy and compliance

Cyber criminals are getting smarter, leveraging highly sophisticated attacks, and adapting their tactics to exploit any weakness to ultimately achieve their goals. How do you secure branch offices that are at remote locations and are not staffed by the same IT or security experts that you have at your headquarters site?

Large organizations need a branch office security solution that is affordable, agile, and manageable at scale to close the branch office security gap.

SOLUTION

CloudGuard Edge is a small footprint virtual security gateway with advanced threat prevention that can be centrally deployed and managed within minutes, making it an ideal security solution for branch offices. CloudGuard Edge integrates with leading branch office network vendors to provide comprehensive threat-prevention security, zero-day protection, agile delivery, management and automation across Software-defined WAN (SD-WAN) and uCPE deployments.

Companies with large numbers of remote branch offices get industry-leading protection, accelerated delivery of new services, and reduced operating and capital expense costs. Customers have full control of security policy and data, satisfying privacy and regulation requirements.

VIRTUAL FIREWALL

CloudGuard Edge is a lightweight virtual image of the Check Point Branch Office Security Gateway. It's a small footprint, requiring only 1 GB of memory, 1 GB of disk storage and 1 CPU core. Power on the virtual security gateway and within a minute, your branch office is protected.

CHECK POINT ADVANCED THREAT PREVENTION

Check Point provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. Check Point security products 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 your 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 from known threats. HTTPS inspection safeguards 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 your branch, mobile and cloud-hosted assets from the same zero-day threat.

CENTRAL MANAGEMENT

Customers also have two central management options; cloud-hosted Security Management Portal (SMP) and R80 Security Management. Cloud-hosted Security Management Portal (SMP) streamlines provisioning, maintenance and security policy and event management of tens of thousands of devices. Automating firmware updates and backups and setting security policy plans for common groups of CloudGuard Edge virtual security gateways greatly simplifies security management. CloudGuard Edge sends security logs to the SMP's central log repository. With the pre-defined central reports customers can easily see Infected Hosts, Prevented Attacks, Detected Attacks and Attack Trends.

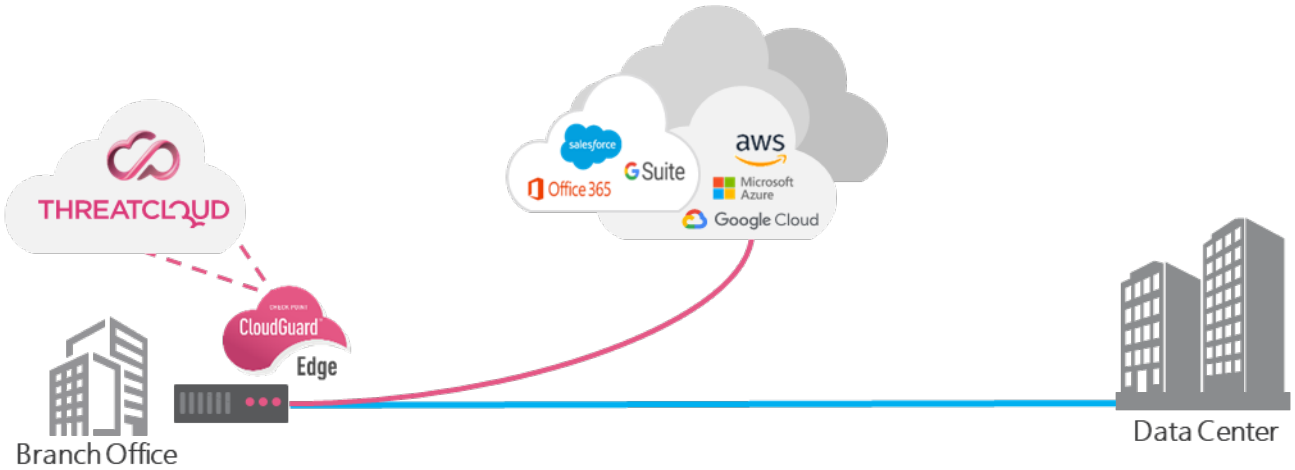
The other management option is the Check Point enterprise R80 Security Management product, the same product that manages Check Point integrated Next-Generation Threat Prevention security gateways on-premises at headquarters and in public and private clouds. This option leverages existing security management infrastructure and provides more granular security policy control. Bringing CloudGuard Edge security logs into Check Point SmartEvent along with security events from other Check Point security gateways, endpoint and mobile devices greatly simplifies threat management. The pre-defined views and reporting highlight the most important events, reducing response times.

INTEGRATION WITH SD-WAN

CloudGuard Edge security gateways are deployed through the SD-WAN management console. This tight integration reduces deployment time, effort, and costs. When CloudGuard Edge is deployed on SD-WAN or uCPE equipment, the CloudGuard Edge virtual security gateway is configured, automatically connected and ready to be centrally managed and monitored by the customer's domain in cloud-hosted SMP or the headquarters R80 Security Management.

OPTIMIZE WAN SECURITY

CloudGuard Edge has been fully tested and integrates with leading SD-WAN and uCPE equipment vendors as well as cloud-hosted services offered by carriers and Managed Security Service Providers. 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

Minimum System Requirements	
Memory	1 GB
CPU	1 core
Disk	1 GB

Software	
Security	Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus and SandBlast Threat Emulation (sandboxing)

Performance					
VMware SD-WAN	Edge 520v	Edge 620	Edge 640	Edge 680	Edge 840
Threat Prevention	100 Mbps	100 Mbps	350 Mbps	500 Mbps	550 Mbps

Note: VeloCloud requires the use of 2 vCores

Management	
Cloud-hosted	Security Management Portal (SMP)
On-premises management	R80.20 or higher

Branch Edge Device	
VMware SD-WAN	Edge 520v, 620, 640, 680, 840
Cisco Enterprise VNF	ENCS 5104, ENCS 5412
Citrix SD-WAN	1100

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