CHECK POINT
Network Security as a Service

CHECK POINT CloudGuard™ NSaaS

CloudGuard NSaaS
Gen V cyber security as a Service

Key Benefits

- Provides advanced threat protection to all remote sites and branch offices
- Always-on, up-to-date with the latest Gen V cyber-security
- Simple and easy 5 minute deployment process
- Reduces operational overhead and TCO
- Excellent SLA with very low latency service

Key Features

- Next Gen Threat Prevention
- Simplified web based management
- On demand automatic scaling
- Redundant zones with auto fail-over
- Sites located world-wide, connect to a site near you

CHALLENGE

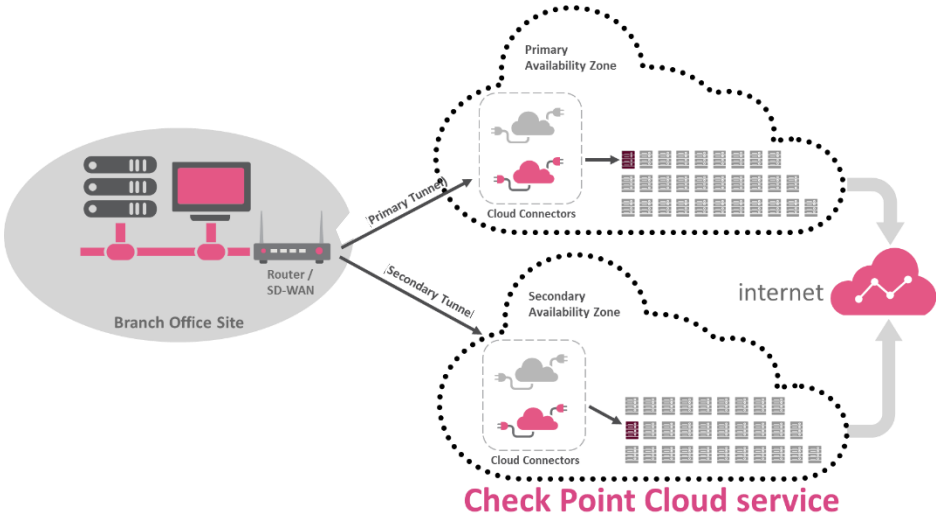
Your security landscape is changing. Protecting and maintaining traditional perimeter defenses, new cloud services, an increasingly mobile workforce and new Internet of Things (IoT) devices can put a strain on your IT staff. This digital transformation also provides threat actors with a larger attack surface to target. A new approach that is agile, cost-effective, easy to maintain and always up to date with the latest security is needed.

SOLUTION

CloudGuard Network Security as a Service (NSaaS) is a cloud security platform offering a maintenance-free, comprehensive, affordable security solution for small businesses, remote sites and branch offices. CloudGuard NSaaS seamlessly delivers the latest and most comprehensive cyber security available, protecting you against the latest fifth generation cyber-attack.

CloudGuard NSaaS doesn't burden your IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing SD-WAN deployments. With a simple and easy setup process, network traffic from your existing router or SD-WAN edge device is tunneled to a primary CloudGuard NSaaS. A secondary CloudGuard NSaaS provides redundancy. This ensures you stay connected and removes the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing your overall CAPEX and OPEX costs.

ARCHITECTURE



ARCHITECTURE COMPONENTS

Cloud Connectors: entry points for all IPsec or GRE tunnels into the cloud infrastructure, Cloud Connectors are grouped in clusters offering redundancy and elasticity natively. A pool of Cloud Connectors is available in each cloud region offering very low latency.

Cloud Gateways: dedicated instances of Check Point security gateways allocated to each customer, security gateway pools automatically expand as demand increases. In addition any hardware or software updates or maintenance is completely transparent to the end user, seamlessly providing the customer with the latest Check Point functionality.

Web Portal: a web portal where all configuration and security auditing is managed, the CloudGuard NSaaS portal is also integrated with CloudGuard SaaS, a CASB solution protecting your SaaS applications and cloud-based emails.

CHECK POINT INFINITY ARCHITECTURE

Check Point Infinity is the only fully consolidated cyber security architecture that provides unprecedented protection against Gen V mega-cyberattacks as well as future cyber threats across all networks, endpoint, cloud and mobile. For instance a threat identified on your network can be automatically propagated as an IoC to protect your mobile and cloud-based assets from the same zero-day threat.

ALL-INCLUSIVE SECURITY SOLUTION

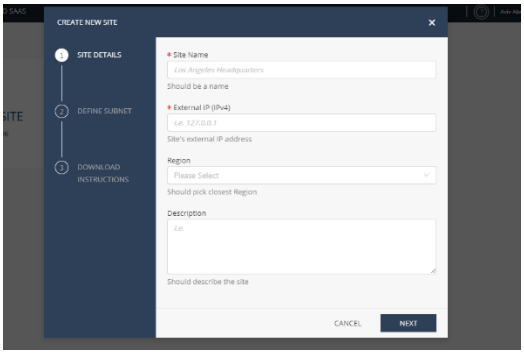
Check Point CloudGuard NSaaS offers a complete and consolidated security solution preventing sophisticated cyber-threats with SandBlast Zero-Day Threat Protection, Sandboxing, HTTPS Inspection, Application Control, Anti-Bot and Antivirus.

PREVENT KNOWN AND ZERO-DAY THREATS

CloudGuard NSaaS protects organizations from both known and unknown threats with Antivirus, Anti-Bot and SandBlast Threat Emulation (sandboxing). As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

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 you see the most important threats with a single view across your 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 you spend remediating incidents.



SPECIFICATIONS

- Outbound Network Firewall
- URL Filtering
- Application Control
- Intrusion Prevention
- Antivirus
- Anti-Bot
- Threat Emulation (sandboxing)
- SSL Inspection
- IPsec and GRE Tunneling
- Redundant Availability Zones
- SAML-based Identity Awareness (available at GA)
- Reporting Provides Security Visibility
- Availability Regions:
  US: South-East, US: North-East, US: South-West, US: North-West, Canada, EU: Germany, EU: Ireland, EU: United Kingdom, EU: France, APAC: South Korea, APAC: Singapore, APAC: Japan, APAC: Australia, APAC: India, Latin America: Brazil

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