nhc. CloudSecure™

Enterprises are increasingly moving their on-premise branch office workloads and applications to SaaS applications. They are adopting software-defined wide area networking (SD-WAN) to intelligently route traffic both 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 because 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 required.

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

Cloud-Delivered Threat Prevention

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

CloudSecure doesn't burden IT staff with deploying or maintaining dedicated hardware. It 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

NHC provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. NHC 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, NHC prevents threats. NHC SandBlast Zero-Day Protection is a cloud-hosted sandboxing technology that quickly quarantines and inspects files by running them in a virtual sandbox to discover malicious behavior before it enters the network.

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

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.

NHC's 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, we deliver a fully consolidated and connected cyber security architecture protecting on-premise, 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

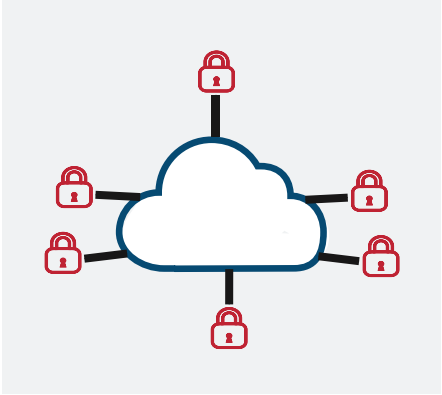
Cloud Connectors:
Entry points for all IPSec or GRE tunnels into the cloud infrastructure, Cloud Connectors are grouped in clusters across different data centers offering redundancy and elasticity. Connecting to a nearby location ensures low latency.

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. You'll be able to 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

EdgeSecure has been fully tested and integrates with leading SD-WAN vendors. The solution enables flexible, automated service chaining from SD-WAN platforms to CloudSecure 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 deployment time 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
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)
Performance	
Single IPsec Tunnel	Up to 870 Mbps per tunnel
Latency	Up to 50 milliseconds[1]
Management	
Cloud-Hosted Web Management	Yes
On-premises R80 Security Management	Yes
Branch Edge Device	
SD-WAN with automation	VMware, Other Generic

(1) The expected additional latency for a branch in the same CloudSecure region

CONTACT US: NHC Headquarters 200 Baker Avenue, Concord, MA 01742
855-600-4NHC | custservice@nhcgrp.com | www.nhcgrp.com