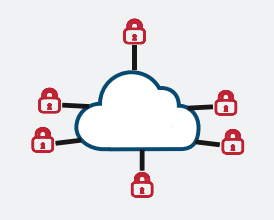
EdgeSecure™ With SD-WAN

Virtual Security Gateway

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 not staffed by the same IT or security experts that you have at your headquarters?

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

Solution



EdgeSecure with SD-WAN 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. EdgeSecure integrates with leading branch office network vendors to provide comprehensive threat-prevention security, zero-day protection, agile delivery, management, and automation across software-defined wide area network (SD-WAN) and universal customer premises equipment (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

EdgeSecure with SD-WAN is a lightweight virtual image of the NHC 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.

NHC Advanced Threat Prevention

NHC provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. NHC security products protect 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 your network. Malware is detected during the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox.

Closing Branch Security Gaps to Protect Against Gen V Attacks

Benefits

- Lightweight VM
- 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

EdgeSecure | Datasheet

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 NHC 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, NHC is 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 indicator of compromise (IoC) 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 EdgeSecure virtual security gateways greatly simplifies security management. EdgeSecure sends security logs to the SMP's central log repository. With the predefined central reports, customers can easily see infected hosts, prevented attacks, detected attacks, and attack trends.

The other management option is the NHC enterprise R80 Security Management product, the same product that manages NHC 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 EdgeSecure security logs into NHC SmartEvent along with security events from other NHC security gateways, endpoints, and mobile devices greatly simplifies threat management. The predefined views and reporting highlight the most important events, reducing response times.

Integration With SD-WAN

EdgeSecure with SD-WAN security gateways are deployed through the SD-WAN management console. This tight integration reduces deployment time, effort, and costs. When EdgeSecure is deployed on SD-WAN or uCPE equipment, the EdgeSecure 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

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 620, Edge 640, Edge 680, Edge 840
Threat Prevention	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
SD-WAN or uCPE Hypervisor	VMware ESXi and KVM