Giving SD-WAN the specialized security solution it needs

Technology, covered.

With more and more business leaders taking steps to tap into the power of cloud computing to enable their communications and day-to-day operations, software-defined wide area networks (SD-WAN) are becoming increasingly common tools for ensuring consistent, high-bandwidth access to cloud applications regardless of where users are located.

Today's enterprise companies require a reliable, robust, and secure network environment to support initiatives to expand their bottom line. SD-WAN provides consistently high bandwidth to maximize performance of cloud applications and managed software services. Furthermore, SD-WAN technology is critical for today's hybrid cloud environments because it brings enterprise-level manageability, performance, and reliability across branch offices and remote locations.

Even these agile and reliable SD-WAN environments, however, require vigilance to protect companies from external threats. After all, networking a series of branch offices and remote locations together opens them up to a higher risk of intrusion. An advanced network requires advanced security integrated into its core. The security solution must also provide simplicity and minimize costs when integrated into the SD-WAN environment while enabling public security compliance across all applicable virtual networks.

Security challenges most often faced by modern businesses include:

- Complexity of managing distributed branches and departments.
- Insufficient bandwidth to monitor traffic effectively against potential threats.
- Outdated network architecture not suited for dealing with advanced malware.

Meeting these challenges is the starting point for enterprise companies seeking security to align with their SD-WAN architecture. At a time when both legitimate business activity and organized malware attacks occur in the cloud with increasing prevalence, the best option for many organizations is network security as a service designed to take security management off the plate of IT staff.

That's where OnX Canada, a Check Point 4-Star Partner, comes in to lock down SD-WAN and hybrid networks with Check Point's CloudGuard Connect and CloudGuard SaaS.

Combining strengths to secure your network

This partnership with Check Point enables OnX to unite Check Point's industry-leading CloudGuard security with custom OnX SD-WAN solutions to support the rapid shift to distributed application architecture and flexible work from anywhere policies. Mass migration of applications to the cloud presents challenges for enterprise security architectures, especially with the increased use of public clouds and multi-cloud deployments. Through the partnership, OnX delivers the proactive security remote workers need while bringing consistent, high-quality bandwidth to access cloud services and private data centers.

With the implementation of Check Point CloudGuard SaaS, OnX ensures the organization blocks attacks targeted at stealing data from typical SaaS applications and cloud e-mal. Once CloudGuard SaaS is in place, OnX delivers comprehensive protection against malware and zero-day threats, sophisticated phishing attacks, and the hijacking of employee SaaS accounts. IT staff also gain access to instant threat visibility and data control and protection.

> "OnX has long leveraged SD-WAN technologies to help customers transition to the cloud and provide a digital transformation path. Organizations now face the challenge of securing this new, flexible, always-on network where an application can live anywhere in the world, and employees can work from anywhere in the world. Check Point's CloudGuard technologies enable our customers to make the best network and application decisions for their organization without the added difficulty of securing a malleable, distributed network. We are now delivering peace of mind, along with our flexibility and convenience."
>
> -Jon Lloyd, Director of Cloud Networking, OnX

For companies looking for a cloud-native, managed network threat prevention service, OnX works with their IT staff to assess risks for on-premises, cloud and branch networks, and all endpoints and mobile devices. From there, OnX deploys a custom implementation of Check Point CloudGuard Connect, a co-managed, full-spectrum security solution for SD-WAN environments.

With CloudGuard Connect at the core of OnX Network Security as a Service, the organization's IT staff is no longer burdened with deploying or maintaining dedicated hardware or managing advanced threat prevention for SD-WAN environments. 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 nearby location. A second connection provides redundancy. This ensures branch offices stay connected and removes the operational overhead of deploying and maintaining security for hundreds or thousands of physical devices.

As a fully managed or co-managed cloud-native solution, OnX Network Security as a Service takes advantage of CloudGuard Connect to provide top-tier monitoring and threat prevention under a manageable OpEx model. Additionally, the solution has the flexibility and scalability to grow on-demand as needed, with no additional hardware required on premises. All of these advantages are delivered with the trusted experience of industry leaders: OnX and Check Point.

Key Differentiators from OnX

- OnX combines VMware SD-WAN by VeloCloud Partner Innovation Award expertise with Check Point's highest level 4-Star Partner experience to deliver comprehensive cloud-native network security.
- Decades of SLA-based OnX managed s
- ervices experience for core practice areas that deliver operational excellence and remove day-to-day monitoring and management of technology environments and applications, now expanded to cloud-native security.
- Unlike standard security platforms that only detect threats, OnX Network Security as a Service leverages Check Point CloudGuard Connect and CloudGuard SaaS to deliver active threat prevention to uncover malicious behavior in a virtual sandbox before hackers can enter the network.
- OnX Network Security as a Service combines cloud-based CPU-level inspection with OS-level sandboxing through Check Point technology, preventing infection from the most dangerous exploits and all targeted and zero-day attacks.
- OnX deploys advanced threat prevention to remote sites and branch offices in minutes. As a cloud-native architecture, Check Point CloudGuard is elastic, scalable, and provides dual tunnels for 99.999% uptime and 50ms latency.
- OnX Network Security as a Service brings predictable monthly pricing for top-rated branch office and remote site

Technology, covered.

threat prevention with a 100% cyber attack catch rate.

Check Point CloudGuard Advantages

Advantages of Check Point CloudGuard Connect

- CloudGuard Connect provides network firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, Threat Emulation (sandboxing), and full SSL inspection capabilities.
- Additional CloudGuard Connect advantages include:
  - Prevention of unknown attacks in malicious files using sandboxing.
  - Prevention of known attacks using domain, URL reputation, and IPS signatures.
  - Prevention of access to malicious websites using URL Filtering, Application Control, and Antivirus domain and URL reputation.
  - Prevention of infected hosts communicating back to Command and Control servers.
  - Full NG Firewall access control and HTTPS inspection.

Advantages of Check Point CloudGuard SaaS

- CloudGuard SaaS is cloud-native threat prevention for real SaaS threats.
- More than just a cloud access security broker (CASB), CloudGuard SaaS blocks attacks targeted at stealing data from SaaS applications and cloud e-mail.
- CloudGuard SaaS provides complete protection against malware and zero-day threats, sophisticated phishing attacks, and the hijacking of employee SaaS accounts.

Rethink your branch security approach

As your network modernizes, so too must your threat prevention strategy. Take the next step and complete your standalone SD-WAN or hybrid network architecture with a cloud-native security solution that offers simple and intuitive web-based management. OnX can guide deployment and manage Check Point CloudGuard technology that sets up your entire network and devices for optimal security with a minimal investment of time, effort, and personnel.

Contact the experts at OnX for more information on how to lock down your standalone SD-WAN or hybrid network with

> "Given today's advanced cyber threats, it is critical to protect enterprise branch offices connected to the cloud with SD-WAN. Check Point CloudGuard Connect is integrated with leading SD-WAN vendors in the cloud to secure branches in minutes. We're excited to partner with OnX to help drive enterprise digital transformation, with a special emphasis on branch office SD-WAN security."
>
> - Erez Yarkoni, Head of the Telco Division, Check Point Software Technologies