CBTS advanced, cloud-native threat prevention

Hosted cloud security with Check Point CloudGuard and Custom SD-WAN integration

As organizations continue the migration of branch office workloads and applications to the cloud, many have implemented SD-WAN to route traffic intelligently between data centers using existing MPLS lines and directly to cloud services via local internet. Additionally, with today's rapid shift to remote working, applications are distributed across multiple clouds, many of them public, making enterprise network security extremely challenging.

Because branch offices and remote sites connect directly to cloud services using local broadband, the organization's security risks increase dramatically. By bypassing centralized data center security, branches and remote locations expose the enterprise WAN to multi-vector cyber attacks, which can hit the network, endpoints and mobile devices, and cloud environments as part of an organized campaign.

Recognizing the need for a new approach to branch and remote site security, CBTS partnered with Check Point® Software Technologies to deliver cloud-based network threat prevention services. As a Check Point 4-Star Partner, CBTS experts integrate Check Point's industry-leading CloudGuard cloud-native security with highly customized SD-WAN solutions, closing the security gap of today's distributed application architecture and flexible work-from-anywhere policies.

Seamless integration with SD-WAN and a unified threat and access management platform can significantly reduce an organization's operational expenses by up to 40%.

The CBTS and Check Point Advantage: Security as a Service

By combining CBTS SD-WAN expertise and Check Point's CloudGuard Connect and CloudGuard SaaS, CBTS strengthens remote site and branch connectivity with cloud-delivered security services. Remote workers get the proactive security they need with consistent, high-quality bandwidth for accessing their cloud services and private data centers.

Check Point CloudGuard Connect is the top-rated threat prevention platform, updated in real time with the latest ThreatCloud intelligence. The flexibility of CloudGuard Connect gives CBTS the option of deploying branch office security in minutes from the cloud or on-premises. Seamless integration with SD-WAN and a unified threat and access management platform can significantly reduce an organization's operational expenses by up to 40%. With CloudGuard Connect in place, SaaS, IaaS, and branch office assets are all protected from sophisticated threats. Additionally, the platform delivers dynamic scalability, intelligent provisioning, and consistent control across physical and virtual networks.

Active threat prevention makes all the difference

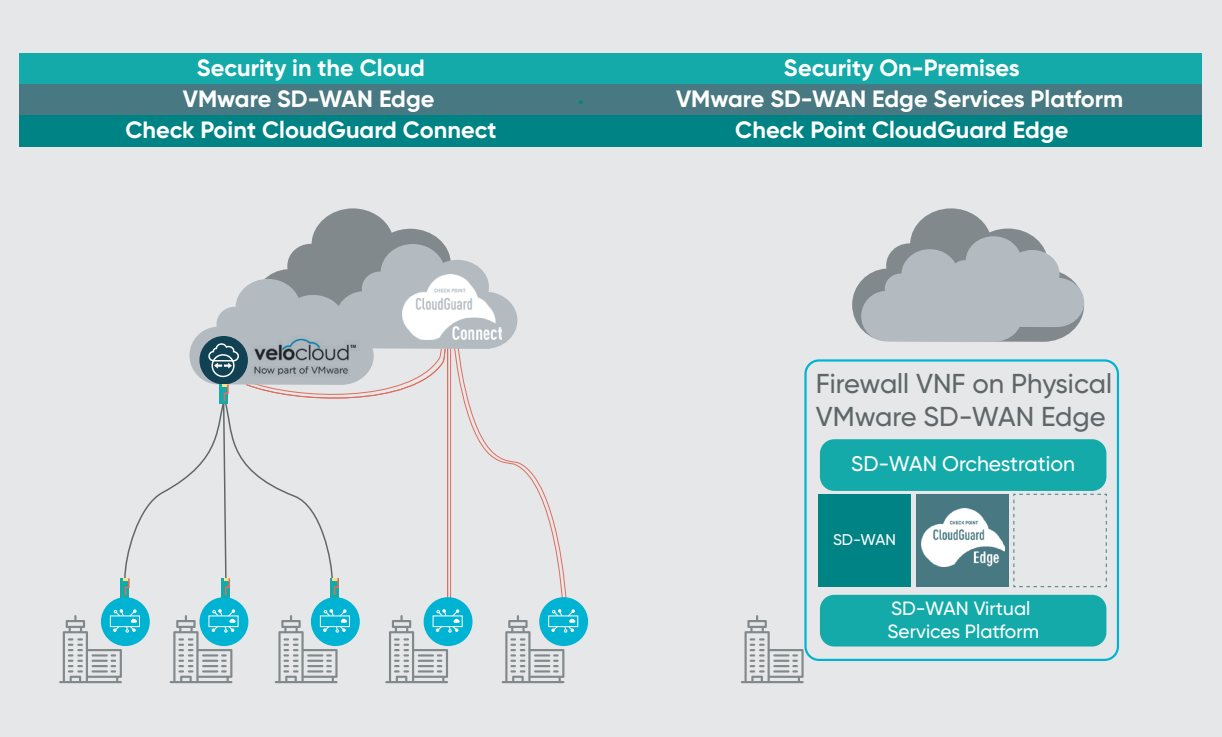
Unlike security detection platforms that only detect threats, Check Point delivers active threat prevention. Check Point SandBlast Zero-Day Protection uses cloud-based sandboxing technology to quarantine and inspect files, uncovering malicious behavior in a virtual sandbox before it can enter the network. Malware is detected by SandBlast at the exploit phase before hackers can apply evasive steps attempting to bypass the sandbox. By combining cloud-based CPU-level inspection with OS-level sandboxing, Check Point prevents infection from the most dangerous exploits, and all targeted and zero-day attacks.

Furthermore, because Check Point consolidates security architecture across on-premises, cloud, and branch/remote networks, and endpoint and mobile devices, identified threats automatically propagate as an IoC (Indicator of Compromise) to protect all company assets from the same zero-day threat.

Finally, Check Point includes IPS, Anti-Bot, and Antivirus to protect from known threats, Application Control and URL Filtering to enforce safe web use, and HTTPS inspection to prevent threats inside encrypted HTTPS channels.

Branch Office Security-as-a-Service Architecture

CBTS is bringing Check Point CloudGuard SaaS to market. CloudGuard SaaS is a cloud service tailored for real SaaS threats. More than just a cloud access security broker (CASB), it blocks attacks intended to steal data on common SaaS applications and cloud e-mail. It provides complete protection against malware and zero-day threats, sophisticated phishing attacks, and hijacking of employee SaaS accounts. Users also gain instant threat visibility and data control and protection. Check Point and CBTS can offer differentiated security services to customers moving towards borderless computing (SASE and CASB).



Benefits

- Delivers maintenance-free, advanced threat prevention to remote sites and branch offices in minutes.
- CloudGuard Connect is a cloud-native architecture; elastic, scalable, with dual tunnels for 99.999% uptime, and 50ms latency.
- Predictable monthly pricing for branch office security and top-rated support.
- NSS Top-Rated Threat Prevention with 100% Cyber Attack Catch Rate.

Features

- Simple and easy one-click provisioning reduces deployment time, effort, and cost.
- Single pane of glass view across the entire infrastructure, enabling immediate response to security incidents.
- Second connection providing redundancy.
- Network traffic from the VMware SD-WAN Edge device is connected over a low latency GRE or IPsec tunnel to a primary cloud-hosted network security service at a nearby location.
- Maintenance-free security for hundreds and thousands of physical devices.

CBTS Network Portfolio