As enterprises increasingly move their on-premises branch office workloads and applications to SaaS applications, they are adopting Software-defined Wide Area Networking (SD-WAN) to intelligently route traffic 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, as the 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 needed. It’s time to rethink how security is delivered to remote branch offices.

CLOUD-DELIVERED BRANCH OFFICE SECURITY

Check Point CloudGuard Connect and CloudGuard Edge provide cloud-delivered zero-day threat prevention from Check Point that is tightly integrated with leading Wide Area Network (WAN) providers including leading SD-WAN vendors and Managed Service Providers (MSP) who already manage customer Internet connections and know how to deliver efficient services at scale. The CloudGuard Connect service and CloudGuard Edge virtual machine (VM) integrate with network management and orchestration systems to secure any organization with remote branch offices in minutes. Operation efficiency of the cloud-delivered Check Point unified threat and access management platform reduces operational expense by up to 40%.

The CloudGuard Connect cloud-hosted security service delivers maintenance-free, advanced threat prevention to remote sites and branch offices in minutes. Existing branch office routers or dedicated SD-WAN devices connect securely to the CloudGuard Connect service over GRE or IPsec tunnels to secure cloud and Internet bound traffic. With a seamless integration with leading SD-WAN vendors, customers can easily implement security across thousands of branches where there are no local IT resources.

The CloudGuard Edge virtual machine (VM) is for those enterprises that need on-premises security for data privacy or data location requirements. CloudGuard Connect gateways can be deployed using virtual security gateway software running on existing branch office IT equipment including dedicated SD-WAN or universal Customer Premises Equipment (uCPE) devices.
BRANCH OFFICE THREAT PREVENTION

Customers using either the CloudGuard Connect service or the CloudGuard Edge VM get Check Point NSS top-rated threat prevention with a 100% cyber-attack catch rate updated in real-time with the latest ThreatCloud intelligence.

PREVENT ZERO-DAY THREATS
Check Point provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. Check Point protects SaaS applications, IaaS and branch office assets from sophisticated threats with dynamic scalability, intelligent provisioning and consistent control.

Check Point SandBlast Threat Emulation (sandboxing) prevents threats in malicious files. SandBlast Zero-day Protection is a cloud-hosted sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters the network. 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.

Check Point threat prevention technologies consistently receive high scores in independent third party tests. The Recommended Rating in NSS Labs 2019 BPS Group Test marks Check Point's third NSS Labs Recommended in 2019 and the 20th NSS Labs Recommended rating since the company began testing with NSS in 2010.

SHARED THREAT INTELLIGENCE
Check Point ThreatCloud is a fully consolidated and connected cyber security architecture protecting on premises, cloud and branch networks as well as endpoint and mobile devices from advanced persistent threats. Check Point ThreatCloud intelligence prevents over 7,000 zero-day attacks daily. Threats identified on one device are automatically propagated as an IoC (Indicator of Compromise) to protect branch, mobile and cloud-hosted assets from the same zero-day threat.

GRANULAR, EASY TO MANAGE NGFW
Check Point CloudGuard Connect and CloudGuard Edge enforce safe web use with over 8,000 predefined applications. Security administrators do not need to spend time creating application signatures. They can simply pick from one of the 8,000+ available applications or use one of over 100 predefined categories to create the access control security policy. Categories include both applications and sites, making application control and URL Filtering policy management a breeze. In addition IPS, Anti-Bot and Antivirus protect branch offices from known threats and HTTPS inspection safeguards companies from threats trying to hide inside encrypted HTTPS channels.

Consolidate Security and Threat Management
Orchestrate Network Management and Operations