Check Point and Silver Peak Optimize Enterprise WAN Security

CLOUD-FIRST CHALLENGES

Cloud application performance

Backhauling cloud-destined traffic to the corporate data center impairs application performance

Security service chaining

Manual configuration is complex, cumbersome, inconsistent and time consuming

Maintaining current application and security definitions

Lack of daily application and security updates exposes the enterprise to vulnerabilities

SOLUTION BENEFITS

Highest quality of experience

Secure local internet breakout from the branch delivers highest cloud application performance to users

Automation enhances business agility

Automated configuration of CloudGuard Connect accelerates SD-WAN security service deployments

Consistent app QoS and security policy enforcement

Automated daily threat and application updates ensure continuous, consistent policy enforcement across the enterprise

Enterprises continue the migration of business-critical applications, workloads and services out of the corporate data center and into the cloud at an accelerating pace. Savings in both CAPEX and OPEX along with the architectural advantages of migrating applications to Software-as-a-Service (SaaS) offerings or hosting them in secure, highly available public Infrastructure-as-a-Service (IaaS) instances, accessible to users from any device with internet connectivity, are key factors driving this change. However, new WAN and security architectures must also be deployed to deliver the highest cloud application performance while mitigating risks to enterprise security.

The traditional Wide Area Networking (WAN) model based on routers, backhauls cloud-destined traffic from the branch over expensive private MPLS services to the corporate data center where the traffic is processed through a full stack of security services before being passed to the internet. But MPLS lines are costly and applications and workloads residing in the cloud experience the best performance when traffic is sent directly to the internet from the branch, an architecture commonly referred to as local internet breakout. While local internet breakout brings clear advantages with respect to overall application performance, it can complicate network security. Direct branch access to the internet increases the attack surface and lacks robust security policy enforcement unless expensive next-generation firewalls are deployed — and managed on an ongoing basis — at every branch location. Most enterprises find the associated equipment costs and IT administrative overhead with that model unsustainable.

New Cloud-First Security Approaches

Cloud-first enterprises require a new approach to intelligently optimize branch WAN connectivity that is cost-effective, easy to maintain and is always up to date with the latest application and security definitions. It's time to rethink WAN architecture including how security is delivered to remote branch offices.

Check Point and Silver Peak have partnered to create a joint solution which addresses the network security challenges inherent with a cloud-first architecture. The joint solution enables flexible, automated service chaining from the Silver Peak Unity EdgeConnect™ SD-WAN edge platform to the Check Point CloudGuard Connect cloud-hosted security service.

The initial configuration is centrally orchestrated and service chaining is fully automated. Application security policies are defined once and propagated to all sites in contrast to the branch firewall security model requiring device-by-device configuration and management. Centralized management reduces both the time to deploy and IT resource costs, whilte providing consistent policy enforcement and reducing risk across the enterprise.

EdgeConnect intelligently directs traffic to Check Point security processing resources wherever they reside:

- As a cloud-hosted security service with Check Point CloudGuard Connect
- Physical appliances adjacent to EdgeConnect in the corporate data center
- Co-located with EdgeConnect in the branch when using CloudGuard Edge

Check Point Advanced Threat Prevention

Check Point provides organizations of all sizes with integrated, advanced threat prevention. Check Point security offerings protect SaaS, IaaS and 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, Check Point prevents threats from detonating their payloads on their target hosts. Check Point 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. 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.

The Check Point solution also includes Application Control and URL Filtering to enforce safe web use, along with IPS, Anti-Bot and Antivirus to protect from known threats. HTTPS inspection safeguards from threats hiding inside encrypted HTTPS channels.

Furthermore, Check Point 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. Threats identified on one device can be automatically propagated as an IoC (Indicator of Compromise) to protect your branch, mobile and cloud-hosted assets from the same zero-day threat.

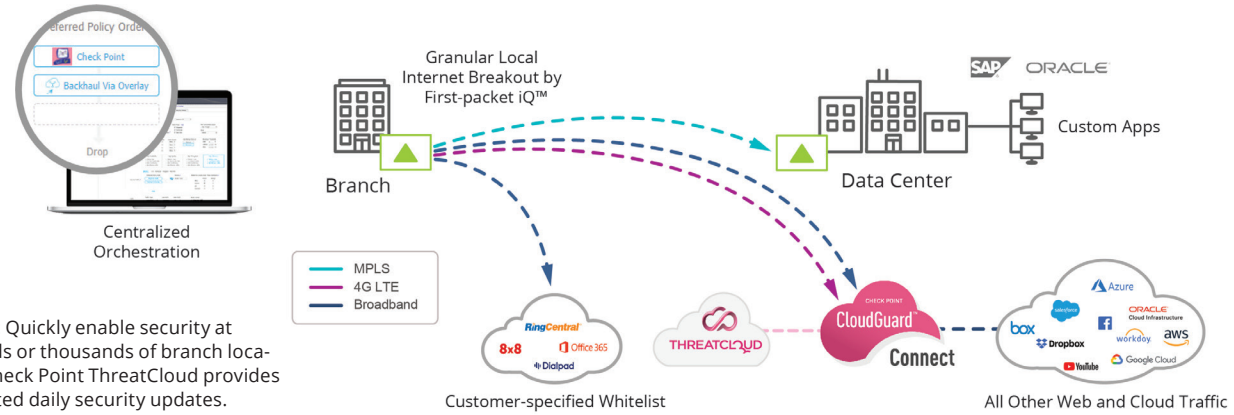

Figure 1: Quickly enable security at hundreds or thousands of branch locations. Check Point ThreatCloud provides automated daily security updates.

The Cloud-hosted Security Advantage

Remote branch offices pose significant challenges to the corporate IT staff. Each new site adds equipment, management, maintenance and connectivity costs. Add to this the risks associated with a breach in security from yet another threat vector or the complexity of remediating a remote infected device.

CloudGuard Connect adds advanced threat prevention capabilities to Silver Peak EdgeConnect SD-WAN deployments, and because it is cloud-hosted, CloudGuard Connect does not burden IT with deploying and maintaining dedicated security hardware. With a simple and easy setup process, network traffic from EdgeConnect SD-WAN edge devices is forwarded over IPsec tunnels to primary and backup CloudGuard Connect service locations. In order to minimize network latency, the CloudGuard Connect service uses geolocation information to determine the service locations closest to a given branch. From the Silver Peak Unity Orchestrator™ console, IT inputs Check Point subscription credentials to initiate automatic configuration of primary and backup IPsec tunnels from each EdgeConnect branch device, enabling device, network and security service redundancy.

Within the CloudGuard Connect service, security updates are completely automatic, providing maintenance-free security for hundreds to thousands of physical devices, reducing your overall CAPEX and OPEX costs.

Check Point's centralized management provides an intuitive, simple on-boarding process that incorporates security policy configuration and monitoring. Powered by Check Point SmartEvent, IT can see the most important threats with a single view across the entire infrastructure to:

- 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.

The SaaS Advantage

SaaS applications like Office 365, Salesforce, ServiceNow, Dropbox and Box experience the best performance when application traffic is sent directly across the internet from the branch. Silver Peak Cloud Intelligence aggregates ever-changing information about SaaS applications and provides automated daily updates to EdgeConnect appliances including the addresses from which the providers' applications and data are being served. This information is distributed to all branch locations without IT intervention, enabling EdgeConnect to dynamically steer SaaS traffic along the optimal path for any user at any location on the network to any SaaS destination.

The cloud improves efficiency, both for the business and for those trying to attack it. In addition to CloudGuard Connect, Check Point offers CloudGuard SaaS, a Cloud Service Access Broker (CASB) service with a cloud-to-cloud API architecture that protects enterprise data by preventing targeted attacks on SaaS applications and cloud-hosted email.

With CloudGuard SaaS enterprises can eliminate the primary SaaS threat: account takeovers. From SaaS behaviors and configurations, to logins from compromised devices, CloudGuard SaaS detects unauthorized access, using transparent, strong authentication to block account hijacks. To stop clever phishing attacks and email spoofing, CloudGuard SaaS AI engines analyze hundreds of indicators like language and email metadata to block more phishing techniques than any other solution or CASB.

Deploy CloudGuard SaaS seamlessly and centralize monitoring via an intuitive web portal common to CloudGuard SaaS and CloudGuard Connect.

The IaaS Advantage

Adopting public cloud infrastructure means security is now shared between you and your cloud provider. Check Point CloudGuard delivers automated and elastic security to keep assets and data protected while staying aligned to the dynamic needs of public cloud environments. The Silver Peak CloudGuard integration directs application traffic and workloads hosted in public cloud IaaS providers like AWS, Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure to their closest instances to branch locations. This ensures that end users experience public cloud-hosted application performance that is as high as that for applications hosted in the data center or private cloud.

The Hybrid Security Advantage

Check Point is uniquely positioned within the industry to support customers that want a hybrid model, where the customer can mix and match physical Check Point appliances with CloudGuard Connect cloud-hosted security and CloudGuard Edge virtual instances. This range of architectural alternatives enables the enterprise to gracefully migrate from the current posture of appliance-based security at all branch offices, to a hybrid mix of appliance-based and cloud-hosted security. Through the migration, Check Point hybrid deployment provides consistent security policies to all traffic across the enterprise as they gradually introduce local internet breakout to the branch with CloudGuard Connect.

The MSSP Advantage

The EdgeConnect SD-WAN edge platform offers unique flexibility, enabling service providers to differentiate their managed SD-WAN services in the following five ways:

- Support for new tiered services
- Ability to deliver performance-based SLAs
- Application delivery and WAN transport visibility services
- Integrated WAN optimization-as-a-service
- Service chaining with managed security solutions

The Check Point CloudGuard Edge virtual security gateway fits well with MSSP solution sets, providing:

- Next-generation firewall capabilities
- Advanced threat prevention
- Centralized security and event management
- APIs to orchestrate provisioning and orchestration

About Check Point

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device-held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About Silver Peak

Silver Peak, the global SD-WAN leader, delivers the transformational promise of the cloud with a business-first networking model. The Unity EdgeConnect self-driving wide area network platform liberates enterprises from conventional WAN approaches to transform the network from a constraint to a business accelerant. Thousands of globally distributed enterprises have deployed Silver Peak WAN solutions across 100 countries. Learn more at silver-peak.com.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com

SP-SB-CHECK-POINT-AND-SILVER-PEAK-01XX20