



A Lumen Connect® Solution

Network Infrastructure On-Demand: Next-Generation Security for Multi-Cloud Networks

SOLUTION BRIEF: CHECK POINT + ALKIRA

The growing need for business agility is driving organizations to transition critical applications from on-premises data centers to public cloud environments and SaaS offerings. This digital transformation is forcing enterprises to reevaluate traditional on-premises security perimeter architectures, which are not optimized for the distributed nature of cloud applications.

Enterprises seek to transition their familiar and trusted stateful next-generation network security services from on-premises data centers and colocation facilities into the public cloud environments they serve. While cloud environments offer global presence and vast compute resources, they lack the necessary routing, policy, and operational controls enterprises require for streamlined cloud firewall deployment. The do-it-yourself (DIY) approach for cloud network security results in significant virtual machine instance sprawl, sub-optimal resource consumption, and complex traffic management scenarios—challenges greatly exacerbated in multi-cloud environments.

Enterprise IT teams tasked with defining cloud architecture are forced to make compromises in network design and product selection as they balance cost against operational complexity.

SOLUTION BENEFITS



Consolidated Security Services

Eliminate sprawl of firewall instances through consolidated firewall deployment in Alkira Cloud Exchange Points



Uniform Security Policy

Significantly reduce the time to provision by moving the full network into Infrastructure-as-Code operation leveraging the rich Alkira portal APIs.



Optimized Resource Consumption

By leveraging Alkira with Terraform, the network will become consistent with configuration drift being minimized.



Auto-scale

Embracing DevOps practices enables a joint toolchain across the entire infrastructure stack, including networking and security, with increased and safe collaboration.



Simplified Operations

Reusable Terraform configurations, managed in version control, provide a consistent and controlled method for managing networking and security infrastructure lifecycle.

SECURING CLOUD WITHOUT THE COMPROMISE

The joint solution from Check Point and Alkira allows organizations to confidently transition their security infrastructure to a cloud-delivered as-a-service model, avoiding the complexity of navigating native single-cloud and multi-cloud architectures. Joint customers can continue operating with familiar Check Point security management tools and security policy constructs, while the Alkira Platform fully automates the provisioning, licensing, service insertion, scaling, and health monitoring of Check Point CloudGuard Network Security gateways.

CloudGuard is available from the Alkira network services marketplace. Alkira's solution seamlessly inserts CloudGuard security gateways at any point in the Alkira global cloud backbone, providing stateful security controls for any on-premises, cloud, and Internet application traffic.

SOLUTION DETAILS

Check Point CloudGuard can be rapidly provisioned into one or multiple globally distributed Alkira Cloud Exchange Points (CXP) to provide security policy enforcement for application traffic between any set of endpoints connected to the Alkira global cloud backbone. Security policy can also be enforced for ingress and egress Internet traffic through regional Internet breakouts.

Simply select Check Point CloudGuard from the Alkira network service marketplace and be guided through an automated provisioning process with options for choosing SMS or MDS management platform, bring-your-own (BYOL) or pay-as-you-go (PAYG) licensing model, auto-scaling high and low-water marks, target network segments, and service billing tags.

Once provisioned, Check Point CloudGuard hosted within the Alkira Cloud Exchange Point can secure a range of use cases:

- ✓ Security policy to and between public cloud workloads
- ✓ Cloud-hosted, stateful firewall services for branch and data center locations
- ✓ Regionalized Internet breakouts for secure SaaS applications access
- ✓ Cloud DMZ environment for Internet-facing applications
- ✓ Shared cloud application services for partners and M&As

Alkira connectors form the basic unit of connectivity within Alkira Cloud. They support various connectivity needs for on-premises and cloud environments, such as standards-based IPsec, SD-WAN, remote access VPN, private cloud cross-connects, Internet, and cloud-native connectivity for AWS, Azure, and GCP cloud workloads.

The connectors are isolated into different segments and optionally grouped within segments to create micro-segmentation. Segmentation and micro-segmentation (groups) can be extended toward Check Point CloudGuard to maintain isolation for network policy (e.g., line-of-business segmentation), compliance (e.g., PCI DSS, HIPAA), or deployment environment separation (e.g., production, development, and staging) purposes.

Alkira intent-based policy provides granular selection of application traffic, based on 6-tuple or application recognition, for redirection to provisioned CloudGuard instances. By selectively sending flows that explicitly require firewall inspection, firewall resource consumption can be managed to enable effective right-sizing.

During redirection, Alkira's routing fabric automatically tracks session state to ensure symmetric connection steering through firewall instances while maintaining original source and destination IP addressing without network address translation (NAT). Where multiple firewall instances are provisioned, the Alkira routing fabric natively manages load balancing across these instances in an active-active fashion.



Configuration of policy is made easy with Alkira's visual policy manager, which provides a straightforward approach to policy scoping and inspection while simplifying auditing for assurance and compliance purposes.

Check Point CloudGuard security policy provisioned within the Alkira solution is managed from Check Point security management servers reachable via private or public connectivity. Configuration, rich security policies, and the full breadth of features visibility of the CloudGuard instances, including day-2 operations to monitor platform health and traffic utilization, application traffic redirection, and system resource consumption.



SUMMARY

Alkira offers Check Point CloudGuard as part of the Alkira network services marketplace. It allows organizations to simplify their cloud and multi-cloud networking journey while utilizing the rich security capabilities offered by the Check Point solution. The entire integrated solution is consumed as a service, unlocking a true cloud-native networking experience that is highly resilient, performant, and secure.



About Alkira

Alkira, a Lumen Connect solution, is the on-demand platform that connects every cloud, site, partner, and AI workload with agility and simplicity. No hardware to deploy, software to manage, or capacity planning required. The Alkira solution is trusted by Fortune 100 enterprises, leading system integrators, and global managed service providers. Learn more at alkira.com and follow us @alkiranet.vw



ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cybersecurity 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.