CHECK POINT + SKYHIGH

EXTENDING SECURITY TO THE CLOUD

Benefits

- Visibility into all cloud services used within the enterprise along with detailed risk ratings for each service
- Governance workflow to enforce risk-based polices on acceptable cloud service usage and streamline the review of requested cloud services
- Threat Protection to detect data exfiltration attempts and prevent the use of high-risk services
- Seamless integration between Skyhigh and Check Point and frictionless deployment requiring no device agents, no VPN, no change to existing workflows.
- Compliance with industry regulations by enforcing policies on data uploaded to cloud services and taking remedial action on violations.
- Closed loop remediation enabled by Skyhigh's cloud usage insight leading to policies enforced within Check Point.
- Corporate data protection using tokenization of user-specific information before usage logs are uploaded to the Skyhigh cloud.

INSIGHTS

Cloud services are seeing massive adoption by enterprise users, with the average company now using 1,154 cloud services and the average employee using 30 cloud services at work. But, many of these services are used without IT approval and have questionable security controls, which put the company at the risk of data loss.

JOINT SOLUTION

Check Point and Skyhigh have partnered to extend enterprise visibility, governance and threat protection to the cloud so that enterprises can secure their cloud usage and better manage cloud services and workflows. Check Point next generation firewalls provide customers with advanced data and network security protection, enabling employees to work freely and securely online. Employee cloud usage logs generated by the Check Point next generation firewall are processed and analyzed by Skyhigh to provide visibility into cloud applications used by employees and the security risk associated with each of these services. To control access to risky services, IT can create governance policies in Skyhigh that are enforced by the Check Point firewalls.

VISIBILITY INTO CLOUD USAGE

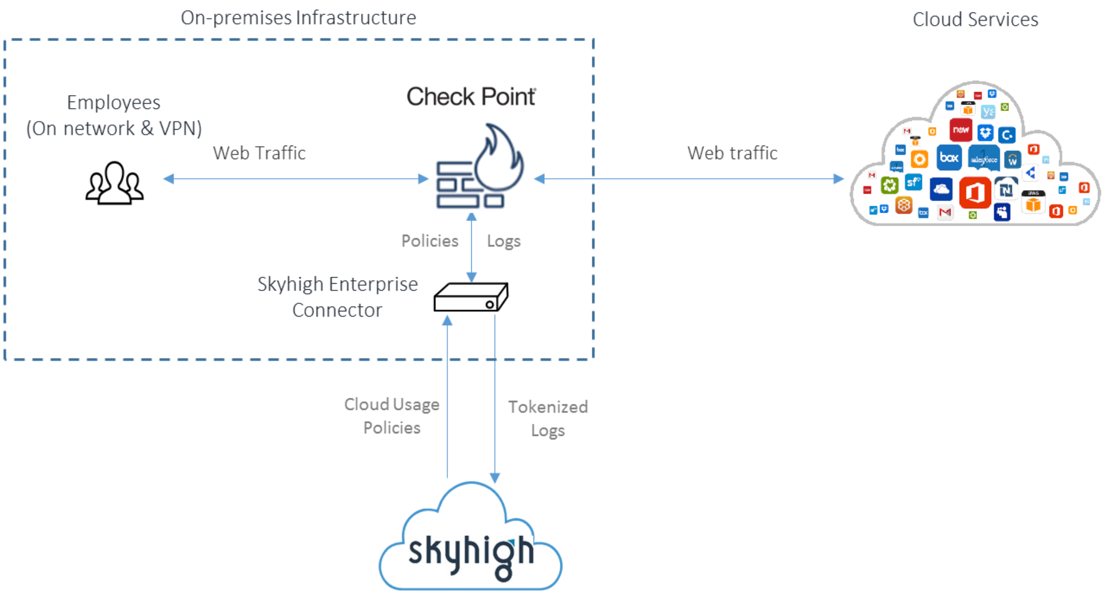
Skyhigh and Check Point provide IT teams with visibility and governance capabilities to better manage the increasing enterprise usage of cloud services. Check Point maintains detailed logs of all cloud usage, which are processed by Skyhigh's enterprise connector, tokenized to remove sensitive information such as user IDs, IP addresses and uploaded to the Skyhigh cloud. Here, data is matched with the Cloud Registry of over 17,000 cloud services and a risk rating is calculated using over 50 attributes. Using the Skyhigh dashboard, customers can get visibility into the risk score, risk benchmarks and usage analytics, which include summarized statistics such as the number of cloud services in use, traffic patterns and usage over time.

CLOUD GOVERNANCE

Companies using Skyhigh and Check Point can define governance workflows by enforcing risk based policies on cloud usage. One example is to block all cloud services which are above a specified risk rating to minimize the risk of data loss. Also, workflows can be defined to consolidate usage to a sanctioned service. If a company has deployed Box as the standard file sharing service, policies can be implemented to either block other file sharing services or to display real-time coaching messages to steer employees towards Box.

CLOUD THREAT PROTECTION

Skyhigh and Check Point capabilities can be used by organizations to detect and mitigate and prevent data loss threats. Skyhigh leverages machine learning to identify traffic patterns indicative of malware or botnets exfiltrati ng enterprise data via shadow IT cloud services. So, it can provide insight into cloud services that are seeing high uploads and downloads of data along with their risk ratings. This information can enable IT to enforce policies within Check Point to block cloud services seeing high traffic or sudden spikes in uploads as they could represent an exfiltration threat.



Check Point and Skyhigh enable visibility and threat protection for enterprise cloud usage

CLOUD DATA LOSS PREVENTION

To protect data and remain compliant, companies can use Skyhigh and Check Point to enforce data loss prevention (DLP) policies on data uploaded to shadow cloud services. The policies are defined in Skyhigh and when data goes through Check Point firewalls, SSL connection is terminated and information is sent to Skyhigh for inspection via ICAP protocol. Skyhigh inspects this content based on policy definitions and Check Point can either allow or block the upload based on remediation policy.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT SKYHIGH

Skyhigh Networks, the cloud security and enablement company, allows enterprises to safely adopt cloud services while meeting their security, compliance, and governance requirements. Over 500 enterprises including Aetna, DIRECTV, General Mills, HP, and Western Union use Skyhigh to gain visibility, manage threats, ensure compliance and protect corporate data across shadow and sanctioned cloud services. Headquartered in Campbell, Calif., Skyhigh Networks is backed by Greylock Partners, Sequoia, and Salesforce.com.