Hewlett Packard Enterprise | skyhigh

Solution brief

Cloud Security with HPE Security ArcSight and Skyhigh

Enabling Visibility and Threat Protection for Enterprise Cloud Usage

About HPE Security

HPE is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advance correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

About Partner

Skyhigh Networks, the leading cloud security and enablement company, allows enterprises to safely adopt cloud services while meeting their security, compliance, and governance requirements. Over 600 enterprises including Aetna, DIRECTV, General Mills, HPE, 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, **Salesforce.com**, and Thomvest Ventures.

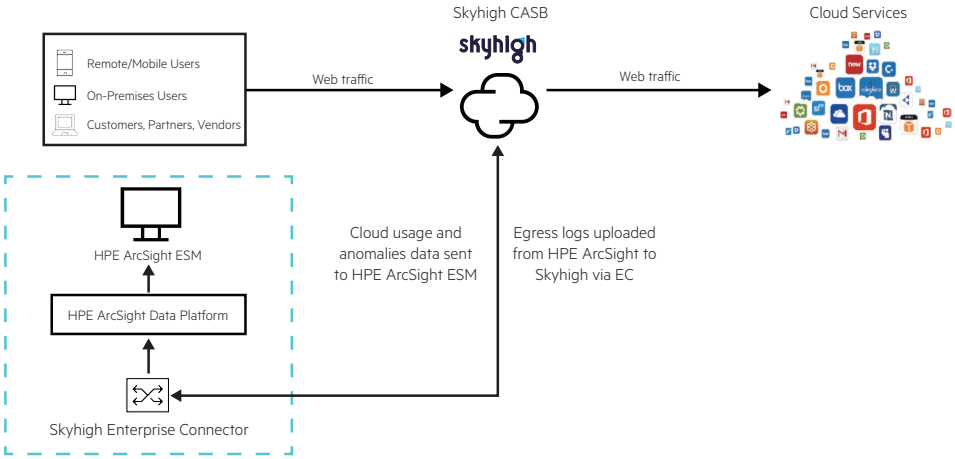
The average enterprise uses 1,427 cloud services yet most of these services are not sanctioned by IT. The use of shadow services for business functions has led to increased risk of unauthorized data access and data exfiltration.

Furthermore, the adoption of multiple sanctioned cloud services, such as Office 365, Salesforce, and Box has led to corporate data moving outside of company premises. While these solutions have a secure infrastructure, companies are vulnerable to accidental and malicious exfiltration by employees. Companies are looking to secure their corporate assets as they adopt cloud services.

HPE and Skyhigh address customers' cloud security requirements by providing visibility into shadow cloud usage as well as highlighting threats associated with insiders, compromised accounts, and privileged users. By providing a holistic view of the threat landscape, IT teams can quickly address security vulnerabilities and protect company data.

Key Benefits:

- Visibility into all cloud services used within the enterprise along with detailed risk ratings for each service
- Detection of anomalous usage associated with insiders, compromised accounts, and privileged users
- Consolidated view of the threat landscape including cloud and on-premises log sources
- Seamless integration between Skyhigh and HPE Security ArcSight
- Frictionless deployment requiring no device agents, VPN or changes to existing workflows



Use Cases:

Cloud Visibility: Skyhigh integrates with HPE Security ArcSight to extract web usage logs and uses its cloud registry to analyze and provide details on cloud services accessed, risk ratings, data uploaded, and user counts. Cloud analytics information is then sent to HPE Security ArcSight for monitoring.

- IT teams monitoring ArcSight can find out that 20 employees have uploaded over 4 GB of data to ZippyShare, a high risk cloud file sharing service.

Cloud Threat Protection: Skyhigh detects threats from insiders, compromised accounts and privileged users and sends anomaly data to HPE Security ArcSight for analysis.

- A sales person downloading an unusually high amount of data from Salesforce is flagged so IT can take remedial action in case this person is exfiltrating sensitive customer data.

Cloud compliance: Skyhigh can be used to enforce policies to comply with regulations. Skyhigh sends policy violation data to ArcSight for threat analysis.

- If a user attempts to upload a document containing SSN numbers, Skyhigh flags this as a policy violation and remediates as specified. This information is then sent to ArcSight for further security analysis and other remedial actions.

Learn more at

hpe.com/software

skyhighnetworks.com/

Sign up for updates

a00003744ENW, March 2017