skyhigh

Case Study

Cisco Systems

For more info, visit www.skyhighnetworks.com

Case Study: Cisco Systems Takes Control of Cloud Services

Company Description:

Name:	Cisco Systems
Location:	San Jose, California
Size:	60,000+ employees, 2012 revenues of over $46 billion
Description:	The world's leader in networking and communications products and services

Challenge:

With dozens of business units spread across the globe including numerous acquired companies in various stages of integration, Cisco Systems did not know which cloud services employees were accessing over company networks. The increased use of these services complicated data loss protection (DLP) efforts by increasing the number of vectors and destinations by which critical company information could be transported outside of secure corporate networks and into unknown, unregulated, and insecure locations in the cloud. "We had no comprehensive way of knowing what services were in use, where outgoing data was headed for, and what risks these cloud services implied for our business," explains Cisco's Director of Information Systems Desmond Murray. To solve this problem Murray wanted a tool that would:

- Discover and identify all cloud services running on Cisco networks including SaaS, PaaS and IaaS
- Provide a detailed, actionable and timely risk analysis of each identified cloud service
- Fingerprint likely sources of and probable behaviors indicating data leakage across various key asset types
- Find out which cloud services are popular in order to prioritize creation of authorized services
- Provide visibility into the utilization levels of paid cloud services to measure and monitor the "Shelfware Tax"

Solution:

Cisco decided to deploy the Skyhigh Networks Cloud Security Services Manager to get a better handle on Shadow IT usage and illuminate its cloud services footprint. Murray's team collected log files for network traffic from key business units and uploaded the log data into the Skyhigh Networks' CloudRegistry™ discovery and analytics engine. The deployment took less than a day. The engine identified dozens of unauthorized cloud services operating on the Cisco networks. "The number of cloud providers we were using was definitely a bit of an eyebrow raiser," says Murray. "We knew there would be a good number but we were surprised by exactly how many showed up." Murray's team also received from Skyhigh Network's CloudRisk™ module actionable risk ratings of each service in the form of a simple 1-to-10 rating based on detailed analysis of over 30 risk factors. Previously cloud service risk assessment was a one-off activity that required significant time and effort on the part of Cisco's information security and systems teams for each additional cloud service. "With Skyhigh, we get this comprehensive view and full visibility," says Murray. "This dashboard driven capability that was never there before and it allows us to make fast policy decisions."

> ***"This dashboard driven capability that was never there before and it allows us to make fast policy decisions..."***
>
> Desmond Murray,
> Director of Information Systems

In addition, Murray was able to use Skyhigh Networks' Hadoop-powered CloudAnomaly™ algorithmic behavioral detection engine to set up rules to highlight and then block anomalous activities that carried a high probability of data or information leakage. "If a Business Unit has average activity around downloading of key data in a given week, with Skyhigh we would be able to see a spike in downloads over the cloud service in question and flag that user," says Murray. Through the Skyhigh service, Murray was able to:

- Discover and quickly assess the risk for all unauthorized cloud services running on the company networks
- Identify services that could be legitimized and brought under better control with minimal risk to help employees do their jobs with the tools they wanted
- Immediately shut down unauthorized cloud services that carried excessive security, legal, privacy, compliance or data leakage risks
- Build behavioral screens based on business and data loss risks that would block activities on approved cloud services which appeared overly risky
- Track popularity of different cloud services to understand employee usage to begin to consolidate multiple types of the same service into a single, approved service
- Begin granular usage monitoring of cloud services to spot "Shelfware" that could be pruned, consolidated, or eliminated entirely

Problem	Solution	Result
No comprehensive way to see which cloud services being accessed from Cisco networks	Run log-files through Skyhigh to identify which services were being accessed	Complete visibility into all cloud services running on Cisco networks
Measuring risk of cloud services is a time-consuming, one-off activity	Skyhigh delivers detailed risk ratings based on over 30 factors including penetration testing of service, authentication methods, data encryption, and more	Instantly actionable risk information on all detected cloud services
No single comprehensive tool for DLP monitoring or highly customizable algorithm mechanism for anomaly detection	Skyhigh allows Cisco to set specific behavioral triggers that indicate a higher risk of data loss in an activity or prevent those activities before they can be completed	Significant improvement in DLP. Better security for critical company data
Multiple accounts across multiple services delivering similar functionality (i.e., Box.net, DropBox, SugarSync). Inefficient way to purchase services, greater security risk by splitting usage across three services	Skyhigh allows Cisco CIO to determine which types of cloud services are heavily used and who should be the preferred vendors	Gained ability to pull services on-premises or into better pricing structures with higher levels of admin capabilities and security
Difficult to know which specific parts of cloud services users access the most and deliver the most value. For example, certain pages and sections inside Salesforce.com may get significantly more traffic	Skyhigh not only provides visibility into services in use but also into what parts / URLs / sections of those services are most heavily used	Delivers valuable usage information for UI / UX teams and provides insights into what types of services and / or offerings or collateral are most useful to employees
Shelfware - underutilized or barely utilized cloud services	Skyhigh tracks usage of cloud services and even maps that usage back to individual users, business units, or internal functions (sales, marketing, engineering)	Identifies which cloud services licenses are getting the most use and allows CIOs to negotiate for better prices, trim unused services, or otherwise improve utilization of cloud services