Case Study

Equinix

For more info, visit www.skyhighnetworks.com

Case Study: Equinix Safeguards Employee Use of Cloud Services

EQUINIX

Company Description:

Name:	Equinix, Inc.
Location:	Redwood City, California
Size:	2700+ employees, 2012 revenues of over $2 billion
Description:	The world's largest data center operator and a provider of direct connection services to over 4,000 customers, Equinix is the "Home of the Internet"

Challenge:

As a company, Equinix has embraced the new generation of cloud services and has allowed employees to adopt online tools quickly and easily to perform their jobs as efficiently as possible. However, company global information security officer, George Do, had begun to grow concerned that he had no visibility into exactly which cloud services were being used by his employees. "We knew employees were using a lot of services and we didn't want to stop them from using any legitimate tool but we needed a better understanding of what was happening," says Do.

What's more, the process of approving new cloud services for use by employees required roughly 30 man-hours of due diligence by Do's staff of three security experts. "It was very taxing for a small staff like ours," says Do. This process involved direct calls to CTOs of cloud services companies as well as significant manual one-off efforts to verify security practices and risk factors. To discover cloud services that had not been declared by employees but represented risks, Do's team had to pore over reams of log files because existing tools for managing log files focused more on cyber attack risks and less on cloud services risks. Do wanted a tool that would:

- Discover and identify all cloud services in use by Equinix employees including file sharing, collaboration tools, IaaS, CRM and others
- Reduce the time and cost of vetting new and existing cloud services
- Provide anomaly detection to spot behaviors that likely indicated data leakage
- Allow Equinix to control access to cloud services and limit access to services deemed to present serious security, legal or compliance risks

Solution:

Equinix subscribed to the Skyhigh Networks Cloud Services Manager to discover the true scope of its cloud services footprint and make the lengthy approval process for new cloud services more efficient. Do's team collected data for network traffic from firewalls and proxies and uploaded it to the Skyhigh Networks CloudRegistry™ cloud services repository. Within minutes, Skyhigh discovered more than 200 cloud services in use, including many that Do had not been aware were in use or even existed. "I had expected a good amount, but the sheer diversity of services was surprising to me," says Do. "Many services I would not have expected showed up in the analysis, including some that we decided we needed to add because they filled a legitimate need we had not foreseen."

Additionally, Do's team received specific risk ratings for each service generated by the Skyhigh Network's CloudRisk™ cloud risk analytics engine, which takes into account more than 30 risk factors in calculating a simple 1-to-10 rating (1 being least risk and 10 being riskiest). "Having those ratings from a source we can trust means we can cut time spent onboarding a new cloud service down to 3-4 hours," says Do. "It has allowed my team to become far more efficient, and I love the fact that Skyhigh continually updates its ratings because we would never have time to go back and regularly check up on approved services."

> ***"I had expected a good amount but the sheer diversity of services was surprising to me..."***
>
> George Do, Chief Security Officer

To spot anomalous behaviors that might indicate data leakage or ongoing security problems, Do had been examining a combined, bespoke solution of several pieces of software that would analyze log files and then set new proxy and firewall rules. The Skyhigh Networks CloudAnomaly™ analyzer, which uses Hadoop to fingerprint and highlight potential bad behavior, allows Do to simplify the whole process."

With Skyhigh Networks Do was able to:

- Discover all cloud services used by Equinix employees
- Rate the risks posed by each service in a far more efficient, process-driven manner
- Reduce by 10x the manhours required to approve a new cloud service
- Identify several classes of popular services that he had not realized his users needed and which could be brought into the approval process
- Block the handful of cloud services that carried excessive security, legal, privacy, compliance or data leakage risks

Problem	Solution	Result
Difficulty identifying which cloud services are in use	Use Skyhigh Cloud Services Manager to identify which services are being accessed	Quickly and easily discovered over 200 cloud services used by Equinix employees
Calculating risk of cloud services is time-consuming and expensive	Skyhigh delivers detailed risk ratings for each cloud service based on over 30 factors including penetration testing of service, authentication methods, data encryption, and more	10x reduction in manhours and costs required to research and approve a new cloud service
Unable to systematically track data leakage or identify anomalous behaviors	Skyhigh provides a Hadoop-powered anomaly detection engine to spot triggers that indicate the risk of data leakage	Equinix can use Skyhigh to augment and potentially replace a customized, significantly more expensive system consisting of three or four discrete products
Limited understanding of which new cloud service offerings employees might want	Skyhigh helps Equinix CIO determine which types of cloud services are heavily used that may not be known as requirements for employees	Equinix reprioritizes approval process of new types of cloud services and enables to get needed cloud services faster