

Equinix Manages Shadow IT and Enforces Security, Compliance, and Governance Policies for Box



Equinix

Customer Profile

Headquartered in Redwood City, California, Equinix connects the world's leading businesses to their customers, employees, and partners through data centers in 44 markets across five continents. In the US, Equinix operates data centers in Atlanta, Boston, Chicago, Dallas, Denver, Los Angeles, Miami, New York, Philadelphia, Seattle, Silicon Valley and Washington DC.

Industry

Technology

As a company, Equinix has embraced a new generation of cloud services that allow the organization to enable its employees' adoption of online tools quickly and easily so that they can perform their jobs as efficiently as possible. However, the company's Global Information Security Officer George Do began to grow concerned that he lacked visibility into exactly which cloud services were being used by employees.

Connect With Us



CASE STUDY

"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.

Managing Shadow IT and Accelerating Cloud Service Security Evaluations

What's more, the process of approving new cloud services for use by employees required roughly 30 person-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 or security departments of cloud service companies, as well as significant manual one-off efforts to verify security practices and assess 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 cyberattack risks and less on cloud services risks.

Do wanted a tool that could meet all of their needs, including the ability to discover and identify all cloud services in use by Equinix employees, reduce the time and cost of vetting cloud services, provide anomaly detection to spot behaviors that likely indicated data leakage, and prevent access to high-risk cloud services.

Equinix leveraged McAfee® MVISION Cloud to discover the true scope of its cloud services footprint and make the lengthy approval process for new cloud services more efficient. Using MVISION Cloud, Do was able to discover all the cloud services in use and quickly assess their risk. "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."

This enabled Do to implement new services that supported various use cases for Equinix's business units. "Having those ratings from a source we can trust means we can cut time spent onboarding a new cloud service down to three to four hours," says Do. "It has allowed my team to become far more efficient, and I love the fact that MVISION Cloud continually updates its ratings because we would never have time to go back and regularly check up on approved services."

Do and his team also use MVISION Cloud's integration with their firewalls and proxies to serve just-in-time educational messages that coached users away from high-risk services to enterprise-sanctioned services, such as Box.

Challenges

- Difficulty identifying which cloud services were in use and sourcing individual risk scores are overly time consuming
- Unable to systematically track data leakage in the cloud
- Needed to classify data headed to Box and enforce data loss prevention and collaboration policies

Solution

- McAfee MVISION Cloud for Box
- McAfee MVISION Cloud for Shadow IT

Results

- Quickly discovered all the cloud services used by employees and reduced cloud service assessment time and resources by 90%
- Gained actionable intelligence about cloud data leakage
- Extended data loss prevention and collaboration policies to Box meeting security and compliance requirements

CASE STUDY

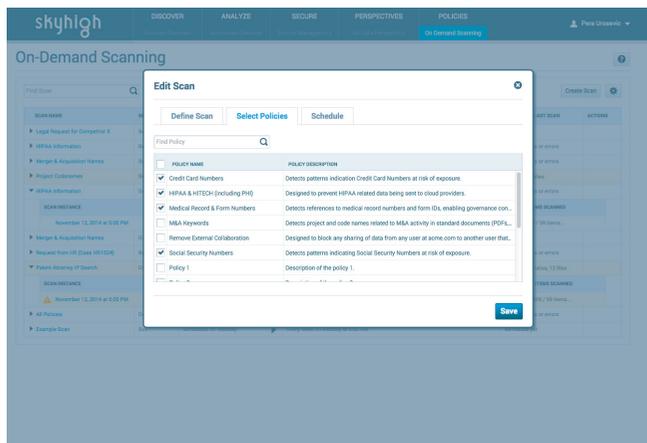


Figure 1. McAfee MVISION Cloud's DLP helps ensure compliance with internal policies and industry regulations.

Extending Security, Compliance, and Governance Policies to Box

With Shadow IT cloud usage effectively managed, they turned their focus to enforcing security, compliance, and governance policies for their sanctioned services. The ability to extend Equinix's existing on-premises data loss prevention policies into the cloud for file-sharing and collaboration services, like Box, was a high priority for Do and his team. By adding MVISION Cloud for Box into the IT portfolio, Equinix was able to ensure compliance with both internal policies and industry regulations.

In utilizing MVISION Cloud's behavioral analytics, Equinix has also been able to baseline normal user behavior and detect anomalous activity automatically across multiple dimensions, including: data sensitivity, access count, volume, direction and geography. In doing so they can protect against risks like compromised accounts and misuse.

Additionally, Do and his team gained the ability to not only audit collaboration activity with third parties within Box, but also enforce collaboration control policies dictating appropriate sharing permissions based on the sensitivity of the data. For example, they can set policies allowing for sharing of important files only with authorized users from business partners with corporate email domains and not those with personal accounts.

Implementing MVISION Cloud for Shadow IT and Box has provided the Equinix team with the tools they need to enable their users with the best services possible and ensure that those services are being used in accordance with their security, compliance and governance policies.

"Overall, working with McAfee has allowed us to not only enable our users to use the services they enjoy and that we trust, but has also allowed us to expedite the procurement process while reducing our overall risk posture," says Do. "It has been a win-win for the entire organization."

"Having those ratings from a source we can trust means we can cut time spent onboarding a new cloud service down to three to four hours."

—George Do, Global Information Security Officer



2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 3835_0418
APRIL 2018