CASE STUDY

McAfee
Together is power.

Allied Irish Bank: Journey to a Secure Cloud

Increasing employee productivity while conforming to regulation

Allied Irish Bank

Customer Profile
Located in Dublin, Ireland, Allied Irish Bank is a financial services firm with 14,000 employees that offers institutional and corporate banking services, as well as personal banking services, including loans of all types and insurance.

Industry
Financial Services

Allied Irish Bank's ambition is to be the leading retail, small-to-medium enterprise, and corporate bank in Ireland and the best bank for owner-managed businesses in Great Britain delivered through digital distribution channels. Delivering on this ambition requires innovation in IT services, including the secure adoption of cloud services by employees.

Connect With Us

Management Starts with Visibility

The CIO has overall ownership for cloud access across the organization so that there is a common approach and single scheme for cloud policy, CSP review, approval and enforcement. "This is not a process that is purely an IT function," says David Cahill, security strategy and architecture manager, "Other departments are heavily involved in making the decisions. We are a big tick box, but we also need the approval from other groups such as legal, compliance, and risk."

With a well-defined and mature process to review and validate all external IT services and partnerships, the Remote Access Forum meets monthly to review requests and authorize requests for external connections and data flows. It has a defined checklist of requirements, multiple steps for provisioning, and a team that reviews and validates all external connections and approves them for use.

It was clear over a year ago that the process was missing some cloud services—lines of business were initializing services outside this process for specific requirements. "AIB's initial step into cloud adoption security was driven by needing to get visibility into Shadow IT," said Cahill. "We couldn't just stick our heads in the sand. We could see that, realistically, there was a degree of activity outside the formal process."

The initial engagement using McAfee® MVISION Cloud was to identify the cloud services in use, their associated security ratings, and the amount of traffic being uploaded and downloaded, thereby quantifying the organization's risk.

"We found a large number of undocumented and unauthorized cloud services in use once we got the visibility we needed. We realized that setting and enforcing classifications and policies would be a much larger piece of work than initially expected," said Cahill.

Allied Irish Bank used the solution's Cloud Registry to review their users' cloud traffic. Having granular visibility into each cloud service's attributes and overall risk scores allowed Cahill and his team to categorize cloud services into different risk levels and focus on the highest-risk services first.

The team was then able to connect with each business unit and discuss the risk associated with each service. To Cahill's relief, all of the unsanctioned services in use by the different business units at Allied Irish Bank had legitimate business purposes, with many of the services being used by the development teams seeking ways to increase their productivity to deliver new services to the bank's customers. Many of the cloud services hadn't been detected by existing control mechanisms at Allied Irish Bank because some of the users had privileged access that superseded existing policy standards (such as authority to use nonstandard browser configurations so that they could test their own code).

"One of the unforeseen benefits of deploying MVISION Cloud was the detailed reporting," says Cahill. "We are able to provide the business units with more information on their users' work to help improve and enable productivity, as the data was more salient and useful than the data provided by standard web proxy logs."

Challenges

- Gain visibility into Shadow IT usage
- Identify and classify cloud service providers
- Ensure procedures are robust and employees educated

Solution

- McAfee MVISION Cloud

Results

- Reduce risk of cloud access by employees
- Faster decision-making to add cloud services to the approved list
- Enable an agile workforce and prepare for future cloud applications

The Remote Access Forum now knew the services in use and their risk level, allowing them to create a list of trusted and authorized services. "As we well know, if we say 'no,' the users will find a way to do what they want to anyway. So instead of saying 'No, you can't do this,' we are now able to say 'Here's a secure and approved alternative' and there is now a published list of approved services for users to choose from," he explained.

Allied Irish Bank sees security as a shared responsibility between the company and the cloud service providers and, as a result, has set up a Security Supplier Relationship Management function purely focused on the security aspects of their suppliers. One of the prime sources for decisions made by this team is the attributes provided by MVISION Cloud. There is an Allied Irish Bank project to visit all major providers and conduct a thorough security review process, asking them about their accreditations, to demonstrate their security credentials, and ensure that they are still partners that Allied Irish Bank trust.

Evaluations of Microsoft Office 365 and ShareFile

As Cahill and his team look to the future and evaluate what the next steps are in their cloud journey, they are evaluating Office365 and ShareFile to see the capabilities and architecture required to provide support in a secure manner and realize that it can't all be done overnight.

Advice to other Organizations

Cahill said, "When I talk to my peers in other organizations, we are all facing the same issues, and we have a shared responsibility around security. Securing the cloud is a huge issue, and our strategy includes breaking the task into three steps."

The three steps he enumerated are;

Step 1: Identify where you are as an organization today.

Step 2: Understand how you want to transform and where you want to go.

Step 3: Set achievable milestones for your journey, and make a plan that you can mobilize, getting you from point A to point B.

"Each one of these steps represents significant progress, but you're not going to boil the ocean and achieve everything overnight," added Cahill. "We are 12 months into our journey, and we're still not at the end. However, we're making good progress."

> "We are able to provide the business units more information on their users' work to help improve and enable productivity as the data was more salient and useful than the data provided by standard web proxy logs."
>
> —David Cahill, Security Strategy and Architecture Manager

McAfee™
Together is power.

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