RISC Networks™

Identifying Cloud, Data Center, and Infrastructure Security Vulnerabilities Through Cloud Discovery

Table of Contents

Cloud Discovery – An Overview

The State of Cloud Discovery

Cloud discovery is the process of analyzing and evaluating current IT environments to determine the most efficient way of using the tools available to plan and complete a successful cloud migration while at the same time improving security and protecting data.

A recent survey found that 75% of IT and security professionals said data center consolidation is important – and 53% said technical difficulties are delaying decisions on these projects. A very small number – 25% - have done nothing in regards to a cloud migration.

These numbers indicate the following: most IT professionals know the value of moving to cloud – improved performance, added security safeguards, improved stability, lower cost of ownership – but simply do not know where to start due to the difficulties of a successful move.

Difficulties of running on the cloud include the following:

- Tracking unmanaged cloud applications - successfully identifying all applications being used by employees, which employees have access to certain apps, and how applications are being used.
- Interoperability – which refers to the ability of systems to communicate with one another. After a migration, the newly set up cloud environment should be compatible with multiple cloud providers – making it possible to switch cloud providers without having to make software changes.
- Dependency Mapping – Dependency mapping enables IT teams to determine the risk and impact associated with changes and problems within a network. The rapid increase of cloud service and data center use makes it difficult to track relationships between interdependent applications and servers.
- Data security – This is the most common concern. 76% of IT execs that are thinking about moving to a cloud system are most concerned with security. Finding an expert to help move data from physical servers into the cloud secures data and saves time and money.
- Lack of support – a lack of support is the most common complaint during and after a cloud migration. Support is key and enables IT teams to continue to do their job and allows customers to continue to experience a seamless transaction.

There is a deeply held fear when it comes to any type of change in IT. Cloud discovery can alleviate this fear by securing data, increasing efficiency, and creating visibility within cloud based networks.

How Cloud Discovery Affects the Industry

With the transfer of data from physical on-site servers into the cloud, tracking the use of cloud applications, user authentication, and customer data presents a new set of problems.

For example, Shadow IT poses a major problem for IT professionals. Shadow IT is when employees bypass the rules established by their IT department and use their own apps and resources, without explicit permission, to perform their job. Often times, Shadow IT solutions are not in line with the security requirements of the organization, therefore putting the company, and consumer data, at risk.

Many of these concerns are addressed through strategic Cloud Discovery.

Cloud Discovery has improved the overall efficiency of IT teams and the companies they work for – and this efficiency has improved consumer trust.

Here Are Five Key Benefits of Cloud Discovery:

1. For companies without robust IT departments, cloud discovery provides them with experts that can help securely manage their day-to-day cloud operations.

2. Cloud updates are provided in smaller increments over time, as opposed to larger, all-at-once updates, allowing users to easily absorb the changes.

3. The continuous updates provided by cloud discovery provide quicker solutions when things don't run as efficiently as possible – this is especially useful when systems are scaled up or down quickly, which the cloud allows.

4. Return on investment is huge with cloud discovery – for example, identifying unnecessary servers, delivering quicker cloud conversions, and providing inventory & usage based cloud cost models are just a few of the ways to increase ROI.

5. Discover and classify all assets – determining which applications are suitable for the cloud and are able to work interdependently and communicate with each other.

Companies That Can Benefit from Cloud Discovery

It is a safe bet that most, if not all, companies can benefit from cloud discovery. Cloud discovery provides all of the value of moving to the cloud, while providing the safest, most efficient move, improving the work of IT teams, entire organizations, and providing a positive, secure, and trusting consumer experience. Examples include:

- Small organizations that lack a robust IT team
- Companies that often have to deal with 'peak traffic.' For example, large holiday rushes to a company's website requires server preparation – having a cloud provider fixes this issue and avoids crashing
- Companies with employees that work remotely and/or use personal phones, tablets, and computers to perform their job – ensuring data security
- Companies that do business in many locations can benefit from cloud discovery – allowing employees to securely collaborate across different applications on different servers without having to be in the same location
- Large organizations that want to improve their agility – the ability to launch cloud based applications quicker to support rapid operational and strategic changes

Pain Points Associated with Cloud Discovery

With all of the benefits provided by the cloud and cloud discovery services, it would be wrong not to talk about the pain points associated with cloud discovery.

Addressing these key points will help make the conversion a success – and helps to keep in mind the needs of employees and the concerns of customers.

Speed bumps to be aware of:

All applications being used through Shadow IT are found through the discovery process. IT will have a hard time taking these apps away once employees have begun relying on them to do their job effectively. This will cause some friction. Be prepared for this and come to the table with solutions

Don't forget the human aspect — assuming software alone is the solution to a cloud migration. Automated migration tools work well for like-to-like server migrations but are not designed for more complex operations like reconfiguring, updating, or transforming servers. A skilled IT staff kept in the loop along the way will be key to these intricate steps that require more technical skill. If a team simply doesn't have the resources to do this, let the cloud service provider know

Communication — especially when classifying applications and current & non-current digital assets. Transparent communication is one of the easiest variables to control and will aid in the success of the migration

Have a *legacy application upgrade/succession plan* in place. Through the application discovery process, the IT team will find legacy applications that are vital to the team and need to be migrated to the cloud. A plan needs to be in place regarding either upgrading the legacy app OS or moving forward with the current OS.

With either decision, the team needs to plan for the worst – i.e. an app implosion during a cloud migration with the OS upgrade. If the decision is made not to upgrade the legacy app OS, take the time to determine the security of the app after the migration as well as how long the app will work after the cloud migration.

Cloud discovery will bring compliance challenges to the forefront. Again, have a plan and set aside the time to address all of these issues.

What is Cloud Discovery?

As stated earlier, **Cloud discovery** is the process of analyzing and evaluating current IT environments to determine the most efficient way of using the tools available to plan and complete a successful cloud migration while at the same time improving security and protecting data while using the cloud.

To simplify this definition, let's look closer at the process.

Cloud discovery enables enterprises to have visibility into all of their different applications in use across their organization - namely, to battle ***Shadow IT.***

Security Concerns Related to Shadow IT

Often times this causes users to have multiple usernames and passwords for the same application, adding to the security threat associated with Shadow IT – including data leaking outside the organization in unexpected ways, unknown and unmanaged supply chain dependencies, and inefficiencies resulting from non-negotiated contracts.

Shadow IT is a problem, whether an IT team believes it or not – here are those numbers:

- A *recent survey* found that 80% of employees use non-approved applications
- Another study found that 8% of organizations actually know the truth about Shadow IT in their organization
- One-third of all employees are saving work data to external 3rd party cloud applications
- The average organization has over 733 unique 3rd party cloud apps within their environment – and one-third are considered high-risk

Cloud discovery provides a full dashboard off all applications being used, their risk scores, who is using them, and employee risk rankings. And, judging by the numbers above, every organization needs to consider a cloud discovery service. The risk of not performing an exhaustive evaluation isn't worth risking the long-term future of your company.

How is Cloud Discovery Linked to Security?

Organizations are at a higher risk of a data breach when employees adopt cloud apps and services without any involvement from IT.

When employees begin to use personal devices for work or create individual accounts on cloud apps without the knowledge of IT for work related tasks – like office productivity, email, document sharing and storage, or using CRM tools - **data can no longer be tracked or secured.**

For example:

- **When apps and data cannot be tracked,** former employees may have access to business-critical data
- **Untracked app usage** causes an inability to identify and track *cloud administrators*, making it impossible to create and edit user permissions, change configuration settings, or extract and delete entire data sets

Security is the Main Concern When Moving to the Cloud. That's Why Successful Migrations Start with Portfolio Analysis.

The best way to address this concern is through cloud discovery. We already know that cloud discovery provides full visibility into one's data environment. Here are some specifics regarding gaining this visibility through a portfolio analysis:

> A cloud diagnostic dashboard is used in cloud discovery to provide application usage details; who is using certain applications, when applications are being used, and what type of device they are being used on. The cloud dashboard also looks at individual users and individual applications - assigning risk factor scores to each for further visibility when managing and controlling application usage
>
> Cloud discovery tracks key analytics by dividing applications into categories (e.g. sanctioned and non-sanctioned), showing the total number of cloud apps being used, total users, traffic volume, as well as complete information of each individual app

These two examples show how cloud discovery can manage cloud app usage and reduce the risk of a data leak. Continuous discovery scans keep the dashboard updated and can analyze usage by department and by individual user. Cloud discovery - and the information it produces - is fully customizable based on organizational needs.

Cloud Discovery Strategies and Best Practices

Top priorities when building a safe cloud environment:

- Actively monitor what cloud apps are in use and who is using them.
- Know the security settings of each application – e.g. password complexity requirements, password lock-out policies, timeout periods, and administrative privileges.
- Analyze user accounts to discover dormant or orphaned accounts and accounts that are accessed by users who are not in the organizational directory.
- Assess the data and analytics regarding user activities to develop usage policies to reduce cloud app related risks.
- Include business intelligence with cloud discovery data. Include application users into the discovery phase, informing them of blackout periods, user acceptance plans, uptime requirements to plan the migration window, and SLAs to plan for high availability infrastructure at the destination environment.
- Create a wave plan – which is best for organizing multiple move groups.

What to Do with the Information You Discover

First, review the cloud discovery dashboard. This is where all of the insight is - including the various risk levels associated with users and applications. Start by reviewing the following:

- Look at the overall cloud app use in your organization – then look at the top app categories being used, and how much of this usage is from sanctioned applications and non-sanctioned applications. Identify any users that pose a security risk based on non-sanctioned app usage and then investigate.
- Evaluate the credibility and reliability of the applications being used across the organization. Within the dashboard, each app is displayed along with a total score, representing the assessment of the apps maturity of use for the enterprise. This number is based on security, compliance, and basic facts about the company that produces the app.
- The IT team will have all of the necessary information and now needs to perform a full analysis and draw conclusions to determine which applications and servers belong in the appropriate move groups based on the facts provided in the discovery process. This analysis will form the different ***move groups.***

How RISC Redefines Cloud Discovery

At RISC, we use a four-step strategic cloud discovery that addresses every security threat and company goal you have.

1. Project Initiation – RISC Networks will conduct an engagement kickoff meeting to set expectations about the purpose of the engagement, the delivery approach, and the timelines. This includes:

- An introduction to the delivery team, their roles, and their responsibilities
- Project goals and the purpose of the engagement
- Explanation of the expected engagement deliverables and work products
- Confirm prerequisites have been met prior to the engagement start

2. Asset Discovery and Validation – RISC Networks' professional services team will assist with Asset Discovery and Validation by doing the following:

- Conduct joint WebEx session to deploy the Virtual Appliance and begin discovery
- Review the Asset Report to validate all expected assets are discovered and accessible
- Assist with resolving inaccessible, in-scope devices
- License all in-scope workloads

3. Application Review Classification & Cost Analysis

- Review customer completed application questionnaire and prepare for analysis
- Review discovery data to ensure CloudScape platform visibility into all critical system dependencies
- Perform application stack rationalization for up to five applications
- Perform inventory and usage based on cost analysis for the discovered IT estate and the five applications
- Review discovery data to identify up to three opportunities for early migration

4. Customer Enablement – We will conduct a knowledge transfer workshop to review best practices for using CloudScape in Discovery and Cloud migration planning.

- Review Cloud Cost reporting including inventory and usage reporting for instant matching and total daily cost
- Review the application stack rationalization process on up to five additional applications
- Includes up to two working sessions of up to two hours each – conducted via WebEx
- Review available online resources

What we deliver upon completion:

- Infrastructure Asset Report
- Licensed portal with up to five defined application stacks
- Inventory and usage based cloud cost models
- WebEx hosted final review

About RISC Networks

IT leaders face tremendous challenges today, higher expectations to deliver on strategic business initiatives, while keeping up with constant technological innovation and transformation. They're looking for new ways of solving problems faster with more efficiency and to help plan new projects and to deliver new technologies into their organizations more effectively and with the least amount of impact on the business and their customers.

RISC Networks stands apart from other vendors with an industry leading Software-as-a-Service (SaaS) delivered, comprehensive IT Operations Analytics (ITIOA) platform that enables IT leaders to transform their businesses with more relevant information with the least amount of effort. RISC Networks analytics encompass three key areas:

Cloud Infrastructure-as- a-Service (IaaS) Migration Analysis – Gives IT organizations greater visibility, flexibility and control over the cloud lifecycle planning process, while significantly increasing the success of workload migrations.

Cloud IaaS Landscape Analysis – Automates the identification and analysis of IT infrastructure readiness for cloud migration and transformation. By collecting IT infrastructure inventory and performance data, this helps IT leaders properly scale, price, and compare the best cloud providers for their actual workload performance and usage.

IT Infrastructure Assessment and Analysis – Helps IT leaders improve the efficiency, agility, and resiliency of their IT infrastructure through a comprehensive assessment of network, server and unified communication components.

RISC Networks™

Visit us at RiscNetworks.com