RELIAQUEST

Securing the Cloud:

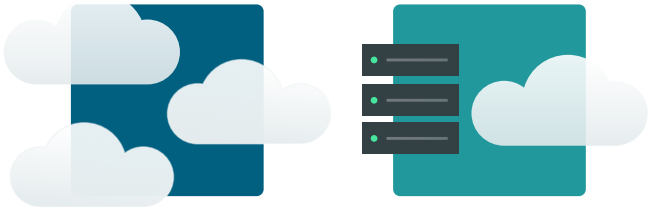
How to Increase Cloud Visibility to Power New Business Opportunities

As enterprises migrate critical data to the cloud, how can security teams increase visibility into the cloud and across environments to reduce risk, detect and respond to threats faster, and continuously mature security programs?

Introduction

Cloud adoption continues to accelerate in the enterprise – as does the complexity of cloud infrastructure. Ninety-three percent of enterprises now have a multi-cloud strategy, while 87 percent have a hybrid cloud strategy, according to a recent industry survey of 750 enterprise cloud decision makers.[1] Migrating data to the cloud has become a strategic way to optimize business opportunities while minimizing risk. But with the move to the cloud comes concerns about seeing and studying threats to these complex storehouses of data, as well as the need to understand what is normal, baseline behavior.

STRATEGIES USED AMONG ENTERPRISES, 2020 STATE OF CLOUD REPORT



93% MULTI-CLOUD

87% HYBRID CLOUD

The cloud platforms themselves, led by Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, can add to the challenges of visibility. It's common for organizations to build complex infrastructure on top of cloud platforms – such as multiple applications across Kubernetes clusters on top of AWS's cloud infrastructure. But the usual methods of gaining visibility into data and threat activity, such as accessing raw security logs, are not as easy to deploy when the infrastructure is built on a platform the security team doesn't own or manage. A cloud vendor's logs may not be what's needed for the desired levels of visibility and analysis. And without this visibility, teams can't be confident in their analysis of security threats or create benchmarks for improving cloud security.

[1]Flexera, Cloud Computing Trends: 2020 State of the Cloud Report
https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

Equipped with an awareness of what stands in the way of visibility into the cloud – such as disparate and disconnected methods for organizing data – and a lineup of solutions and strategies that can shed light on hard-to-access areas of the cloud, security teams can bring cloud-based data and threats out of the shadows. Security teams can do this by becoming proactive about threats in the cloud and making plans for normalizing data under a single standard, using automation to improve data-gathering and analysis, and continuously measuring and improving cloud visibility, instead of reacting to bad actors' behavior after the damage is done. Normalizing data under one standard is also more cost-efficient: By gaining the ability to search and analyze activity across many cloud platforms, security teams save the time and expense of moving or removing cloud data in order to make it more visible.

WITH VISIBILITY COMES SECURITY:

As the saying goes, you can't protect what you can't see. And if cloud data is multiplying by leaps and bounds, there's even more that needs to be seen and managed.

In this paper, you'll learn:

WHY you need greater visibility into the cloud

HOW to identify the most important roadblocks to cloud visibility

WHAT practices and technology solutions can improve visibility across data that spans multiple cloud platforms

Benefits of more visibility into the cloud

With visibility comes security: As the saying goes, you can't protect what you can't see. And if cloud data is multiplying by leaps and bounds, there's even more that needs to be seen, integrated, and managed. Ideally, this visibility spans not just cloud platforms, but also security information and event management (SIEM) systems, endpoint detection and response (EDR) systems, and more.

Here's why visibility into the cloud is a must-have for building a best-in-class security program.

RISK REDUCTION

Staying on top of threats requires ongoing vigilance – and a proactive, not reactive stance to detecting and mitigating threat activity. Visibility into the cloud, as well as the apps running along with data, allows organizations to reduce risk.

Once your security team gains this visibility, it must also apply relevant security controls to data in the cloud, based on what needs to be protected. For example, if customer data is stored in the cloud, organizations must assess the risks that data breaches pose to this critical information. The cloud platform itself might not provide the data or visibility you need to assess security – such as whether internal applications, databases, or websites aren't running properly, or whether API keys have been exposed.

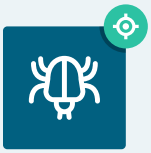
Another way to reduce risk through visibility is by auditing access permissions. By monitoring who has access to applications, security teams can better understand the activity and who they see in their apps.

SIMPLIFIED CLOUD MANAGEMENT

If organizations are relying on multiple cloud platforms and apps – for instance, building their cloud infrastructure on Azure as well as AWS – then greater visibility allows them to more effectively manage complex cloud environments. Security teams can search for threat patterns simultaneously across multiple platforms, especially as they layer apps and infrastructure into the cloud instead of manually searching across each one.

FASTER REACTION TIMES

If you have visibility into the cloud, you want the ability to react quickly to what you can see. When security teams see threat behavior, automation allows them to quickly gather data and take action against behavior such as lateral threats. By matching automation with visibility, security teams gain speed as well as data-gathering capabilities and the ability to launch proactive threat hunting campaigns across all environments, rather than individually.



THREAT HUNTING

Organizations migrating to the cloud need the ability to search for abnormal behavior and attack commonalities. With greater visibility, security teams can better examine attacker threat behaviors and time ranges. Just as with risk reduction, threat hunting paired with visibility allows organizations to proactively weed out security threats. Companies that create a cloud-based app that might be subject to new vulnerabilities can re-examine threat profiles for that app to expose patterns of threat behavior.

THE ABILITY TO DRIVE BUSINESS VALUE

With cloud visibility, organizations can see where malicious traffic is coming from, detect Indicators of Compromise (IOCs) that signal potential issues in customer-facing apps, and ensure uptime and continuity – all of which improve the business, and all of which are possible through greater cloud visibility. A business may drive value by keeping customer-facing apps up and running; it may drive value by improving security reporting to its board; or it may drive value by marketing its security capabilities as a competitive differentiator. In all these cases, visibility can accelerate this value creation.

MATURING YOUR SECURITY PROGRAM

Metrics and measurements can help define value of the security program, therefore helping you communicate value to other stakeholders like the board of directors. By measuring visibility and sharing value metrics with boards, organizations can gain budget for new security program enhancements, and take part in strategic decision-making – all of which help mature security.

Visibility into the apps running in the cloud and related data allows organizations to proactively identify and mitigate threat activity.

Overcoming the hurdles to cloud visibility

DATA VOLUME

The sheer volume of data stored in the cloud inhibits visibility. Add complex multi-cloud and hybrid cloud environments, and it's easy to see how visibility can be obscured. A related problem is knowing which data sources to analyze, and which ones have meaning in terms of security. Based on an informal ReliaQuest survey of approximately 200 enterprise CISOs, it's estimated that most enterprises have visibility into about 40 percent of their data; of that 40 percent, only about 10 percent is actionable, which raises the question of how to increase visibility into actionable data.

VARIOUS METHODS FOR ORGANIZING DATA

To gain visibility into cloud data – and to identify that 10 percent of data that is truly actionable – security teams need answers to questions about data organization, such as:

- Where will the logging tools reside?
- What compliance regulations dictate where the data lives?
- What "behind the scenes" cloud infrastructure logs should also be gathered and monitored for unauthorized/malicious activities?

UNDERSTANDING WHAT "NORMAL" IS

Security teams need baselines for what's normal and not in terms of traffic and user behavior. Can organizations gain visibility into enough of the cloud environment to create these baselines? Can they view that sliver of actionable data on which to decide what is normal? And how can organizations understand how data moves between clouds?

DATA CORRELATION ACROSS MULTIPLE CLOUDS

In a multi-cloud and hybrid cloud world, organizations are likely to move data among clouds – for example, from a storage app like Dropbox into a CRM app such as Salesforce. The problem with gaining visibility across these clouds is similar to the challenge of gaining visibility across on-premise systems: integrating and correlating data across multiple tools. As noted in ReliaQuest's recent paper, Six Steps to Adopting Automation for Faster Detection and Response, the issue of too many tools, plus too little integration of tools, adds up to more data noise than a team can analyze and understand – all of which leads to less visibility into threats and less-efficient security teams.

COMPLIANCE CONCERNS

Organizations that need to comply with regulations imposed by GDPR, HIPAA, or PCI-DSS need to be concerned about where data resides, what type of data is in the cloud, and how long it must be stored. If data can't be removed or shifted to other clouds, it's not easy to gain the necessary visibility. In addition, organizations worry that they may inadvertently view data that is private – or that unauthorized people have access to cloud data.

With a unified view of data, security teams can perform analysis and threat hunts faster, without the need for extensive knowledge of each technology's field names, syntax, or query language.

4 strategies for confidently increasing cloud visibility

1. SETTING BASELINES

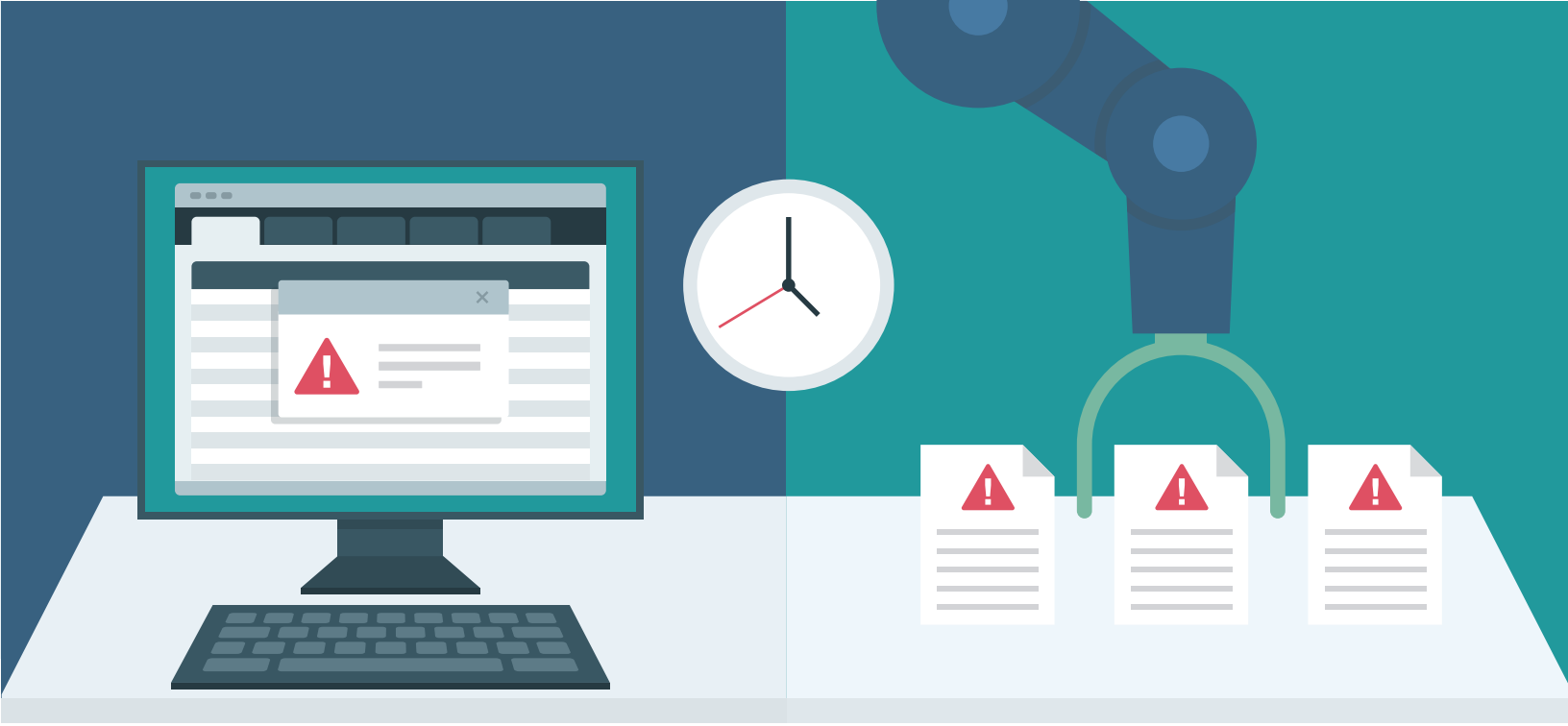
Teams need consistent tools and processes for establishing normal activity in the cloud. With these baselines established, security teams can make sense of what they see to detect and investigate activity. For example, they may notice alerts for anomalous activity, which appear when AWS CloudTrail logs show someone doing activities they haven't done before, including unusual user access, denies, API calls, or commands after authentication.

2. NORMALIZING DATA INTO A SINGLE STANDARD

Not every person on a security team may be familiar with the syntax for AWS, Google Cloud Platform, and Microsoft Azure. It's somewhat ambitious to assume security personnel know the ins and outs of every single cloud and that teams can easily get up to speed on the syntax, query languages, and alert logic across best-of-breed security tools.

It's far easier to train analysts on a single standard, as well as enabling their access to manage many different data sources in a single view. Teams need the ability to aggregate and normalize tool-specific fields across integrated technologies to effectively correlate and query across technologies. A translation engine, which maps and normalizes fields, provides analysts with not only a unified view across technologies, but also a mechanism for analysts to query across tools in their preferred syntax or language such as JSON.

With a unified view of data, security teams can perform analysis and threat hunts faster, without the need for extensive knowledge of each technology's field names or search language – speeding time to analyst productivity and time to respond.



3.ADOPTING AUTOMATION

Security teams should spend their time investigating leads from data – not gathering the data manually from their many cloud platforms. Automation allows teams to skip the data-gathering phase and go straight to investigations and take action.

With more time to use their access to data, teams can implement training around the difference between normal and abnormal user behavior. They can also direct data about event types that don't need immediate action into storage (for use in future threat-hunting activities), or to the organization's SIEM for actionable events. In addition, teams can re-classify severity and dynamic scores based on additional context learned over time.

Overall, automation can be used to improve enrichment, triage, and remediation actions. Enrichment plays not only save time but also apply consistent intelligence to activities such as threat hunting: Instead of relying on team members' varying levels of skill and experience, security analysts can use automation to minimize the chances of errors and missteps.

> **Automation plays a key role in increasing visibility into cloud platforms: look for opportunities to automate beyond remediation, such as in the data-gathering phase, so your team can quickly and consistently investigate events and proactively threat hunt.**

4. MEASUREMENT AND CONTINUOUS IMPROVEMENT

Visibility can be measured: In fact, such measurements are valuable to security leaders looking to benchmark strengths and improve security. Metrics and measurement on visibility help drive maturity in security programs by justifying ROI, including security teams in strategic business decision-making, and building budgets for future security initiatives. For example, understanding your cloud footprint and your percentage of visibility can help your team identify the 10 percent of actionable cloud data on which the team should focus attention.

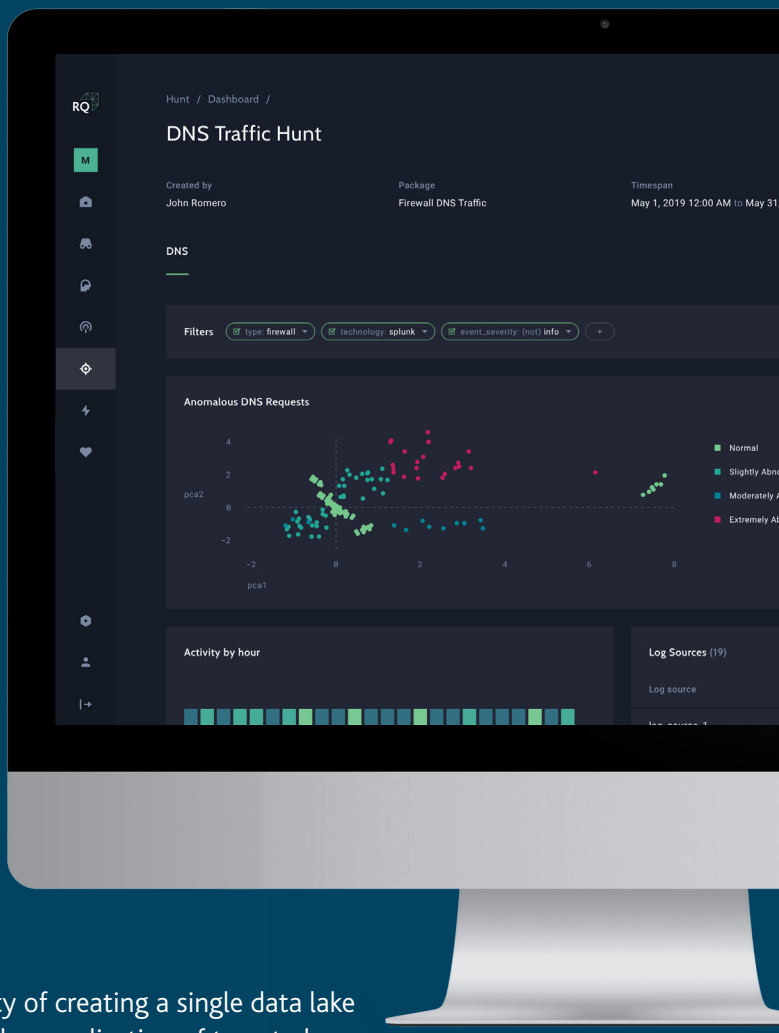
The business value of visibility

The flip side of the saying, “you can’t protect what you can’t see,” is the top-line benefit of greater cloud visibility: When you can see data, you can protect what’s most important to your business.

Stopping threats is a vital benefit, but visibility does more than help block attackers: It aids in decisions related to where data should live, how data types are exposed to varying levels of risk, and how resources will be applied to clouds. Visibility also streamlines compliance tasks. When they understand more about where data resides and its risks in the cloud – and by avoiding unnecessary movement of data in the name of achieving visibility – organizations can meet compliance requirements while still improving control over their environments.

By baselining, tuning, and continuously monitoring current security investments, security teams can ensure performance and apply the proper controls required to gain visibility across cloud environments and enable new business opportunities.

How ReliaQuest GreyMatter Correlates and Integrates Data for Increased Cloud Visibility



ReliaQuest, a global leader in cybersecurity, delivers industry-leading visibility and automation on demand across complex environments with a platform purpose-built to protect organizations from security breaches. GreyMatter is the first cloud-native SaaS solution that integrates and improves an enterprise's on premise and multi-cloud technologies, unlocking the power of next generation cybersecurity. By increasing visibility through the platform's proprietary universal translator and use of automation and artificial intelligence, GreyMatter saves security teams valuable time and increases effectiveness by enabling automatic and continuous threat detection, threat hunting, and remediation.

ReliaQuest GreyMatter provides holistic visibility to recognize threats across all of your environments and attack surfaces, including cloud, without the impracticality of creating a single data lake to perform analysis. Through on-demand aggregation and normalization of targeted, fragmented data into a single, cohesive view, ReliaQuest GreyMatter enables faster, more comprehensive threat investigations as well as retrospective IOC searching and long-term behavioral analysis threat hunting.

LEARN MORE ABOUT RELIAQUEST GREYMATTER

> **ReliaQuest GreyMatter increases visibility into the cloud by integrating and normalizing data from disparate technologies, so you always have a unified view to immediately and comprehensively detect and respond to threats.**

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com

Copyright © 2018 ReliaQuest, LLC. All Rights Reserved. ReliaQuest, RQ, and the ReliaQuest logo are trademarks or registered trademarks of ReliaQuest, LLC of its affiliates. All other products names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All other information presented here is subject to change and intended for general information. Printed in the USA.