What Are the Benefits and Challenges of Improving Cloud Visibility?

Devolutions

ORGANIZATIONS OF ALL SIZES STORE THEIR DATA IN THE CLOUD

The cloud is nothing new in the world of technology and it has already become mainstream. Organizations of all sizes store their data in the cloud and use various cloud-based solutions for different purposes. Some organizations don't even know they are interacting with the cloud when using certain types of software.

Given the growing popularity of cloud solutions, it's no surprise that cloud visibility has become a subject of increasing research. Numerous studies have provided us with valuable insights into cloud security and the way we use cloud solutions. For example, according to research, about 75% of organizations have experienced problems with virtual machine security because they didn't have proper cloud visibility.

Common Challenges

Researchers have also discovered that the increase in IT complexity is influenced by the increasing number of remote workers and the growing number of devices. However, there is one factor above all that is making the biggest impact on the rise of IT complexity — and that's cloud visibility. Launching something is easy, and anyone can easily spin up a cloud instance. While it's easy to forget such details, the complexity increases.

One important factor that poses challenges for visibility is the complexity of cloud configuration. Infrastructures and applications are getting increasingly more mature and sophisticated. They generate large volumes of diverse monitoring data. For instance, a typical enterprise has at least three monitoring tools, four data-ingestion tools, and many security analytics tools that have their own logs and dashboards.

There are billions of log records, and many of them are just strings of text. Therefore, traditional log management approaches often fail to provide the context and visibility necessary to analyze attacks. Without proper visualization capabilities and advanced analytics, a response to cloud security incidents can take more than 200 days.

Obscured Visibility

A customer of the public cloud is responsible for securing their traffic flows and data in the shared security responsibility model. However, this responsibility becomes a problem if an organization doesn't have the necessary visibility into its cloud assets when working with multi-cloud and hybrid environments. Quite often, organizations are unable to monitor some common problems and don't know who accesses its cloud applications and services, or where the traffic is coming from.

Therefore, it's no surprise that research data shows that gaining visibility into data traffic and applications is the main priority for the majority of public cloud users. Nevertheless, 87% of organizations are afraid that the lack of visibility might hide various security threats, while only 20% of companies are able to monitor their cloud environments properly.

Dynamic Applications

Self-contained, single-tiered, and monolithic applications can run on cloud infrastructures without any problem, but they do not possess the flexibility and agility of cloud services and resources. As a result, more and more users are choosing microservice architectures, where applications consist of multiple autonomous services that communicate using lightweight protocols like HTTP and REST APIs. In such cases, each of these

services has its own database requirements, logic, and UI. As a result, there's a need for a development team that would manage the modular application, making sure all the components are properly optimized.

The cloud-native microservices led to the development of two advanced cloud technologies: containers and Functions as a Service (FaaS), which are serverless. FaaS separates the application layer from the infrastructure layer. Simply put, developers specify the infrastructure requirements when building their code. Fully-managed services like AWS Lambda can run their event-triggered code, scaling the resource automatically depending on the requirements.

Containers offer another level of abstraction. These are standard software units that include code along with all the dependencies. As a result, applications can run flawlessly in different computing environments. The container image is run by a container engine as a stand-alone executable package. In this case, the container engine makes sure that the software will work the same, no matter what host operating systems and infrastructures are used.

Compute services of cloud-native applications usually have short lifespans and are designed to be ephemeral. Attackers cannot be in a system long enough, so they are forced to switch tactics, but the problem doesn't disappear. "For example, attackers can scale such applications automatically and create short repetitive tasks," notes Sarah Lobert, a security expert from the writing services review website Best Writers Online. "Put simply, they can steal not the whole credit card number at once but a few digits at a time. Monitoring attacks of this kind is especially difficult."

The Benefits of Improving Cloud Visibility

Finding the root cause of problems with application performance can be a big problem for businesses that rely on machine data. The reason is that machine data is not precise enough because it comes from multiple sources and cannot simplify the analysis using a common language. To get useful service assurance information, you need to aggregate the machine data. Therefore, there is a need for not only sophisticated algorithms but also increased human involvement in the process so that you can find the necessary information in this abundance of data.

When the complexity and cloud expansion accelerate, this method leads to visibility restrictions and obstructs a business' agility by increasing Mean Time to Resolution (MTTR), which is the average time between the moments when the issue was reported and solved. If organizations want to capitalize on the features of cloud solutions, they have enough visibility to monitor their entire hybrid or multi-cloud infrastructure. This way, they can ensure higher efficiency and improve their MTTR.

A smart approach is to monitor all the IP packets that cross the delivery infrastructure of the service and

to analyze them in real-time. This way, organizations can better understand the way applications perform and determine any potential problems with service delivery. IP packets of wire data are obtained from applications directly, using transactional conversations.

Wire data is extremely accurate and reliable. In addition, it perfectly fits the analytical purposes because it's delivered in a common language. Developers can improve visibility and use more efficient solutions by consistently monitoring wire data and accessing actionable datasets with information on issues as they happen. This is one of the best approaches if you want to improve situational awareness.

Final Thoughts

Since enterprises are changing all the time, and the elements of on-premise and cloud infrastructures are also evolving, the success of digital transformation becomes directly dependent on the visibility across the whole infrastructure. Whenever IT changes, there are new possibilities for failure, and these risks affect organizations when they move to the cloud.

Improving cloud visibility, organizations can avoid a number of issues associated with security threats and application performance. This way, it becomes possible to improve the efficiency of many processes, understanding what may cause certain problems and coming up with effective solutions.