DivvyCloud

2020 Cloud Misconfigurations Report

Breaches Caused by Cloud Misconfigurations Cost Enterprises Nearly $5 Trillion in 2018 and 2019

Executive Summary

Data breaches occur for many reasons, but breaches caused by cloud misconfigurations have been dominating news headlines in recent years. DivvyCloud researchers compiled this report to substantiate the growing trend of breaches caused by cloud misconfigurations, quantify their impact to companies and consumers around the world, and identify factors that may increase the likelihood a company will suffer such a breach.

Enterprises struggle to implement proper cloud security, resulting in more than 33 billion records exposed in 2018 and 2019 alone.

Foreword

The adage of “move fast and fail fast” is losing relevance in a cloud-centric world. In the spirit of agile development? Sure, but when it comes to cloud security, failure is not an option. Yet the sheer number of data breaches substantiates an unsettling trend organizations are not prioritizing cloud security. Frustratingly, the underlying issues that cause these breaches “misconfigurations” are often not complex. Meanwhile, consumers, regulators, and partners expect due diligence from the organizations entrusted with their data. Having an unprotected server is not an acceptable reason for a breach, nor is any other misconfiguration.

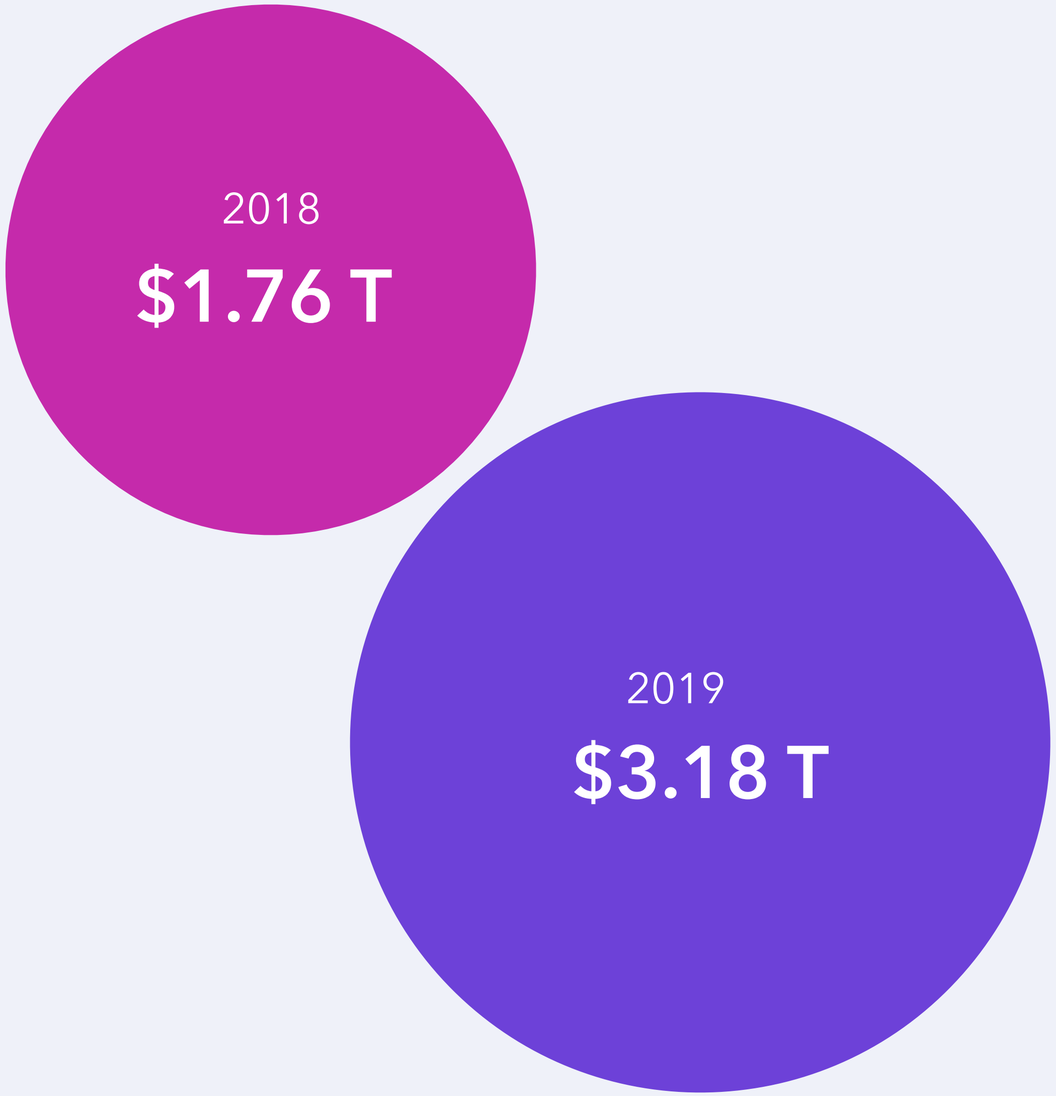
When moving at the speed that technology enables within the cloud, configuration management is key. Organizations need to think about things like the “reasonable person” standard. For example, when receiving medical care, would a reasonable person expect to receive a consultation from their physician before being treated? If a physician proceeded with treatment before discussing the diagnosis and treatment with a patient, would a jury find the physician negligent in a court of law? Most likely, a jury would indeed find the physician negligent.

As you’ll see in this report, organizations are not approaching cloud security management with such standards in mind, and their negligence is evident in the number of data breaches that we see in this report. Perhaps it would be more comforting if there were only a few industries experiencing these issues, but that is not the case. This is a widespread problem affecting every industry, and it’s something that we need to solve collectively. No industry or company can choose to ignore this problem because it’s only gaining more momentum, and it’s clearly not going away. Let's take a look at some of the data!

Anthony Johnson

Former CISO at multiple Fortune 100 companies; currently Managing Partner at Delve Risk

Prior to joining Delve Risk, Anthony served as the Global CISO and Managing Director for multiple Fortune 100 companies, including Fannie Mae and the Corporate & Investment Bank at J.P. Morgan Chase & Company.



The High Cost of Cloud Misconfigurations

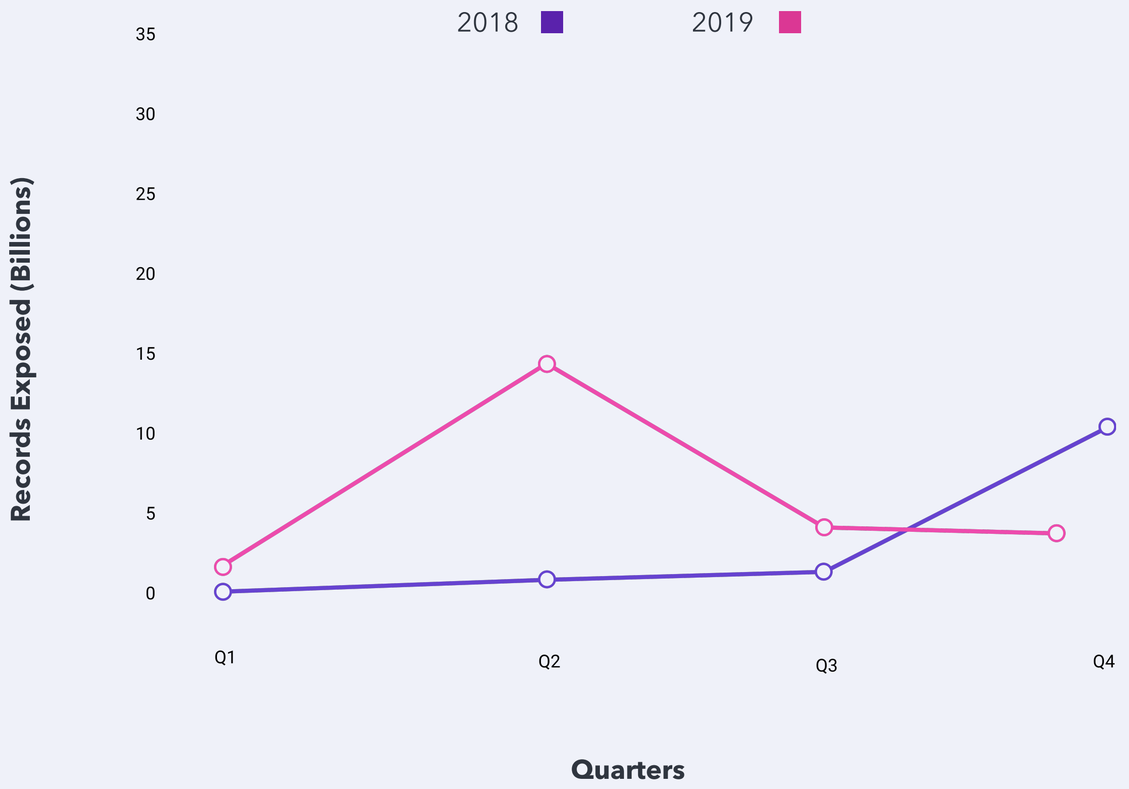
Breaches caused by cloud misconfigurations in 2018 and 2019 exposed nearly 33.4 billion records in total. According to the Ponemon Institute's 2019 report, the average cost per lost record globally is $150. Multiplied by the number of records exposed, misconfigurations cost companies worldwide nearly $5 trillion in 2018 and 2019 alone.

Gartner estimated that the worldwide public cloud services market was $182.4 billion in 2018 and $214.3 billion in 2019. This means that the cost to companies due to breaches caused by cloud misconfigurations is more than 12 times the amount of worldwide investments in cloud services. Therefore, companies must adopt proper cloud security in order to protect this investment and prevent devastating costs associated with data breaches.

Tracking the Impact of Cloud Misconfigurations

Researchers observed an upward trend in the data. Year over year from 2018 to 2019, the number of records exposed by cloud misconfigurations rose by 80%, as did the total cost to companies associated with those lost records. Unfortunately, experts expect this upward trend to persist, as companies continue to adopt cloud services rapidly but fail to implement proper cloud security measures. In 2018, there were a total of 11.8 billion records exposed with a total cost of $1.76 trillion. By 2019, that number rose to 21.2 billion exposed records, and the cost rose to $3.18 trillion.

It is important to note that these are conservative estimates, as not all of the breaches examined in this report could quantify the exact number of records exposed. What's more, according to a report from McAfee, 99% of all misconfigurations in the public cloud go unreported—meaning the actual total number of breaches caused by misconfigurations and total associated costs to companies are likely far greater.

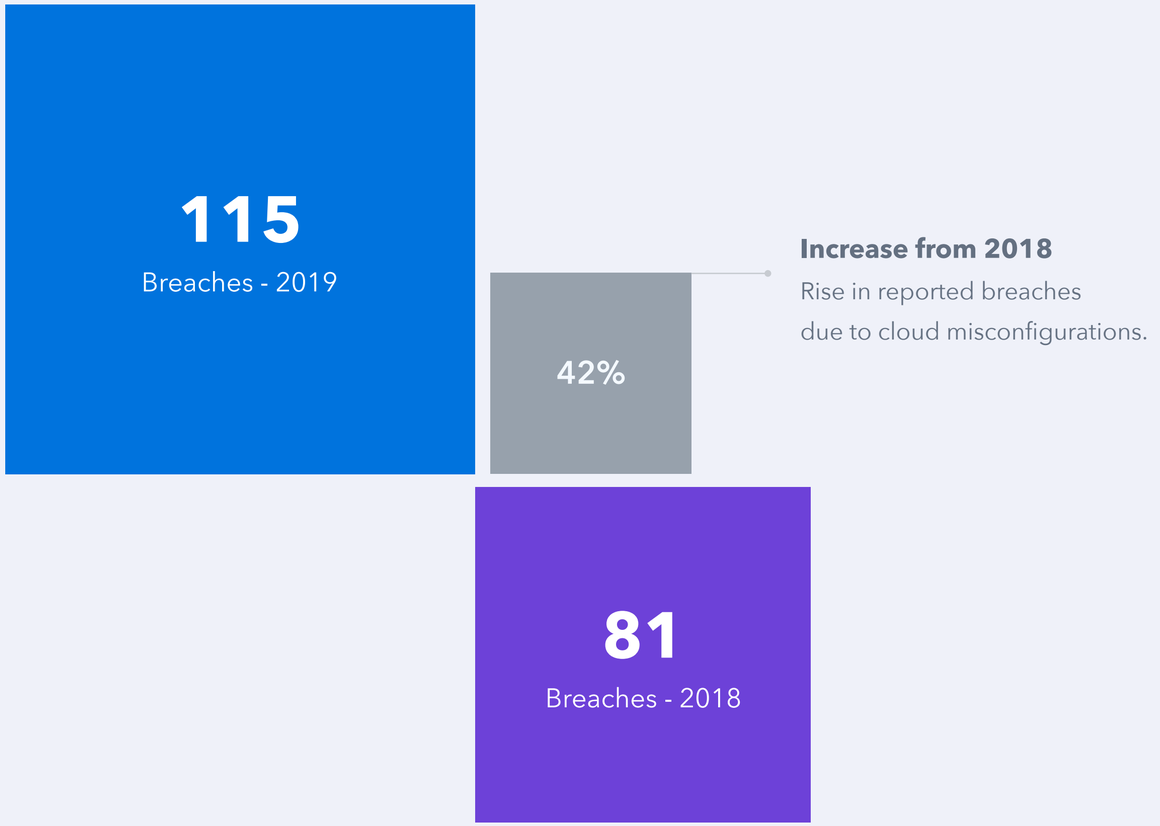


Quarter	Records Exposed	Quarter	Records Exposed
Q1 2018	26,003,688	Q1 2019	1,144,659,753
Q2 2018	534,541,784	Q2 2019	13,762,097,400
Q3 2018	959,874,897	Q3 2019	3,197,787,100
Q4 2018	10,234,978,357	Q4 2019	3,085,749,185

Data Breaches on the Rise Worldwide

In 2018, 81 major breaches attributed to cloud misconfigurations were reported, and in 2019, this number rose to 115—a 42% increase. This trend directly correlates with rising adoption rates of cloud services. As companies flock to the cloud for its speed and agility, they often fail to implement and enforce proper security.

Interestingly, 76% of all records exposed occurred during the nine-month period from Q4 2018 to Q2 2019. The second quarter of 2019 was the most devastating in terms of the number of records exposed, accounting for 42% of all records exposed due to misconfigurations that year.



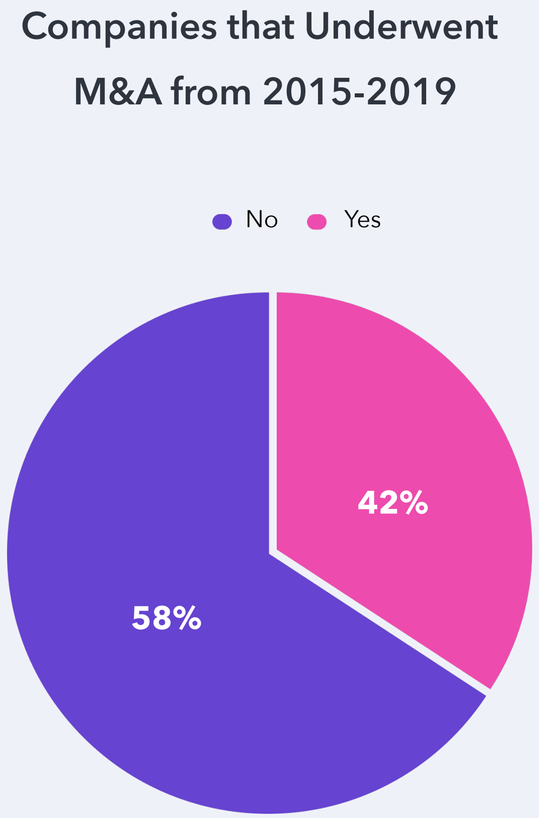
The Cloud Native Difference

While it's difficult to pinpoint exactly when the first "cloud native" companies were founded, a strong case can be made for the year 2010, based on wider availability and popularity of the tools required to truly be cloud native. By evaluating the companies that suffered data breaches due to cloud misconfigurations, we see a strong correlation between the likelihood of a breach and the year a company was founded. In 2018 and 2019, 68% of the companies that suffered a data breach caused by a cloud misconfiguration were founded prior to 2010. Only 6.6% of these companies were founded in 2015 or later. These statistics indicate that older companies that are transitioning to the cloud are having a harder time implementing and continually enforcing proper security controls over their cloud environments when compared to younger companies "born in the cloud."

The M&A Factor

The Marriott/Starwood breach that was first reported in late 2018 serves as a prime example of how failing to execute proper due diligence during mergers and acquisitions (M&A) can lead to massive security blunders. Knowing how complicated it can be to securely merge disparate IT environments, the researchers of this report analyzed whether companies undergoing recent M&A transactions were more likely to experience a data breach due to cloud misconfigurations, and indeed they found a positive correlation.

Out of the companies identified in this study, 73 experienced an M&A transaction between 2015 and 2019 (nearly 42%). Notably, three of those companies experienced more than one data breach due to a cloud misconfiguration between 2018 and 2019. Companies undergoing M&A must ensure they apply proper security, governance, and compliance to all data across the disparate IT environments involved in the deal, including data stored in the public cloud. Data breaches can also negatively impact M&A deals before they are finalized, or cause them to fall through altogether. For example, in the Verizon-Yahoo merger, after it was discovered that the Yahoo breach was much more extensive than originally thought, Verizon slashed its offer by $350 million.



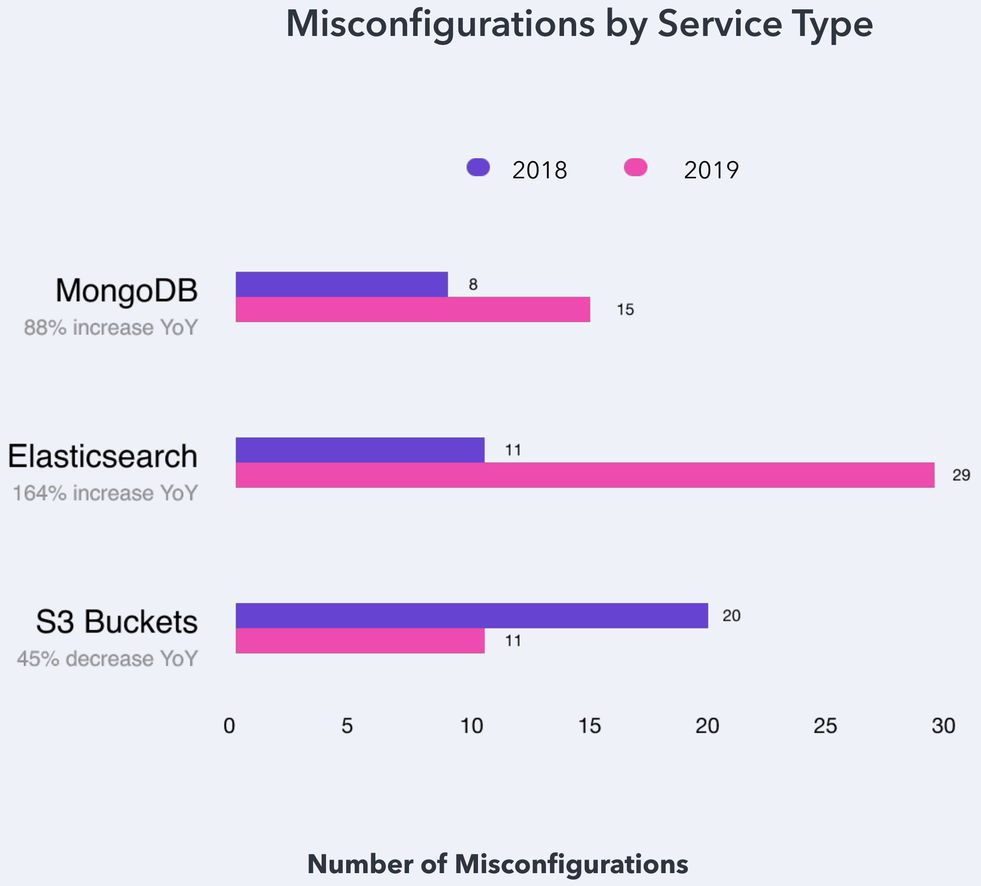
Misconfigurations Don’t Discriminate

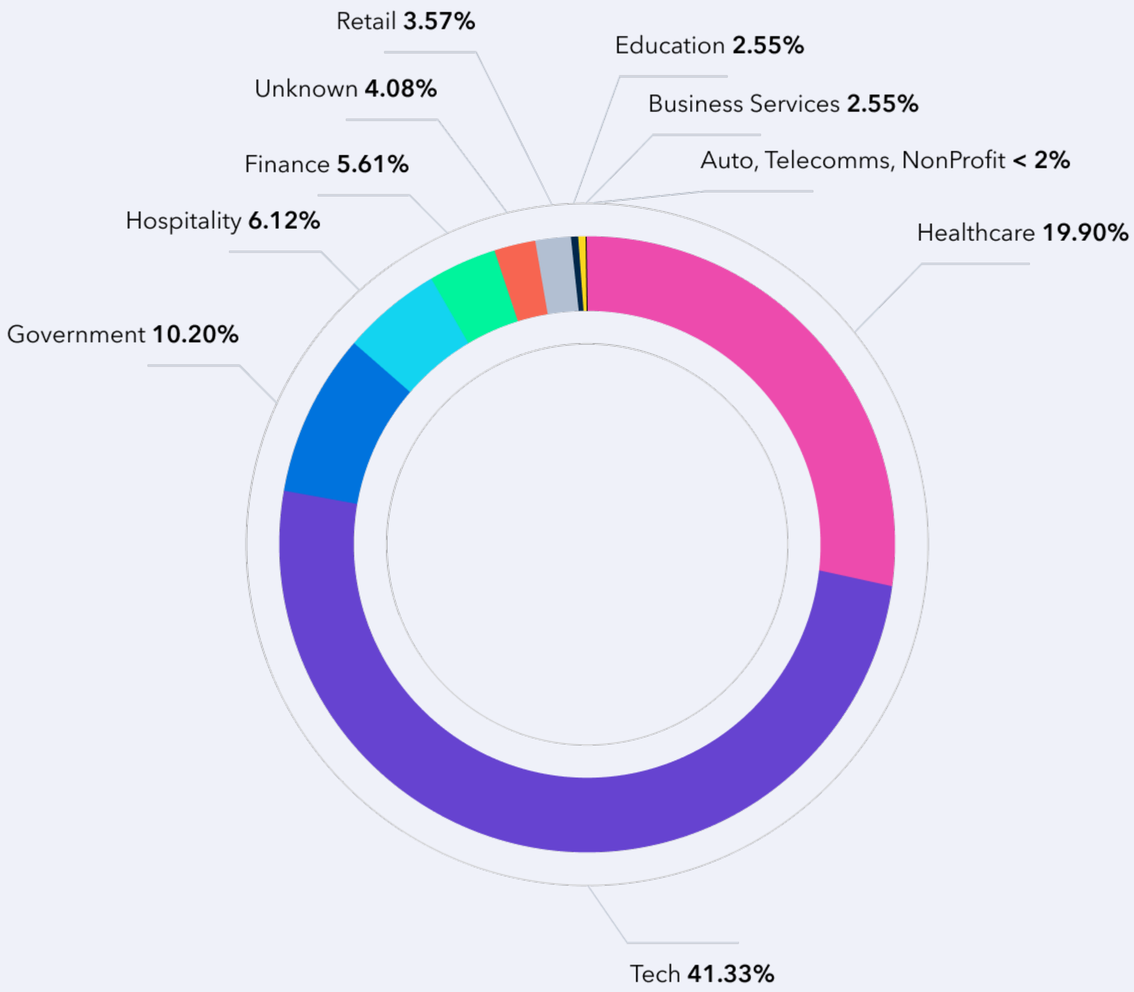
In analyzing the 196 data breaches caused by cloud misconfigurations, the researchers evaluated the type of services involved in each incident and found:

- Elasticsearch misconfigurations accounted for 44% of all records exposed in 2018 and 2019, and was also the most common database breached across all platforms (20%)
    - The number of breaches caused by Elasticsearch misconfigurations nearly tripled from 2018 to 2019
- S3 bucket misconfigurations accounted for 16% of all breaches
    - S3 bucket misconfigurations decreased 45% from 2018 to 2019
- MongoDB misconfigurations accounted for 12% of all breaches
    - MongoDB misconfiguration instances nearly doubled from 2018 to 2019

AWS services compile the bulk of the breaches evaluated in this report, however, though Microsoft Azure, Google Cloud Platform, and Kubernetes make up the minority of total incidents, this is still a big deal as misconfigurations plague all cloud services.

These facts and figures are not a reflection of the native security capabilities of each of the cloud service providers. Gartner estimates that through 2025, at least 99% of cloud security failures will be the customer’s fault.





Breaches by Vertical

Of the incidents evaluated in this report, 41% were breaches of Tech companies, followed by Healthcare at 20%. Government agencies accounted for 10% of the breaches, followed by Hospitality at 6%, Finance at 6%, Retail at 4%, Education at 3%, Business services at 3%, and other services at 7%.

Why Do Cloud Misconfigurations Plague Companies?

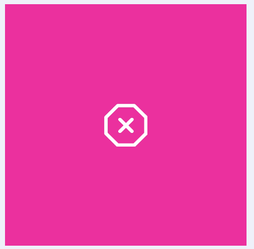
Most enterprise companies implementing a public cloud strategy are doing so quickly out of necessity—they need to innovate to maintain a competitive edge, which requires the agility and speed only the cloud can offer.

However, as the results of this report (and the litany of headlines) clearly demonstrate, organizations that lack a holistic approach to security are more vulnerable to undue risk mostly caused by:

INEXPERIENCED USERS

FAILURE TO SHIFT FROM OUTDATED SECURITY MODELS

LACK OF UNIFIED CLOUD VISIBILITY



UNPRECEDENTED RATE OF CHANGE SCALE AND SCOPE

Seemingly overnight, we witnessed the shift from career IT and security professionals who understood the security process, to people who had never thought about security when deploying applications in their infrastructure. The number of people touching cloud infrastructure has dramatically increased. In the past, you may have had 40 people in an organization touching infrastructure at any moment. Today, it’s common to see 3,000 people deploying applications and making engineering changes to a given infrastructure. Production deployments have accelerated from weekly to hourly. These continuous integration and continuous deployment (CI/CD) approaches lead to massive infrastructures encompassing large numbers of users making simultaneous changes. These factors lead to loss of control and self-service bypass that doesn’t take into account security, governance, or even compliance—all of which are critical lessons to engrain in IT teams. These enterprises are failing to improve security, take control, and minimize risk as they embrace the dynamic self-service nature of public cloud and container infrastructure. As a result, they’re suffering data breaches, which are devastating not only their organizations, but the public as well.

More often than not, when a breach makes headlines, it’s the company that owns (or is entrusted with protecting) the exposed data whose reputation suffers, not the underlying cloud service provider. When it comes to security, there is a shared responsibility relationship between customer and cloud service provider. The cloud service provider is responsible for securing the underlying components of cloud services—a task they typically fulfill without issue. The customer is responsible for securing *how* they use the cloud services, including properly configuring identity and access management (IAM), storage and compute settings, threat analysis and defense, and the security of the application and data processed and stored in the cloud. It’s the customer’s end of the bargain that is most frequently overlooked. As previously mentioned, Gartner predicts that through 2025, 99% of cloud security failures will be the customer’s fault, rather than that of the cloud service provider.

Best Practices

To avoid cloud misconfigurations, companies need to immediately shift toward a new model of security that provides continuous controls and enforces secure configurations of cloud services, instead of attempting to do so weeks, months, or years later. This shift should not be viewed as a one-time event; rather, it should be monitored and enforced constantly and in perpetuity, as the dynamic, software-defined nature of the cloud leads to frequent changes.

Organizations need a security solution that provides the automation essential to enforce policy, reduce risk, provide governance, impose compliance, and increase security across a large-scale, hybrid cloud infrastructure. Automation takes the headache out of making cloud infrastructure secure in a shared responsibility world by providing a framework for what organizations should be doing via a continuous, real-time process. By leveraging security automation, companies can stay agile and innovate while maintaining the integrity of their technology stacks and applying the unique policies necessary to operate their businesses. Companies also need an easy-to-use interface from which they can manage their existing cloud infrastructure.

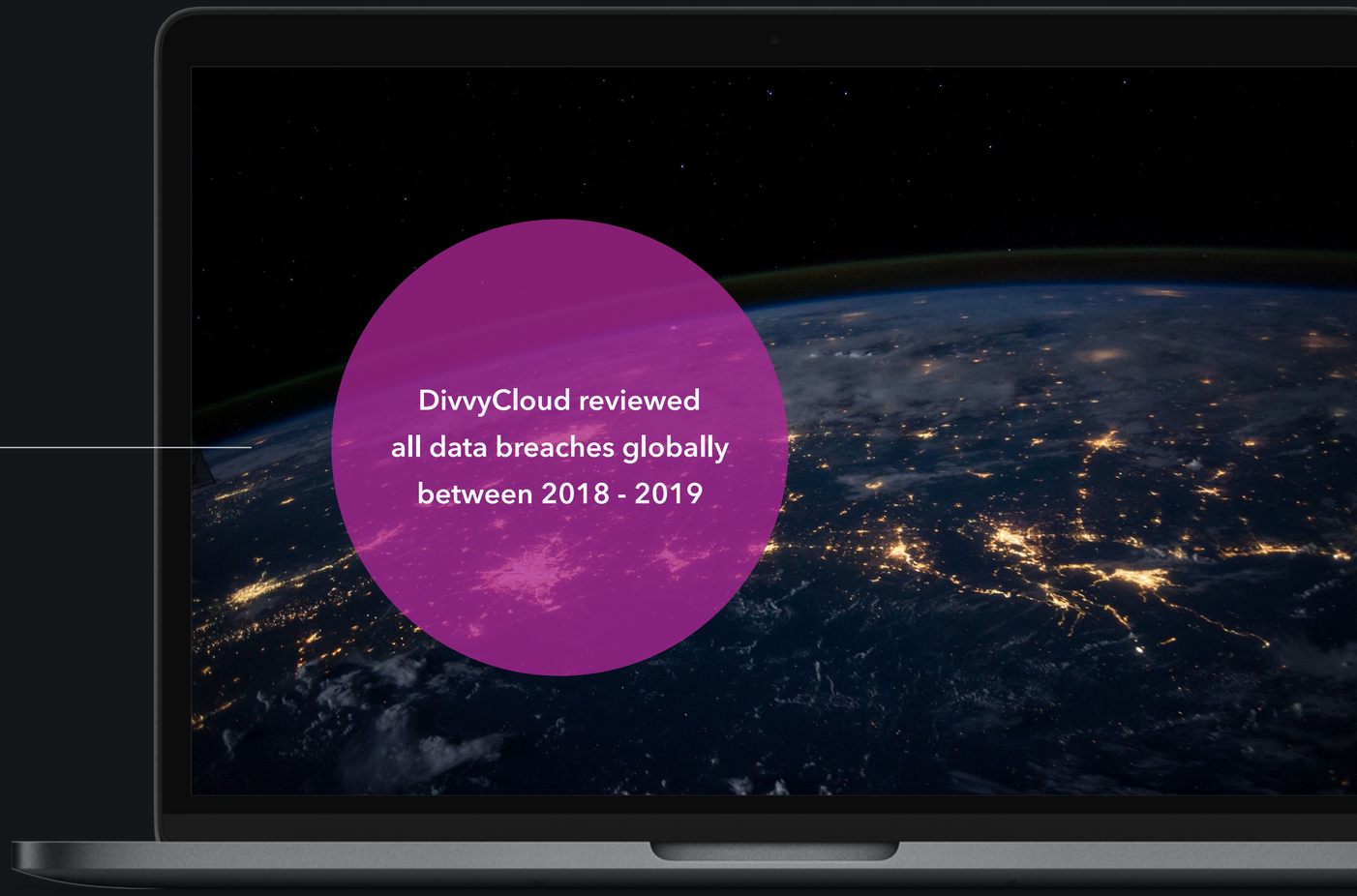
At scale, policy enforcement cannot and should not be performed manually. Security automation can discover and automatically take action to address policy infringements or security issues (like an exposed Elasticsearch database), or even alert the appropriate personnel of the issue so that it may be remediated. However, an automated cloud security strategy is difficult to plan and implement correctly right away. It takes time to establish a set of remediation policies that work because they must be tailored to specific business needs.

The first and most important step toward achieving automated remediation is to ensure the culture supports it. Only after ensuring all members of a company's IT staff are fully committed to using automated remediation can the company develop the appropriate policies that fit the needs of their day-to-day operations. Data breaches caused by cloud misconfigurations are going to continue to make headlines even though most are caused by simple, easily preventable mistakes. As companies adopt cloud and container environments, they need to simultaneously take control of their cloud security models and fulfill their share of the responsibility if they wish to keep their cloud out of the news.

Methodology

DivvyCloud researchers reviewed all data breaches globally that were first publicly reported between Jan. 1, 2018, and Dec. 31, 2019. The details of each breach were evaluated to determine if the primary cause was a cloud misconfiguration, and only breaches that were definitively attributed to cloud misconfigurations were included in this report. In total, 196 separate data breaches were identified.

The impact of the breaches were then aggregated and data analyzed to provide the analysis included in this report.



About DivvyCloud

DivvyCloud protects cloud and container environments from misconfigurations, policy violations, threats, and IAM challenges. With automated, real-time remediation, DivvyCloud customers achieve continuous security and compliance, and can fully realize the benefits of cloud and container technology.

To learn more about how to prevent cloud misconfigurations, speak with DivvyCloud's cloud security experts today.