SAFE SECURITY

A Silver Lining to

CLOUD SECURITY

Quantification of Digital Business Risks

Table of **Contents**

Executive Summary

Technology Review tracked the coinage of the term 'Cloud computing' back to late 1996, and to an office park outside Houston. NetCentric's founder, O'Sullivan, who dug up paper copies of 15-year-old business plans from NetCentric and Compaq showed not only extensive use of the phrase "cloud computing," but also described, in accurate terms, many of the ideas sweeping the Internet today.

Fast-forwarding to 2020 - McAfee found the use of cloud services had increased by 50% between January and April 2020 as compared to 2019, and not unexpectedly hackers have followed suit. Cybercrime has increased on these platforms by more than 600% with the greatest concentration on collaboration services like Microsoft Office-365.

While the global cloud market is worth about $325 billion and more than 90% of organizations leverage cloud technology in some way across the enterprise, the manner in which the technology is deployed can have a massive impact on security. A Nominet report found that 92% of organizations are leveraging cloud-based security solutions, with 88% currently engaging in or planning to adopt cloud and software-as-a-service (SaaS) platforms and 71% actively deploying the tech.

With this surge in forced digital transition of several enterprises during COVID-19, threat actors have doubled their efforts to exploit the distractedness wrought by the world's response to the pandemic. There are important changes needed to implement new delivery models for security in a distributed work-from-home environment.

Data from a McAfee report shows that the increased risk of cloud-native threats brought by threat actors targeting cloud services far exceeds the risk brought by changes in behaviour by employees simply working in a new, remote location. According to the report, organizations that suffered a breach within the last 12 months were more likely to believe the cloud poses a greater risk than those companies that did not. When it comes to securing the cloud, about half of organizations are leveraging firewalls, email security, anti-malware or antivirus, or data loss prevention.

Currently, there is no method or mechanism to verify the security status of your cloud assets in real-time and objectively. Unlike the tangible model of on-premise databases, cloud computing and serverless databases do not have the advantage of 'premise' or perimeter security. Moreover, the belief that native security controls provided by the Cloud Security Providers (CSP) are sufficient for the business to be secure is often misinterpreted. Cloud service providers often give a certain number of security services but they are not as mature and rarely cater to other CSPs. This creates a layered multi-cloud environment that is a complex situation to secure. Since innovation and evolution in this domain is too fast for security tools to be relevant for a long time, businesses need to hire/ recruit the right personnel or outsource cloud-security to firms who are updated with current TTPs leveraged by cybercriminals Also, as the leveraged trends change, the remediation steps for the same alter accordingly.

The most crucial role that security teams play while ensuring a good cloud cyber risk posture is to be able to simplify the generated data and identify exactly where the vulnerabilities lie. There is an immediate and pertinent need to create a method in the madness. There is a need for a real-time, unified, hybrid and consistent approach which can be provided by Digital Business Risk Quantification solutions/platforms.

The Instability of Cloud Environments

Being on the cloud heightens the complexity of any organization's cyber security planning.

- Cloud assets were involved in about 22% of breaches in 2020
- Cloud misconfigurations are the leading initial threat vectors responsible for 19% of malicious breaches.
- Undergoing an extensive cloud migration at the time of the breach increased the average cost of a breach by more than $267,000, to an adjusted average cost of $4.13 million
- Through 2025, 99% of cloud security failures will be the customer's fault.
- Through 2024, 80% of companies that are unaware of the mistakes made in their cloud adoption will overspend by 20 to 50%.
- Cloud breaches involved an email or web application server 73% of the time. Additionally, 77% of those cloud breaches also involved breached credentials.

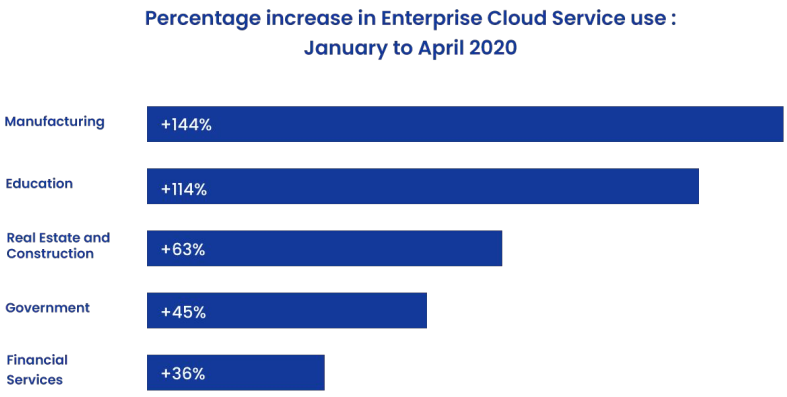

Figure 1. Increase in Cloud Service use by vertical

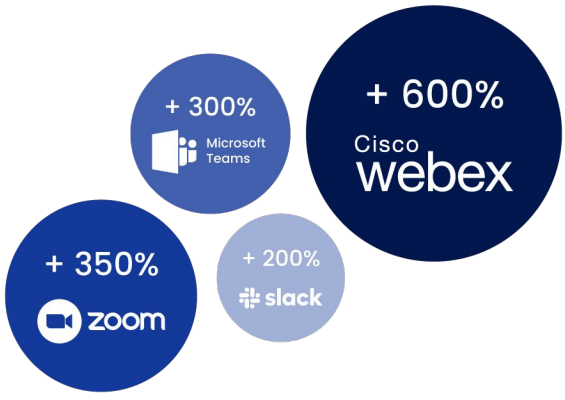

Figure 2. Increase in collaboration cloud service usage measured week 11 of 2020

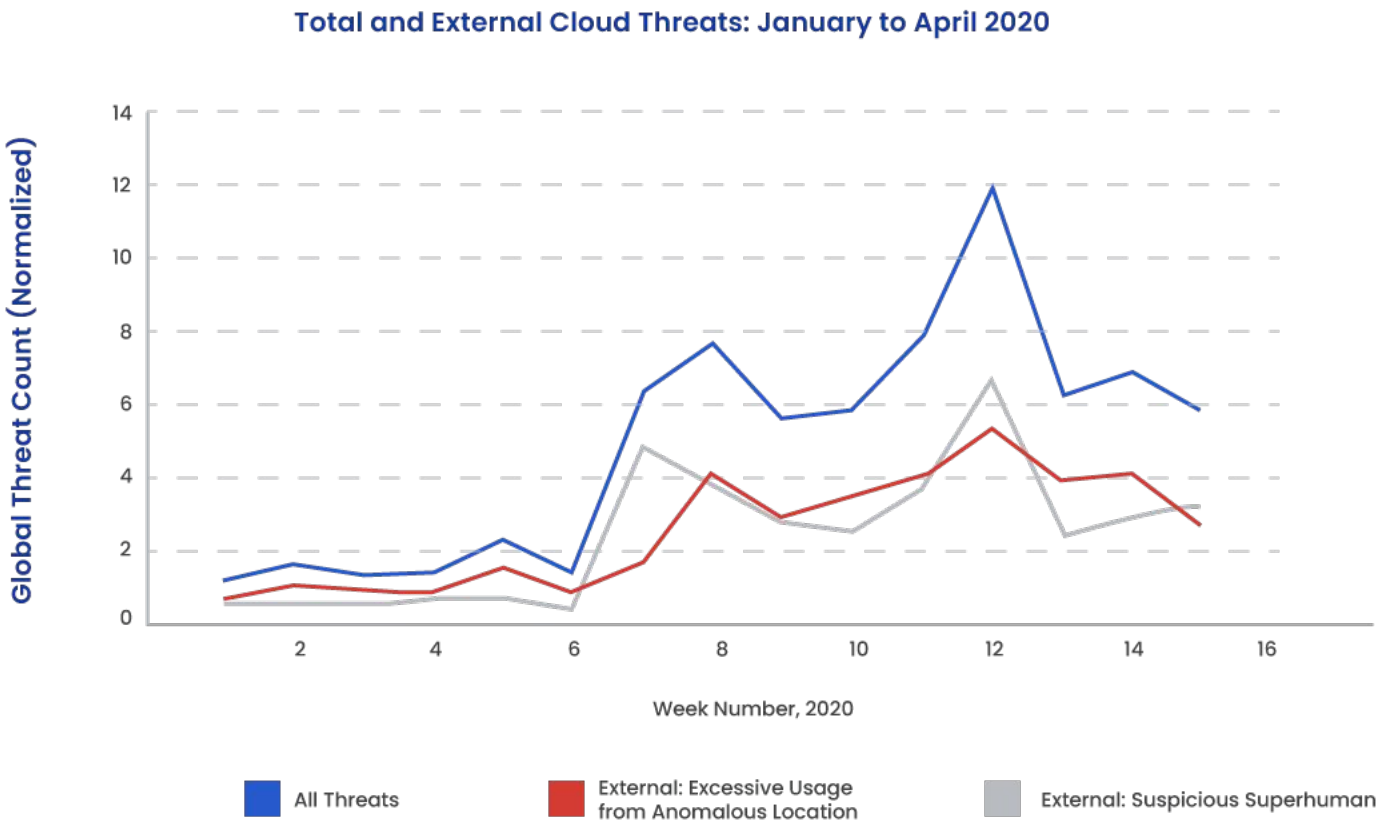

Figure 4. Cloud Threat event across all industries

Gartner has found that almost half (47%) of CEOs are being challenged by their boards to digitally transform to improve their growth prospects and customer relationships. With multiple Cloud Service Providers in the market, each suiting different needs of the business, CIOs and CISOs are dealing with increasingly complex cloud infrastructure, thereby cybersecurity strategies that depend on numerous homogeneous Identity and Access Management (IAM) and Privileged Access Management (PAM) solutions, each unique to an IaaS provider.

The most common multi-cloud security issue is the potential for misconfigurations, and the temptation to simply weaken authorization processes to make sure everything moves from one app to another smoothly. For example, 66% organizations leave back doors open to attackers through misconfigured cloud services. The more disparate cloud components added, the more that visibility also becomes a problem. This is often the reason that unsecured data buckets are found and breached.

Challenges faced by the security team What considerations should be made?

Before Migration	After Migration
First and foremost, you need to know if you have enough technology to understand the entire landscape on-cloud, which is in itself very fluid and dynamic.	On-premises billing and budgeting is quite different from that on-cloud. Your team needs to spend adequate time in understanding where and how additional charges apply in order to streamline expenses.
Rather than trusting the word of a technology provider, many companies have come to rely on third-party certifications for evaluating the security architecture and processes used by cloud providers. One of the most important of these is SOC 2 certification.	In order to reduce expenditure, there should be no restrictions or compromise on the security standards. For this, organisations can rely on trusted advisors who are subject matter experts to guide you with respect to ROI and necessity of services.
What role does your company play in the protection of your data (if any) and what is the cloud service provider company's role in protecting your data and mitigating security incidents? Where do the servers reside, physically? Are there any legal consequences regarding your data privacy you should know about for having your data stored there?	Ensure continued cyber security vigilance with real-time monitoring of cloud assets. Reassess configurations for each bucket/ asset. Most commonly overlooked are cloud misconfigurations which leave an entry point vulnerable to exploitation.

Before Migration	After Migration
Who has access to your data? What is your company's policy for ensuring authorized employees access only?	For preventing external hacks and data theft, the system must be architected to prevent as many types of attacks as possible. Also, application providers must use internal personnel and external consultants to run frequent penetration testing.
What uptime guarantees are there in the standard service level agreement (SLA)?	You need to pay attention to things like system changes and software updates of the tools and applications you use, as well as changes and updates on the platforms you use or that you allow to connect with your network. You need to ensure that these changes don't affect your security posture, and take steps to address any issues that arise.
Do they perform penetration tests? When was it last performed and what were the results?	Keep abreast with changes in policies/ guidelines surrounding physical security of the servers and data centres and disaster recovery plans.
How do they protect access to GUI and API? What are the service provider's terms about any metadata you generate while using their service/platform/application?	Switch on the 'out-of-the-box' security services provided by cloud providers since they provide good value for the initial assessment.
What are their physical and digital security measures for protecting their data centers and other facilities?	Ensure that cloud based security services which your team may not be regularly reviewing are attended to.
Do they have a ready disaster recovery playbook or plan? How often do they perform drills? In the case of a data center disaster, where do they backup your data?	Attune new security tools and services based on your business needs and identify gaps where you need to deploy other solutions.

The role of digital business risk quantification in Cloud Security

Cloud security, unlike physical security, is a shared responsibility. The definite missing link and perhaps, one of the prime reasons cloud security is a concern is the blurred visibility into the real-time security status of your cloud assets. There is complete freedom of customisation and enterprises' security teams should have a proper training and understanding of which controls are beneficial to them and which could be a drain on resources- both financial and otherwise.

This prioritisation of action points is where digital business risk quantification solutions can be a game-change for enterprises. With a real-time and consistent metric across all assets on-cloud generating an objective, unbiased and continuous assessment provides a unique opportunity to assess the enterprise's on-cloud cybersecurity posture.

Digital business risk quantification solutions provide the enterprise with a clear understanding of how likely they are to get breached based on the risk faced by the enterprise through its cloud infrastructure with individualised 'scores' across the hybrid or all-on-cloud environment. This score is an output of all the cybersecurity feeds, external threat intelligence and Frequency-based EC2, S3 and IAM Rules Assessments, Cloud Security Configuration Assessments and many more. These can be either single, hybrid or multiple-cloud platforms that an enterprise leverages in order to carry out smooth business functions.

SAFE and Digital Business Risk Quantification for you

Today, businesses lack a dynamic, real-time and consistent visibility of their organization-wide hybrid technology stack that is constantly evolving. They need a platform that quantifies risk consistently across their technology verticals to ensure an “apples to apples” comparison and helps to identify the places which need immediate attention. SAFE gives a dynamic, real-time and consistent “score” between 0 to 5 to every cloud instance, IP address and application in your environment and has the ability to dynamically group them together to monitor their overall cyber risk posture.

SAFE takes a one-time API access to your Vulnerability Assessment, Endpoint detection and response and Security Information and Event Management tools and then aggregates the data daily while factoring in the micro and macro scores. SAFE also performs an API-based assessment of popular SaaS tools such as Office 365 and GSuite.

SAFE enables enterprises to monitor People, Processes, Technology, Cybersecurity Products and Third-party Vendors across their hybrid/ multi-cloud environment as SAFE seamlessly integrates with your existing cybersecurity strategy to provide a real-time, objective, consistent and unified on a single dashboard across all verticals and the organisation's technology stack.

One of the biggest advantages SAFE brings to an organization is a prioritization matrix of a curated to-do-list, generated from globally accepted ATT&CK MITRE framework. Out of all the vulnerabilities that are identified, only SAFE can point out your TSAR vulnerabilities. These are a list of most leveraged Tactics, Techniques and Procedures (TTPs) by cybercriminals mapped specifically to your enterprise’s geography, industry and size.

Case Study

The hack on a 45B$ Bank, exposes the state of cybersecurity across the financial services industry. With this breach, one out of every three citizens in the United States have been affected.

What Really Happened:

On March 12, 2019, IP address 46.246.35.99 attempted to access the bank's data. This IP address was controlled by "Ipredator", a company that provides VPN services. Ten days later, the hacker used a WAF-Role account to execute the LIST Buckets Command several times. This command returns a list of all buckets owned by the authenticated sender of the request. These commands, we believe, originated from TOR exit nodes. As per the bank, the WAF-Role account does not, in the ordinary course of business, invoke the List Buckets command. On the same day, the hacker used the same account to execute "Sync" Command multiple times to obtain data from a critical file named "April 21" from the bank's data folders of buckets, which included files that contained credit card application data along with other information.

How could have SAFE helped?

With its daily assessments and real-time scans, SAFE can be configured to assess the configuration status of all buckets across the cloud infrastructure Whether you have a single or tens of thousands of cloud instances, your organisation should be able to stay one step ahead of fixing the elements in its cyber environment before they are exploited. This is where continuous risk quantification gives you an edge. It enables you to tackle cybersecurity problems in real-time, by assimilating threat signals from various cybersecurity sources, cutting through on-premise, hybrid and multi-cloud work environments, spanning across people, processes and technology.

Risk Quantification is like placing a name to a face- making identification, resolution and comparison of problems simpler and faster. It enables you to place an actual value to your cyber risk posture in real-time to provide a consistent risk metric as a common language between the security team, the Board, other stakeholders and customers.

www.safe.security | info@safe.security

Standford Research Park,
3260 Hillview Avenue,
Palo Alto, CA - 94304

SAFE SECURITY