Cloud adoption is boosting productivity but complicating data regulation. We're here to help.

Shine a light on your data and make cloud adoption a breeze

kaspersky BRING ON THE FUTURE

Executive summary

Organizations have long been increasing their cloud adoption to build cohesion and boost productivity. Since the onset of the pandemic, however, this has gone into overdrive. Security has been left behind and businesses are finding out the hard way.

Today, nearly half of all data breaches[1] occur in the cloud. This should come as no surprise, with businesses relying on a glut of cloud service providers whose IT maturity far exceeds their own. But while the provider may have everything in check at their end, this is only half the battle.

Securing your data at the organizational level is key to safe cloud adoption, and this is only achieved through visibility. Few organizations can classify all of their data. And in the absence of visibility you risk noncompliance – or worse, breaches that result in fines, reputational damage or even business loss.

It doesn't have to be this way, and cloud adoption can in fact be a breeze. Shining a light on the data in your organization makes it easier to classify, track and protect, so you can accelerate your cloud journey without fear.

In this paper we'll discuss cloud adoption risks, examine the origins of weak data security and, ultimately, help you regain control of the cloud.

The rise in cloud adoption

Benefits such as scalability, economy and reach are encouraging businesses to migrate to the cloud and embrace digital transformation. This has ramped up to hyper speed since the onset of the pandemic, with companies looking to boost their collaboration and productivity while being geographically dispersed. Such was the rush to facilitate widespread remote working that Microsoft witnessed two years of digital transformation in just two months[2], and now 90% of businesses[3] spend more time in the cloud.

Small to medium sized businesses (SMBs) run smaller workloads than enterprises but are in fact the cloud's fastest adopters[4]. In their bid to facilitate remote working, 53% now exceed 1.2 million US dollars annually[5] on cloud computing. The benefits are of course numerous. Capital One, for example, reduced development environment build time[6] from months to minutes by migrating to the cloud; AppLovin reduced latency[7] on its bidding platform by 25% and J.B. Hunt boosted user satisfaction[8] by 10%.

Some companies, however, are wary and believe that guarding IT operations onsite is safer than outsourcing. But while surrendering your technological control isn't easy, a third party can protect your data better than you might think, especially if you choose the right fit.

Public v private: a tale of two clouds

Not all clouds are built equal. The **private cloud model** is essentially private data hosting: one cloud for one organization and no shared resources. It's especially popular in sectors with the tightest data regulations, such as government, healthcare and finance, where a breach can cost millions of dollars.

Private cloud

Advantages	Disadvantages
Secure	Costly
Bespoke	Resource-intensive
Optimized	Difficult to scale
	Limited remote access

The **public cloud model** involves making digital assets publicly available over the internet. These services are typically subscription services – think software as a service (SaaS) – and the cloud service provider (CSP) looks after hardware, software and supporting infrastructure. The major players in this field are Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure.

Public cloud

Advantages	Disadvantages
Scalable	Compliance doubts
Cost effective	Less secure
Reliable	Migration effort
Low effort	

O'Reilly found that two thirds of organizations[3] use a public cloud, which is more than those using on-premise infrastructure (55%) or a private cloud (45%). Most of those organizations also reported using multiple CSPs, which is where things become increasingly tricky from a data security perspective.

Choosing the right model for both your business's existing functions and its growth potential is crucial – as is gaining visibility of the data you control.

What increased cloud adoption means for data security

Nearly half of all data breaches[1] now occur in the cloud. The speed at which we've moved – most of us pushed by the pandemic – has left security playing second fiddle, and half of all cloud adopters[9] are concerned. Nine out of ten users[10] store sensitive data in the cloud (public or private), and the 10% who don't have cited compliance and control concerns. While these concerns can be addressed with the right technological support (something we'll discuss shortly), they are not disproportionate: 45% of organizations[11] have already experienced a cloud-based data breach or failed an audit involving cloud data. This proves that even the data you consider secure can be problematic without the correct controls in place.

Data security risks in the public cloud

When you use the public cloud, there are typically three parties involved: your organization, your customers and the CSP. In a data breach, your organization is considered the data owner, your customers the data subject and your CSP the data holder. (If company secrets such as balance sheets are spilled, then your organization is also the data subject.)

The finger is often pointed at the data controller – that's you – during a breach. However, in the right context **and with the right evidence at your disposal**, it's possible that the data holder, the CSP, will be held responsible. And this could save you time, money and credibility.

Having visibility of your data is crucial so that you can classify your information assets (think customer databases) and manage related risks. You should ask the following questions at the first opportunity in your cloud journey:

- Do you have the expertise and/or resources to maintain strong cloud security standards?
- Which industry or government regulations must you comply with?
- What data is under your control?
- Who can access that data?

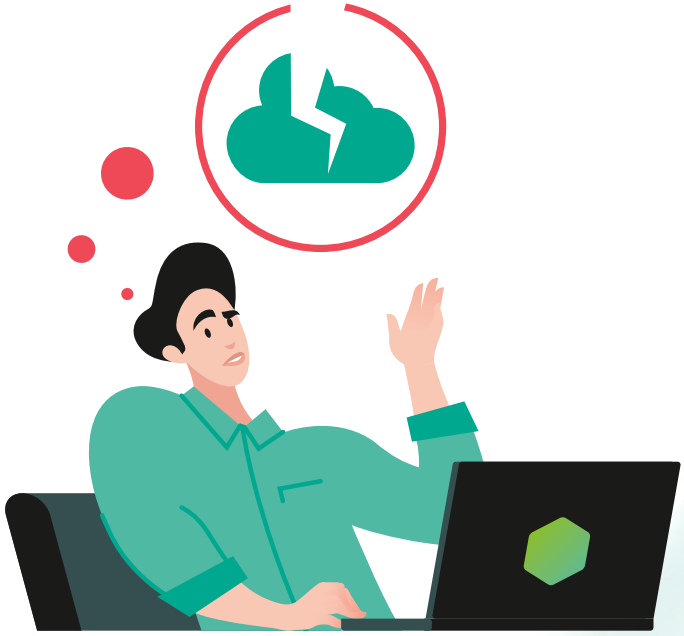
Before we discuss data visibility more, let's examine the role of a key player in cloud data security – your people.

The human factor

There are several ways an unauthorized party may gain access to your sensitive data in the cloud, but your people are number one. Nine in ten SMBs[12] that have experienced a data breach affecting their public cloud infrastructure said social engineering was part of the attack. The top three data types stolen were personally identifiable information (PII), customer payment information and user authentication credentials. They all spell trouble, yet their compromise often stems from seemingly innocuous incidents, including:

- An employee leaving a laptop unattended in a coffee shop
- A marketer sharing account details with a third-party agency
- A tired engineer cutting corners at the expense of file security

You can minimize the risk of social engineering attacks by using an endpoint security solution that protects mail servers, clients and browsers. Many products, however, do this alone and fail to deliver the oversight required to track data on cloud-based platforms. And what you can't see, you can't protect.



cloud security alliance℠

This gap between the perceived effectiveness of CSP security controls and confidence in organizations' abilities to protect sensitive data in the cloud could be due to the difference in security resources when comparing CSP and cloud users. Equally, it points to organizations' need for additional security measures beyond CSPs' built-in security features.

– The Cloud Security Alliance, "Sensitive Data in the Cloud"

Organizations lack confidence

The Cloud Security Alliance reported[10] that most organizations find their CSP security controls to be effective – but they **lack confidence in their own ability** to protect sensitive data in the cloud. (Only a quarter of businesses exceed "moderate confidence" in their ability to protect sensitive data in the cloud.) This uncertainty goes hand in hand with inaction: 43% of businesses[1] either haven't started applying or are in the early stages of applying security practices to their cloud environment.

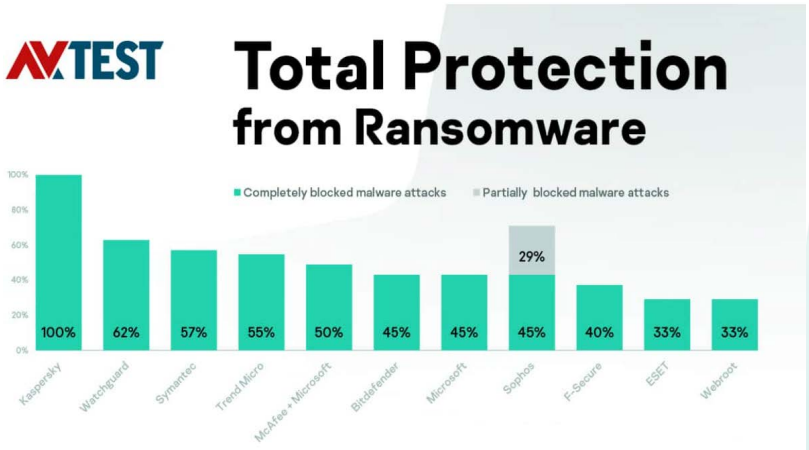
Because your organization is likelier to be breached as a result of social engineering than a mistake by your CSP, it's important to establish measures that protect your endpoints and provide visibility of the data in your cloud environments. At present, 22% of organizations[11] can classify very little of their data and just a quarter can classify it all. Mishandling that data can lead to the types of breach that cost SMBs millions of dollars annually.

Take control of your data with Kaspersky Endpoint Security Cloud

We can help you get control of your data security and compliance no matter where you are on your cloud journey. You don't need to spend huge sums to meet the security pace set by CSPs – **Kaspersky Endpoint Security Cloud**, our prime offering for SMBs, provides the straightforward, affordable protection you need to get up to speed and avoid data breaches. Better still, you'll be up and running in minutes, thanks to the easy setup direct from the cloud.

First line of defense

Kaspersky Endpoint Security Cloud offers extensive cloud data security features but also does the basics well, protecting you from known and advanced malware threats, ransomware (100% protection[13]) and phishing – the root cause of many breaches. What's more, we'll find and patch vulnerabilities in your systems so you can focus on what you do best.



Data Discovery (and data protection)

You can make inappropriate cloud app usage a thing of the past with Cloud Discovery, a tool that helps you find and then restrict the use of inappropriate or unauthorized cloud resources. Sources of a potential data breach are rapidly tracked down and eliminated, helping you maintain confidence and compliance.

Preset templates allow you to easily identify confidential and sensitive information related to PII* and payment data. You'll see when it's shared on Teams, OneDrive, SharePoint – **almost any Microsoft Office 365 service** – allowing you to enforce remediation to maintain data integrity and meet compliance goals.

And even if a device is lost or stolen, you can protect your data with remote encryption capabilities.

AVTEST

Personal Identifiable Information Protection: Sensitive Data Discovery test.

Learn more

*Not all types and regions supported.
Please see our full list of coverage.

Compliance confidence

We understand that local regulations such as the General Data Protection Regulation (GDPR) can be intimidating when you're looking to adopt the cloud. There are dozens of individual articles to comply with and this can be overwhelming. However, Kaspersky Endpoint Security Cloud will give you the confidence and tools you need to comply.

GDPR Article 32, "Security of processing", for example, requires you to ensure a level of data security appropriate to the level of risk presented by processing personal data, and ensure that anyone with access to personal data doesn't process it (except under your instructions and in accordance with the requirements of the laws).

That's quite a mouthful. Here's how we simplify it:

Your requirement	Our solution
Look at where you're storing data	**Data Discovery** helps you detect the processing and storing of personal data in services that can be accessed by external parties, which could lead to a potential data breach
Look at why you're storing data and for how long	**Data Discovery** helps you discover data that has been stored longer than necessary (or longer than specified by your data retention policy)
Find ways to control user access to data	**Device controls** prevents users from connecting external and removable devices (other than those approved by the IT department) to their computers in order to move data
Implement data protection mechanisms such as encryption on mobile devices	**Encryption management** protects data in the case of a lost or stolen device, no matter where that device is
Assess your levels of data security risk	Full visibility as you grow

Our research has shown that the average SMB holds only around 160 files with sensitive data in its cloud storage, with just 15% of these (about 24 files) being shared outside the business. Continuous reporting from Kaspersky Endpoint Security Cloud and the occasional manual fix of a risky share are all you need to stay compliant.

Conclusions

Is your cloud adoption accelerating? It's time to shine a light on your data so you can enjoy the benefits without looking over your shoulder. In this paper we've described the increased uptake and immense benefits of cloud usage while highlighting your areas of concern. With us on your side, you can minimize the risk of a cloud-based data breach, remain compliant and protect your business from the usual threats – all through a web browser.

Kaspersky Endpoint Security Cloud comes in three tiers and is delivered on a per-device basis, so you only pay for what you need.

It's time to bring on the future.
Get your 30-day free trial today.

About Kaspersky

Kaspersky protects over 400 million users and 240,000 companies. Est. 1997.

We are a private international company with the holding company domiciled in the UK.

We transform our leading security intelligence into real protection for our clients. Empowering you to use technologies in your life and business safely and with confidence.

25 years +

of experience in the cybersecurity industry

400 million +

customers use our products worldwide

200 +

countries and territories benefit from our products

Bibliography

1. IBM. (2022). Cost of a Data Breach Report. IBM.
2. Spataro, J. (2020, April 30). Two Years of Digital Transformation in Two Months. Microsoft.
3. Loukides, M (2021, December 7). The Cloud in 2021: Adoption Continues. O'Reilly.
4. Grand View Research. (2021). Cloud Computing Market Size Report. Grand View Research.
5. Flexera. (2022). State of the Cloud Report. Flexera.
6. Amazon AWS. (2020). Capital One Completes Migration from Data Centers to AWS, Becomes First US Bank to Announce Going All in on the Cloud. Amazon AWS.
7. Mehta, N & Birnbaum, J. (2021, July 23). AppLovin Builds on Google Cloud to Transform Mobile Marketing. Google Cloud
8. Google Cloud. (2021). J.B. Hunt Executes Speedy Yet Seamless Cloud-to-Cloud Migration. Google Cloud
9. Nutanix. (2021). 4th Annual Nutanix Enterprise Cloud Index. Nutanix.
10. Cloud Security Alliance. (2022, December 7). Sensitive Data in the Cloud. Cloud Security Alliance.
11. Thales. (2022). 2022 Thales Cloud Security Study. Thales.
12. Kaspersky. (2019). Understanding Security of the Cloud. Kaspersky.
13. Kaspersky. (2022, July 19). AV-TEST Finds Kaspersky Security Solutions for Business Deliver 100% Ransomware Protection. Kaspersky.

Find out more about **Kaspersky Endpoint Security Cloud**

Kaspersky
Endpoint Security
Cloud

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/about/transparency

Proven.
Transparent.
Independent.