zscaler™

How to Overcome the **Top Five Data Protection Challenges** in a Cloud-First World

The rapid shift to digital business models that use cloud services, such as SaaS and cloud service providers, is the latest development in the information revolution. Like other revolutions of the past, the change the cloud brings offers tremendous benefits as well as significant new challenges.

The core of the current revolution is the collection and use of distributed data. The data organizations collect, analyze, and use to gain insights has completely changed the way we do business. Big data analytics, cloud computing, and AI help to automate the use of that data to allow businesses to better engage with customers and employees. This makes data more valuable than it ever has been, and its accessibility enables organizations to run their business in ways that couldn't have been dreamed of even a decade ago.

With these benefits come new and difficult challenges. In the past, users were on the network and the data resided centrally within the data center along with applications. Access to the data was strictly controlled by IT and usage was well known. The shift to the cloud has allowed more collaboration across individuals and lines of business (LOBs), accelerating the speed of business and reducing costs.

The side effect is that the data and applications are now outside the data center and running in someone else's infrastructure, users are often working remotely, and the connection between users and applications is now, simply, the internet. This shift has completely changed the role of IT from a local security enforcer to a global business enabler, allowing safe cloud adoption and data distribution, while preventing data exposure and maintaining increasingly rigid industry and regulatory requirements.

Of course, securely enabling this new reality of distributed data and cloud adoption across the organization isn't simple, and to do so you must first overcome a number of challenges.

What are the challenges?

CHALLENGE #1

Encrypted traffic hides data loss

Encryption has shifted from the exception to the norm in an attempt to ensure secure transactions to the internet and cloud applications. In fact, according to the latest Google Transparency Report,[1] 95 percent of traffic that Google sees is encrypted. If your data protection solution isn't classifying and controlling data in encrypted traffic, you will be missing the majority of sessions in which data exposure and misuse is a possibility. This is especially true of SaaS applications that rely on secure, encrypted connections to the application for exchanging data.

How to overcome it

Anyone can offer partial decryption of traffic and, when there was limited encrypted traffic between your users and applications, that was good enough. Now that the majority of traffic is encrypted, you should look for an offering that has the architecture to deliver 100 percent decryption of sessions across SaaS and public cloud applications.

A key advantage of digital business models is the ability to rapidly scale and change based on evolving business needs and initiatives. Decryption of traffic must not only support your organization today but must be built on an architecture that can rapidly scale to ensure that your traffic continues to be decrypted as your organization changes and grows.

What to avoid

The traditional method of placing firewall or proxy appliance-based offerings at the edge has been proven to be incapable of keeping up with the demands of full traffic decryption. In fact, these offerings do not decrypt by default and require exceptions to enable decryption, slowing traffic to a level that the appliance can handle. They leave you with a choice of risking data exposure along with threats that can proliferate across the encrypted connections—or you can slow traffic down to a crawl.

In addition, there are a number of offerings that claim to be a cloud service, which would seem to mitigate the limitations of appliances, but if you dig deeper, you will discover that they are merely virtual appliances running in the cloud with the very same limitations as their hardware siblings. Worse, they lack the hardware-based decryption assistance, making the ability to decrypt traffic even more challenging.

Bottom line

Look for a cloud-based offering that was built for complete decryption of traffic across cloud applications and one that can scale dynamically based on demand and keep up with your changing business needs automatically.

[1] https://transparencyreport.google.com/https/overview?hl=en

CHALLENGE #2 Gaps between data protection services

With data becoming distributed across SaaS and public cloud applications, and each of them being created and maintained by individuals and LOBs across the organization, controlling data can be daunting. Unfortunately, many of the tools developed to address data challenges are focused on a single application type or deployment.

For example, a cloud access security broker (CASB) service is used to secure SaaS applications, while a secure web gateway (SWG) with data loss prevention (DLP) is used to secure internet applications, and cloud security posture management (CSPM) is used to secure public cloud applications. Each of these provides a partial picture of data protection across the organization, but there are gaps between products and teams that can lead to complexity, redundant functions across teams, and gaps in visibility and control over data exposure across applications.

How to overcome it

Gartner recently defined a security model that addresses the challenge of centralized cloud security and put data protection as one of its central elements. This model is called the secure access service edge, or SASE. SASE calls for a unification of cloud security services to allow for a centralized policy for application access and data usage across cloud applications.

Look for a SASE-based offering that offers consistent, cloud-delivered data protection under a single policy. It should be able to inspect data at rest and in motion across SaaS as well as public cloud and private data center applications to ensure that only authorized users have access in accordance with the company's data access policies.

What to avoid

Many companies will claim to be SASE or say that they offer unified data protection. If you look deeper, you will often see multiple disconnected services functioning as separate overlays, using separate policies and data classification engines across cloud application types. When services are designed as multiple overlays requiring redundant, disconnected policies and multiple agents, they leave gaps in visibility and add complexity to deployment and management.

Bottom line

Look for a unified, SASE-based, cloud-delivered offering that can ensure data protections across cloud applications and users. It must be a single offering to simplify deployment and ensure maximum protections.

CHALLENGE #3

Limited context when controlling data usage

As your organization transitions to new digital business models, it's incumbent on IT to ensure the business is enabled to use cloud apps and services, while ensuring that they can do so safely. This means that the focus shifts from black-and-white decisions on access to more granular usage visibility and control.

The challenge is that most data protection options offer limited information on which to make decisions about the use of data in the cloud. Without full context—who is attempting access, the user's location, the state of the application—it is impossible to offer the granular control needed to enable effective and safe data usage.

How to overcome it

What's needed is a cloud offering that uses an enterprise-class data classification engine that provides deep, content-based analysis and DLP along with context on user location, identity, posture, and behavior. This context ensures that access and fine-grained usage controls are in place based on the current state of the user and applications, and they can be changed over time.

Ideally, this context is provided through integration with identity and access management (IAM) and endpoint detection and response (EDR) vendors. This integration with the organization's larger security implementation is important, because it enables policy to include context, and it does so without added complexity or the need for additional personnel.

What to avoid

Avoid offerings that focus only on data classification and provide black-and-white deny/allow verdicts in policies. Offerings that control access to applications and data without user context or application status do not enable IT to function as a business enabler and instead follow the legacy model of enforcer that stifles business and prevents agility and growth. You should also avoid offerings that do not integrate with your IAM and EDR implementations, because they are unable to use posture checking and identity as context to control the access and use of data in cloud applications.

Without full context, data is vulnerable to exposure to users that end up with greater rights than they should safely have, or that stifle application usage with overly strict controls.

Bottom line

Look for offerings that offer complete context of data access and usage to allow safe application usage without limiting business flexibility and agility.

CHALLENGE #4

Poor user experience

When applications and users were on-prem, the user experience was under IT's control to plan for, identify, and resolve issues. Now, with more applications in the cloud than on-prem and the majority of employees working remotely, the infrastructure in use is now the internet itself. This presents a new challenge for IT: to ensure that users have a great experience when the majority of what they utilize is out of the organization's control.

How to overcome it

As you look to secure data access and usage across cloud applications, it is critical that your data protection is delivered consistently as a unified offering and is delivered to ensure a low-latency and high-bandwidth connection. This requires an offering that embraces the concept of SASE, which puts the data security as close to the user as possible, using direct peering with application vendors to eliminate latency and maximize throughput.

What to avoid

Avoid appliance-based offerings that require traffic to be backhauled to a central location, which causes latency and bottlenecks that adversely affect the user experience. With users working remotely and applications in the cloud, backhauling traffic negates the agility and efficiency benefits of digital transformation.

In addition, avoid cloud-based offerings that rely on virtual appliances (VMs), which utilize the same legacy architectures as appliances. They lack the scale and agility of a cloud-native offering and require the same redirects to a centralized cloud service, which create high-latency, low-bandwidth connections and prevent a good user experience.

Bottom line

Look for offerings that comply with the SASE requirements defined by Gartner.[2] They should place the data protection engines as close to the user as possible, preventing backhauling and a poor user experience.

[2] https://www.zscaler.com/sase

CHALLENGE

#5

Compliance violations across clouds

One of the most significant challenges of distributed data across cloud applications is ensuring that regulatory and industry regulations are met and maintained as individuals and LOBs use cloud services. Without visibility across cloud applications and services, as well as the ability to remediate violations, an organization can quickly face fines and loss of business.

How to overcome it

Look for an offering that provides unified compliance reporting across clouds and SaaS applications, giving you a single view of the impact and audit results. Depth of industry and regulatory adherence are critical components of the solution, as any gaps in reporting will leave blind spots in your cloud compliance assurance.

Once violations are discovered and analyzed, they need to be resolved. Seek out offerings that provide multiple paths to remediation, including automated remediation based on standards as well as your own defined policies.

What to avoid

Offerings that provide limited standards support will leave gaps in visibility, analysis, and remediation that could lead to violations.

While visibility is critical across clouds, it is only partially useful without remediation. Avoid offerings that only provide reporting of compliance or offer limited manual remediation of violations. Violations require rapid response, which requires an automated process to ensure compliance is constantly maintained. Often, organizations rely on separate services and reports for violations in SaaS and public clouds. Avoid this separation in reporting and remediation across application types, because it increases complexity for deployment and usage and limits visibility and control of violations.

Bottom line

Look for an offering that provides broad visibility into industry and regulatory compliance, with analysis and automated remediation across cloud applications as a unified service.

The Zscaler approach to data protection

Zscaler™ data protection follows your users and the applications they are accessing, always protecting you against data loss. Zscaler inspects your traffic inline, encrypted or not, and ensures your SaaS and public cloud applications are secure, giving you the protection and visibility you need. The Zscaler Cloud Security Platform was built with compliance in mind, offering you an essential tool for complying with all major regulations and making data protection painless.

Because of its time in the market, Zscaler has proven its architecture was built to scale, currently processing up to 160B transactions at peak periods and performing 175K+ unique security updates—every day.

The Zscaler SASE-based architecture is delivered across 150+ data centers globally, ensuring every user gets a secure, fast, and local connection no matter where they connect.

Learn more

To learn more about data protection go to **zscaler.com/dp**

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler connects users to applications and cloud services, regardless of device, location, or network, while providing comprehensive security and a fast user experience. All without costly, complex gateway appliances.