eclypses®

WHITE PAPER

The Next Generation of Data Security in Hybrid Cloud Infrastructure

Document ID: ECLYPSES-1532395320 - 312
Version: 2.0

For companies looking to stay competitive and maximize efficiency, the cloud can be quite appealing. The cloud can provide major advantages through integration of powerful cloud-native services, scalable hosting resources, and the ability to scale back IT budgets. In addition, a 2020 Centrify and CensusWide survey revealed that 48% of organizations have accelerated transitions to the cloud in the years following the COVID pandemic. Still, while migration to cloud services was seen as the easiest path to achieve the required business objectives, these changes have added risk vectors and imposed some ideological and strategic hurdles for network and security teams.

HYBRID CLOUD ENVIRONMENTS

Since applications have different requirements and workflows, it often makes sense to build a hybrid cloud approach. Hybrid cloud infrastructures combine some combination of cloud-native services, cloud-hosted custom applications, and data with on-premise resources. With hybrid, an organization can have much more control over their data, workflows, and variable costs and make use of the advantages of both environments.

Statistics at a Glance:

As many as 89% of companies use a multi-cloud approach. While 80% take a hybrid approach, utilizing public and private clouds.[1]

Nearly 8 out of 10 companies incorporate multiple public clouds, and 60% report using more than one private cloud.[2]

56% of companies with more than $500 million in revenue have adopted a hybrid cloud approach.[2]

7 out of 10 IT leaders think it's difficult to realize the full potential of a digital transformation without a solid hybrid cloud strategy.[2]

DATA STORED ON-PREMISE

Many companies such as large financial institutions, government agencies, and healthcare organizations have strict regulations or security requirements that may necessitate the use of on-premises data storage. For others, some companies may prefer to keep their data on-premise for increased control and security over their data. In hybrid cloud environments like this, front-end applications might be deployed in the cloud to capture, use, or display sensitive data.

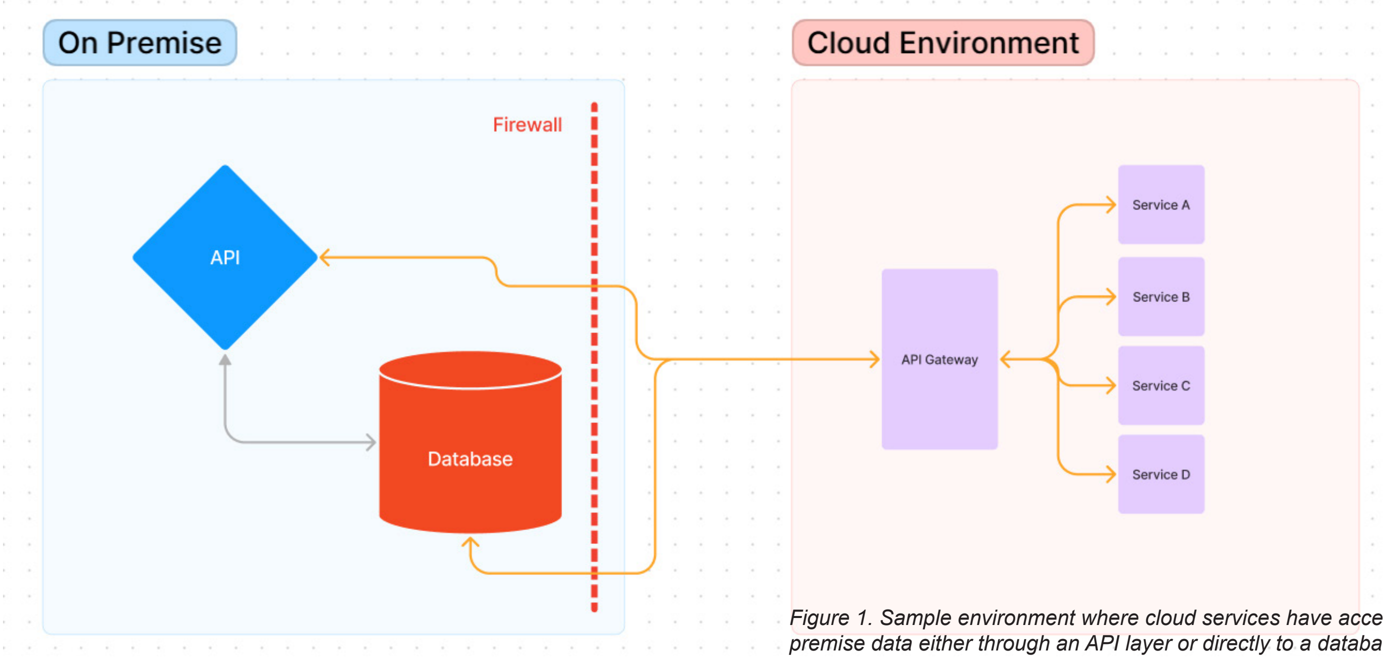

Figure 1. Sample environment where cloud services have access to on premise data either through an API layer or directly to a database.

MULTIPLE PRIVATE CLOUD ENVIRONMENTS

In an article published by G2, 80% percent of organizations that responded reported using multiple public clouds. In a multi-cloud environment, a company isn't tied to a single provider and can choose which solution best suits their business needs. A common example of using multiple clouds is when an organization runs a Confluent Kafka cluster in AWS, with alternative cloud-native and self-hosted consumer services using the data.

COMBINATION OF CLOUD AND ON-PREM APPLICATIONS

Sometimes, large organizations accrue technical debt from legacy applications, acquisitions, and investments in hardware and infrastructure. While it might seem ideal to consolidate technical resources in a single location, it might simply be unfeasible and multiple environments must be maintained indefinitely.

SECURITY-RELATED CHALLENGES

Hybrid Cloud environments are naturally more complex, requiring multiple networks, data sources, and applications to be able to exchange data at the speed of business. Perhaps more importantly, however, is the need to secure the data – especially when the data is in the custody of a third party.

When nearly half of all data breaches take place in the cloud, it is essential to secure data as it moves and when it is used.

SECURING DATA-IN-MOTION

There are many companies that offer Cloud and Network security. Typically, when dealing with data-in-transit, the prevailing school of thought focuses on the network and transport layers. For the transport layer, TLS has long been the technique for establishing a Secure Socket Layer (SSL) for network requests between services. In addition, native cloud and third-party companies offer many network-level solutions such as Virtual Private Cloud (VPC) and Virtual Private Network (VPN) to create secure tunnels between environments.

For many organizations, data is one of their most valuable assets. When data is constantly in motion between cloud and on-premises environments, a breach in the certificate authority or a zero-day within a network security appliance might be extremely expensive to mitigate. Couple that with sheer number of integrated security services and platforms available in the cloud marketplace, an organization may only be as secure as its weakest link.

Worryingly, today’s ‘best practices’ may already be obsolete. Even though TLS 1.2 and 1.3 are unbroken today, the US Government cautions of hackers stealing data today so quantum computers can crack it in the future.

SECURING DATA-IN-USE

Persistent data, especially unstructured data such as files or documents, have long been protected at-rest by Network-Attached Storage (NAS). Large cloud providers and third-party organizations have developed ways to virtualize and cluster these storage systems while allowing cloud services to access them. For this use-case, TLS and VPN are also employed to protect the data as it moves to the consuming service.

As organizations modernize their hosting environments, many have adopted scalable, distributed event-streaming architectures for real-time data. Apache Kafka is currently used by over 70% of Fortune 500 companies. In Hybrid Cloud environments, this data must be accessible while remaining encrypted whenever possible and able to be decrypted by individual services on demand. To accomplish this, most services employ Key Management Services (KMS), in which an API service delivers encryption keys directly to the applications producing and consuming Kafka data.

Using third-party Key Vaults can add a lot of new risk vectors to an organization. The use of old or mismanaged ciphers, outdated asymmetric encryption techniques, and insufficient protection for man-in-the-middle attacks are certainly points of concern. Introducing points of failure or bottlenecks are operational headaches as well. However, trusting a third-party to manage encryption keys is surrendering control of your data, and this risk might be one of the more compelling reasons for a new generation of data security.

Risk	Risk Types
KMS	• Confluent and your Cloud Provider have access to your data • Single point of failure/truth • Credential stuffing, phishing
RSA	Man-in-the-middle (MiTM) Factoring cyberattack, quantum computing
TLS 1.2	Certificate creation, mangement, certificate authority
Static Symmetric Encryption Key	Brute force If the key is broken (RSA, KMS), all produced data is vulnerable
Injection, Replay	Data immutability and validity

THE ECLYPSES APPROACH

Eclypses MTE is a patented, award-winning, data transformation solution that focuses on data. As a next-generation method of security, Eclypses can provide Quantum Resistance today to ensure that if your edge security fails, it fails securely.

1 **Eliminates known application security threats, such as:**
- Man-in-the-middle
- Replay, Delay, Injection
- Packet Inspection
- Pattern Recognition
- Credential Harvesting

2 Built-in **endpoint verification, data immutability** with **audit transparency**

3 **Compliments existing security** and integrates in the **next release cycle**

4 **Embedded security** at the **application, data,** and **business asset level**

In hybrid cloud environments, Eclypses MTE can be embedded directly into applications in a single release cycle, or integrated into Web, Mobile, IoT, or Kafka environments using our toolkits. The technology is horizontally scalable and is not dependent on Eclypses SAAS, Web API, or hosted services. In addition, Eclypses MTE is complementary to existing security investments that may already exist.

In the end, Eclypses allows an organization to ensure that the data is secured without surrendering control of the data. Application developers and operations engineers deliver security on their terms, while network and cloud security engineers can focus on operational efficiency and high availability without worry. When it comes to the most valuable assets at an organization, immunization is cheap while triage is expensive.

REFERENCES

1. Duarte, F. (2023, March 22). Percent of corporate data stored in the cloud (2023). Exploding Topics. https://explodingtopics.com/blog/corporate-cloud-data

2. 160+ Fascinating Cloud Computing Statistics for 2023. (n.d.). G2. https://www.g2.com/articles/cloud-computing-statistics

3. Security Magazine. (n.d.). https://www.securitymagazine.com/articles/93654-pandemic-has-accelerated-cloud-transformation-for-nearly-half-of-organizations

4. 40+ cloud security statistics you need to know in 2023 | Resmo. (n.d.). https://www.resmo.com/blog/cloud-security-statistics#:~:text=Roughly%20half%20of%20all%20data,public%20or%20private%20cloud%20models

5. O'Neill, P. H. (2021, November 8). The US is worried that hackers are stealing data today so quantum computers can crack it in a decade. MIT Technology Review. https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

6. Apache Kafka vs Confluent: Comparing Features & Capabilities. (n.d.). Confluent. https://www.confluent.io/apache-kafka-vs-confluent/

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today’s environments, called MTE.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, IoT devices and Kafka data streams. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses’ patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

contact@eclypses.com
www.eclypses.com
(719) 323-6680