Whitepaper

Data-centric approach to zero-trust security

Defending cloud data against the modern array of threats requires a data-centric approach to security. It is not enough for Zero-trust security architecture to be identity-aware; it needs to incorporate data visibility and control along with data intelligence to be successful.

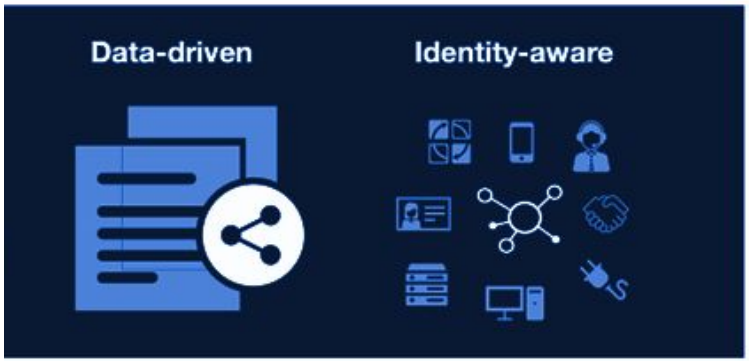
Zero-trust for cloud data

Security leaders of enterprises undergoing a digital transformation realize that to ensure customer protection adequately and enable a digital workforce, they must abandon traditional perimeter-based security and focus on the data with a Zero Trust security architecture.

A Zero Trust approach for cloud data:

1. Never assumes trust — “trust” is continuously assessed through a risk-based analysis of all available information;
2. Fundamentally shifts the focus from the perimeter to the data itself; and
3. It makes security architecture and operations data-driven, and identity-aware rather than static and perimeter-centric

Figure 1: Components of Zero Trust



Information security teams need to take a data-centric approach. They need to gain visibility into the interaction between users, applications, and data across many cloud environments, geo-locations, and third-party APIs. The data-centric approach means setting and enforcing policies irrespective of where the critical data is stored and accessed. The process requires deep and contextual visibility of cloud data within the broader security ecosystem of the enterprise.

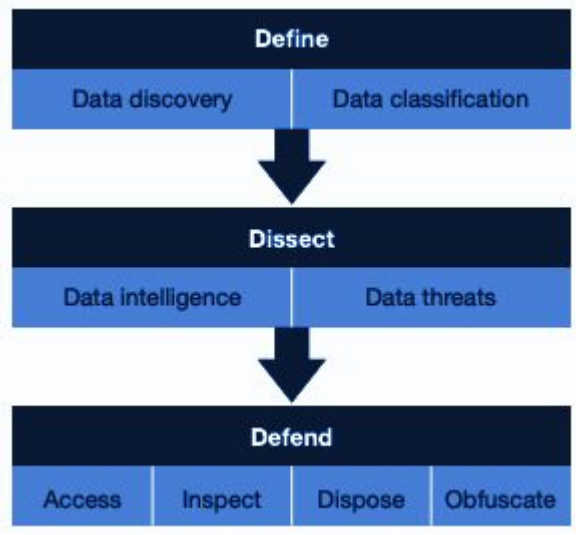
	Data Visibility & Control Ability to apply universal security policies to protect data regardless of users/apps, location or cloud provider	Discover and classify data
		Assess risks to sensitive data continuously
		Adopt least access privilege
		Encrypt data at rest and data in motion
	Data Intelligence Real-time analysis and visibility with contextual information to identify threats, address vulnerabilities, and uncover incidents in progress	Gain visibility across networks, devices, apps, users, and data
		Augment analysis with contextual information: Data criticality, time, location, traffic flows, user identity, access privileges, query types, 3rd party vendor reputation, API drift, etc.

Data Security and Control Framework

In organizations with huge amounts of data, security and privacy teams often don't know where to start. One of the good references is Forrester Research's *Data Security and Control Framework*. The framework breaks down the problem of controlling and securing data into three areas:

- ***Defining the data.***
- ***Dissecting and analyzing the data.***
- ***Defending and protecting the data.***

Figure 2: Data Security and Control Framework



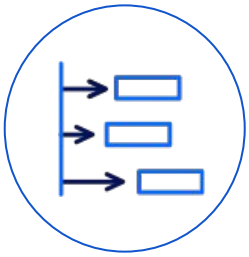
(source: The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research Inc., October 16, 2019, Heidi Shey and Enza Iannopollo)

Defining the Data in the cloud

You can't protect it all: It's too operationally complex to encrypt and mask everything, and it's too costly given all the other responsibilities. In many cases, it's not even necessary: GDPR, for example, covers personally identifiable information of your customers and employees specifically. Discovery and classification are critical to understanding better what you need to protect.

Data Classification

Security professionals, together with their counterparts in privacy, can significantly benefit from classification levels based on data value and risk. The classification of data (e.g., files in cloud object stores, cloud database fields, etc.) can change as the value of the data changes over time. Proper data defense depends on accurate classification over time for identifying the data and its level of sensitivity. Effective classification can also indicate whether you must archive the data for compliance purposes or whether it's subject to privacy constraints.



Identifying sensitive data and classifying it into PII, PHI, etc

Building an inventory of sensitive data across cloud environments

Data Discovery

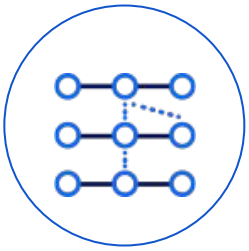
To protect data, you must first know where users and applications have stored it in the cloud. Enterprise data is typically strewn across global data centers, employee devices, SaaS file shares, cloud object stores, cloud data warehouses and data lakes. Security teams must undertake a data discovery project to locate and index existing data and develop a lifecycle approach that continuously discovers data as users create it throughout the extended enterprise network.

Dissecting the Data in the cloud

Knowing your data and its relationships is necessary to protect it effectively. This requires building data intelligence. Similarly, knowing the latest threats and vulnerabilities that could affect data stored in the cloud is important to protect your most sensitive data.

Data intelligence

The business value of the data drives security strategy and granular policy. For example, for the most sensitive data, the security team can deploy solutions that will automatically stop exfiltration — without human intervention. It's also important to understand the state of data: How does this data normally flow, and how should it flow? Who is using this data, how often, and for what purpose? What type of queries are normal vs. atypical? Why does the business have this data, how is it collected, and what is its useful life cycle? What are the consequences if data integrity is compromised?



Understanding data relationships and flow of sensitive data

Data Threats

Tracking threats targeting data stored in cloud environments

Identifying risks and insights into sensitive data usage can guide decision-making. For example, comparing vulnerabilities affecting cloud environments such as AWS, Snowflake and real-time threat data will tell the organization where its most vulnerable data assets lie and help it create defenses that are more targeted and proactive. Linking risk and insights from a cloud data protection platform and other sources like Cloud IAM, security teams can more quickly detect potential breaches or insider abuse.

Defending the Data in the cloud

There are four primary ways to defend data from exfiltration, breaches and ransomware.

Control access

To secure data throughout your cloud environment, limit the number of people who can access data and continuously monitor their access levels throughout their employment. Security and privacy professionals don't always recertify access when an employee shifts roles within the company. Employees accumulate access and privileges as promoted or transferred within the firm. Security teams also don't have insight into the access privileges of third-party users.

Enforcing least privilege access to cloud data

Inspect data usage patterns

Inspecting data usage and finding atypical queries

Atypical queries or anomalous usage patterns can alert security teams to potential abuses. Both cybercriminals and malicious internal users will leave artifacts of their attempts to breach your data security controls. Enterprises should inspect and log all traffic on internal and external networks. Continuous evaluation of data usage patterns can enable better fine-grained roles within an organization.

Dispose of data when no longer needed

Cloud data warehouses make it easy to create copies of data and share it across the enterprise. The ease of copying creates more risk as the 'shadow data' may not have the same security controls and may not be used. With proper classification and supporting controls, you can defensively dispose of any sensitive data no longer required by real business interests, compliance mandates, or data preservation obligations for investigations or litigation. Sensitive data that is not used but remains accessible becomes dark data, which opens up attack surfaces that be easily fixed.

Disposing data when no longer needed

Obfuscate data

Cybercriminals use underground markets on the internet to buy and sell sensitive data, such as credit card numbers, credit reports, and even intellectual property. You can devalue data using data abstraction and obfuscation techniques like encryption, tokenization, and masking. Cybercriminals can't easily decrypt or recover data that you've encrypted or otherwise obfuscated — and then that data no longer has any value on the black market.

Encrypting and masking sensitive data

Conclusion

Zero-trust architecture should focus on identity and data. It must be based on deep contextual visibility of cloud data within the broader security ecosystem of the enterprise. This approach empowers security and risk professionals to defend their businesses from data breaches. All controls aligned to avoid data breaches should be the goal of Zero Trust.