MTE as a Policy

A Breakdown from Eclypses CIO, Jefferson Dance

What is required of security under Data Governance for Data Protection?

Under Data Governance for Data Protection, security plays a crucial role in ensuring the confidentiality, integrity, and availability of data. Here are some key requirements:

1. Access Control: Implementing robust access controls ensures that only authorized individuals can access sensitive data.
2. Data Encryption: Encryption should be applied to sensitive data stored in databases, files, and during transmission over networks to prevent unauthorized access.
3. Data Masking and Anonymization: For non-production environments or when sharing data for certain purposes
4. Data Loss Prevention (DLP): DLP technologies can help prevent unauthorized data leakage by monitoring and controlling data transfers, both within the organization and externally. .
5. Data Classification: Classifying data based on its sensitivity level helps prioritize security measures and ensures that appropriate controls are applied to different types of data.
6. Auditing and Monitoring: Implementing logging, auditing, and monitoring mechanisms helps track access to data and detect any suspicious activities or unauthorized access attempts.
7. Incident Response and Data Breach Management: Having an incident response plan in place is critical for effectively responding to security incidents and data breaches.
8. Compliance with Data Protection Regulations: Ensure that security measures align with relevant data protection regulations such as GDPR, CCPA, or HIPAA.
9. Employee Training and Awareness: Employees should be educated about their roles and responsibilities regarding data protection.
10. Continuous Improvement: Data governance for data protection should be an ongoing process, with regular assessments, audits, and updates to security measures to adapt to evolving threats and regulatory requirements.

Problem: Business trying to manage risks to their data and data shared with third parties via API (Application Programming Interfaces) and other applications do not have an effective tool to be able implement at the operational layer while at the same time provide policy level coverage to the business while reducing risk to third party exposure in environments they do not control.

According to the "Cost of Data Breach Report 2023" by IBM, third-party vendors were responsible for USD 216.4 million of the total cost oof data breaches. 67% of data breaches were detected on the third-party side.

How does Eclypses MTE help organizations secure data, set policy and improve security while sharing data both internally and with third parties?

Eclypses MTE allows organizations to set Eclypses MTE as a policy across an organization and third parties in applications both web and mobile and API for internal sharing and for consumption of data by third parties. No matter where your data flows your key asset, can be protected with no third-party reliance or attack vector that can leave you on the hook for reputation and material impacts. Eclypses MTE enables an organization to treat risk across 7 of the 10 key areas for Data governance and protection while simultaneously improving confidentiality, integrity, and availability with a FIPS 140-3 validated and certified data security product.

Eclypses MTE allows organizations to share data seamlessly and securely internally, across the globe, or with third parties and partners in a manner with full data protection that completely mitigates and eliminates 32 of the most common application and data attack vectors and vulnerability issues that increase risk, time to market, and can increase cost.

When an organization sets Eclypses MTE as a policy, they unlock significant benefits and business outcomes:

1. Time to market – Eclypses MTE is efficient and optimized, treat in hours what previously two months or even years. Improve data security, data governance Today, immediately! Saving time, capital, and resources
2. Improving Compliance – improve your security posture and compliance in an easy to implement cost effective manner. A focused solution right at the asset that matters the most THE DATA!
3. De-Risk your Data – multiple penetration tests, FIPS 140-3 validation and certification. Eclypses MTE allows your data to move securely wherever it needs to go. Without the ability to access your application, credentials or confidential data, your business can operate smoothly, without the risk or worry of having to wonder if your data can be breached and the financial headaches that come with it.
4. Improved operations – Eclypses MTE seamlessly integrates with all modern enterprise security operations and logging platforms. No longer does a security incident have to become a breach, Eclypses MTE secures the data even if there is an exploitable operating system or application-level vulnerability.
5. Data Integrity – Eclypses MTE allows organizations to ensure that all data generated or consumed by the application is verified and secure. Our unique data verification process does not allow data to be processed that is not validated. In any model, you get the cleanest, purest, data from your applications. Eclypses MTE will drop any packets foreign to it, allowing your data sets to be usable faster, with guaranteed integrity.

Doc ID: Eclypses-1532395320-501
Version No: 3.0