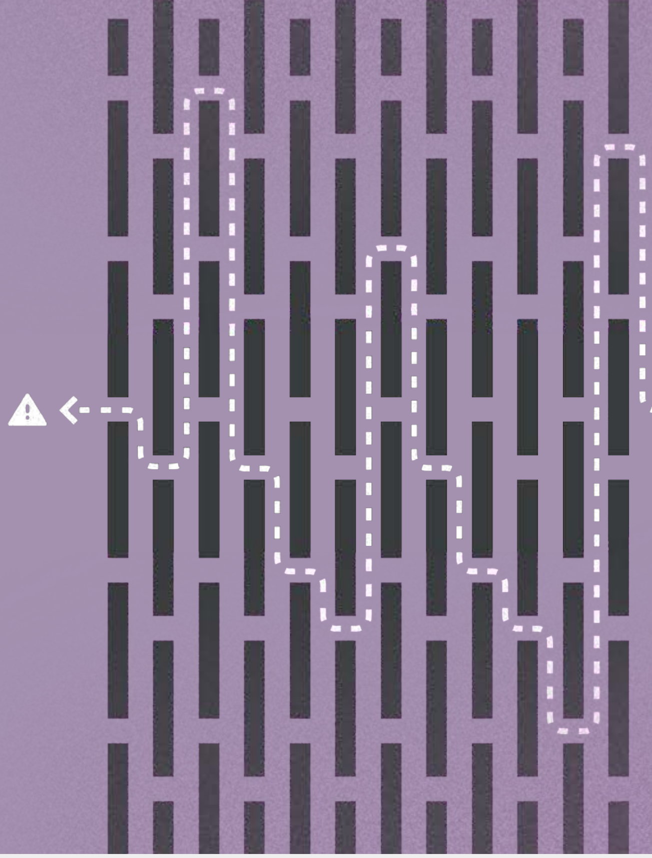
The Payment Card Industry Data Security Standard (PCI DSS) was introduced in 2004 by major credit card companies to standardize and bolster security measures for data protection.



Its primary goal is to protect cardholder data from theft and secure and strengthen payment card transaction systems.

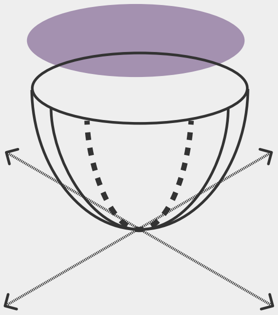
Organizations dealing with cardholder information are required to comply with this standard, and non-compliance can lead to hefty fines. Over the years, the standards have been updated to tackle evolving threats and technologies. The reception of PCI DSS has been mostly positive, with many organizations believing that it provides a foundational blueprint for data security. However, some critics argue that compliance can be cumbersome and doesn't guarantee total protection from breaches.

In many ways, PCI DSS provides a roadmap for security teams to secure sensitive data by instructing teams to maintain rigorous standards for protecting cardholder data by:

1. Encrypting sensitive information
2. Ensuring only authorized individuals can access the data
3. Enacting strict access controls and authentication measures
4. Implementing logging and monitoring in order t0 track any access or modifications to sensitive data
5. Running regular audits to ensure compliance and identify potential vulnerabilities

PCI DSS Components Relevant to Email & Cloud Environments

Non-compliance can result in significant penalties, making adherence to PCI DSS a top priority for any organizations dealing with cardholder information.



Mandate	Citation	Description	Implication	Material's Solution
Stored Data Protection	Requirement 3	Protect stored cardholder data.	Sensitive data stored in emails should be protected	Identify, label and implement access controls for financial information at the message-level.
Encryption	Requirement 3.4	Render PAN (Primary Account Number) unreadable anywhere it is stored.	PANs in email, if stored, should be unreadable	Identify, label and redact PAN in mailboxes at the message-level.
Access Control	Requirement 7	Restrict access to cardholder data by business need-to-know.	Not all staff should access emails containing sensitive data.	Identify financial data in workspaces and monitor who has access to the emails and where they have been sent.
Access Authentication	Requirement 8	Identify and authenticate access to system components.	Ensure that only authorized individuals can access emails with PANs.	Implement authentication controls on a per-email basis, not just at an account-level.
Monitoring	Requirement 10	Track and monitor all access to network resources and cardholder data.	Log and monitor any access to emails with sensitive data.	Identify sensitive content in workspaces and monitor how, when and by whom the content is accessed.
Data Retention	Requirement 3.1	Keep cardholder data storage to a minimum and retain only what's necessary for business.	Limit the amount of sensitive data stored in emails.	Identify, label and redact sensitive content in mailboxes at the message-level.
Secure Systems	Requirement 6	Develop and maintain secure systems and applications.	Any application or system storing emails should be secured.	Provide visibility, implement breach prevention measures, improve security posture, and secure sensitive data.