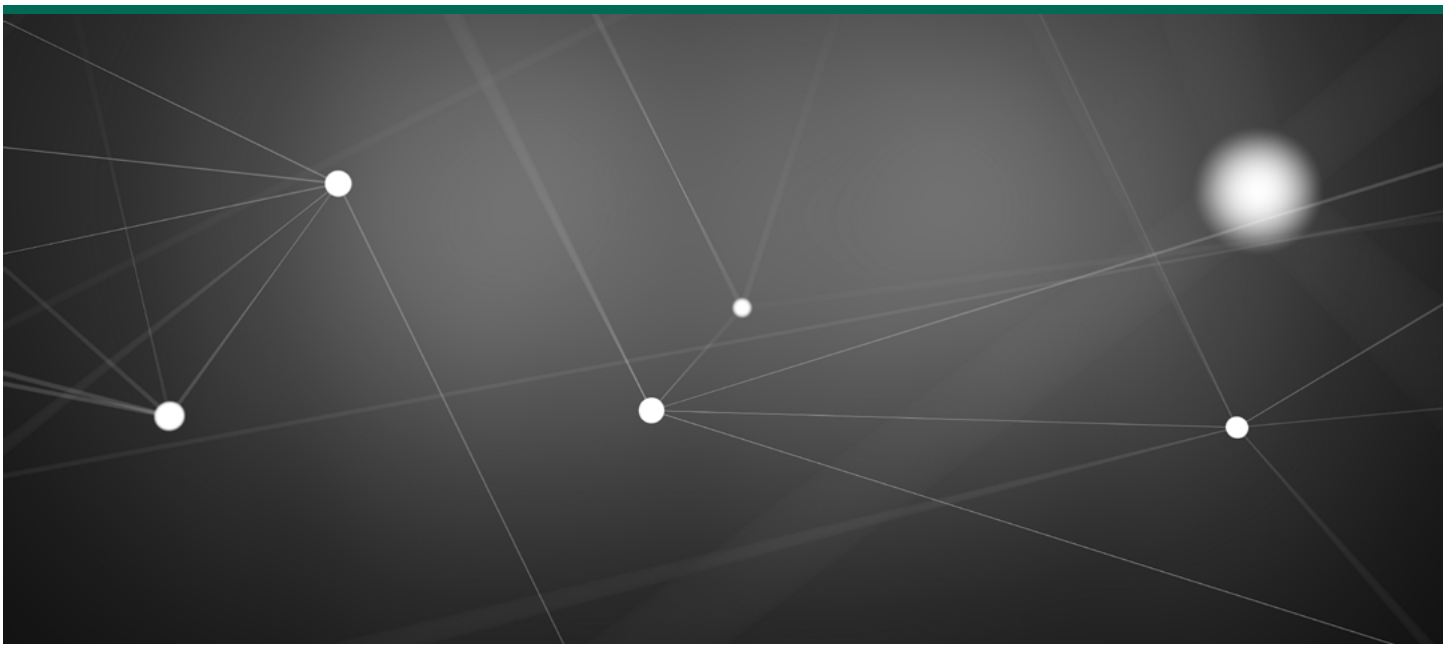
FORTRA

GUIDE *(Clearswift)*

PCI DSS 4.0 – What Is Best Practice?



Addressing compliance via the redaction of credit card information from documents and emails

The Payment Card Industry Data Security Standard (PCI DSS) has been in place since 2004, with the overarching goal of protecting cardholder data and preventing data breaches. Ensuring compliance with this legislation is vital, but can be complex and challenging, especially given that requirements are continually changing. There was a significant update when the EU General Data Protection Regulation came into force in May 2018, and the most recent update – PCI DSS 4.0 – emerged in April 2022. The COVID-19 pandemic had a great impact on the PCI update with its impact on the volume of online transactions, the increase in use of point-of-sale (PoS) machines, and the subsequent effect on storing card-holder data in cloud platforms. All this meant attackers evolved their modes of attack and organizations need to update their own modes of defense. While the database issues and solutions are well known, the real challenge is around un-structured data. When credit card information finds its way into email and documents, these are then transferred around and outside the organization creating unnecessary risk.

A PCI DSS 4.0 Overview

The main principals have remained the same with PCI DSS 4.0, but the requirements have evolved somewhat. They have been redesigned to focus on security objectives to guide how security controls should be implemented.

Customized implementation is the most significant. It looks at the intent of the objective and allows organizations to design security controls to meet it. This means businesses can adapt implementation procedures and meet requirement intent. Other amendments include the need for stronger authentication requirements, acknowledging the role of Identity and Access Management (IAM) in safeguarding cardholder data, and expanded applicability for encrypting cardholder data.

These changes are now active, although there is a transition period ending on March 31, 2025. This is intended to provide organizations with time to plan and implement changes to meet the updated requirements.

Risks and Consequences

PCI DSS was one of the first global standards which applies across a broad spectrum of businesses. In essence, if you want to accept credit cards as payment, then you (or your supplier) must comply with the standard.

There are fines involved with non-compliance, ranging between $50-$90 per cardholder who has been compromised, and there are other time-based fines while compliance is being established. These can vary from $10,000 / month up to $100,000 / month, so not insignificant. However, the real risk is the removal of processing of data, i.e. credit cards will no longer be accepted, and for many organizations this means that their business will grind to a halt.

All the other consequences relating to a breach also remain, from the loss of reputation from customers, partners, and suppliers to increased audit fees as well as the remediation and potential litigation costs.

With GDPR, the fines have the potential to be even more crippling. There is an upper limit of €20 Million or four percent of global turnover, whichever is greater, and we have already seen some astronomical fines for GDPR breaches.

PCI DSS 4.0 has not increased the penalties for non-compliance, but the consequences are already severe and clear for all parties to see.

Inbound and Outbound

For many organizations, receiving email with credit card details is an everyday occurrence. Customers who think it is better to send in details rather than talk to a person, or those who struggle with the online web portal, are two reasons why this occurs. Upon receiving the email, the natural response is to reply to it, and this can cause a problem, as then the organization will be sending PCI data over an open channel, which is a data breach – even if the data is going back to where it has come from.

Traditional Data Loss Prevention (DLP) solutions will identify the credit card number and block the email. This 'stop and block' action causes frustration from the customer, who doesn't know if the information has been received, the employee, who can't get the response back, and the IT or audit and compliance departments who need to investigate the problem and remediate accordingly.

While a data loss incident can be a disaster for an organization's reputation, there is now a new imperative around inbound information as well. Unwanted data acquisition can create problems just as much as data leaving the organization. There are a couple of scenarios which should be considered.

PCI Data on a Non-PCI DSS Compliant Network

For many organizations, the processing of credit card details is outsourced to a third party, meaning that they don't need to be PCI DSS 4.0 compliant. Even within banks, there are segments of the network which are not PCI DSS compliant, as there is theoretically no need for them to be so. Of course, theory and practice are two different things and so receiving details does happen. At this point, audit and compliance become involved to investigate the issue and remediate the problem.

Data Sent in Error

How many times have you sent or received data in error? The chances are that it has happened, hopefully not too frequently, but across all employees then it can happen far more frequently than you might imagine. In many cases, the information that has been shared is not a compliance issue, but sometimes it is. Furthermore, 'hidden' information in spreadsheets or reports can create a data loss risk. When GDPR came into force, the new tenet of shared responsibility made the problem of receiving unauthorized information a serious issue.

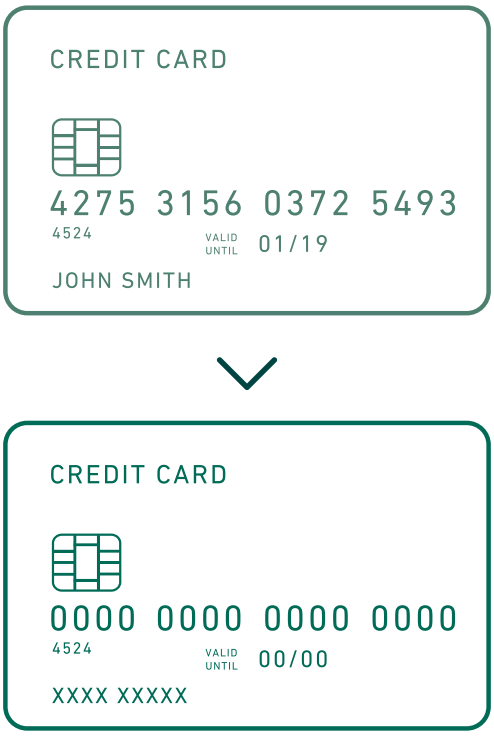
In a world where electronic communication is critical to most businesses' success, the drawbacks of traditional DLP blocking communication and collaboration mean that it is seldom deployed. The risk associated with lost business is significantly greater than the issues of solving the problem. Fortunately, there is a different way, one where the content can be adapted on-the-fly to ensure that communication continues and the risk of exposure to unauthorized data is removed, whether it is inbound or outbound.

An Adaptive Solution

Clearswift has been a leader in email and web security for more than 20 years and understanding the issues with traditional DLP set about mitigating the problem by creating Adaptive DLP. The concept is relatively simple - remove the information which breaks policy and leave the rest to continue to its destination – and critical to compliance with PCI DSS 4.0.

Adaptive Redaction has three components:

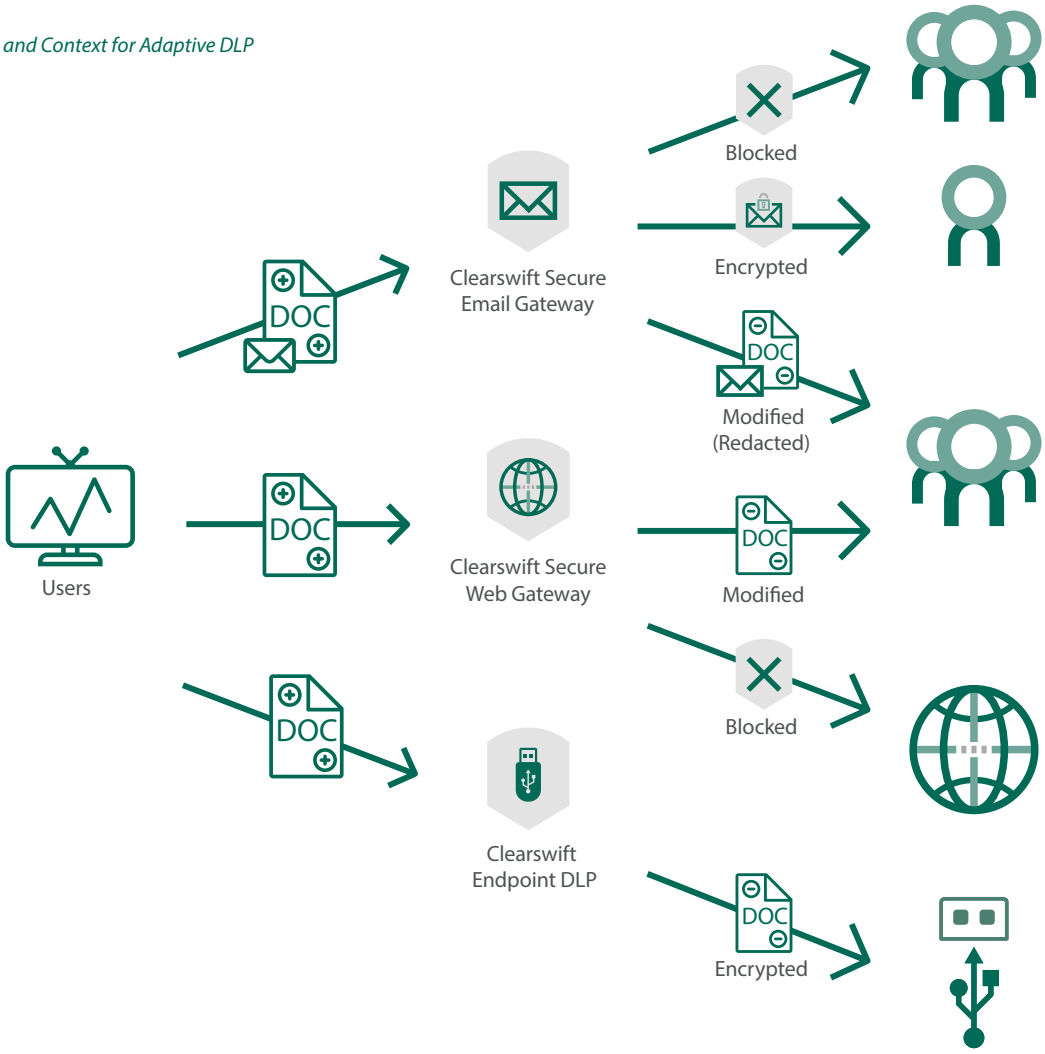
1. Data Redaction: Remove the information you can see. For example, the credit card number in an email, and replace it with hashes. This functionality also removes information which has been hidden, for example in a hidden column or row in a spreadsheet which contains PCI data.
2. Document Sanitization: Remove hidden information such as that in document properties, revision history and document fast save data.
3. Structural Sanitization: Remove active content, which is the most frequent method for ransomware to infiltrate an organization.



Within security, there is a saying "you are only as strong as your weakest link". In practice this means that all communication channels need to be covered. Whether this is email, the web or the endpoint, where copying information to a USB stick or other removable media can create risk.

Clearswift's adaptive approach is built around a common Deep Content Inspection (DCI) engine, this ensures that a policy can be defined in one place but used across all communication channels. The action taken might differ depending upon the channel used, see Figure 1. So for an email, it might be that data redaction is applied, whereas someone trying to upload data to a collaboration site (e.g. Microsoft OneDrive) has the data transfer blocked, or copying to a USB stick may result in the information being encrypted.

Figure 1: Content and Context for Adaptive DLP



A fully flexible policy ensures that there is sufficient granularity to make a decision based on the content, the context (who is doing what) and the communication channel.

Distributed Operations

When putting a DLP solution in place, even an adaptive one, there will be security events which occur. Some of these will inevitably be where the policy is overzealous and needs to be altered, but there is an immediate need to get the information which has been blocked to the destination. Clearswift's solution integrates with Microsoft Active Directory (or any other LDAP service) to enable DLP events to be routed to the manager of the person who caused the infringement rather than just to an individual or department.

While the security events can go to a specific person or department, we have found that routing them to the manager means the operational overhead for a DLP solution is significantly reduced. The manager has the context around what was being done and can, if the circumstances allow, release the original with a simple click of a URL in an email, See Figure 2.

The introduction of distributed operations has meant that even SMEs can deploy a cost effective DLP solution without the need for additional IT staff.

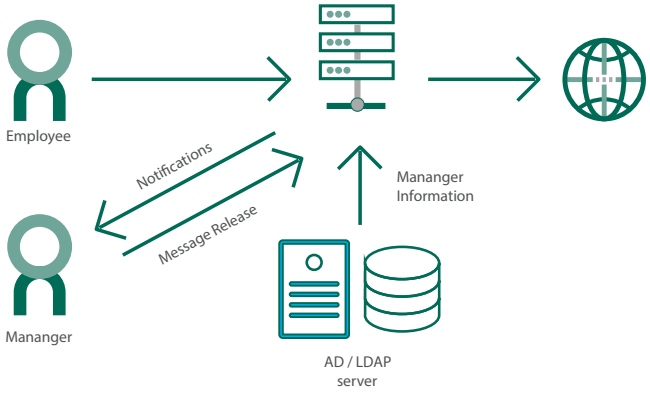


Figure 2: Distributed Operations reduces operational costs

Augmenting Existing Security

The Clearswift Adaptive solution can be used standalone, or in conjunction with existing email and web gateways or other DLP solutions. This means there is no need to 'rip and replace' the existing products in order to get the benefits of an Adaptive DLP solution. Furthermore, should the time come to upgrade to a Clearswift gateway, the Adaptive DLP policy can be quickly and easily transferred to a gateway product, whether that is on-premise or in the cloud.

Legacy Data

Dealing with data 'today' leaves potential risk in legacy data which has distributed itself around the organization, whether in reports or other files. Clearswift's Data-At-Rest scanning ability for endpoints and servers can readily identify those systems which have PCI data on them. The scans can also extend to cloud-based drives to ensure that critical data has not been uploaded in an unauthorized manner. A simple report may suffice, or automated remediation, for example moving all the affected files to a secure server, are available. Based on policy, the risk of legacy data can be addressed in a granular manner.

Summary

When it comes to PCI DSS 4.0 compliance, the impact of non-compliance can be catastrophic to a business. The fines can be significant, but the removal of being able to process credit cards can shut a business down until compliance has been achieved and assured. Even for those businesses who have outsourced their handling there remains a risk that data will be sent to them in error.

From a compliance perspective, how data falls into unauthorized hands makes little difference whether it is a hacker from outside, a malicious insider or a mistake. A solution is needed.

Traditional DLP solutions have a number of significant drawbacks, particularly for SMEs whereas a next generation Adaptive DLP solution will mitigate the risk without creating undue additional operational costs. A consistent policy across all communication channels, operating on both inbound and outbound traffic, ensures that credit card information can be kept safe in all circumstances.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.