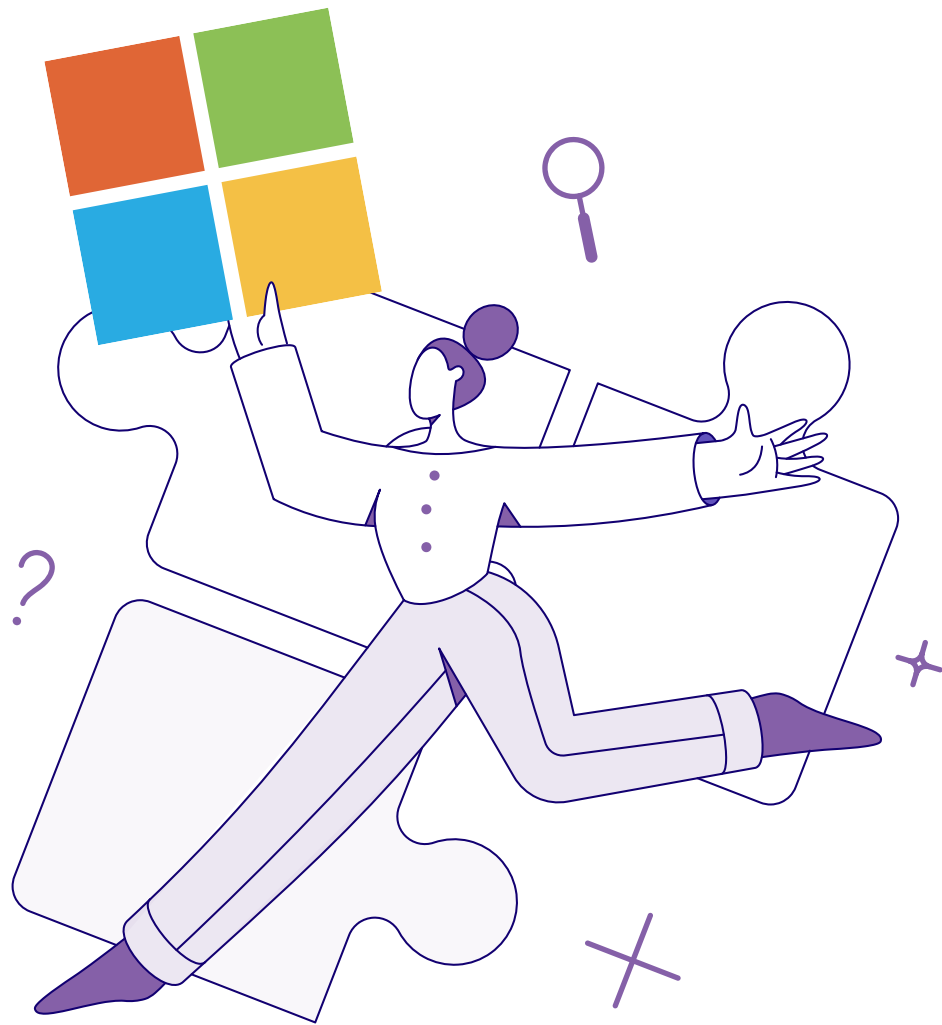


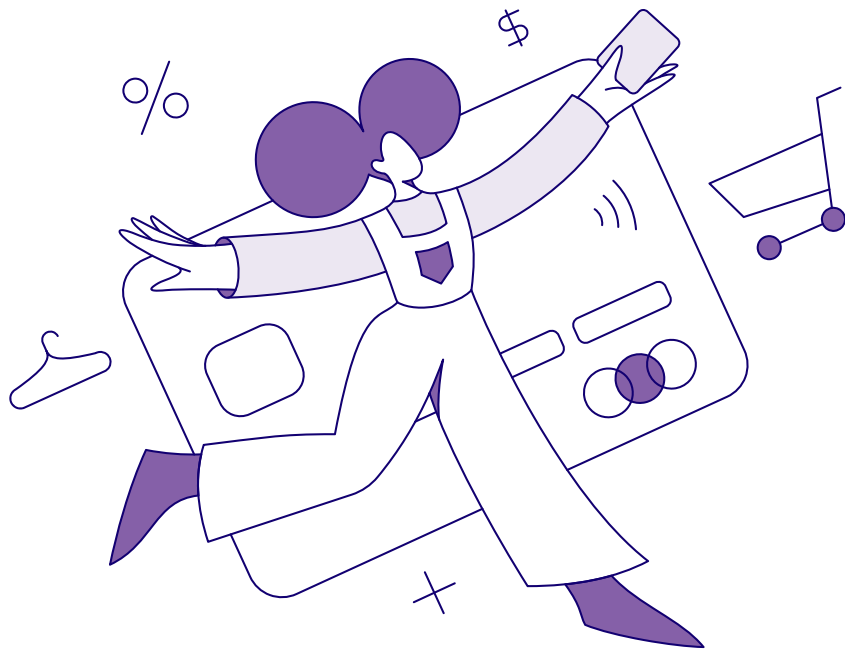


Collaboration of PCI Data from Microsoft 365



WHITE PAPER

Ilya Pozharsky | CISSP -CISM -CMMC RP
Vice President Security and Compliance Solutions



Introduction

Data security is a critical concern for any organization handling sensitive information, especially those involved with payment card data. The Payment Card Industry Data Security Standard (PCI DSS) was established to ensure that organizations handling credit, debit, and other card types control cardholder data and reduce credit card fraud.

Many organizations struggle to ensure that their systems comply with PCI standards. This includes their productivity applications such as Office 365. Microsoft has provided an attestation of compliance for Microsoft Azure, SharePoint Online, and OneDrive for Business for storing and processing PCI data (as per Microsoft's Service Trust Portal [PCI DSS](#) at microsoft.com) as well as some other services. However, Microsoft specifically does not attest to Exchange Online being PCI compliant.

Companies working with PCI data typically need to share and collaborate with this data with external parties. Usually, PCI data is managed in applications that are used specifically for payment processing. The data is stored in a structured format and in secure protected locations that, along with the applications themselves, must meet the 12 PCI DSS requirements:

12 PCI DSS requirements:

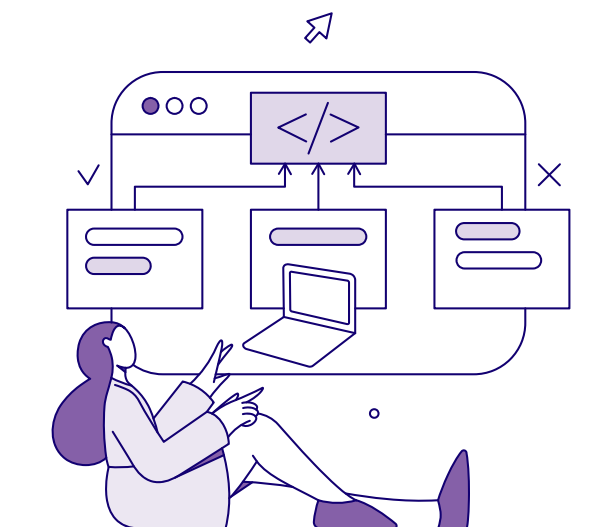
1. Install and maintain a firewall configuration
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt the transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

Ensuring that data in these applications and structured sources is protected and the environment is compliant is “easy.” Unfortunately, in many cases, organizations need to use and process this data outside of these applications. Business lines typically need to collaborate with this type of data with users both inside and outside of the organization. Many times, this collaboration involves unstructured data (i.e., files), which makes it more challenging to meet PCI DSS requirements.

Thankfully, when it comes to internal collaboration, organizations can take advantage of Microsoft’s 365 SharePoint Online and OneDrive infrastructure to store data in a compliant way, as these environments have been certified at Service Provider Level 1 for PCI data ([Payment Card Industry \(PCI\) Data Security Standard \(DSS\) - Microsoft Compliance | Microsoft Learn](#)).

In addition to meeting PCI regulatory requirements, Microsoft 365 provides a great user experience by enabling Modern Collaboration, or link-based sharing, that allows collaborators to work on a single file. While SharePoint and OneDrive can be used to collaborate on files with external parties, many organizations, especially financial services companies, disable that capability due to multiple reasons (including granularity of controls and tenant restrictions that block access to 3rd party sharing applications, including other M365 tenants). Unfortunately, email, which is still the most widely used sharing method, is not compliant with PCI DSS.

Organizations still struggle to provide the appropriate guardrails to ensure their users stay compliant. eShare can help! eShare provides a platform that integrates with Microsoft 365 productivity and security controls, helping organizations navigate these challenges in multiple ways. Advisory services offered by eShare’s Microsoft Security and Compliance experts ensure that an organization’s M365 environment is configured optimally to ensure compliance.



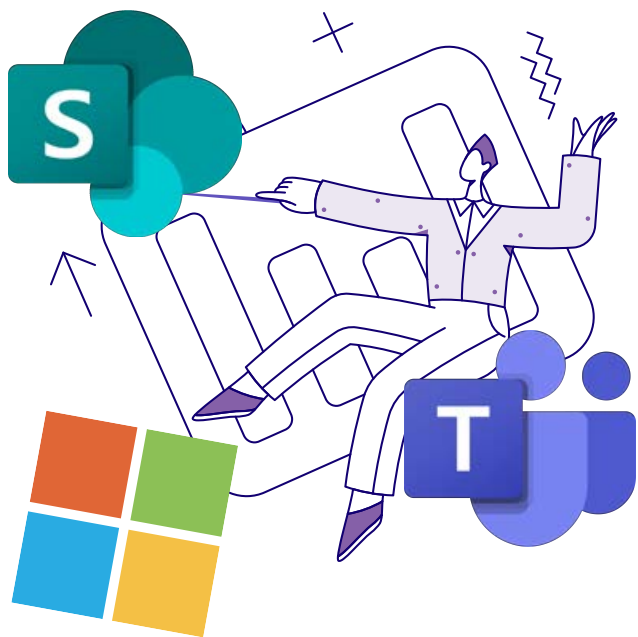
“

In addition to meeting PCI regulatory requirements, Microsoft 365 provides a great user experience by enabling Modern Collaboration, or link-based sharing, that allows collaborators to work on a single file.

”

How eShare Works

eShare is a SaaS solution built on top of Microsoft 365 (eShare can also integrate with other cloud data repositories) to extend MSFT's external collaboration capabilities. Organizations can leverage it to secure modern collaboration by sharing data with external parties while keeping data within their own tenant without the need to introduce guest accounts into their environment. Deep integrations with identity providers, MSFT Graph, Purview Information Protection, and DLP provide a great user experience while offering organizations the required visibility into their data usage. These integrations also provide fine-grained controls to ensure their sensitive data is shared securely.



- Allows highly secure file sharing from the native Teams & SharePoint UX, even when native external file sharing is disabled, while keeping data in the source tenant
- Bring your own Identity: integrates with IDPs such as Entra ID for an SSO experience and can bridge multiple identity providers and repositories
- Integrates with M365 data governance by inspecting documents/graph for Purview Sensitivity Labels and/or DLP and automates sharing policies based on those signals
- Extends the benefits of Modern Collaboration to any external party, including those with no Azure identity (e.g., Google shops, B2C)

What Companies Need to Do

First, companies need to appropriately discover and classify their data. Data classification is not the same as tagging data. These separate functions are often conflated, but data classification is simply the task of identifying what data exists in a document or repository. Microsoft's classification includes over 350 out-of-the-box sensitive information types, as well as the ability to create custom data types to match the organization's actual data. Administrators can configure custom sensitive information with Regex, Exact Data Match, Fingerprinting, and even machine learning leveraging Trainable Classifiers.

Once the data is classified (identified), downstream solutions can provide controls based on that classification. Microsoft Purview DLP, Sensitivity Labels with Purview Information Protection, Data Lifecycle Management, and other tools can use these classifications to protect and manage files and data. Leveraging several of these features along with eShare to provide active controls for external sharing is paramount in meeting regulatory requirements such as PCI DSS.

What Companies Need to Do

eShare enhances data security and compliance with PCI DSS by ensuring that sensitive payment card information never leaves the security of the enterprise's own Microsoft 365 tenant. This approach guarantees that all data remains within the control of the organization, thus complying with PCI DSS requirements that demand the protection of cardholder data through secure storage and handling practices.

The eShare platform integrates with M365 File and Container Sensitivity Labels as well as DLP alerts, leveraging signals from these products to define access controls that are automatically applied based on policies driven by the classification and/or label assigned by Microsoft Purview. eShare integrates with organizations' IDPs to not only create a great user experience but also to bridge identities from multiple IDPs to ensure anyone who accesses PCI data externally does so via a compliant portal with data staying in the data owner's M365 compliant repository with named access by external parties.

eShare's internal governance solution ensures only the appropriate internal users have access to PCI data by controlling the oversharing challenge most organizations struggle with when collaborating with not just external parties, but internal colleagues as well.

eShare is designed to never access or store the data itself.

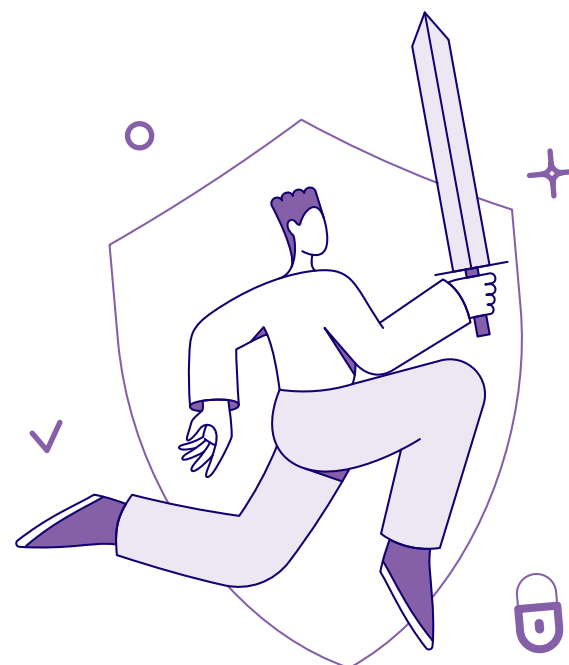
It operates by enabling secure sharing and collaboration directly within the tenant's existing infrastructure, thus avoiding any external data processing or storage that could pose a risk to data security.

This architecture also allows organizations to continue to leverage their current investments with Microsoft 365 to protect cardholder data in addition to the access controls and governance via eShare.

“

The eShare platform integrates with M365 File and Container Sensitivity Labels as well as DLP alerts, leveraging signals from these products to define access controls that are automatically applied based on policies driven by the classification and/or label assigned by Microsoft Purview.

”



What Companies Need to Do

- **Install and maintain a firewall configuration:**

Data does not leave the organization's Microsoft 365 environment when collaborating with external parties, so existing controls continue to apply

- **Do not use vendor-supplied defaults for system passwords and other security parameters:**

eShare integrates with the organization's IDPs to ensure appropriate password security is applied

- **Protect stored cardholder data:**

eShare provides active controls on data being shared externally by keeping it in the originating data repository and providing data-centric policy-based access controls

- **Encrypt the transmission of cardholder data across open, public networks:**

Microsoft 365 encrypts data at rest. eShare encrypts all access and communication of data in transit to meet stringent regulatory requirements

- **Use and regularly update anti-virus software or programs:**

M365 offers robust anti-virus and advanced threat capabilities via the M365 Defender suite of products

- **Develop and maintain secure systems and applications:**

M365 and eShare are built using a security-by-design methodology. That being said, cloud computing does require a Shared Responsibility model. eShare's advisory services combined with Microsoft 365 and the eShare external collaboration platform help organizations ensure they are configured in the optimal way to protect cardholder data while enabling the business with a great user experience

- **Restrict access to cardholder data by business need-to-know:**

eShare protects cardholder data via policies created by the organization. The business can define what external entities are contractually allowed to view/process cardholder data on behalf of the organization and programmatically apply the appropriate guardrails to ensure the effectiveness of these controls.

eShare's new M365 Internal Enterprise Sharing Governance solution will help ensure internal access follows the business need-to-know requirements as well

- **Assign a unique ID to each person with computer access:**

eShare integrates with the organization's IDPs and policies to ensure each user has their own identity to access cardholder data

- **Restrict physical access to cardholder data:**

All data is contained in the Microsoft 365 cloud, eliminating physical access to cardholder data

- **Track and monitor all access to network resources and cardholder data:**

eShare's robust analytics platform provides granular reporting on all access to sensitive data. We can provide visibility to all access by external and internal users leveraging the platform

- **Regularly test security systems and processes:**

eShare's advisory services help organizations devise their data governance strategy, including developing and executing test plans to validate the effectiveness of controls

- **Maintain a policy that addresses information security for all personnel:**

eShare's policies integrate with the organization's governance strategy to ensure policies are applied for all users, internal personnel, and external collaborators



Ilya Pozharsky | CISSP -CISM -CMMC RP

Vice President Security and Compliance Solutions

For more information on how eShare can help your organization ensure PCI DSS compliance while leveraging Microsoft 365

[in Ilya Pozharsky](#) www.eshare.com