eSHARE

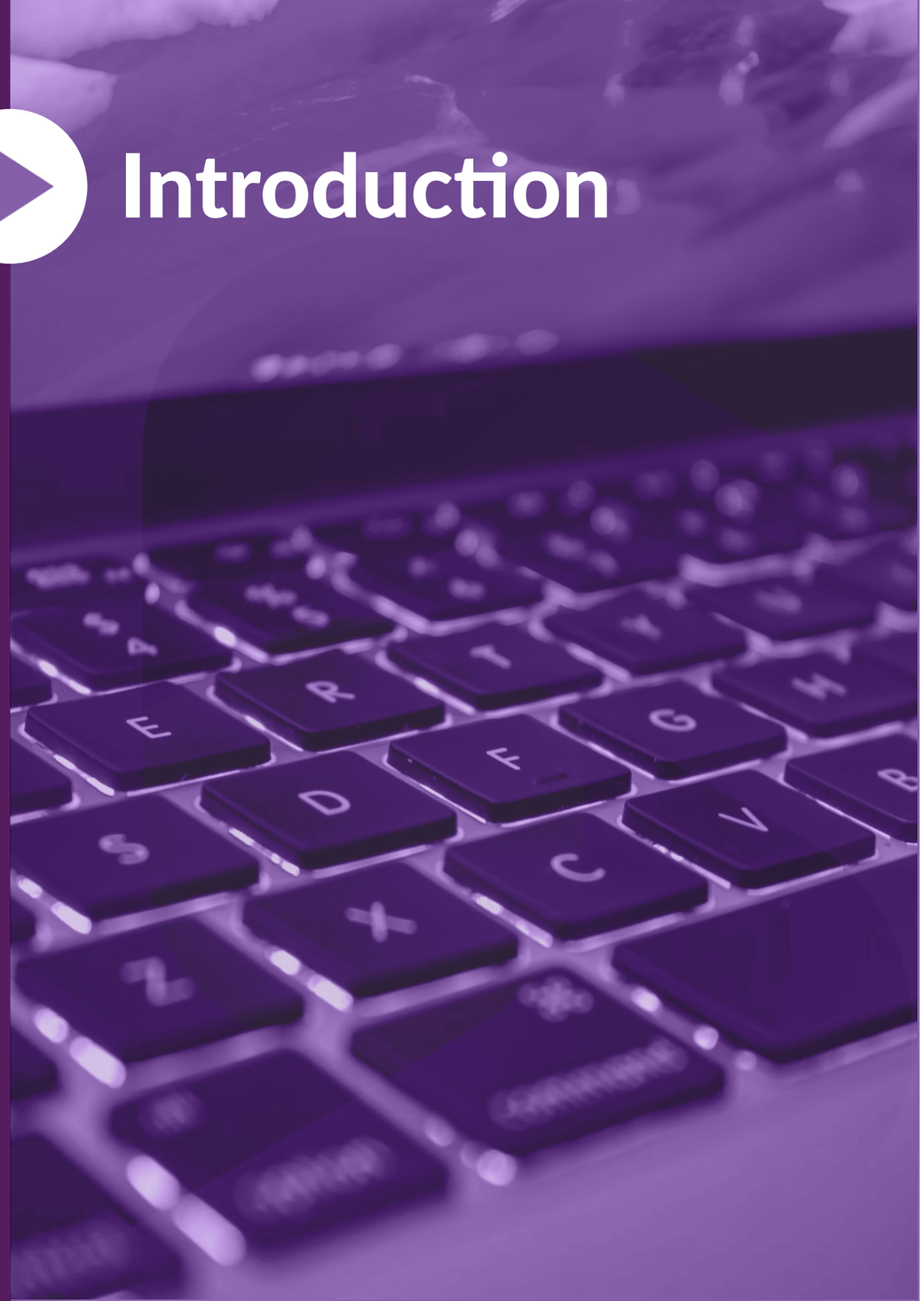
The 5 keys to:

Balancing data governance and business needs

Collaboration, reimagined.

www.eshare.com

Table of contents



Introduction

In the evolving landscape of digital technology and data management, the role of a Chief Information Security Officer (CISO) has never been more critical. CISOs are tasked with the delicate and demanding balance of robust data governance with the dynamic needs of businesses.

This document, titled "The Five Keys to Balancing Data Governance and Business Needs," provides a comprehensive roadmap to navigate this intricate balance. Our focus here is on five critical areas, or keys, each with its unique role in the overall structure of effective data governance: "Enhancing User Experience," "Mastering Identity Management," "Maintaining Branding and Domain Consistency," "The Power of Robust Policy-Driven Tools," and "The Key Role of Data and Analytics."

These keys are not independent entities but integral components of a holistic approach towards managing data governance in line with business needs.

As we delve into each key, we explore their relevance, the challenges CISOs face, and best practices to ensure effective implementation.

By understanding and applying these keys, CISOs can create a harmonious environment that seamlessly blends stringent data governance with the operational needs of the business. This balance is pivotal for the success of modern organizations in an increasingly digital and interconnected world.

1 **"Enhancing User Experience"** explores how to streamline data governance processes to optimize both internal and external user experiences.

2 **"Mastering Identity Management"** focuses on the importance of effective identity management systems in maintaining secure yet fluid collaboration.

3 **"Maintaining Branding and Domain Consistency"** illustrates the importance of consistent branding in data sharing and how this can increase trust and reduce friction in external collaborations.

4 **"The Power of Robust Policy-Driven Tools"** highlights the potential of flexible, comprehensive policy tools in securing data and supporting business operations.

5 **"The Key Role of Data and Analytics"** delves into the integral role of data analytics in assessing, improving, and maintaining effective data governance systems.

We invite you to peruse this guide, confident that it offers valuable insights and actionable strategies. These can empower you to steer your organization's data governance strategy effectively, ensuring it aligns perfectly with your business needs.

Key 1: Enhancing user experience

Introduction:

Navigating the realm of data governance can be a challenging endeavor for Chief Information Security Officers (CISOs). Striking a balance between enforcing robust security measures and ensuring smooth business operations is crucial.

One essential element often affected by this delicate balance is the user experience.

It's undeniable that stringent security measures can have a negative impact on user experience, affecting productivity, morale, and satisfaction among both internal and external users.

As we delve into this issue, it's essential to remember that tools and controls for data governance should ideally enhance work processes, not complicate them.

The impact of data governance on user experience:

Often, data governance and security measures are seen as hindrances to smooth operation. They may add additional steps to processes, require more time from users, or may not be intuitive to use. These measures can lead to decreased productivity as employees grapple with complex systems, and can also lower morale as work processes become more cumbersome. Furthermore, external users may become frustrated with difficult access procedures, potentially affecting business relationships and customer satisfaction.

The importance of a balanced approach:

While data governance is undeniably crucial for protecting sensitive information and maintaining compliance, it's equally important to ensure that these measures do not impede business operations. An approach that balances stringent data governance with the needs of the business can help ensure a positive user experience, leading to increased productivity, higher morale, and improved user satisfaction.

Strategies for enhancing user experience:

To create this balance, it's essential to incorporate user-centric design principles when implementing data governance tools and controls. These may include:

1. **Ease of use:** *Systems should be easy to navigate, with intuitive interfaces and clear instructions. This can help reduce the time employees spend learning new systems, allowing them to focus on their core tasks.*
2. **Automation:** *Automating certain processes, such as data classification or access control, can help remove some of the burden from users, making their work processes more efficient.*
3. **Education and training:** *Providing comprehensive training can help users understand the importance of data governance measures, and teach them how to use systems effectively and efficiently.*
4. **Feedback loops:** *Implementing mechanisms to gather user feedback can help identify pain points and areas for improvement, ensuring continuous enhancement of the user experience.*

Conclusion:

CISOs face a critical challenge in striking a balance between robust data governance and the needs of the business. However, by placing user experience at the forefront of data governance strategies, it's possible to create a more productive, positive, and satisfying work environment for all users.

View Demo

Key 2: Mastering identity management

Introduction:

Identity management stands as one of the most critical aspects of data governance that Chief Information Security Officers grapple with.

The challenge lies in achieving an approach that is simple, straightforward, manageable, and meets both governance requirements and business objectives.

An effective identity management strategy ensures users have the appropriate access to resources, while also mitigating risks associated with unauthorized access.

In this paper, we will explore the challenges faced by CISOs in managing identities and how to strike a balance between security and business needs.

Challenges in identity management:

The rapidly evolving digital landscape has brought a multitude of identity management challenges, including:

1. **User authentication:** *The need for simple yet secure authentication measures is paramount. Complex or cumbersome authentication can lead to user frustration, non-compliance, and ultimately, lowered security.*
2. **Scalability:** *As organizations grow, their identity management systems need to scale as well. The challenge lies in maintaining a system that is not only secure but can also handle an increasing number of identities without sacrificing user experience.*
3. **External users:** *Managing the identities of external users, such as contractors or partners, brings unique challenges, especially in maintaining the appropriate level of access.*
4. **Regulatory compliance:** *Adhering to ever-evolving data privacy regulations while ensuring efficient identity management can be a formidable task.*

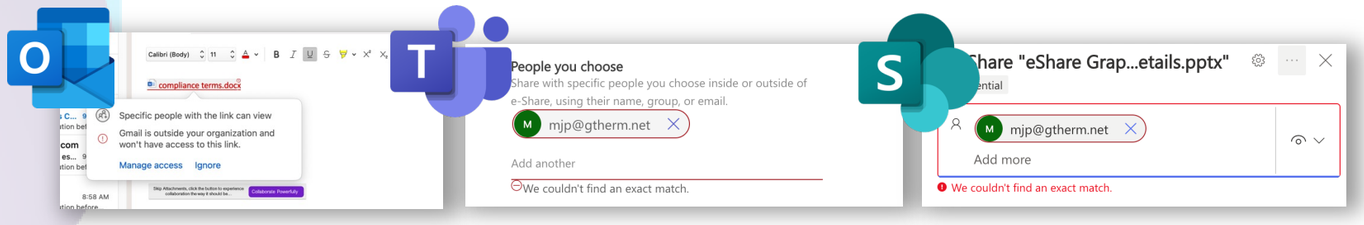
Balancing identity management and business needs:

To create a robust identity management strategy that aligns with business needs, CISOs should consider the following tactics:

1. **Streamlining authentication:** *Implement solutions like Single Sign-On (SSO) or Multi-Factor Authentication (MFA). These technologies increase security while providing a more straightforward process for users.*
2. **Scalable solutions:** *Adopt identity management systems that are scalable, accommodating growth without impacting user experience or system performance.*
3. **Role-based access control (RBAC) and attribute-based access control (ABAC):** *Implementing RBAC and ABAC can help manage both internal and external users' identities. By granting access rights based on roles or attributes, you can maintain security while ensuring users have the access they need to perform their tasks.*
4. **Automated provisioning and deprovisioning:** *Automating the process of creating and removing identities can help ensure that no unauthorized users have access to systems and that new users gain access quickly.*
5. **Compliance tools:** *Use tools that can help manage identities while ensuring compliance with regulatory standards, such as GDPR or HIPAA.*

Conclusion:

In conclusion, while identity management poses unique challenges, a well-planned strategy can balance both data governance and business needs. By implementing user-friendly, scalable, and role-based systems, CISOs can ensure the integrity of their organization's data, enhance user satisfaction, and meet business objectives.



Key 3: Maintaining branding & domain consistency

Introduction:

In a world increasingly wary of digital threats, maintaining branding and domain consistency across the user experience is crucial for any business, not only to preserve brand value and recognition but also to instill trust and confidence among users.

Yet, maintaining this consistency while adhering to data governance and security standards poses unique challenges for CISOs.

In this paper, we explore the importance of branding and domain consistency, the challenges faced in maintaining it, and strategies to achieve a balance between robust data governance and preserving brand identity.

Challenges in maintaining branding and domain consistency:

1. **User trust:** Users are more suspicious of irregularities in branding and domain changes. A sudden change from a core domain to a different one (like SharePoint or Box) can make them question the legitimacy of the content.
2. **Brand dilution:** Security measures, if not properly implemented, could undermine the millions spent on establishing and maintaining a corporate brand.
3. **Multiple brands:** Companies grown through acquisitions often maintain multiple brands. Representing the correct brand and corporate identity depending on the audience can be complex.
4. **Blocked domains:** There's a risk that the domains used by companies may be blocked by external parties such as partners, vendors, or contractors, hindering progress.

Balancing branding, domain consistency, and data governance:

To ensure branding and domain consistency without compromising data governance and security, CISOs can consider:

1. **Consistent branding across platforms:** *Consistently use logos, colors, and other brand elements across all platforms. This can be achieved by creating a set of branding guidelines to be followed across the organization.*
2. **Custom domain naming:** *Custom domains should be set up for various platforms (e.g., SharePoint, Box) to maintain domain consistency. This practice increases trust among users as they don't see a drastic domain switch.*
3. **Branding management systems:** *Use of centralized branding management systems can help ensure consistency, especially for organizations with multiple brands.*
4. **Domain reputation management:** *Regularly check and manage the reputation of your domains to avoid being blacklisted or blocked by recipients.*
5. **User education:** *Train users to recognize your official domains and branding to increase their confidence while interacting with your platforms.*
6. **Partner with IT and marketing:** *CISOs should closely work with IT and Marketing teams to ensure security measures don't compromise branding efforts.*

Conclusion:

In conclusion, while the importance of branding and domain consistency in building trust and value can't be overstated, it's equally essential to ensure robust data governance. By implementing strategies that align branding efforts with data governance policies, businesses can not only enhance security but also uphold their brand's integrity and reputation.

Key 4: The power of robust policy-driven tools

Introduction:

The rapidly evolving digital landscape has expanded the realm of data security and governance, demanding a fresh approach to traditional security strategies.

One such approach is embracing robust policy-driven tools to enable data-centric security. The right mix of these tools can significantly empower CISOs to strike a balance between governance, compliance, and user efficiency.

This paper discusses the importance of robust policy options, the associated challenges, and the strategic deployment of these tools to harmonize business needs and data governance.

Challenges in implementing policy-driven tools:

1. **Complex data access needs:** *The sheer number of data access and sharing combinations make it a challenging task to establish comprehensive and effective policies.*
2. **Integration:** *Ensuring seamless integration of various tools like data labeling, data retention, Data Loss Prevention (DLP), external collaboration, etc., can be a complex task.*
3. **Balancing risk and efficiency:** *Striking a balance between risk-appropriate controls and user efficiency requires a deep understanding of business needs, compliance requirements, and the capabilities of security tools.*

Harnessing the power of robust policy-driven tools:

To overcome these challenges and establish effective data governance, CISOs can consider the following strategies:

4. **Adopt a data-centric approach:** *Prioritize data protection at its core by focusing on the security of the data itself, regardless of where it resides or moves.*
5. **Select versatile tools:** *Choose tools with robust and flexible policy options to meet varying data access and sharing requirements.*
6. **Ensure seamless integration:** *Opt for tools that integrate well with other systems to create a unified and effective data protection ecosystem.*
7. **Risk-appropriate controls:** *Implement controls in alignment with the data's sensitivity and the level of risk associated with its access and sharing.*
8. **Regular policy reviews:** *Perform regular audits and reviews of data protection policies to ensure they stay relevant and effective in the face of evolving threats and changing business needs.*
9. **User training:** *Educate users about policies, their importance, and how to apply them in their daily operations.*

Conclusion:

In conclusion, while policy-driven, data-centric security tools can help establish robust data governance, it's equally important to ensure these policies and tools align with business needs, fostering productivity and efficiency. Through strategic implementation and regular policy reviews, CISOs can achieve a balance between robust data governance and operational agility.

View Demo

Key 5: The key role of data and analytics

Introduction:

In an environment defined by copious amounts of data, data logging, analytics, and alerting are crucial elements of a comprehensive strategy.

Leveraging these components efficiently provides vital insights into data usage, flow, duplication, and compliance, enabling organizations to strike a balance between governance and operational efficiency.

This paper explores the importance of data and analytics in harmonizing governance and business needs, along with the inherent challenges and potential solutions.

The importance of data and analytics:

1. **Enhanced compliance:** *Data logging and analytics provide tangible evidence of adherence to regulatory standards, enabling organizations to prove compliance.*
2. **Risk identification:** *Analyzing data usage and flow helps in identifying potential risks and threats to the security infrastructure.*
3. **Need recognition:** *Patterns of blocked data sharing attempts can be identified using data analytics, indicating areas where controls may need adjustment for operational efficiency.*
4. **Informed decision-making:** *Data analytics provide critical insights about data usage, aiding C-suite executives and managers in strategic planning and decision-making.*
5. **Spotting data duplication:** *Advanced analytics can highlight issues like data duplication or replication, facilitating streamlined data management.*

Interoperability with analytics tools:

Effective data analysis isn't just about gathering information; it's also about making this data easily accessible for deeper insights. Therefore, it's essential for data governance tools to integrate seamlessly with popular analytics platforms like PowerBI, Tableau, and Splunk. Such integration enables organizations to combine and analyze data from multiple systems, providing a more comprehensive understanding of their data landscape.

Challenges in implementing data and analytics:

1. **Volume and variety of data:** *The massive amount and diversity of data in today's businesses can pose significant challenges to meaningful analysis.*
2. **Data privacy:** *Ensuring data privacy during analytics is complex, particularly with stringent regulations surrounding data protection.*
3. **Technical expertise:** *In-depth data analytics often require specialized skills, which may necessitate additional training or recruitment efforts.*

Strategies for implementing data and analytics:

1. **Invest in the right tools:** *Opt for data analytics tools capable of managing the volume and variety of your data, and ensure they integrate well with widely used analytics platforms.*
2. **Incorporate analytics into security strategy:** *Include analytics as an integral part of your security strategy for prompt identification of potential threats and risks.*
3. **Conduct regular audits and reviews:** *Undertake regular audits to ensure compliance and update data management strategies based on analytic insights.*
4. **Develop clear policies:** *Formulate and implement clear policies regarding data analytics to ensure adherence to privacy regulations and seamless data exchange between systems.*

Conclusion:

In conclusion, data and analytics form the backbone of modern data governance strategies. Despite the associated challenges, strategic utilization of these tools can pave the way for data-driven decision-making, enhancing regulatory compliance and business productivity.

Bonus content:

The art and science of data labeling with Microsoft purview information protection

Introduction:

Data labeling, a pivotal facet of effective data management, security, and compliance, can be a daunting task.

With a comprehensive tool set, Microsoft Purview Information Protection empowers organizations to label data efficiently and precisely.

This guide presents the top ten strategies to leverage Microsoft Purview Information Protection for effective data labeling, all the while balancing governance needs and business operations.

Top 10 Strategies for effective data labeling with Microsoft purview information protection:

1. **Identify the data sources:** *Recognize the variety of data sources in your organization, like file shares, databases, email systems, and more. Microsoft Purview Information Protection supports various data sources and can automatically discover and classify your data.*
2. **Develop a classification and control policy:** *Construct a policy outlining different data types and prescribe appropriate controls for each file type.*
3. **Use a limited number of sensitivity labels:** *A restricted number of sensitivity labels simplify the data labeling process and ensures organizational consistency.*
4. **Establish a default policy of general business:** *A default general business policy guarantees accurate data classification across the board, even in the absence of specific individual or team policies.*
5. **Configure file-based classification:** *Microsoft Purview Information Protection offers customizable labels for file classification. The goal is to label 100% of your files according to your organization's specific needs.*
6. **Label your containers:** *Begin data labeling with container labeling. Apply labels to entire data stores to ensure the classification and labeling of all the data within.*
7. **Utilize auto-classification:** *Auto-classification capabilities facilitate automatic label application based on content, meta-data, or other attributes, thus saving time and effort.*
8. **Empower knowledge workers to adjust classification:** *Grant your knowledge workers the ability to alter classification as necessary to prevent labeling from hindering productivity.*
9. **Monitor and audit data labeling:** *Regularly review and update your data classification policy and supervise the application of labels to ensure consistency and accuracy.*
10. **Provide ongoing training and education on cata labeling:** *Regularly educate your employees about data labeling best practices, the importance of data labeling, and staying up-to-date with regulatory requirements and industry standards.*

Conclusion:

Microsoft Purview Information Protection provides an all-encompassing set of tools for data labeling and protection. By effectively utilizing these strategies, you can ensure proper data classification, labeling, and protection, thus balancing governance and business needs.

Summary

In our digitally-driven world, the role of a Chief Information Security Officer (CISO) is vital in protecting sensitive information while maintaining an environment conducive to productivity and growth.

Balancing data governance with business needs can be an intricate task. Still, understanding and implementing the five key areas discussed in this document can help you navigate these complexities effectively.

We have considered five main keys that form the pillars of balancing data governance and business needs:

Enhancing User Experience: Creating a seamless and positive experience for both internal and external users despite the implementation of robust data governance tools and controls.

Mastering Identity Management: Implementing efficient identity management systems to facilitate secure and fluid collaboration within and outside the organization.

Maintaining Branding and Domain Consistency: Ensuring that consistent branding is maintained during data sharing to increase trust and reduce friction in external collaborations.

The Power of Robust Policy-Driven Tools: Leveraging flexible and comprehensive policy tools to support secure data management and business operations.

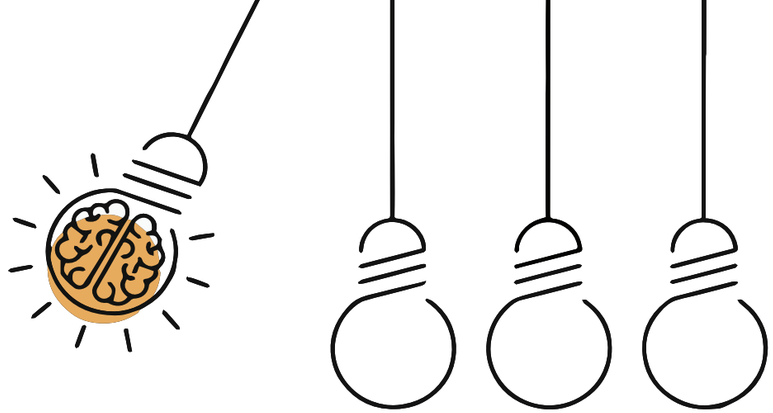
The Key Role of Data and Analytics: Harnessing the power of data analytics to assess, improve, and maintain effective data governance systems.

Each of these keys is an integral part of the holistic approach required to successfully balance data governance with the operational needs of the business. As you apply these keys, remember that effective data governance is a continuous journey, not a destination. It requires constant adjustment, flexibility, and a deep understanding of both the technology and people involved.

We hope this guide provides valuable insights and strategies to empower you as a CISO, steering your organization's data governance strategy effectively to align perfectly with your business needs. We believe that striking the right balance between data governance and business needs can lead to enhanced productivity, better user experience, and robust data security, key components for success in today's digital world.

View Demo

eShare advisory services:



Introduction:

We recognize the challenges data labeling and other governance issues pose in today's cloud-based, collaborative world.

With our extensive experience assisting some of the world's largest companies, eShare is well-prepared to guide you through the intricacies of data labeling and governance, and efficiently address these and many other challenges.

Our services aim to ensure the satisfaction and engagement of your employees, customers, and partners, thus giving you a significant competitive advantage.

You can't enable modern collaboration with yesterday's strategy and tools

The founders of DLP are bringing you eShare Advisory Services for Microsoft 365 to solve governance problems such as…

- How to "DLP" your links
- How to solve broken & blocked links
- Maximize your M365 E3/E5 investment
- Enable a data-centric & zero-trust strategy
- Label 100% of your data
- Remove governance friction
- Promote collaboration & productivity

Case studies:

HEALTHCARE

Business transformation via secure email & compliance reporting automation

The insurance industry handles an extraordinary amounts of sensitive information. Not only do they face fines for data breaches, but also disruption of the complex processes required to provide coverage. This insurer launched a new line of business with a focus on dedicated Care Coordinators and email-based communications to improve member satisfaction and healthcare outcomes. This required them to raise their expectations of secure email and find a solution provider to meet them.

U.S. GOVERNMENT AGENCY

VDR for sharing case files with DOJ

The Office of Inspector General (OIG) of a U.S. Government Agency had been using BlackBerry Workspaces (formerly WatchDox) for sharing case files with the Department of Justice and others. A new solution was needed to address mounting issues with ease of use and reliability and to leverage Microsoft 365.

MULTI-NATIONAL PHARMA

Securing their emerging market growth

The Office of Inspector General (OIG) of a U.S. Government Agency had been using BlackBerry Workspaces (formerly WatchDox) for sharing case files with the Department of Justice and others. A new solution was needed to address mounting issues with ease of use and reliability and to leverage Microsoft 365.

ENTERPRISE SOFTWARE PROVIDER

File sharing with customers using Teams & SharePoint

The company wanted to expand its use of Teams to include file sharing with its customers, but the native Guest access feature of Teams could not be limited to a specific Teams channel. And the company was unwilling to restructure its implementation of Teams to accommodate this limitation. A solution was found in eShare.

GLOBAL RETAILER

File transfer in/out of China with no disruptions

Many retailers operate in a global marketplace that is locally regulated. Their branded products must be developed and produced at lightning speed and their supply chains flexibly adapt to design and manufacturing changes as they occur. To achieve all this, data must flow smoothly to partners throughout the world, without compromising the information assets that ultimately provide time-to-market and exclusivity advantages.

"Kudos to eShare for providing the simplicity and auditability our existing solution could not. Your contribution allowed our PCI tokenization project to move forward without compromises."

— Lead Security Architect

"We have "N" users that need to share files with "X" external parties over "Y" channels; eShare is the hub to allow this to happen freely, securely and without collaboration choke points."

— Chuck Deaton, former Deputy CISO Humana

View More Case Studies Here

About eShare:

Helping companies share files & collaborate securely between customers, partners, and supply chain with Microsoft 365 and Google Workplace productivity suites.

eShare was founded in 2012 as nCrypted Cloud to provide highly-secure external file sharing solutions built upon already existing cloud file sharing services. Though the company initially focused on the consumer market, it quickly became clear that Microsoft, Box, Dropbox and Google were not fully meeting the needs of enterprises who wanted to use their cloud file storage and sharing services to share regulated and proprietary data with clients, partners, suppliers and other outside parties. Re-branded as e-Share in 2017, we are solely focused on meeting the external file sharing and content collaboration needs of medium to large sized enterprises.

Our super angel investors are former executives of Webex, Cisco, Microsoft, Broadcom and SpaceX. In addition to eShare, these investors were among the angel investors in Zoom Video, SentinalOne and Palantir. Our angel investors include Eric Yuan, the founder of Zoom, Dan Scheinman and Sameet Mehta. Prior to serving as eShare's President and Chief Product Officer until 2022, Ken Venner was a founding angel investor in eShare while the CIO of Broadcom. Ken later spent 6 years with SpaceX as their CIO and now serves as the CIO of Sierra Space. eShare's venture capital investors include Granite Hill Capital Partners, which specializes in global information technology companies.

Leverage Microsoft 365 for external file sharing and content collaboration

Many organizations already use Microsoft 365 for data sharing and storage. However, some find that the native controls available for secure external data sharing are insufficient. To compensate, they disable guest access to Teams and external file sharing from OneDrive and SharePoint Online, leading to the use of expensive and complicated point solutions for external file sharing. eShare offers the necessary rights management, authentication integration, and user-friendly branding to enable external file sharing and modern collaboration within Microsoft 365, without relying on guest access or external file sharing.

Significantly reduce data security risk by 93% without changing user behavior

Email remains the most popular file sharing tool, with 3.9 billion users. Attempting to block or encrypt attachments is often counterproductive, reducing productivity without effectively mitigating risk. eShare offers a seamless solution that automatically converts attachments into links, eliminating the need for users to change their behavior. Our usage statistics show that even with the right permissions, 90+% of recipients do not download attachments from your Microsoft 365 tenant, but prefer to use modern collaboration methods withing the eShare platform . By using eShare's link-based sharing, organizations can meet business needs without permanently sharing their files.

Extend Zero Trust policies to include external collaborations

Zero Trust security strategies that prioritize least privilege access are now standard for many organizations. However, extending these policies to external collaborators has been a challenge. eShare offers a solution by applying Zero Trust policies that grant external recipients the minimum rights necessary to meet business needs, based on Microsoft Purview sensitivity labels where available, when files are shared externally. This approach ensures that external access is always limited and in compliance with organizational security policies.

Industries we serve:

Health and Sciences

Humana

Cigna

Takeda

APOTEX

4G CLINICAL

Financial Services

London Stock Exchange Group

Morgan Stanley

VOYA FINANCIAL

CITADEL

Sculptor

Clear.Bank

Tech and Manufacturing

GE Aerospace

SIERRA SPACE

VARDA SPACE INDUSTRIES

SDI

magic leap

STEELMET

VIOHALCO

Gov't and Education

INSPECTOR GENERAL

USO

Imperial College London

Peace Corps

BROWN

Retail and Consumer

VICTORIA'S SECRET

Bath&BodyWorks

HercRentals®

KRAFT SPORTS + ENTERTAINMENT

Getting started with eShare is easy:

1 Connect:

Click here to schedule a brief discovery call to see how we can help you balance your data governance and business needs.

2 Comprehensive demo:

After your discovery call, we'll schedule a brief but comprehensive demo that is tailored to your specific business outcomes.

3 Get started:

Once all of your questions are answered, getting started with eShare is quick and easy. You'll have a dedicated success team assigned to your account to support your teams on-boarding and implementation process.

Get Started

eSHARE

Collaboration, reimagined.

Get Started

www.eshare.com