

EBOOK

WELCOME TO THE JUNGLE

Safeguarding your most
valuable asset—your data

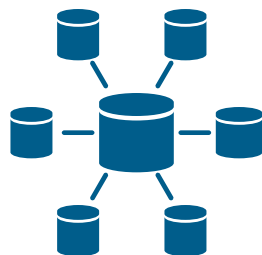


Sweet Child O' Mine:

The two sides of data

Value

Data drives your business, but it needs to be accessed, shared, and used to capture its full potential.

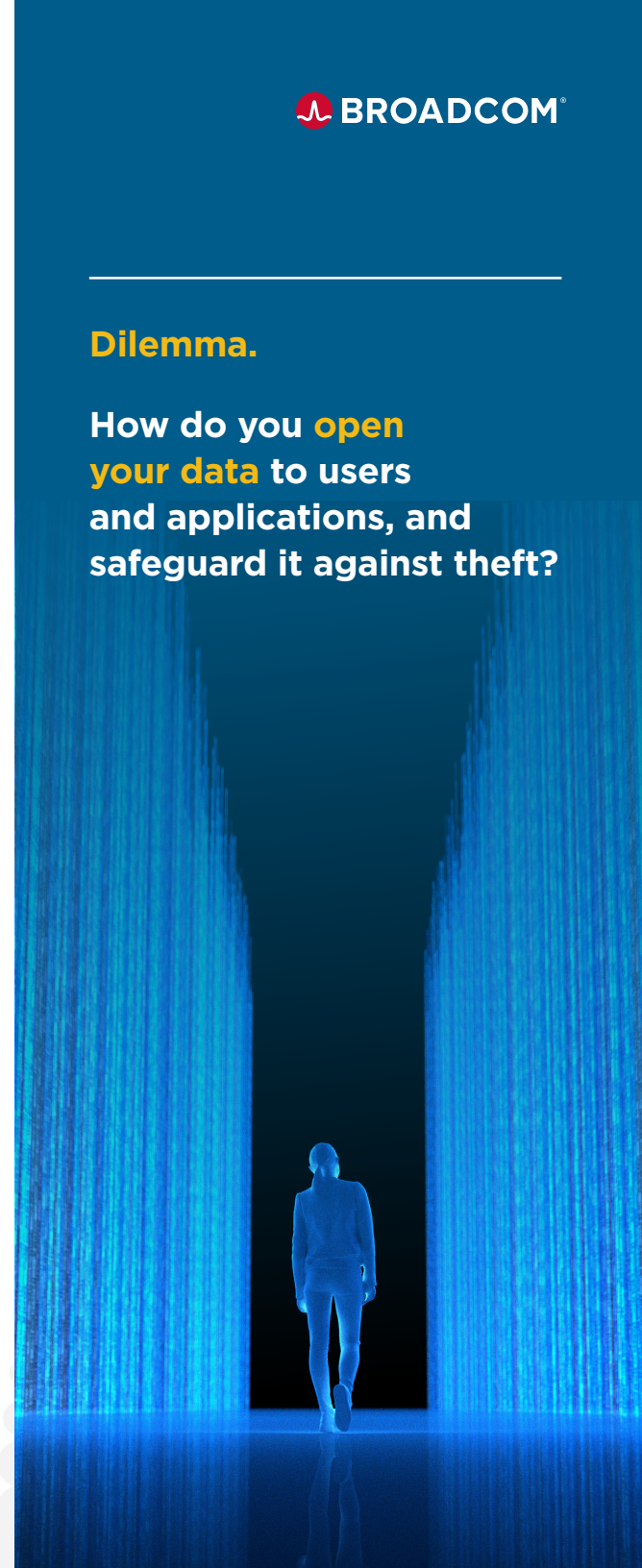



Target

If your data is valuable, hackers want it and will exploit any security gaps to get it.

Dilemma.

How do you **open your data** to users and applications, and **safeguard it against theft?**





In 2021, an estimated **79 zettabytes of data was generated worldwide**, and this is expected to double by 2025.

Paradise City:

Exponential data growth

We are in the early stages of the Fourth Industrial Revolution—the digital economy.

Data breaches remain a significant threat to enterprises, with the average total cost reaching nearly \$5 million globally in 2024, marking a 10% increase from the previous year. These breaches are predominantly financially motivated, accounting for 95% of incidents, and often involve complex social engineering scams¹. The rapid expansion of the digital economy has led to an unprecedented surge in data creation. The volume of data created worldwide as of 2023 is 120 zettabytes and is expected to reach 181 zettabytes by the end of 2025².

This vast and continually growing data landscape presents significant challenges for organizations striving to protect data throughout its lifecycle. The increasing volume and complexity of data and sophisticated cyber threats necessitate robust and adaptive security measures to safeguard sensitive information effectively.

1. Livewire (October 28, 2024)
2. Big Data Analytics News, 2024

November Rain:

The business challenges



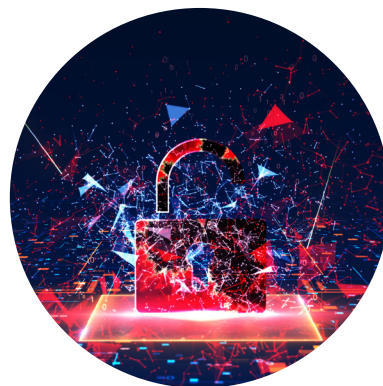
Human Error

How easily can one accidentally leak sensitive data?



Data Sprawl

Do you really know where your data is right now?



Targeted Attacks

Are you prepared against the assumed breach?

If creating data is easy,
**how hard can it be to
protect it?**

91% of organizations experience outbound email security incidents due to data loss and exfiltration.

— 2024 Email Security Risks Report

It's so Easy: To err is human

As the shift to a mobile and remote workforce has become the norm for many organizations, the freedom of being able to work from anywhere creates challenges.

The first challenge is shared file servers, which have become the central means of collaboration in today's workplace. Additionally, many companies now offer cloud-based file sharing, which enables users to access shared information anywhere. However, without proper protection, this shared data becomes an easy target for those looking to gain sensitive information maliciously and a potential route for sensitive data to accidentally leak.

The second challenge is email, which remains a vital business communication channel, facilitating seamless employee collaboration. However, the 2024 Email Security Risks Report reveals that 91% of organizations experience outbound email security incidents due to data loss and exfiltration, with 94% suffering negative consequences.

How do you securely share data without incurring additional risk?

One in a Million: Data, data everywhere

Duplication is an understatement.

Approximately 90 percent of all global data is estimated to be replicated, meaning that only 10 percent of new data is being created annually³. Think about that. How much of the data in your organization is copied and duplicated across your hybrid enterprise?

More importantly, do you even know where to find the data that needs to be protected? Data is a living thing, and it can spread throughout an organization faster than a virus. The first step to safeguarding your data is to find where it is being stored. But even after you see it, think about how much it costs to protect the same data in all of these locations! It only takes one security gap in one system to put this data at risk.

3. Big Data Statistics 2023: How Much Data is in The World? FirstSiteGuide.com

“Data often has no true owner, with data sets stored—sometimes in duplication—across sprawling, siloed, and often costly environments.”

— Kayvaun Rowshankish,
Senior Partner, McKinsey & Company
July 31, 2023

“A comprehensive data protection strategy will assist companies in complying with privacy laws and regulations, thereby **avoiding fines and qualifying for Safe Harbor.”**

— World Economic Forum, 2023

You Could Be Mine: Barbarians at the gates

Technology has long played a pivotal role in business strategy and growth, but IT modernization initiatives have expanded the attack surface, exposing security gaps and amplifying the risk.

Despite the robust security mechanisms and technologies deployed to protect data, the bad guys are still getting in. Reported data breaches continue to rise. According to the [World Economic Forum](#), traditional cybersecurity measures are increasingly being rendered obsolete by cybercriminals' growing sophistication. Furthermore, the 2023 IBM Cost of a Data Report found that 82 percent of breaches involved data stored in the cloud.

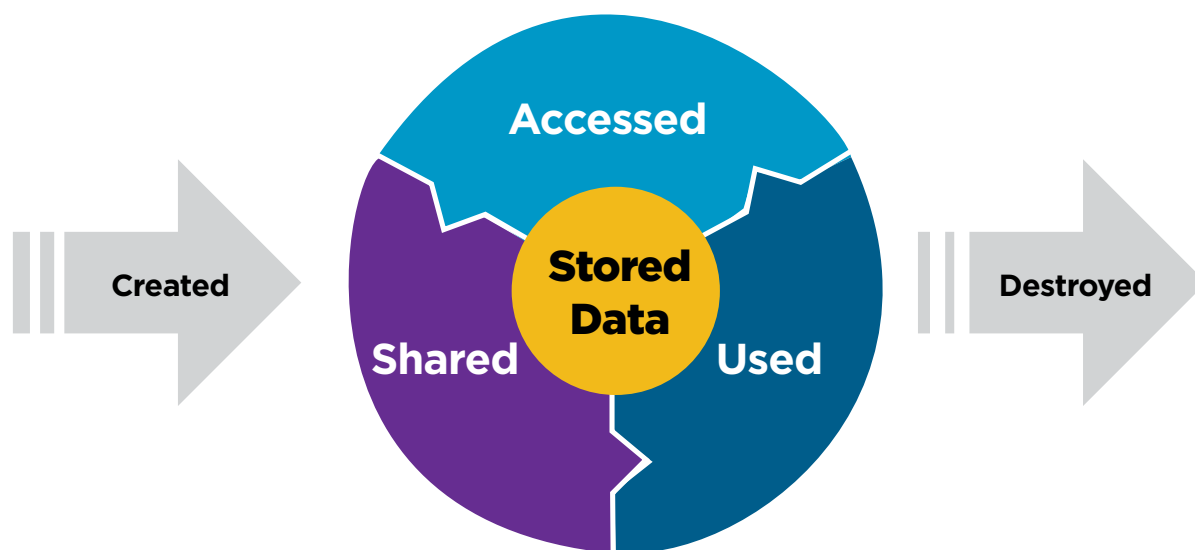
To counter this, organizations are adopting Zero Trust because to assume breach is one of its major tenets. For most organizations today, the primary driver behind deploying an encryption solution is to lessen the impact of a potential data breach and protect customer privacy. In fact, regulatory requirements make encryption a necessity for many. Companies that need to comply with regulations such as Continuous Diagnostics and Mitigation (CDM), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the EU General Data Protection Regulation (GDPR) must have an auditable encryption solution in place to protect the privacy of customer data.

Knocking on Heaven's Door:

All is not lost, there is hope

In the most basic model, data is created and stored until it is no longer needed and can be destroyed.

While the data is in your custody, it must be accessed, used, and shared to yield its full potential and value. It is at risk and needs to be protected from cradle to grave. When the data is no longer needed, it must be completely destroyed so there is no chance of recovery.



Here are **five key best practices** that can help you address your data lifecycle protection strategy:

1. Discover, classify, and consolidate sensitive data to minimize threat surface.
2. Encrypt data that is in your custody, and fully destroy it when it is no longer needed.
3. Implement a modern identity fabric to enforce Zero Trust access to data.
4. Patch and harden endpoints that store data to eliminate security gaps.
5. Assign ownership to each unique piece of data to improve accountability.

**ARE YOU DOING
ENOUGH TO PROTECT
YOUR DATA ACROSS THE
ENTIRE LIFECYCLE?**

**Broadcom® cybersecurity
solutions can help you
answer that question **with
a confident yes.****



Out to Get Me:

Why partner with Broadcom

Broadcom offers three differentiators over the competition when considering a vendor to help protect your data.

MOST SECURITY



Broadcom cybersecurity solutions safeguard data at every stage of its lifecycle.

MOST COVERAGE



Broadcom cybersecurity bridges the hybrid environments to safeguard data everywhere.

MOST TRUSTED



Broadcom cybersecurity has protected the world's largest customers for over 50 years.

For more information, please read our Safeguarding Data throughout its Lifecycle Solution Brief.



For more information, please visit our website at: www.broadcom.com

Copyright © 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

WTT-JUN-BR101 April 4, 2025