TREND REPORT

Data Security Market Trends

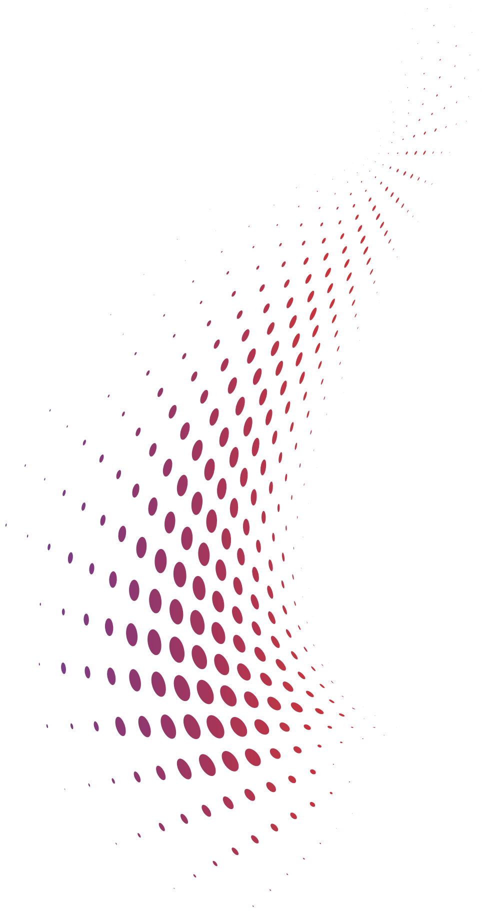
Evolution of Data Security

Sotero

The Current State Of The Market

The current state of the data security market is beyond messy and convoluted, yet this very disarray holds an immense opportunity for those taking on this market. Existing security offerings are fragmented, with situational and point solutions littering the security landscape. Indicative of this, security is incredibly complex due to the historic underfunding and confusion in the market, and what is the best approach to address this complexity. Security is both an enormous challenge to face and equally challenging to solve. The notion of systems being protected because they are in a protected environment is outdated and ineffective. Breaches and new intrusion mechanisms are evolving on a daily basis. Indicative of this are the countless daily articles on data breaches and data loss.

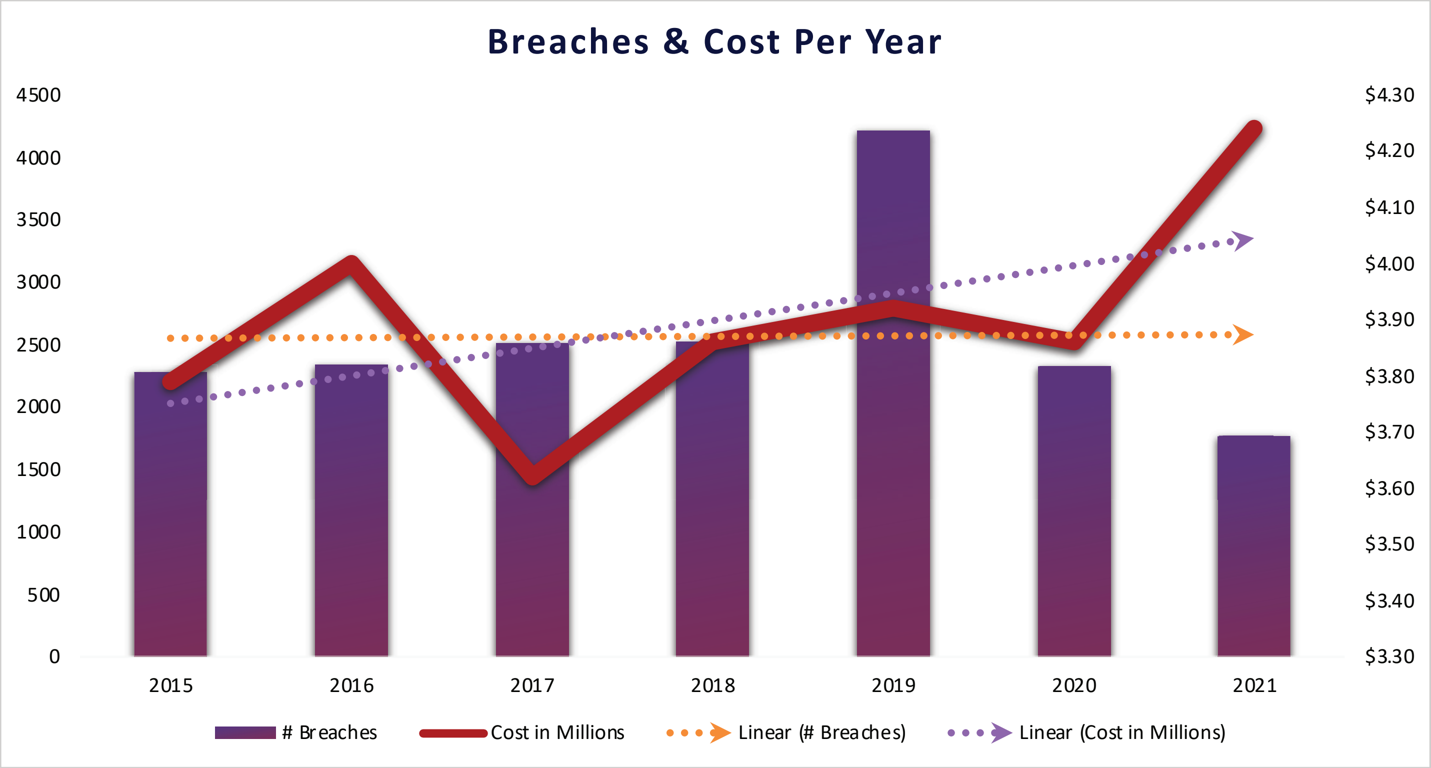
Data Breaches And Trends



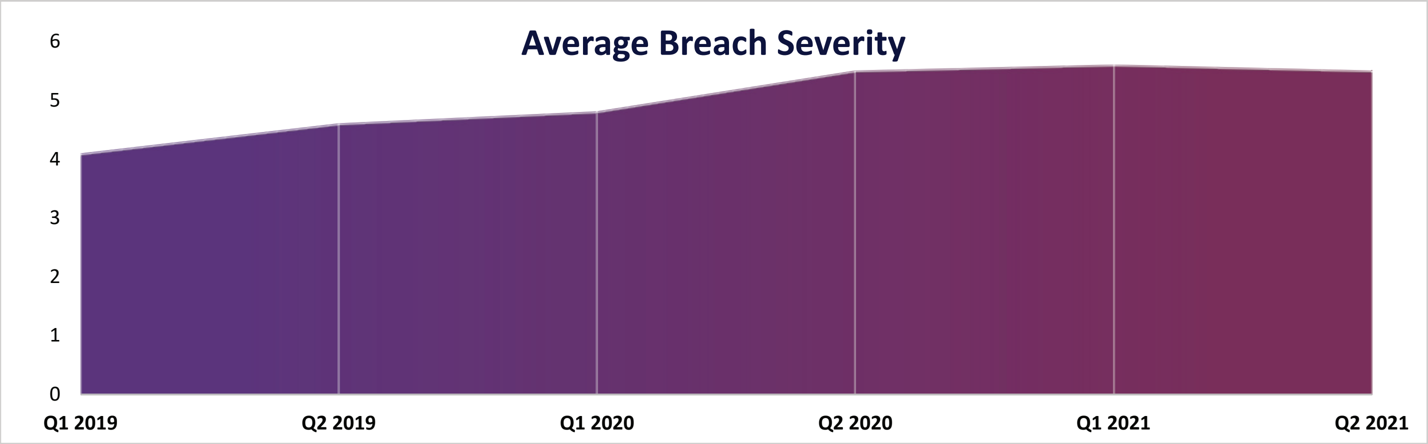
The number of breaches has decreased since the start of the COVID pandemic, but has, on average, remained steady since 2015. However, the average total cost of a data breach has increased significantly (11.9%) year over year from $3.79 Million in 2015 to $4.24 Million in 2020[1]. Even more critical is that the increase in severity of breaches occurring since Q1 2019 to date has been spectacular. The average breach severity in Q1, 2019 was 4.1 compared to Q2, 2021 average breach severity of 5.5.[2] These trends are a telling sign that threat actors have been and will continue to pursue organizations' most critical assets - their data at an accelerated pace. Once the pandemic subsides, part of the workforce will return to work, which will drive complexity to another level between a combination of remote and in-person workforce and a slew of new technologies that remain from the pandemic and remote workers.

Companies can no longer afford to accommodate existing vulnerabilities in their systems, nor can they afford to have a lack of oversight of their security products due to the complexity of their security ecosystem. For data-centric technology, it is paramount that security takes a data-first approach, this translates into an increased need for solutions that can protect data anywhere, any time, and at scale in an easy to manage fabric that connects existing security solutions in a seamless manner.

Data Security Market Trends



Sources:
2021 Mid-Year Report: Data Breach QuickView from RiskBased Security
IBM Security: Cost of a Data Breach Report 2021



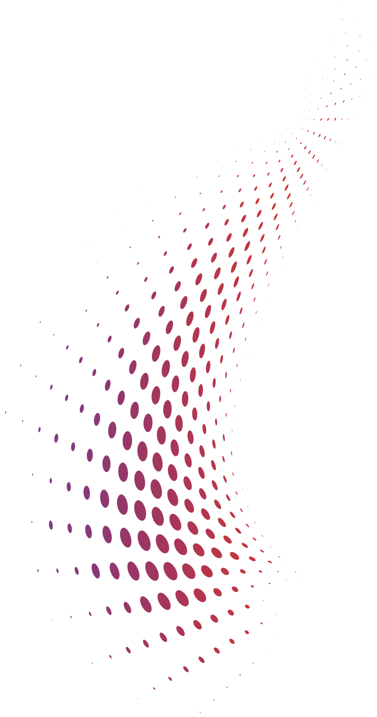
*__Source:__
2021 Mid-Year Report: Data Breach QuickView from RiskBased Security
**"Breach severity consists of a number of factors, such as type of data exposed, how the breach took place, and follow-on events such as regulatory actions and consumer lawsuits".

Point of Inflection and Market Opportunity

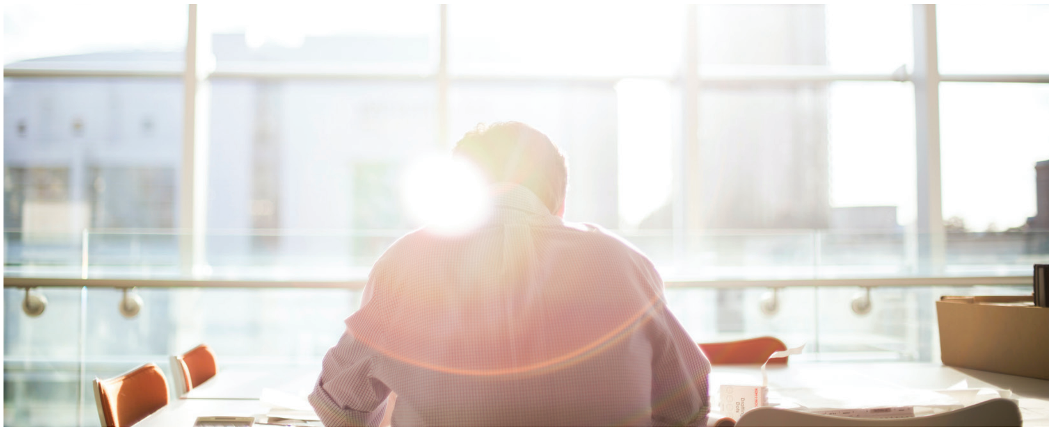
At the same time the market is undergoing an inflection point. This is driven by the emergence of the cloud, IoT, ever growing amounts of data that no longer reside in a centralized location, but is starting to move to the edge, and the emergence of new technologies. Technology adoption and solution integrations are evolving faster than security advancements. If this isn't concerning enough, criminals are adapting even faster - they are usually many steps ahead of both developers (products) and security personnel in identifying and exploiting new and existing vulnerabilities, ranging from organizations to critical infrastructure.

Security teams have broad adoption of products that are mostly remaining from legacy product offerings. If given the choice, security personnel will try to solve a security gap with an existing, well-known player in the market, one that has multiple security offerings in an attempt to reduce complexity and save budget. However, this approach may check compliance boxes, but it will not protect an organization from attack. These canned solutions are not protecting their most valuable assets (their data) at the data-level. New technologies and products have established themselves primarily in the identification and authentication, analytics, and threat detection (network and traffic level) in the market.

Why Data Security Is A Mess



Driven by compliance and regulations, the majority of solutions centered around data security are platform-specific implementations that have existed for a long time. These solutions are not practical, nor are they capable of scaling and supporting organization's time-to-value. Progress to develop cutting-edge data-centric security offerings have been mostly non-existent and not impactful. This is due to poor implementation capabilities, limitations, and deployment challenges caused by the last generation of encryption offerings that have stymied user adoption. Lack of usability has been another large inhibitor of encryption-based security offerings.



A Data-Centric Approach to Security

Security has largely been focused on the perimeter through user authentication and application-level privilege access management. However, to date very little progress has been made in the space to create a data-centric offering that focuses first on protecting the data to build out a data-centric security framework. Going back to the before-mentioned inflection point, multiple trends in the market that are quickly becoming the norm highlight why it is critical for organizations to adopt a data-centric security posture are:

Exponential increase in data (total amount of data created, captured, copied, and consumed globally is forecast to reach more than 180 zettabytes by 2025, compared to 64.2 zettabytes in 2020)[4]

Increased regulatory pressure (data protection laws in 113 jurisdictions around the world)[5]

Financial and legal penalties related to data loss (51% increase in cost on average for data breach from penalties)[1]

Complex application and technology systems that do not integrate seamlessly, if at all

Rapid adoption of new technologies to drive business outcomes

Multi-cloud environments (90% of large enterprises have adopted multi-cloud)[3]

Emergence and adoption of IoTs and streaming data (140% growth to hit 50 billion by 2022)[6]

Data at the edge (46 billion devices will rely on edge computing by 2023)[7]

The Future - A Data Security Fabric

When it comes to security, a highly vulnerable area that has not been adequately addressed by existing data security technology today is around data and connected systems. The existing ecosystem of solutions consists of many interconnected platforms. Data must be able to move freely, yet securely, between these systems, while integrating with multiple technologies that enable data security at all levels of an organization. The current state of data security, or rather lack thereof, requires an unparalleled data security fabric to address this challenge; thereby delivering connected security for a connected world - in a seamless manner.

Sources:

[1] **IBM Security: Cost of a Data Breach Report 2021**
https://www.ibm.com/downloads/cas/OJDVQGRY

[2] **2021 Mid-Year Report: Data Breach QuickView from RiskBased Security**
https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20Mid%20Year%20Data%20Breach%20QuickView%20Report.pdf

[3] **HashiCorp State of Cloud Strategy Survey**
https://www.hashicorp.com/state-of-the-cloud

[4] **Statista Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025**
https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=The%20total%20amount%20of%20data,to%20more%20than%20180%20zettabytes.

[5] **Morrison Foerster. Catch Up on Privacy Around the World on Data Privacy Day 2021.**
https://www.mofo.com/resources/insights/210127-data-privacy-day.html#:~:text=The%20number%20of%20data%20privacy,European%20Economic%20Area%20(EEA).

[6] **MIT Technology Review. A New Age of Data Means Embracing The Edge.**
https://www.technologyreview.com/2021/08/16/1031738/a-new-age-of-data-means-embracing-the-edge/

[7] **Juniper Research: IoT Connections to Grow 140% To Hit 50 Billion By 2022.**
https://www.juniperresearch.com/press/iot-connections-to-grow-140pc-to-50-billion-2022

ABOUT SOTERO

Sotero is the global innovator and leader in next generation data security. Sotero's data security platform enables our customers with a way to protect data anytime, anywhere, regardless of data store, integration mechanisms, and user tools. The platform is able to control, access, operate, and use data to extract information that drives organizations' business outcomes and innovation. Sotero provides organizations with a scalable and flexible data security fabric that migrates and moves data securely, in all its instances in an interconnected world. Organizations gain complete control over their data privacy, compliance, audibility and governance for use cases ranging from securing data at the edge, IoT devices and streaming data, and anomaly detection.

→ **Learn more at: www.soterosoft.com**

Sotero

99 S. Bedford Street, Suite 106
Burlington, MA 01803
www.soterosoft.com