DATA SECURITY

2021 MARKET TRENDS

Why Data-Centric Security Is Imperative

DATA BREACH COSTS ARE HIGHER

$4.24 Million - Average Total Cost in 2020

The 2020-2021 cost of a data breach has risen 11.9% year over year— the largest single-year cost gain in the last seven years. Part of this escalation is attributable to a 51% cost increase on average from penalties.[1]

DATA BREACHES ARE MORE SEVERE

34% Severity Increase Since 2019

The average breach severity in Q1 2019 was 4.1 compared to 5.5 in Q2 2021.[2] Factors including the exposed data type and cause of breach impact the severity score, as do post-incident events like regulatory actions or consumer lawsuits.

BIG DATA IS EVERYWHERE

Nearly 300% Data Growth Predicted

Driven by rapid cloud adoption, the expansion of SaaS applications, and pervasive IoT use, there's been a surge in data created, captured, copied, and consumed globally. This data is forecast to be over 180 ZB by 2025, up from 64.2 ZB in 2020.[3]

TECHNOLOGY INNOVATION OUTPACES SECURITY

252 Days is the Average to Identify and Contain a Breach [1]

Technology innovation and adoption accelerate while hackers' tools and techniques to identify and exploit vulnerabilities evolve at break-neck speed. Yet, organizations struggle with legacy security products and face a cybersecurity skills gap.

DATA SECURITY IS A MESS

A Data-Centric Approach is Essential to Security Posture

Data is cyber criminals' primary target and the focus of compliance requirements. Yet, Data needs to move freely and securely throughout your ecosystem. A data-centric approach to security enables protection and productivity at all levels.

SOURCES

1 IBM Security: Cost of a Data Breach Report 2021
2 2021 Mid-Year Report: Data Breach QuickView from RiskBased Security
3 Statista Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025

Sotero

WWW.SOTEROSOFT.COM