# Data – Your Friend and Foe

The importance of time-sensitive cyber resilience
when cyber security tools fail to stop the damage

Enterprise data continues to change rapidly in form, size, use, and residence. Rarely does it remain in siloed constructs anymore, limited to certain business units or untouched by the outside world. Data now freely crosses the prior conceived thresholds that limit business potential. It floats about in the cloud, spreads between business units, and flows everywhere.
But for all the change and opportunity that data represents, once it's created or collected, it is under threat of attack and misuse. With the number of reported data breaches doubling in the last ten years, and half a billion records exposed last year, our reliance on information is under increasing threat from a lack of security.

## Data Privacy Legislation

With the exposure of personal data at industrial scale, the growth of data privacy legislation was inevitable. Companies and government agencies collecting and handling personally identifiable information (PII) must now comply with Payment Card Industry Data Security Standard (**PCI DSS**) and Health Insurance Portability and Accountability Act (**HIPAA**) requirements in the United States, the General Data Protection Regulation (**GDPR**) in Europe, and many international and local follow-on laws like Protection of Personal Information Act (POPI Act) in South Africa, Kissel Verileri Korma Kurumu (KVKK) in Turkey, and the California Consumer Privacy Act (**CCPA**).

A lack of explicit data security governance, expose data to breaches that carry explicit costs. The 2022 IBM/Ponemon Institute *Cost of a Data Breach Study* found that:

- The average data breach cost increased 2.6% from USD$4.24 million (2021) to USD$4.35 million (2022), rising 12.6% USD$3.86 million in 2020.

- Ransomware breaches took 49 days longer (326 days) than average to identify and contain.
- 45% of breaches occurred in the cloud. Public cloud were the costliest at an average USD$5.02 million, whereas private cloud breaches cost an average USD$4.24 million and hybrid cloud 27.7% lower than public cloud at USD$3.80 million. However, analysis of the research also shows that organizations still need a mature cloud security posture, regardless of cloud model.

## Structured Data Protection

Organizations stuck in old operational models and mindsets related to data security fail to recognize the importance of company-wide security protocols. To improve, they must address their need for what Gartner calls Data Security Governance and thus protect information in structured and coordinated events, not as an afterthought or remediation after a breach.

Gartner suggests that a data security governance (DSG) framework should be used to identify and prioritize business risks that will be mitigated by data security policies. The creation and execution of data security policies is challenging because there are a large variety of data security products that provide specific security controls, and monitor data access and activity, against specific repositories or processing steps. Data security needs to be better deployed to mitigate the business risks identified through fit-for-purpose assessments, such as a data protection impact assessment (DPIA), data risk assessment (DRA) or a financial data risk assessment (FinDRA)[1].

Adopting a DSG framework requires organizations to ensure that DRA and privacy impact assessments (PIA) are planned and managed throughout the data life cycle to establish and continuously support and develop DSG policies.

[1] Gartner Data Security Hypecycle 2022, Brian Lowans

## Is DSG part of your Cyber Security toolset?

DSG adoption should always be implemented with the flexibility to integrate with existing cyber security and cyber resilience toolsets. Implementing efficient and effective data security controls requires more than just an array of siloed products. Security and risk management leaders should adopt a [data security platform (DSP)] strategic approach to capitalize on their data and share it securely using consolidated platforms.

Adopting a Data Security Platform strategic approach will enable organizations to achieve Gartner's prediction that by 2025, 30% of [Gartner] clients will protect their data using a "need to share" approach, rather than the traditional "need to know" approach[2]. The latter approach synonymous with a conventional Data Loss Prevention (DLP) approach.

## Data Security Platform

Data security platform's (DSP) deliver across a number of categories. There are broad-spectrum DSPs (bDSPs) — which provide strong consolidation for structured data in databases located in the cloud — and data security posture management (DSPM), which offers posture management and data discovery across silos. There are also the traditional data loss prevention (DLP) and data access governance (DAG) products, which are differentiated tools with a narrower primary focus — that have been the solid basis for processing unstructured data to date.

DSP's enable organizations to ensure their business can stay agile, use and share its data to drive business growth, and maintain data security. The priority must be to preserve agility while ensuring that the business can focus on what it does best. Organizations must break the mould of the past and avoid being disrupted by siloed

[2] Gartner Strategic Roadmap for Data Security Platforms, 2022, Joerg Fritsch, Brian Lowans

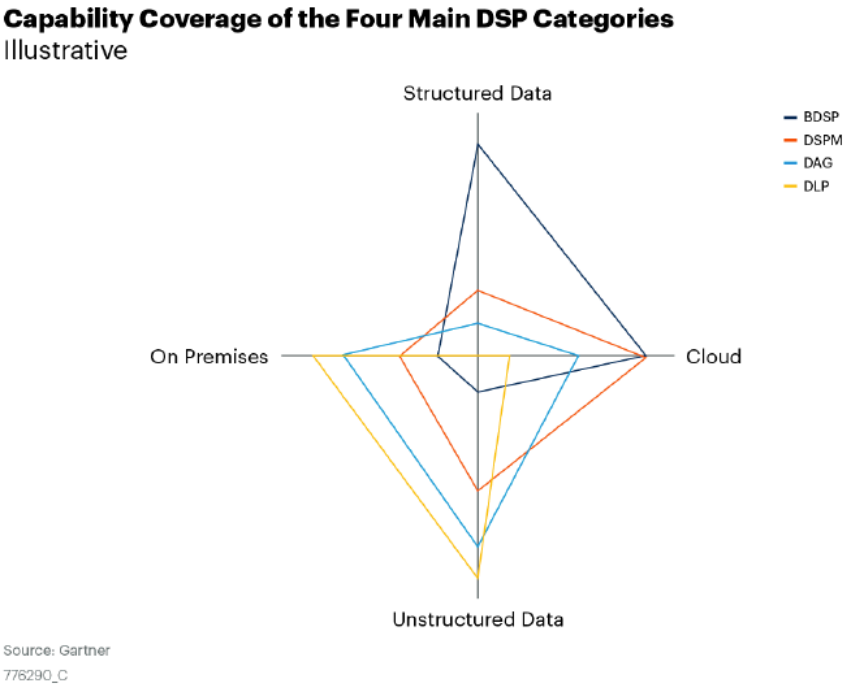
data security controls that were not designed to support these new requirements.

To attain a "need to share" approach with a DSP, can be achieved in combination with adopting real-life examples of Zero Trust[3]. The tenets of Zero Trust and DSP are aligned:

- Mature data discovery
- Encryption
- Data security governance
- Interoperability
- Automation
- Entitlement optimization

Where capability exists the four DSPs mentioned previously should provide the capability coverage illustrated in Fig 1 below:

Figure 1: Capability Coverage of the Four Main DSP Categories




[3] https://www.securityroundtable.org/interview-with-tony-scott-former-federal-cio-on-the-wake-up-call-for-zero-trust/

## CyBrilliance - Advancing Data Security Governance

While you're reading this, attackers are persistently working to breach your networks and internal stakeholders are challenging your data security policies to perform their normal day to day activities. Both groups of individuals are putting your data at risk, intentionally or inadvertently, creating an environment that could damage your reputation, impact customer confidence creating an inconsistency of regulatory compliance.

## Should you adopt Data Security Governance?

Have you ever purchased a flat pack wardrobe and found no instructions to help you build the product, so its end use matches the purpose it was bought for? Without the instructions you cannot guarantee it will function effectively. Cyber security and cyber resilience products are no different, they are ineffective without data security governance policies and processes. All enabling you to achieve the security efficacy promised.

## Don’t overlook the basics - start at the beginning

CyBrilliance believe that to strive for Data Security Governance (DSG) you should first research your options and start by adopting a Data Security Platform (DSP) that aligns to the opinions of Gartner and other recognised thought leaders and CISOs.

Information gathering of an organizations activities, technologies and policies aligned to achieve existing “need to know” enforcement will place security and risk management leaders in strong position for change. You will then be in the best position to introduce a DSP that will increase data protection and risk mitigation for a “need to share” approach.

## Cyber Resilience + Data Security Platform – alignment or overkill?

CyBrilliance is a leading advocate of cyber resilience. We along with security and risk leaders acknowledge that even with the advances of detection and response capabilities of cyber security tools, they will never stop all the attempts of cyber actors to do harm to organizations.

Cyber resilience describes the ability to continue delivering intended business and operational outcomes despite experiencing challenging cyber events, such as mitigating successful cyberattacks and responding to cyber incidents.

DSP's enable organizations to ensure their business can stay agile, use and share its data to drive business growth, and maintain data security. The priority must be to preserve agility while ensuring that the business can focus on what it does best.

CyBrilliance believes that when organizations have the ability to couple together cyber resilience and a data security platform they will:

- Be better informed of all their data, its risk to the business
- Informed of all data location and the lifecycle of it use
- Ensure protection in real-time of all data, wherever it is located
- Have the capability to instantly restore data during operational and exceptional incidents
- Be in a position to retain control during cyber incidents
- Reduce IT resourcing overheads for operational exceptions

## CyBrilliance supports digital businesses

Digital businesses make up the majority of the commercial marketplace. The business advantage in the digital world is data. As digital businesses evolve and grow, so does data. Data – the business differentiator – continues to be at the mercy of the latest cyber criminals armed with an increasing arsenal of cyber vectors. CyBrilliance commits to seek out and make available data security governance tools, such as DSPs alongside our commitment to cyber resilience, to enable organizations to adopt a more effective cyber security and cyber resilience strategies.

## CyBrilliance Selects Actifile Data Security Platform as a Leader in Data Security Platforms.

### Always know the potential cost of current risks to your business

The Actifile Data Security Platform (DSP) can locate and secure sensitive data, calculate potential financial penalties and liabilities, and instantly remediate those vulnerabilities with a one-click encryption process.

Actifile believes that comprehensive and affordable data security solutions, including data loss prevention and data encryption, should be a basic right for all business owners, and easier to manage.

Actifile's Data Security Platform aligns to Gartner's opinion that a Data Security Governance (DSG) framework should be used to identify and prioritize business risks that will be mitigated by data security policies.

"Traditionally, data security has been delivered by disparate products, which has resulted in operational inefficiencies and an inability to support, for example, data risk assessments"
Hype Cycle for Data Security, 2022, Gartner ID G00771466

Actifile is at the forefront as the emergence of Data Security Platforms (DSP) is expected to help bridge the gaps in discovery and control capabilities in a more orchestrated and scalable way.

Existing data loss and security platform event-driven approaches are outdated and resource heavy. They require extensive ongoing rules management and do not have the intelligence to follow the data wherever it resides and whenever it is accessed.

Actifile is different in that it combines many of the critical attributes of a DSG framework such as Data Classification, Data Monitoring, Data Risk Assessment (DRA), Privacy Impact Assessment (PIA) and Financial Data Risk Assessment (FinDRA). This approach, in a feature rich (easy to use) platform can help to mitigate the business risks associated with privacy requirements, ever-growing security threats and accidental data disclosures.

## Enterprise risk management and cyber resilience capabilities

The Actifile Data Security Platform provides detailed insights and protection to enable businesses to continually locate all data and its use – regardless of whether the systems and data are known or shadow IT.

## Major advantages of the Actifile Data Security Platform

- Automated data monitoring and risk assessment that is always up to date.
- Continuous financial impact analysis aligned to your privacy and governance regulations.
- Adaptive data centric encryption makes sensitive data completely unreadable in the event of a breach.

- Sensitive data is secured anywhere it travels, on any device.
- Secure data management and exchange throughout your supply chain and IT ecosystems.

**Actifile software is an autonomous data guard, your silent watchdog.** It constantly patrols your IT ecosystem protecting against both internal and external threats. Sensitive data detection and automated data mapping operates 24/7, allowing instant remediation of vulnerabilities with one-click encryption


**Having located and mapped sensitive data, Actifile can provide clear data and cyber risk quantifications.** Sensitive data is always worth something to someone. You may be targeted by hackers right now, or hostile third parties may be attempting to suborn your employees. Even basic system failures or thoughtless mistakes by honest employees can have catastrophic consequences for your business.

**Actifile's pre-emptive data encryption delivers a level of protection that simply cannot be matched by any event-driven data encryption solution.** The Actifile DSP 1-click encryption function gives a choice of full immediate encryption or delayed encryption. File-level encryption is fully automated.

**Monitoring data flow in real-time, Actifile can immediately identify sensitive data and assign a security classification to protect it.** A typical business may have sensitive data spread across multiple silos and end users, including remote devices and cloud shares, 3rd party partners and shadow IT. Sensitive or confidential

data may also be in the possession of subcontractors, freelancers, or even former employees.

**IT managers need to be firmly in control of all sensitive data at any time.** Actifile's automated pre-emptive data audit gives them the tools to conduct immediate audits over their entire IT ecosystem. An Actifile data security audit creates an indelible log that maps every data-related event. You can check back to any specific date, time or location and see a clear record of data ingress and egress, as well as the creation of sensitive data.

**Actifile overview for MSPs (Managed service providers)**

Read how some of our customers are using Actifile Data Security Platform to advance their Data Security Governance.

<Awaiting Logos from Guy>

Talo

Solid State

Noted

GOAN

MOWI

CyBrilliance Data Security Governance | Data: Your Friend and Foe | Industry Report

## *About CyBrilliance*

*CyBrilliance is an internationally minded global master distributor headquartered in Ontario, Canada.*

*With CyBrilliance you have a diverse group of experts in marketing, sales, cyber, operational technologies, advertising, and other disciplines, representing EMEA, India, Canada, and the US.*

*We are all devoted to telling the Cyber Resilience story and serving customers in ways that account for local needs and cultures, as well as addressing the needs and wants of specific audiences and stakeholders.*

*We are a channel partnership focused organization that extends across EMEA, Asia Pacific, North and Southern America.*

*CyBrilliance LLP*
*The organization is registered as a limited liability partnership registered in Canada, with registered number xxxxxxx.*
*CyBrilliance LLP, 5236 Cherryhill Crescent, Burlington, Ontario, L7L 4C4, Canada.*