July 2021

IBM Hyper Protect Data Controller

Protecting data wherever it goes and generating a projected 335% ROI

IBM **IT Economics Consulting & Research**

The cost of a security breach

An information security officer may sleep soundly knowing their organization's data is on an IBM Z® system, encrypted at rest and in flight, with pervasive encryption protecting it from data loss.

However, data must sometimes leave IBM Z, and that can be a concern. Once the data leaves the confines of a trusted system of record, data loss is no longer the only problem. Privacy breaches become a possibility and can result in substantial expense. According to the 2020 Cost of Data Breach Report by the Ponemon Institute, breaches of 1 million to 10 million records cost an average of $50 million and in breaches of more than 50 million records, the average cost was $392 million.[1]

IBM Hyper Protect Data Controller can guard against both data loss and privacy breaches, and can provide a projected 335% return on investment over five years. For JDBC-addressable data sources within an enterprise, IBM Hyper Protect Data Controller on IBM z15™ T01 and LinuxONE III LT1 is projected to deliver a five year return on investment (ROI) of approximately 335%, with a payback period of seven months, by reducing the cost of securing data and lowering the risk of a data or privacy breach.[2] This paper examines the capabilities of IBM Hyper Protect Data Controller and its potential to reduce costs.

Extending the value proposition of pervasive encryption beyond IBM Z

With the launch of IBM z14® in 2017, IBM announced that its hardware was capable of pervasive encryption while incurring a percentage increase in CPU utilization in the low single digits – on average, around 2.6%.[3] With faster encryption and on-chip compression in IBM z15, that number is even lower.[4] The ability to encrypt data, both at rest and in flight, for a very low cost was welcome news for customers concerned about data security. Labeled "pervasive encryption", the capability could eliminate many threats of data loss potentially caused by non-functional roles that come into contact with the data but are not involved in the primary function of workloads running on the system. For example, a storage administrator needs to be able to move a database from one storage device to another but does not need access to the data inside the database. If the database is encrypted and the administrator has no access to the encryption key, that administrator cannot access the data.

[1] 2020 Cost of Data Breach Report by the Ponemon Institute, https://www.ibm.com/downloads/cas/RZAX14GX

[2] Analysis based on a hypothetical ROI projection for IBM Data Privacy Passports, including the reduced risk of a data privacy breach, reduced risk of industry fines and regulatory penalties, policy enforcement efficiency and audit labor reduction, and the cost avoidance of an in-house equivalent implementation.

Data breach risk is taken from the IBM-sponsored Ponemon report, "2019 Cost of a Data Breach". Potential industry fine or regulatory penalty data is based on a blended combination of penalties across several recent GDPR, HIPAA, and PCI DSS publicly disclosed violations. Costs associated with labor savings in policy enforcement, audit, and in-house implementation and maintenance of a comparable solution are derived from IBM IT Economics data aggregated from client engagements.

A range of values for risk reduction, industry and regulatory fines, and efficiency were considered, producing an ROI between 310% and 360%. Actual ROI will vary by geography, industry, and individual client circumstance.

Data sources must be JDBC-addressable and targets must be able to contact the Data Privacy Passports host to open Trusted Data Objects.

[3] https://techchannel.com/Enterprise/07/2019/z-os-data-set-encryption

[4] https://www.ibm.com/downloads/cas/AM1PYZBB

In addition to data security, however, there is a question of data privacy. Data privacy considers functional roles and the minimum amount of data they require to perform their function, and what consent a data subject has provided to use their data. Within a system of record, interaction with data is constrained by applications. But, outside of that experience, data interaction is less structured. If a data scientist is looking at purchases all made by the same person, do they need to see the card number at all? In short, what does the functional role need to know to get the job done?

It is important to keep in mind that these questions are answered at a particular time and place, for a particular role, and that these rules can change. For example, today it is permissible to display a full credit card number to a customer service agent, but tomorrow a new regulation requires that only the last four digits should be shown.

Another consideration is that data can move. For example, credit card transactions are collected in an application running on IBM Z, but then sent elsewhere in an extract, transform, load (ETL) cycle for analysis by data scientists. The data must be encrypted wherever it goes and only what is required for a given role should be exposed given the most recent set of rules available.

In a typical data center, establishing and maintaining rules may require changing code in various applications, altering stored procedures, or even scrubbing over-exposed data and altering the ETL cycle.

Even if the movement of data is carefully tracked, the issue of data privacy represents a great deal of time and trouble, both of which boil down to expense. You could easily find yourself wishing that data could protect itself.

With IBM Hyper Protect Data Controller, data can protect itself… and with far less time, trouble, and expense.[5]

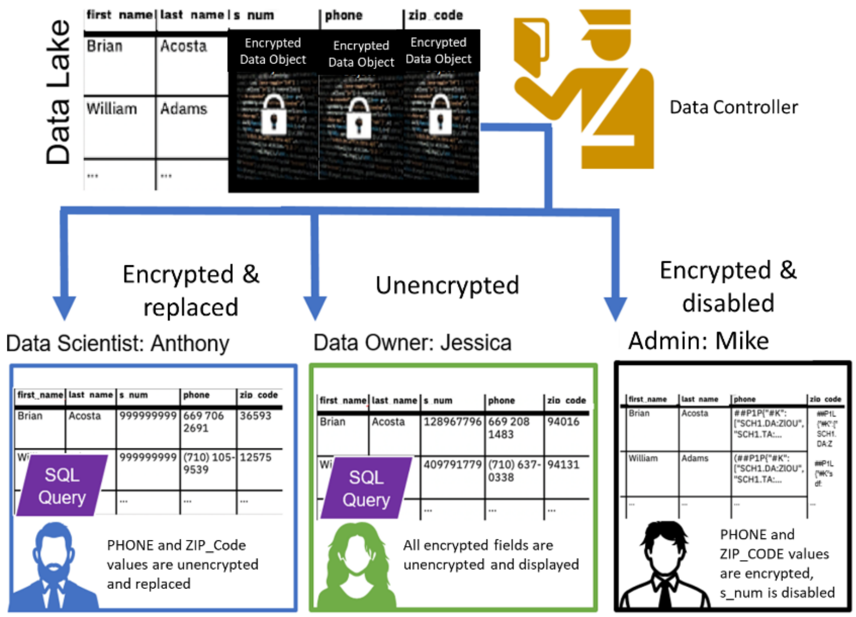
Data Lake
first name | last name | s num | phone | zip code
Brian | Acosta
William | Adams
...
Encrypted Data Object
Encrypted Data Object
Encrypted Data Object
Data Controller
Encrypted & replaced
Unencrypted
Encrypted & disabled
Data Scientist: Anthony
Data Owner: Jessica
Admin: Mike
first_name | last name | s num | phone | zip code
Brian | Acosta | 999999999 | 669 706 2691 | 36593
Wi | 999999999 | (710) 105-9539 | 12575
SQL Query
PHONE and ZIP_Code values are unencrypted and replaced
first name | last name | s num | phone | zip code
Brian | Acosta | 128967796 | 669 208 1483 | 94016
Wi | 409791779 | (710) 637-0338 | 94131
SQL Query
All encrypted fields are unencrypted and displayed
first_name | last name | phone | zip code
Brian | Acosta | ##P1P("#K": ["SCH1.DA:ZIOU", "SCH1.TA:...
William | Adams | (##P1P("#K": ["SCH1.DA:ZIOU", "SCH1.TA:...
PHONE and ZIP_CODE values are encrypted, s_num is disabled

Figure 1: Accessing data in a data lake with IBM Hyper Protect Data Controller

[5] https://www.ibm.com/us-en/marketplace/data-privacy-passports/details

More than just encryption

An information security officer will have several concerns as data moves from a system of record, like a supported IBM Z system,[6] out into the data center and beyond:

- Data remains encrypted. Encryption is at the heart of data protection. Data must remain encrypted in flight to its destination – a data lake perhaps – and it must be encrypted at rest there, as well.
- Privacy is maintained. Applications on a system of record are relied upon to maintain data privacy. Once taken from that system, privacy must remain intact. Proper controls to maintain privacy must be present.
- Protection and privacy are provable. Compliance must be assured, and audits must be straightforward.

IBM Hyper Protect Data Controller is designed to provide encryption in flight and at rest by creating Encrypted Data Objects. An Encrypted Data Object is an encrypted copy of the data along with security information about that data. When accessed, data in the Encrypted Data Object passes through a Data Controller. The Data Controller matches the identity of the requester to access policy and then may decrypt and transform the data. So, where a data owner may see a full credit card number, a data scientist may only see it transformed into a hash of the number. A central Policy Controller, that resides on a supported IBM Z system,[6] implements the policies that a Data Controller enforces. It also manages key material for the encryption and decryption of the data. As data is distributed and accessed, it may be in one of two states:

- Encrypted In this state, the original data is available if policy permits access in some form. It may be decrypted and transformed into an “replaced” state. In this state, it is an Encrypted Data Object.
- Replaced In this state, data access policy has been replaced and the original data is not available. For example, a credit card number may be replaced to only display the last four digits.

One advantage of the IBM Hyper Protect Data Controller approach is that policy may be altered after data has been circulated. Because data passes through a Data Controller at the time of consumption, the policy may be dynamic. For example, a credit card number that was presented as four digits today may be completely replaced tomorrow. Access to data can be revoked altogether by revoking access to the key that encrypts it. Data may be destroyed by simply destroying the key required to decrypt it.

[6] IBM Hyper Protect Data Controller is supported on IBM z15 systems

Projected ROI of 335% over 5 years

Not only can IBM Hyper Protect Data Controller simplify management of security policies. It can also offer a significant return on investment for enterprises seeking to mitigate data loss and privacy breaches. In an IBM IT Economics business value assessment model for IBM Hyper Protect Data Controller on an IBM LinuxONE III LT1 server, a return on investment of between 310% and 360% was calculated over five years. Analysis projected a payback period of less than one year or approximately seven months after examining the four business values.

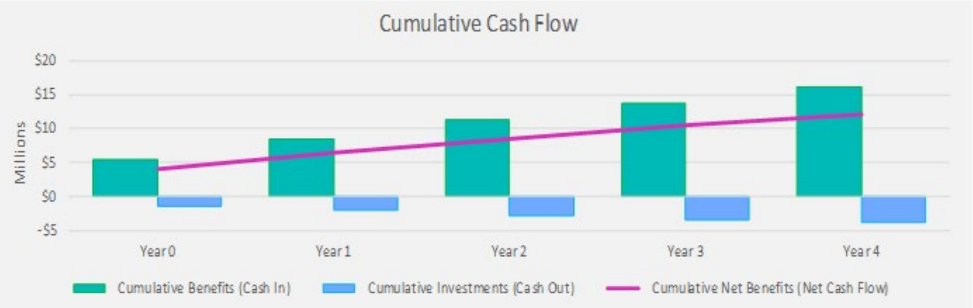

Figure 2: Projected cumulative cash flow in a business value assessment model for IBM Hyper Protect Data Controller

- Reduced risk of data loss or privacy breach
- Decreased risk of industry fines and regulatory penalties
- Increased efficiency of compliance policy enforcement and audits
- Avoided implementation and maintenance costs for an in-house solution

Reduced risk of data loss or a privacy breach

To calculate this benefit, the model forecasted the average cost and likelihood of a data breach as reported by the Ponemon Institute report. The financial risk of data loss or a privacy breach is calculated as the probability of a data privacy breach multiplied by the financial impact of a data privacy breach. So, for example, a 10% probability of a $1 million problem is a $100,000 risk. Since data breaches vary in size, the model uses an annual likelihood of an average size breach of 9.6% by Ponemon.[1]

The model considered that data in a data lake needs to be encrypted to prevent data loss, but there could also be an opportunity for a privacy breach if information is improperly exposed to those with legitimate access to the data lake.

With IBM Hyper Protect Data Controller in the model, the average likelihood of data loss or a privacy breach was estimated to decrease from 9.6% to 2%, or by a factor of 79%, which would yield a reduction in risk exposure of $297,920 annually, assuming no annual increases or fluctuations in probability or financial impact. The model assumes that the average total cost of a data breach could be directly applied to data privacy breach, although we acknowledge the two are not the same.

Decreased risk of industry fines and regulatory penalties

To estimate potential industry fines or regulatory penalties, the model assumes $3 million in fees based on a blended combination of penalties across several General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) publicly disclosed violations.[7]

The model calculated the average penalty per record based on an average size breach resulting in a risk exposure for 27,901 records. The model also assumed a 95% likelihood that an industry body or regulator would pursue a violation under normal circumstances. With IBM Hyper Protect Data Controller in the model the average likelihood of an industry fine or regulatory penalty could be lowered to 10%, or by a factor of 89%, based on eliminating the potential exposure of any Personally Identifiable Information (PII).

Increased efficiency of compliance policy enforcement and audits

By providing a single point of authority, IBM Hyper Protect Data Controller can lower the cost of managing data privacy policy compliance. It removes many points of potential failure, such as separate ETL transformations, access control lists, and various native encryption options, and replaces them with one point of control and one point to audit.

To calculating this benefit, the model estimated five full time equivalents (FTEs) that would normally spend 25% of their time annually on data privacy policy compliance enforcement. With IBM Hyper Protect Data Controller in the model, time spent on compliance policy enforcement could be decreased to 10% annually, or by a factor of 60% per FTE.

Its single point of authority also enables IBM Hyper Protect Data Controller to considerably lower the cost of data privacy compliance audits. To quantify this benefit, the model included ten databases that would need to be audited monthly, and that each database audit would normally take eight hours to complete. With IBM Hyper Protect Data Controller in the model time spent auditing each database could be decreased to two hours, or by a factor of 75%.

Avoided implementation and maintenance costs for an in-house solution

To quantify this benefit, the model examined the cost of developing and maintaining an in-house solution. Based on observations of customer developed solutions, the model estimated an effort of 12 developer FTEs[8] over nine months to build an in-house alternative. In addition to developing an in-house solution, the model assumed an annual average of three FTEs to maintain the in-house solution.

[7] Blended penalty data is based on information from client assessments performed by the IBM IT Economics team. For further information, contact IT.Economics@us.ibm.com.

[8] Full time equivalent cost assumes an average fully burdened hourly rate of $120 for a development effort of approximately 17,280 person hours over nine months.

Lower risks and costs with IBM Hyper Protect Data Controller

IBM Hyper Protect Data Controller can protect data wherever it goes, reducing the risk of both data loss and privacy breaches. With IBM Hyper Protect Data Controller, security policy is maintained in a central Policy Controller, and it is honored whenever Encrypted Data Objects are accessed, wherever they may have gone. Data access may be revoked after the fact, long after data has left the system of record. Data may even be destroyed simply by destroying its encryption key.

In addition to reducing risk, IBM Hyper Protect Data Controller reduces time spent by security staff, auditors, and developers protecting data. All of this combined can bring a significant return on investment. If your organization is looking for data protection efficiencies and lower security costs, contact the IBM IT Economics team for a no-charge security assessment.

About the authors

Mark Moore is a Senior Competitive Analyst and IBM Z Evangelist within the IBM IT Economics and Research team where he focuses on data security. Before joining the IT Economics and Research team he spent more than a decade as an IT Strategy consultant.

James Roca is an Executive IT Economics Consultant within the IBM IT Economics and Research team. James partners with IBM client CIOs / CTOs and their executive leadership teams to identify, evaluate, and define major enterprise-wide digital transformation programs that deliver tangible and long-lasting business value.

(C) Copyright IBM Corporation 2021
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
07/21

All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided “as is” without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

No other publication, distribution or use is permitted without the prior written consent of IBM. Customers who want a "deep drill down" on CPO Competitive Case Studies should be directed to the IBM Competitive Project Office under NDA. An NDA is required to explain CPO’s methodologies, processes and competitive comparison. You can contact IBM Competitive Project Office by sending an email to IT.Economics@us.ibm.com

References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors and are not intended to be a commitment to future product or feature availability in any way.

32027332-USEN-01