Help protect healthcare data and address industry regulations, on-premises and in the cloud



236
Mean time number of days to contain a healthcare breach¹

Safeguard sensitive patient data

With an influx in data breaches, protecting sensitive medical and patient information is imperative for healthcare leaders in organizations of all sizes.

Keeping up with the onslaught of new and existing data privacy mandates can overwhelm even the largest of data security teams. The people, processes and tools responsible for protecting sensitive patient information must address a staggering amount of regulations including:

- Health Insurance Portability and Accountability Act (HIPAA)
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)

Prepare for internal and external threats

Potential compromise can occur among the following healthcare roles, including but not limited to:

- Healthcare providers
- Insurance agencies
- Pharmacies
- Customer service

These incidents can result in major costs and lost time for affected organizations and financial risks and loss of privacy for patients.

\$6.45 M

Average total cost of a data

Average total cost of a data breach reported by healthcare organizations surveyed²

236 dayS

Mean time to identify a data

breach reported by healthcare organizations surveyed³



Help increase visibility, control and response

Healthcare organizations increasingly use a hybrid mix of on-premises, public cloud and private cloud environments to store and share healthcare data. A hybrid multicloud model can be used to help improve the efficiency of electronic medical record systems for sharing and retrieving medical and patient data. However, it can also lead to the following challenges:

- Centralizing the discovery and classification of sensitive data
- Standardizing data access and entitlement controls across environments
- data security risk posture

– Gaining comprehensive visibility into

Help accelerate healthcare data security and address compliance with IBM Security Guardium

Get protection that can follow your data IBM Security Guardium Data Protection solutions are designed to help healthcare

organizations discover, monitor and protect their sensitive data across on-premises and cloud environments. The solutions include built-in step-by-step navigation and embedded instructional videos and tutorials. These features can allow for fast deployment and use.

Three-year potential return on investment

from implementing IBM Security Guardium Data Protection for a composite organization designed by Forrester based on the three interviewed organizations⁴

Time by which the majority of users surveyed realized benefits from implementing IBM

realized benefits from implementing IBM Security Guardium Data Protection⁵

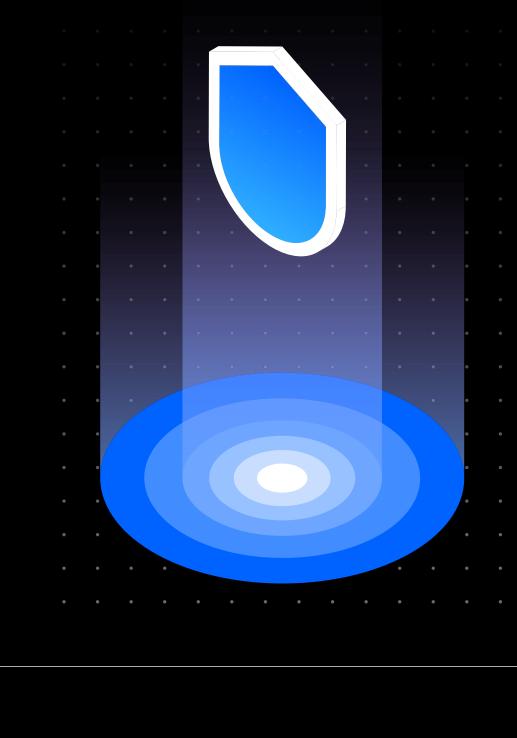
IBM Security Guardium Data Protection can

Help achieve data insight and assessment

help security and compliance teams achieve the following objectives:– Discover and classify sensitive data

- across disparate environments
 Establish data access and entitleme
- Establish data access and entitlement controlsMonitor and assess data activity to identify
- potential internal and external threatsAddress data security risk and government
- and industry mandatesHelp protect critical healthcare data
- from internal and external security risks and address compliance

sponsored by IBM. ibm.com/account/reg/us-en/signup?formid=urx-40683



Learn more ightarrow

IBM

- © Copyright IBM Corporation 2019. IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml
- Ponemon Report: Client Insights on Data Protection with Guardium, independently conducted by Ponemon Institute, June 2019, sponsored by IBM. ibm.com/account/reg/us-en/signup?formid=urx-40683
 2019 Cost of a Data Breach Report, study conducted by the Ponemon Institute; results sponsored, analyzed and reported by IBM Secur
- 2. 2019 Cost of a Data Breach Report, study conducted by the Ponemon Institute; results sponsored, analyzed and reported by IBM Security. ibm.com/security/data-breach
 2019 Cost of a Data Breach Report, study conducted by the Ponemon Institute; results sponsored, analyzed and reported by IBM Security. ibm.com/security/data-breach
- The Total Economic Impact™ of IBM Security Guardium Study, Forrester Consulting, April 2018, sponsored by IBM. ibm.com/account/reg/us-en/signup?formid=mrs-form-2454
 Ponemon Report: Client Insights on Data Protection with Guardium, independently conducted by Ponemon Institute, June 2019,