

Deloitte.



Fusion Managed Services

Managed Data Protection

Safeguarding strategic data in the digital age

The new reality

Ongoing digitalization of processes, transactions, relationships, and even currencies has generated unprecedented risks and opportunities. Cloud migration, new alliances and partnerships, and sophisticated cyber crime have expanded the number and nature of threats. At the same time, mobile devices, data commercialization, cloud applications, IoT, and cognitive technologies have led to new business models, lower costs, enhanced productivity, and new ways of working.

As data has become more valuable, voluminous, and vulnerable, data protection requirements have outpaced many organizations' skills, knowledge base, and technologies. As a result, data protection demands generally exceed the available resources.



Data is now a strategic asset

Executive teams and boards now recognize data as a strategic asset. They value it when they buy or sell a business, seek partners, or engage in innovation. They want it organized, leveraged, and protected.

Data has business value, and it has cost value. Here are some primary reasons why:

- Business value of data translates to increased revenue and profitability. The business value of data stems from opportunities to grow the business, develop products and services, enter markets, create efficiencies, attract partners, and win customers.
- Cost value of data translates to lost or forgone money, intellectual property, partners, customers, privacy, and reputation. The cost value of data stems from the risk of loss, theft, misappropriation, corruption, or exposure of data.

Exponential data growth

44 billion GB

of data was created
every day in 2016¹

463 billion GB

of data will be generated
daily by 2026¹

50x

Machine-generated
data is growing
faster
than traditional
business data²

The size of the
digital universe will

double
every two years²

¹ Jeff Schultz, "Growth of Data," Micro Focus, posted on SlideShare, November 6, 2017

² Peter Ffoulkes, "The Exponential Growth of Data," inside BIGDATA, February 16, 2017.

Moving to **value-based** data risk management

Since organizations cannot completely protect all data, they should develop a program to help the enterprise leverage data for improving business value and protecting its cost value. This is value-based risk management.

After identifying data elements and their value to the business, data protection initiatives can then be prioritized and planned. Failing to create an effective data protection program—or creating one that doesn't account for the value of various data—potentially invites problems. These problems include too many alerts, a false sense of data security, and wasted time, money, and effort.

A value-based approach:

- **Assesses the business value and cost value of the enterprise's data**
 - **Develops a governance structure considering the value of the data, how it can be used, who can use it, and where it can reside**
 - **Creates goals and a roadmap to building the data protection program**
-

Data protection is no longer a do-it-yourself proposition

Single or disparate tools alone cannot protect data, and organizations often struggle to manage them.

Some common challenges include the following:

Organizations have a massive list of data elements they want to protect, and lack of ability to prioritize. In addition, they are rarely positioned to tie the value of data elements to the business.

Extending data protection programs to the cloud requires careful assessment of staff skills, processes, and tools. Cloud adoption can take years, leading data protection programs to consider a hybrid environment of on-premises and cloud applications.

Data loss prevention (DLP) and cloud access security broker (CASB) tools are not set-it-and-forget-it applications. Out-of-the-box rulesets rarely provide real value without customization and tuning by experienced engineers.

Finding and retaining staff with skills to manage technology, and to work with the lines of business to translate requirements into controls, can be difficult.

In addition, cloud migration, data commercialization, post-merger or acquisition integration, or new or evolving regulations can place nearly impossible demands on IT.

Where managed data protection fits

DLP and CASB are complex, high-maintenance technologies and few organizations find it feasible to design and maintain a data protection program, which entails:

Addressing the value of data, regulatory requirements, data access and use policies, operational processes, and end-user training

Integrating tools and processes for ticketing, reporting, monitoring, and asset management, and hiring and managing full-time staff

Assessing outcomes and driving improvement, including remediation, risk reduction, and analysis of trends.

Organizations also benefit from broad industry and regulatory experience and knowledge of leading practices for protecting data in Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments.

Why Deloitte Managed Data Protection?

As data has become more valuable, voluminous, and vulnerable, challenges with safeguarding strategic data have outpaced many organizations' capabilities. Data Protection can help your organization detect and take action against accidental or intentional data exfiltration and misuse, including oversharing and transfer of valued data to personal cloud accounts. Take a new, more structured approach to addressing data risk challenges including endpoints, premises, and cloud environments. Benefits of data protection include:

Achieving business-focused results by aligning program priorities with the value of data, applying leading practices, and translating requirements into action

Faster time to value with rulesets specific to your industry and regulatory requirements

Ability to respond with alert handling, enabling incident remediation, policy tuning, and ruleset modifications

Monitoring and managing the health of applications through tracking, testing, and deploying software updates

Protection of data throughout its lifecycle

Why Deloitte Managed Data Protection? (cont'd)

Deloitte Managed Data Protection provides people, processes, and systems for:

Conducting data discovery and prioritization, so you know what data you have, where it is, who uses it, and for what purposes

Monitoring data access and exfiltration, and restricting download of valued data to unauthorized devices, so you have better control over your data

This in-depth, programmatic approach to data protection provides better scalability than tools-focused approaches and relieves much of the burden placed on organization's IT departments.

Valuing data both on a business-value and compliance basis and on a cost-value and risk basis, so you can assess and prioritize your data protection requirements

Enabling users to remain productive through greater visibility and control over your content and uses of data (including who's accessing your data, what they are doing with it, and whether or not that access is permitted)

Developing a tailored, ongoing data governance model for your organization

Providing visibility into a potential data breach to accelerate remediation



Why Deloitte Managed Data Protection? (cont'd)

Deloitte Managed Data Protection capabilities and outcomes include:

Program management

Achieve business-focused results by aligning program priorities with the value of data, applying leading practices, and translating requirements into action.

Application health and updates

Monitor and manage application health. Track, test, and deploy software updates adhering to stringent change management processes. Conduct periodic system health checks.

Ruleset management

Create and tailor data protection rulesets considering your specific industry and regulatory environment. Accelerate the time it takes for your data protection program to produce value with Deloitte's leading practices and experienced engineers.

Reporting and analysis

Provide trend analysis and risk-reduction recommendations.

Alert handling

Provide timely response and notification to the client when our analysts detect security events that could mean your valued data is being exfiltrated, lost, or exposed.

What sets Deloitte's Managed Services apart is **our know-how**

What sets Deloitte's Managed Services apart is our know-how, and deep experience in helping our clients to address complex cyber issues and challenges. Our Managed Data Protection solution follows a structured approach that leverages our:

1,400

Certified Information Systems Security Professionals (CISSPs)

across the Deloitte & Touche Tohmatsu Limited (DTTL) network of member firms

150+

Certified Information Privacy Professionals (CIPPs)

across the DTTL network of member firms

22,600+ **cyber risk engagements in 2018**
across all major industries

4,000+

cyber risk practitioners

serving US clients

2,000+ **data risk practitioners**

with more than **200 practitioners**
focused on data privacy and protection

21,000+

risk management and security professionals

across the DTTL network of member firms



Advise

- Governance development
- Strategic development
- Assessment of readiness of people, processes, tools
- Development of controls architecture



Implement

- Implementation of controls architecture
- Evaluation of technology
- Design, implementation of program
- Production rollout



Operate

- 24x7 monitoring, management of controls
- Policy governance with data value-based focus
- Triage and escalations
- Risk-based reporting
- Continuous improvement

Make the move to Managed Data Protection

Organizations should prioritize data risk management and place it on an equal footing with traditional information and network security. Given the value of data today, data protection is often the driver that propels an enterprise toward new levels of excellence in managing data risk. That's why it's crucial to adopt a comprehensive approach to data protection that is consistently monitored and managed.

Moreover, when the value of the enterprise's data is clarified, executive teams generally see data protection in a new light.

Please get in touch if you are:

- Lacking a data protection program that can monitor, detect, and respond to risks to your enterprise's data
- Trying to address myriad alerts, gaps, or problems in your existing data protection tools
- Considering the purchase of DLP or CASB tools or want to derive more value from existing DLP or CASB tools
- Working to increase management's awareness of the value of data and the challenges of protecting it
- Advising management on issues in data commercialization, merger or acquisition planning or integration, use of IoT, or adoption of cognitive technologies

The challenge

The organization wanted to move specific applications from on premise to the cloud but needed visibility into and control over valued data. The client also wanted to restrict employees from accessing or oversharing sensitive data and prevent data from moving outside from corporate applications to personal ones.

The approach

Given our mature Managed Data Protection program, the organization engaged Deloitte to assist them with the following:

- Prioritizing data on its value to the business and to compliance activities, and developing governance for uses of data
- Designing and implementing DLP and CASB controls to track data location and movement
- Blocking protected health information (PHI) from being emailed or uploaded to personal email and storage accounts
- Documenting and educating users on corporate policies for acceptable use
- Monitoring, managing, and continuously improving the program to adapt to new risks and business changes

The benefits

The organization now benefits from:

- Value-based data risk management keyed to business and compliance needs
- Actionable alerts with remediation guidance to facilitate incident response
- Reduced exposure to data breaches and noncompliance
- Offloading of DLP and CASB operations so staff can focus on innovative business initiatives
- Ongoing improvement of data protection program maturity

Let's talk.

Parichart Jiravachara

Partner | Risk Advisory

Email: pjiravachara@deloitte.com

Tel: +66 2034 0130

Prateep Puengwattanapong

Director | Risk Advisory

Email: ppuengwattanapong@deloitte.com

Tel: +66 2034 0000 Ext. 11835

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC. All rights reserved.