aws

AWS DATA SECURITY

Strong security enables data-driven decision making

How fresh, relevant secure data can inform your decision making process

Table of contents

INTRODUCTION

Integrating security, compliance, and governance into decision making

Securing the data that informs better, faster decision making

Data security requires the right balance of access and transparency so that organizations are enabled to make faster and better decisions. In many cases, this begins with transformational changes to a company's business processes.

Data is a powerful business asset. Yet, a decade into the cloud era, many organizations continue to struggle to pull meaningful value from their data. Many organizations want data at the center of every business decision, but may experience challenges keeping up with the complexity of managing many stakeholders and options, combined with an evolving security landscape.

Security and governance are foundational to making fast, data-driven decisions. Organizations must control where their data is stored, how that data is used, and who has access to it. This is all underpinned by the decision to build on a flexible and secure cloud computing environment.

This eBook explores the four ways integrating security, compliance, and governance earlier in the modernization journey leads to operational improvements that inform better decision making.

USE CASES

Four ways security supports creating a data-driven organization

Let’s take a deeper look at how a modern approach to security and governance can support the goals of your organization:

1. **Enable faster insights with secure data ›**
2. **Reduce security-incident-related downtime ›**
3. **Reduce overhead with more encompassing data security ›**
4. **Maintain focus throughout your decision making process ›**

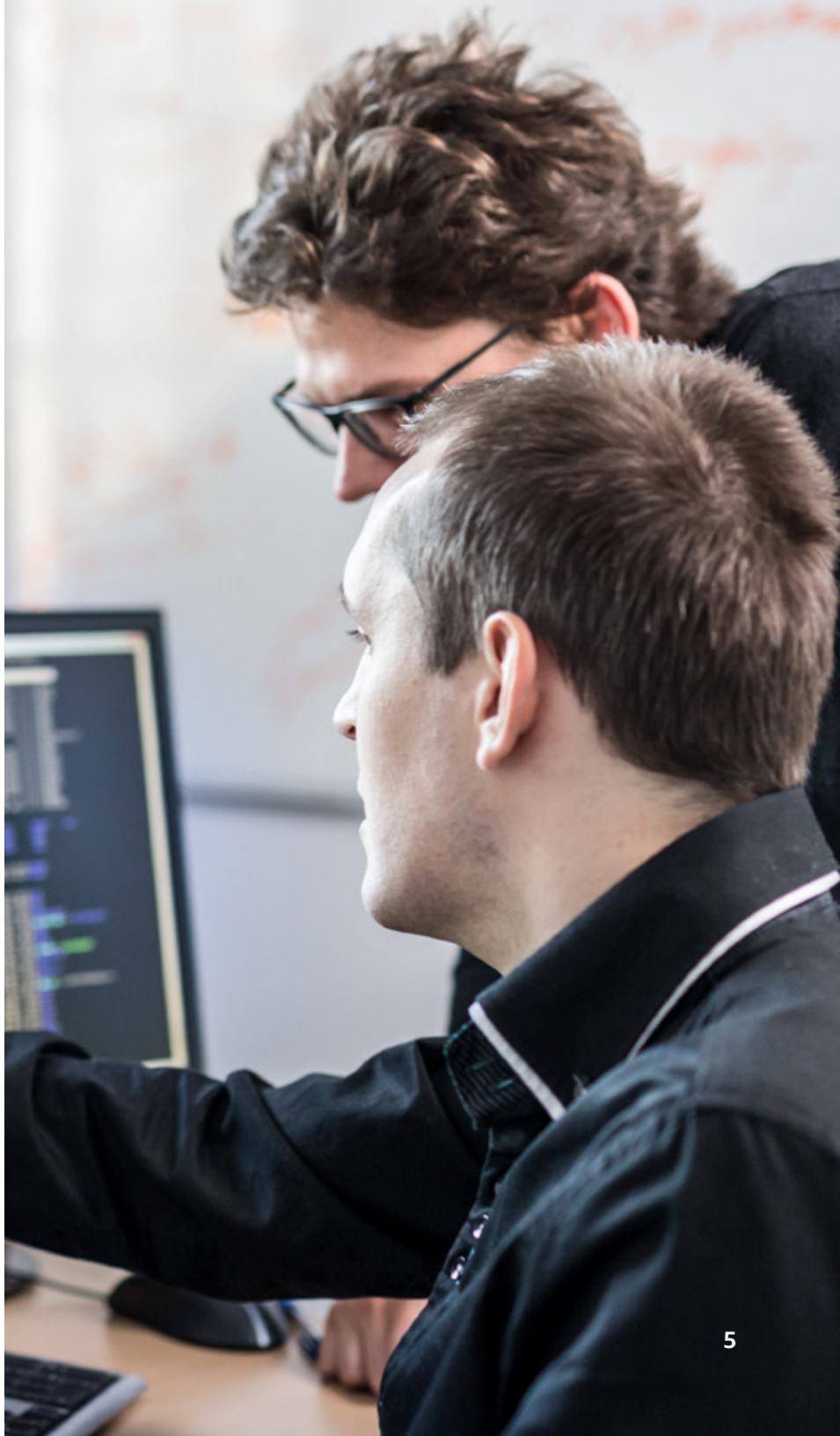
1 Enable faster insights with secure data

The situation

Some organizations are slow to open their data to more employees because they're concerned about security and governance. While organizations strive for a single source of truth, data-driven approaches are often siloed and sporadically spread throughout the organization. This requires breaking down data silos to make data more accessible while maintaining confidence that it is secure with the right governance strategy in place.

The solution

By making data and insights easily accessible to relevant employees and stakeholders, organizations can achieve their goals faster and improve business outcomes.



Where AWS fits in

As part of your governance strategy, having the right identity and access management controls allows your teams to move faster by giving the right people the ability to quickly find, access, and share data.

Amazon Web Services (AWS) is investing across the data journey to enable end-to-end data governance with less effort. AWS Lake Formation makes it simple to govern and audit the actions taken with data in your data lake on Amazon Simple Storage Service (Amazon S3). Lake Formation can also be used to govern data sharing in Amazon Redshift, the Amazon serverless cloud warehousing solution. Amazon DataZone is a new data management service designed to catalog, discover, share, and govern data so that the people who need it can act on it. And for your machine learning (ML) models, Amazon SageMaker has features to help you govern and audit the end-to-end ML development cycle.

ONEFOOTBALL

By simplifying governance, OneFootball saw a 40% increase in the utilization of its analytics infrastructure

OneFootball has grown rapidly to become a popular digital media sites for soccer ("fútbol") enthusiasts. To better use its data for the benefit of the company and 70 million fans of "the beautiful game," OneFootball built a nimbler solution on AWS in just a few days. Since integrating data from its backend databases into its cloud-based data lake, OneFootball has radically simplified data ingestion and helped eliminate legacy extract, transfer, and load (ETL) workloads altogether. Beautiful game, indeed. And with AWS Lake Formation, OneFootball simplified its security management and governance at scale, making data more accessible across the company. This ultimately helped the team see a substantial growth in weekly internal active analytics users—the team's internal key performance indicator—increasing usage of the analytics platform by 40 percent.

Results

- Increased usage of analytics platform by 40 percent for internal daily active end users
- Improved customer sales by 19 percent
- Cut time needed to request and receive data from 4-6 weeks to two days
- Enabled staff to iterate and curate datasets for explorative work more quickly

AWS services used

- **Amazon Kinesis**
- **AWS Lake Formation**
- **Amazon Redshift**
- **Amazon S3**

Read the full case study ›

2 Reduce security-incident-related downtime

The situation

Responding to security incidents can be complex. The immediate loss of productivity, due to the inaccessibility of data, quickly morphs into a greater need for identifying the root cause, patching, updating systems, and more. The disruption caused by security events and issues is often felt throughout the entire organization.

The solution

Users within an organization should know where to report security incidents. Additionally, security staff should develop a deeper understanding of how to respond to security issues. By maintaining stricter security and governance and integrating preparation, education, and training before security issues occur, your organization can keep moving with confidence.

Where AWS fits in

The **shared responsibility model** divides security and compliance responsibilities between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility for and management of the guest operating system (including updates and security patches), other associated application software, and the configuration of the AWS-provided security group firewall.

Raising your security posture is the first step to making sure a security event does not occur within your environment. You can start by reviewing your security program and controls against best practices from AWS such as the **AWS Well Architected framework**, third-party organizations like the **NIST Cybersecurity Framework** or **ISO**, and your internal policies to better understand the responsibilities that fall to you, your partners, and AWS.

SHIFT4 DEVELOPER

Shift4 manages complex online payments, scales to 300% growth on AWS

A reliable, secure, and scalable environment promotes the flawless processing of millions of transactions. Shift4, formerly SecurionPay, has a security-first approach. Maintaining the highest possible level of data security for fast, increasing volumes of transactions is central to its business. Chargebacks, fraud, and failed payments can hamper revenue growth if not managed properly, so **Shift4** turned to AWS to build a secure platform that can reliably process millions of concurrent transactions.

Results

- Scaled to meet 300 percent business growth
- Improved customer sales by 19 percent
- Used data analytics to support smarter business decisions

AWS services used

- **Amazon Kinesis**
- **Amazon QuickSight**
- **Amazon Redshift**

Read the full case study ›

3 Reduce overhead with more encompassing data security

The situation

Many organizations still self-manage their databases, focusing on operational tasks such as hardware and software installation, backups, performance tuning, and configuring for high availability, security, and compliance. This approach comes with it's own unique set of challenges, including the use of a network architected to meet industry and geographic laws and regulations, third-party validation for compliance requirements, and monitoring services for compliance reporting. All that time spent administering and overseeing these concerns means less time analyzing data or innovating on an application and, instead, growing costs across the board.

The solution

The most important steps an organization can take to resolve compliance-related challenges is to ensure they are up to date on global compliance requirements to help meet security and compliance standards for finance, retail, healthcare, and government. By utilizing proper security controls and tools, you can reduce your cost and time to run your own specific security assurance requirements.

Where AWS fits in

AWS has the most comprehensive list of compliance programs, global and industry standards, and local and regional programs. Utilizing AWS can help lower the costs of your security assurance efforts and strengthens your own compliance and certification programs. AWS helps keep security cost-effective,scales with you, and helps you protect your organization's investments and commitment to data initiatives.

Climedo

Climedo Health captures patient-centric, compliant, and secure clinical data using AWS

German EDC (electronic data capture) software provider **Climedo Health** used AWS to create secure, cloud-native, and scalable solutions to better capture and manage clinical data. AWS provided Climedo Health with the scalability it needed while meeting data protection standards.

Results

- Approximately 140 offices were using eDiaries within 12 months
- Time spent tracking symptoms was reduced by 80 percent
- More than 30,000 SMS messages were processed and sent per day from public health offices

AWS services used

- **Amazon Elastic Compute Cloud (Amazon EC2)**
- **AWS Key Management Service (AWS KMS)**
- **AWS Lambda**

Read the full case study ›

4 Maintain focus throughout your decision making process

The situation

Traditional security methodologies are too often overlooked until the end of the decision making process. Security has become everyone's job, not just the security experts. With security as your foundation, and being considered in every part of your business, your team has the confidence to innovate without fear.

The solution

To create this culture of security, consider security implications throughout the decision making process. Good security hygiene is virtually free, and it's effective because it prevents the majority of everyday security exploits. Automating security tasks enables time efficiencies and reduces human errors while keeping you more secure.

Where AWS fits in

Automating security tasks with AWS positively impacts your whole security team, by allowing them to focus more time transforming data into better decisions that drive business results. AWS provides a data catalog that automatically discovers, tags, and catalogs data and provides an easy way to centrally define and manage security, governance, and auditing policies—all in one place.

Velliv

Velliv completes secure, compliant migration

Velliv, one of Denmark's largest pension companies, separated from its parent company in 2018. They needed to build a completely new, independent IT infrastructure. Velliv chose AWS to migrate all of its existing IT stacks to take full advantage of a hundred percent cloud environment. The migration was completed in only one year, which significantly beat IT operations' expectations. Using AWS, Velliv delivered the high standard of security required by the Danish Financial Authority, which was confirmed by external audits. This helped the company to meet the regulatory requirements for its data.

Results

- Company can scale proactively to business needs
- Developers spend less time on infrastructure tasks
- Better visibility into IT costs and usage
- Faster time-to-market using managed AWS services

AWS services used

- **Amazon API Gateway**
- **Amazon DynamoDB**
- **Amazon Lambda**
- **Amazon Simple Queue Service (Amazon SQS)**

Read the full case study ›

Considering data security testimonials

Enable faster insights with secure data

"The company decided that using AWS would not only enable it to rapidly add and modify servers, there would also be other benefits, including better performance, lower costs, better security, and greater availability."

Bandai Namco Studios Inc. (Software)

Reduce security-incident-related downtime

"We do business across various industries, and some of them have very strict requirements regarding data privacy, retention, and security. It certainly helps that AWS carries all these certifications."

Catherine Lewis, EVP of Technology, MiX Telematics (Software)

Reduce overhead with more encompassing data security

"Using AWS, Pacific Life can quickly scale up additional compute capacity with less cost and IT overhead than by adding to its own data center assets, while benefiting from built-in security features in AWS products that help Pacific Life with compliance issues."

Pacific Life (Financial Services)

Maintain focus throughout your decision making process

"We had heard urban legends about 'security issues in the cloud,' but the more we looked into AWS, the more it was obvious to us that AWS is a secure environment and we would be able to use it with peace of mind."

Yoshihiro Moriya, Certified Information System Auditor, HOYA (Healthcare)

CONCLUSION

Securely put data at the center of every decision

Alongside efficient and accurate decision making, security has never been more important. AWS can help streamline your organization's ability to harness data effectively by verifying that data gets into the hands of the right employees and stakeholders, so organizations can achieve their goals faster. AWS is one of the most secure cloud computing environments available today, giving your teams time to focus on running core business initiatives and less time on managing security standards and compliance requirements of the ever-changing world.

AWS provides the necessary levels of security to help ensure your team is empowered to use data to make faster, better decisions while maintaining security oversight to deter misuse of sensitive data.

Resources

Learn about the AWS Shared Responsibility Model in practice ›

AWS Services in Scope by Compliance Program ›

Read more

A Unified Approach to Data Governance ›

Security Best Practices eBook ›

Shared Responsibility Model ›

5 Steps to Building a Modern Data Foundation ›

Best Practices for Security, Identity, & Compliance ›

Security & Compliance Quick Reference Guide ›