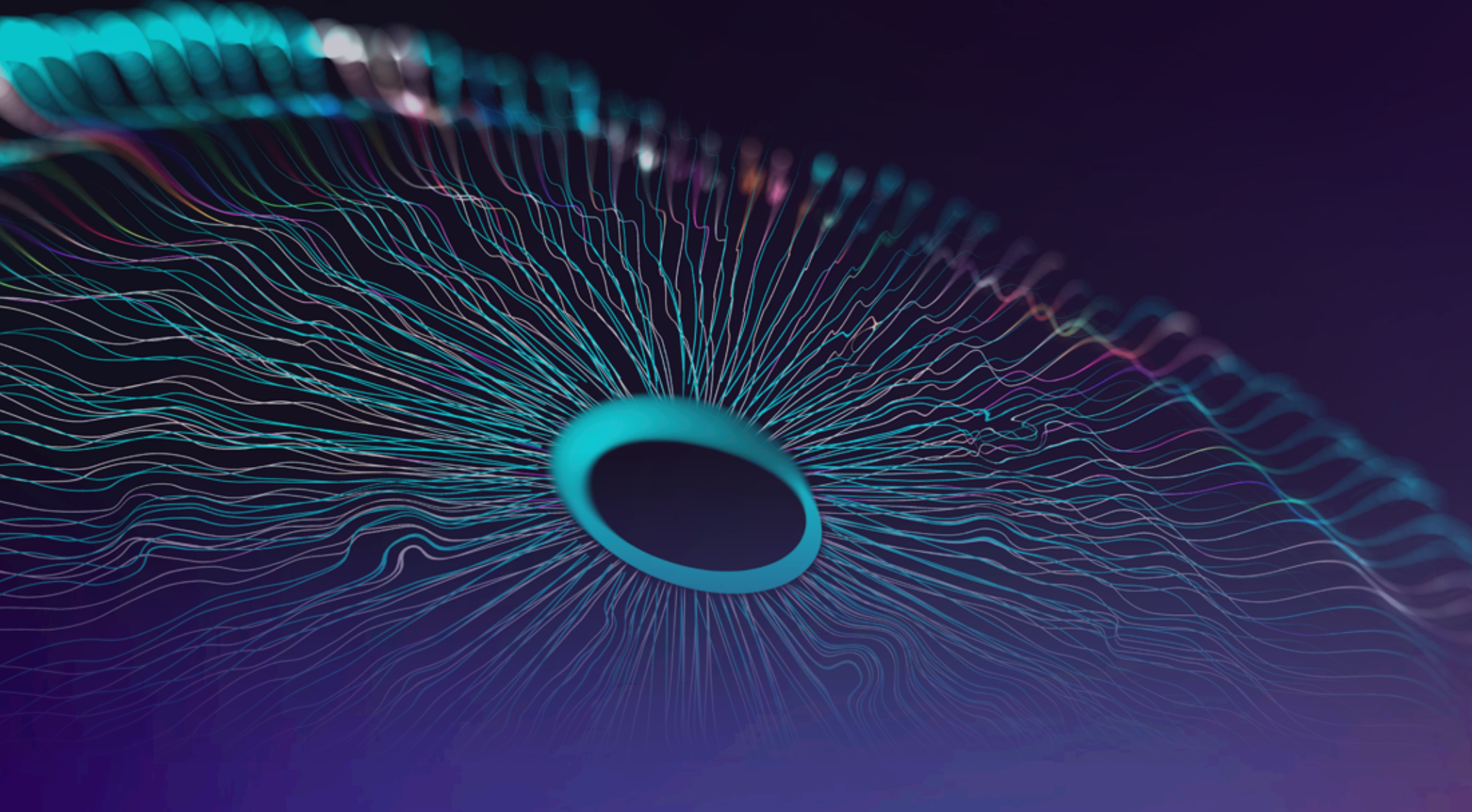
Continuously identify and prioritize security risks

Explore AWS detection and response services

The eBook is intended for security leaders and practitioners seeking effective cloud security risk management, centralized monitoring for enhanced visibility, and improved organizational security.

Table of contents



01

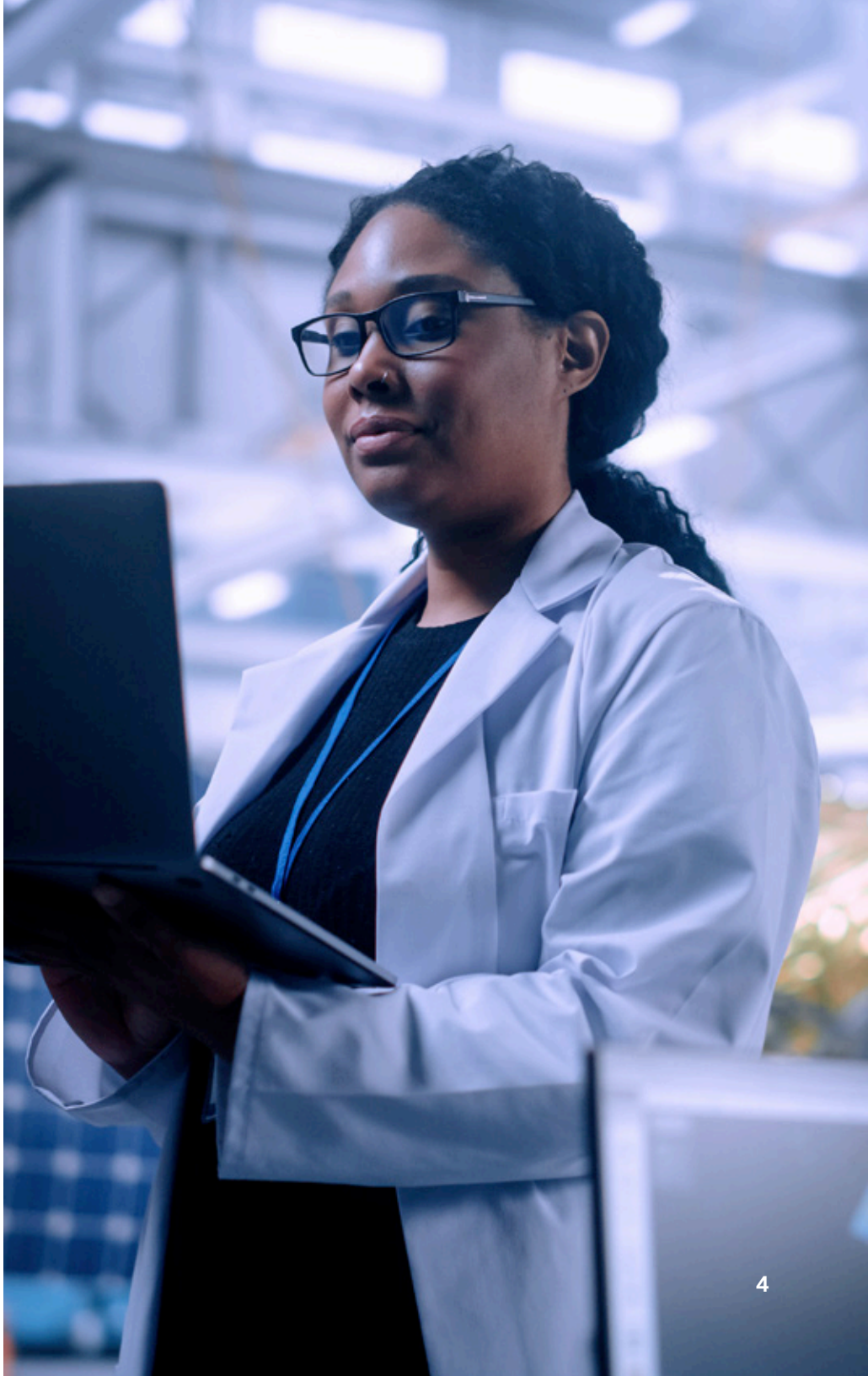
Introduction

01 INTRODUCTION

Avoid security risks

Cloud security is top of mind for every organization. The lack of insightful data on security incidents and the use of disparate security solutions across organizations can lead to unwanted exposure and an increase in security risk. Complete visibility is not always available for security teams, and fragmented security information exposes gaps and can create entry points for malicious actors. With security alerts increasing in volume, teams are tasked with discerning the signal from the noise and turning the findings into actionable information. To safeguard AWS Cloud workloads, applications, and data, organizations must be equipped with security solutions that continuously detect and respond to security risks.

In this eBook, we explore the top concerns of security professionals and learn how leading global organizations are benefiting from Amazon Web Services (AWS) detection and response security solutions by reducing security risks. Discover how you can protect against security threats, enhance visibility into potential risks, and help improve the security posture of your AWS environment. By enlisting AWS detection and response services, you gain access to a comprehensive overview of your security. Now, you can manage and mitigate security risks while reducing time spent, costs, and engineering resources. With both security professionals and developers collaborating on security issues, organizations can successfully overcome security challenges.



02

Challenges and benefits

Evolve cloud security

Addressing security concerns can transform the way you operate, freeing up resources to focus on innovation while enhancing the security of your organization. When selecting security solutions to protect AWS Cloud workloads, resources, and data, it is important to understand the security challenges.

Inability to detect and prioritize security risks

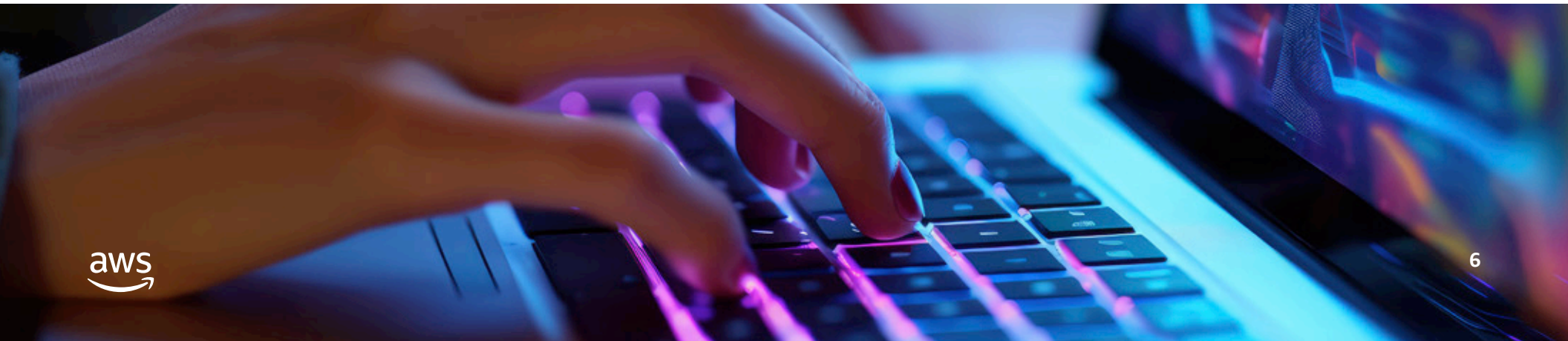
A lack of insightful data makes prioritizing security risks difficult. Staying up to date with the latest security tactics, techniques, and procedures (TTP) to identify threats across a quickly growing number of cloud accounts, networks, and workloads at scale can prove costly and time consuming.

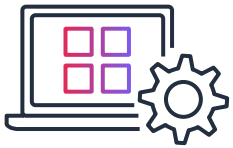
Inadequate visibility leading to security gaps

Many organizations function on a patchwork of disparate, custom-built security solutions. Although these solutions individually offer valuable security telemetry data, they lack a cohesive view and fail to provide visibility. This fragmented approach leads to security gaps, opening the door for malicious actors.

Difficulty prioritizing security alerts

Extracting and prioritizing security findings are critical to reducing your organization's security risks. However, as alerts grow in volume, teams can be left overwhelmed. This can prevent effective analysis that could help ensure they aren't missing critical security risks. In addition, inefficient workflows between security, DevOps, and IT teams prevent insights from being transformed into relevant and actionable alerts.





Lack of centralized security data management

Effective and secure storage of security data requires a supportive technology infrastructure and a centralized data management system. The reality is that organizations are performing time-consuming, complicated, and costly security data aggregations. Running security analytics without centralized security data management in place puts the protection of workloads, applications, and data at risk.

Benefits of AWS detection and response services:

- Protect your AWS workloads against security risks
- Centralize monitoring to enhance visibility into potential risks
- Investigate, protect, and respond quickly to security incidents across your environment
- Drive security innovation across hybrid environments

03

AWS detection and response services

Continuously detect and respond to security risks with AWS Security services

Threat detection and workload protection

Help protect your AWS accounts with intelligent built-in threat detection services that can continuously monitor and report malicious activity and unauthorized behavior.

Vulnerability management

Benefit from vulnerability management at scale with a centralized view of security alerts and findings, help improve compliance, and leverage a fully managed data security service.

Risk management

Gain a comprehensive view of security data, and analyze, investigate, and quickly identify the root causes of potential security issues.

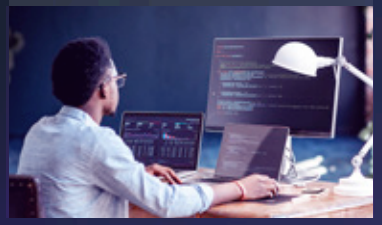
Services

- **Amazon GuardDuty** – Help protect your AWS accounts and workloads with intelligent threat detection
- **Amazon Inspector** – Benefit from automated and continual vulnerability management at scale
- **AWS Security Hub** – Automate AWS Security checks and centralize security alerts
- **Amazon Macie** – Discover and protect your sensitive data at scale
- **Amazon Detective** – Analyze and visualize security data to investigate potential security issues
- **Amazon Security Lake** – Automatically centralize your security data in a few steps

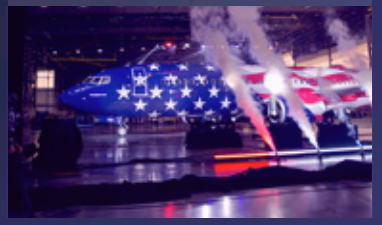
Explore how leading organizations implement security solutions to detect and respond to security threats

VOLKSWAGEN GROUP ›

HELLOSIGN ›



Southwest ›



IPG ›

Expedia ›

04

Use cases

USE CASE 1

Threat detection and workload protection

Defend your accounts and workloads from potential threats by streamlining threat response with automation. Minimize business impact through faster remediation and recovery time.

How Volkswagen Group did it

Volkswagen Group is a global automobile manufacturer that uses on-premises and cloud-based solutions, including applications powered by AWS.

Opportunity

Using over 200 AWS services, Volkswagen Group was looking to strengthen security and vulnerability detection across its AWS accounts. To do this, account owners needed centralized access to security threats and findings and a comprehensive view of security alerts and security posture. An alternative to customizing security controls with an account provisioning system was also needed.

Solution

To protect a quickly growing number of cloud workloads, Volkswagen Group deployed the threat detection service **Amazon GuardDuty** to continuously monitor for malicious activity and unauthorized behavior. **AWS Security Hub** provided centralized access to security threats and findings while detecting threats at the time of account creation. To ease employee workloads, the threat detection process was automated, enabling Volkswagen to automatically identify security threats and quickly deploy solutions to protect its AWS accounts.

VOLKSWAGEN GROUP

"When our users think about using AWS services for security, they're already there. They don't have to go and build a solution from scratch. This in turn saves a lot of time because the users know that the solution is secure and meets the Volkswagen standard. They can focus on building applications and connecting to vehicles."

Sachin Patil, Product Owner for AWS Cloud Foundational Services, Volkswagen Group

Results

- Deployed security services automatically
- Saved time for security team members
- Maintained consistent security controls across the organization
- Reduced AWS account provisioning time by 20–27 minutes per batch

Read the customer story ›

USE CASE 2

Automated and continual vulnerability management at scale

Automatically discover and quickly route vulnerability findings in near real time to appropriate teams to enable immediate action.

How HelloSign did it

HelloSign is an electronic signature and storage solution that was acquired by cloud-based file storage and smart workspaces company Dropbox in 2019. When it acquired HelloSign, Dropbox provided customers the ability to send, sign, and store documents online without leaving Dropbox.

Opportunity

The company was looking to make its service both secure and highly available. It wanted to enhance its security posture with scalable, robust, and customized security tools without the need to offload data to a third-party solution. Security priorities included saving developer time, improving security response time, and averting security events.

Solution

To avoid offloading data to a third party, HelloSign turned to **Amazon Macie**, a fully managed data security service that uses machine learning (ML) and pattern matching to discover and help protect sensitive data, and **Amazon Inspector**, which provides vulnerability management to help improve the security and compliance of applications. To monitor for malicious activity, HelloSign protected its AWS accounts, workloads, and data with **Amazon GuardDuty**. For a comprehensive overview of security alerts and security posture, **AWS Security Hub** aggregated HelloSign's security findings across its AWS deployment. Web applications security leveraged **AWS WAF** against common bots.

HELLOSIGN

"We use the Amazon Inspector findings as part of our patch management automation process, saving a lot of time and resources in updating our software and systems."

Kirtika Dommeti, Senior Security Engineer, HelloSign

Results

- Upgraded security posture in just 6 months
- Automated security features within 3 months
- Streamlined workflow and reduced time-consuming tasks
- Saved roughly 120 hours of work per week through automation
- Saved $1 million annually in triage time for security operations, staffing, and licensing costs

Read the customer story ›

USE CASE 3

Centralized monitoring and continuous cloud security posture management

Help ensure your environment is operating according to security best practices by continuously detecting and remediating cloud resource misconfigurations and compliance risks.

How Southwest Airlines did it

Southwest Airlines is one of the world's largest low-cost carrier airlines, with around 54,000 employees transporting 130 million passengers per year to 101 destinations across 11 countries.

Opportunity

To protect the many integrated applications that keep the airline running safely and smoothly, Southwest Airlines was looking to use cloud-native elements for gathering security insights. It set out to maximize its capabilities by adopting a cloud-native approach to its security operational model.

Solution

To gain a comprehensive view of security alerts and security posture across its AWS accounts, Southwest adopted **AWS Security Hub**. It also leveraged the threat detection service **Amazon GuardDuty** to continually monitor for malicious activity and unauthorized behavior, as well as **Amazon Inspector** to automatically assess applications for exposure, vulnerabilities, and deviations from best practices. Another service within Security Hub is **Amazon Detective**, which made it simple for Southwest to analyze, investigate, and quickly identify the root causes of potential security issues. **Amazon CloudWatch** then aggregated its data from these multiple sources and performed event correlation with rich content to detect actionable security events.

Southwest®

"Using AWS Security Hub, we now have the stronger security capabilities that we need."

Jon Barcellona, Cybersecurity Engineering Director, Southwest Airlines

Results

- Achieved higher visibility into the airline's security operations
- Reduced time and labor required to implement over 350 automated security controls
- Scanned 600,000 resources with 98% compliance across over 350 security control objectives
- Reduced implementation time for new controls from 5–6 weeks to only a week
- Reduced development ideation, production, and activation time from years to only weeks or months

Read the customer story ›

USE CASE 4

Unified security data management

Consolidate and analyze security-related data, facilitate broader visibility, and investigate and respond to suspicious activities and security incidents.

How IPG did it

Interpublic Group (IPG) is an award-winning global provider of marketing solutions and services specializing in advertising, digital marketing, and communications planning. Based in over 100 countries, IPG has more than 58,000 employees.

Opportunity

IPG aimed to achieve a comprehensive understanding of security data and harness analytics tools while retaining control and ownership of its security data.

Solution

IPG deployed the security data management service **Amazon Security Lake** to gain a comprehensive view of security alerts and security posture across its AWS accounts. The solution provided a comprehensive understanding of security data, leveraged analytics tools while maintaining control and ownership of security data, and enhanced security across cloud and on-premises sources. Security Lake has adopted the **Open Cybersecurity Schema Framework** (OCSF), an open standard. With OCSF support, the service normalizes and combines security data from AWS and a broad range of enterprise security data sources.

"We can achieve a more complete, organization-wide understanding of our security posture across hybrid environments. We could easily create a security data lake that centralized security-related data from AWS and third-party sources."

Troy Wilkinson, Global CISO, IPG

Results

- Helped improve searches with consolidated data
- Brought in data types seamlessly—AWS, third party, and on premises
- Retained full control and ownership over data
- Paid only for storage, no ingest fee
- Received more telemetry as more data was brought in
- Searched in real time at speed and scale

Watch the customer story ›

USE CASE 5

Discover and protect workloads and data to meet your compliance obligations

Discover and protect sensitive data and workloads to increase visibility and automate remediation of your data security risks.

How Expedia did it

Expedia helps every type of traveler find the right trip and get the best value by connecting partners and giving access to data, tools, and technology to help build businesses.

Opportunity

Expedia was looking to protect data at scale and monitor and assess data privacy and security with continuous visibility into data security posture. It set out to empower the automation of data and enable automated security. While continuously enriching data is key to success, maintaining both local and global audit and compliance regulations was a necessity.

Solution

Amazon Macie enabled Expedia to gain visibility on data, monitor changes in bucket inventory, and report activity in real time to protect sensitive data at scale. The service helped Expedia enhance data discoverability while reducing its sensitive data footprint. **Amazon GuardDuty** has built-in threat detection capabilities and reports suspicious or malicious access to the data, such as data exfiltration acts. Both these services can be correlated in **AWS Security Hub**. Expedia security teams can then orchestrate and leverage the report findings of both Macie and GuardDuty to tie into where the sensitive information is and whether or not it has been accessed by either malicious or suspicious actors. These services are integrated with automated remediation solutions.

Expedia

"Integrated and automated solutions, this is huge for us. More automation gives us the controls to protect our data faster."

Aaron Miller, Principal Architect, Data Security & Governance, Expedia

Results

- Provided visibility into what the sensitive data was
- Offered threat detection and response
- Performed to discover sensitive data at scale
- Orchestrated downstream governance and data protection
- Discovered where sensitive data information was located
- Revealed whether data had been breached

Watch the customer story ›

05

Conclusion

05 CONCLUSION

Help improve organizational security

In today's security landscape, organizations need advanced detection and response services to operate securely and successfully. Across your AWS environment, AWS detection and response services work together to continuously identify and prioritize security risks while integrating security practices earlier in the development lifecycle.

Architected to be the most secure cloud computing environment available today, and with the most extensive global cloud infrastructure, AWS has broad visibility into emerging security needs. These are integrated into AWS detection and response services, giving you valuable insights and protections against potential security incidents before they can impact your AWS environment. As AWS reinvests its knowledge into its core technologies, it leverages advanced capabilities, such as ML, to detect and investigate possible exposures and potential threats and help ensure the ongoing protection of your workloads and data at scale.

Equip your organization with AWS detection and response services and protect the security posture of your AWS environment.

Learn more about detection and response on AWS ›