AWS Partner Logo

Democratize Security Data with Amazon Security Lake

EBOOK

aws PARTNER

- MSP Partner
- Saas Partner
- Training Partner
- Marketplace Seller
- Network Competency

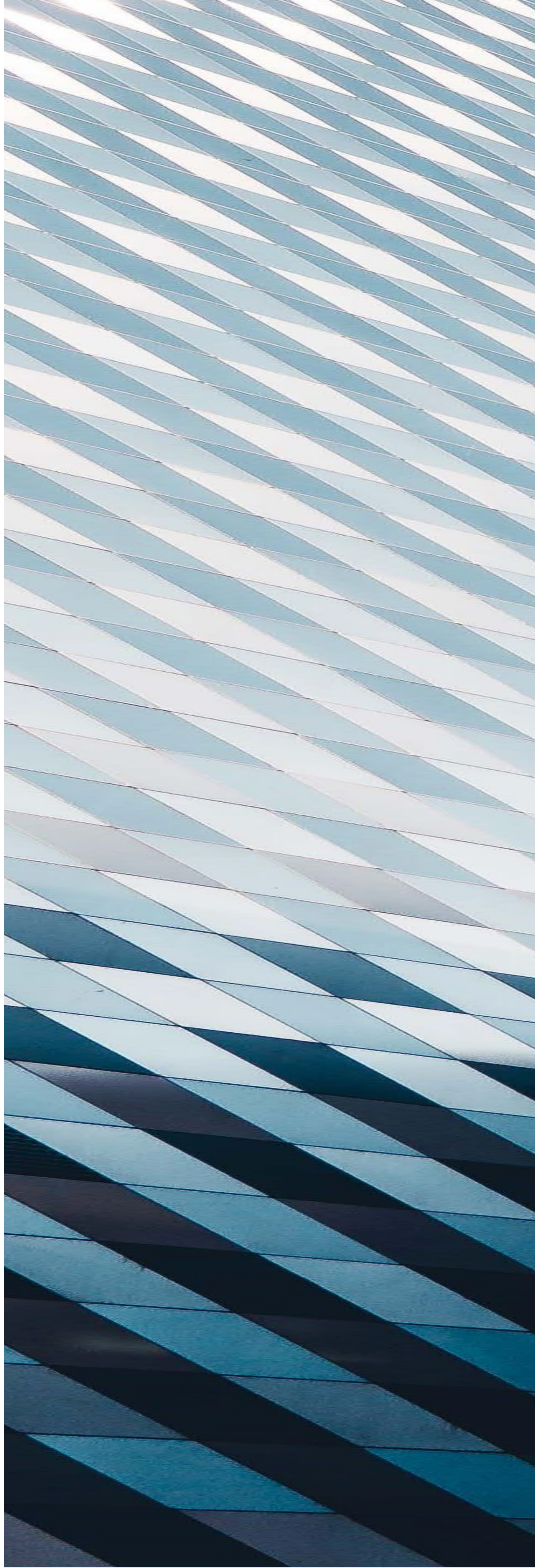


Table of contents

Introduction

It is estimated that in the past four years, the amount of security data generated by organizations has tripled. Some of these data sources include logs from on-premises infrastructure, firewalls, and endpoint security solutions—as well as multiple cloud services and accounts. And they are in different formats, which is complicating the process of using the data to prevent security incidents and threats. As organizations strive to safeguard their digital assets, the challenges of collecting, organizing, and utilizing security data have become apparent. Security teams grapple with the daunting task of identifying and consolidating relevant security data from a multitude of sources. Proprietary formats can render security log data inaccessible without time-consuming conversions. Even when transformed, the resulting data may still be incompatible with security and analytics tools, due to the absence of a standardized schema. This lack of cohesion impedes seamless data ingestion and poses a significant obstacle to comprehensive security analysis. The ongoing effort required to meet stringent security and compliance standards adds yet another layer of complexity, driving up operational costs. To identify potential security threats and vulnerabilities, you could centralize all your logs in a data lake. But even then, defining and implementing security domain-specific aspects can be a struggle. For example, data normalization requires analyzing each log source's structure and fields, defining schemas and mappings, and pulling in threat intelligence. However, with a security lake, you can tackle normalization and other challenges. Let's explore how Amazon Security Lake and AWS Partners help you address these enterprise security data challenges for more accurate analysis and effective protection.

Diving into Amazon Security Lake

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account. Built on top of Amazon Simple Storage Service (Amazon S3), it can:

- **Normalize AWS security logs and event data** in a common structure so that compatible security solutions can use it.
- **Collect, retain, and optimize data** to limit its duplication and multistep data movement and translation.
- **Centralize data visibility** with automatic aggregation that delivers enterprise-wide insights in minutes.
- **Analyze security data** using your preferred analytics tools while retaining complete control and ownership of that data.

Amazon Security Lake has features that specifically address the most common security challenges.

41% of IT and security manager perceive security data analytics technologies as very important to protecting enterprise data

52% of organizations keep security data online for longer periods of time than in the past

28% want to retain security data online but can’t for cost or operational reasons

Sources: BARC, Big Data and Information Security Analytics
CSO, Bracing for the security data explosion
ESG Master Survey Results, Cloud-scale Security Analytics Survey

Amazon Security Lake has features that specifically address the most common security challenges.

Variety of supported log and event sources
Amazon Security Lake automatically collects logs and security findings from more than 100 sources including AWS services and third-party security findings. AWS Partners can send data directly to Amazon Security Lake in the Open Cybersecurity Schema Framework (OCSF) format.

Data transformation
With OCSF support, Amazon Security Lake partitions and converts incoming log data to a storage and query-efficient format. As a result, you can use the data broadly and immediately for security analytics without post-processing. Amazon Security Lake supports integrations with AWS Partners to address a variety of security use cases such as threat detection, investigation, and incident response.

Customizable access management and availability
Amazon Security Lake enables you to customize the configuration of access to your data lake for your security and analytics tools. This includes granting access to datasets from specified sources, such as AWS CloudTrail. This customization and the other Amazon Security Lake capabilities described in this section deliver numerous advantages. Let’s explore them in more detail.

What is OCSF?
Developed jointly by Splunk and AWS, which built on the ICD Schema developed at Symantec—now part of Broadcom Software—OCSF is an open standard anyone can adopt to simplify security data normalization.

OCSF delivers a simplified and vendor-agnostic taxonomy for security data that can be adopted in any environment, application, or solution provider.

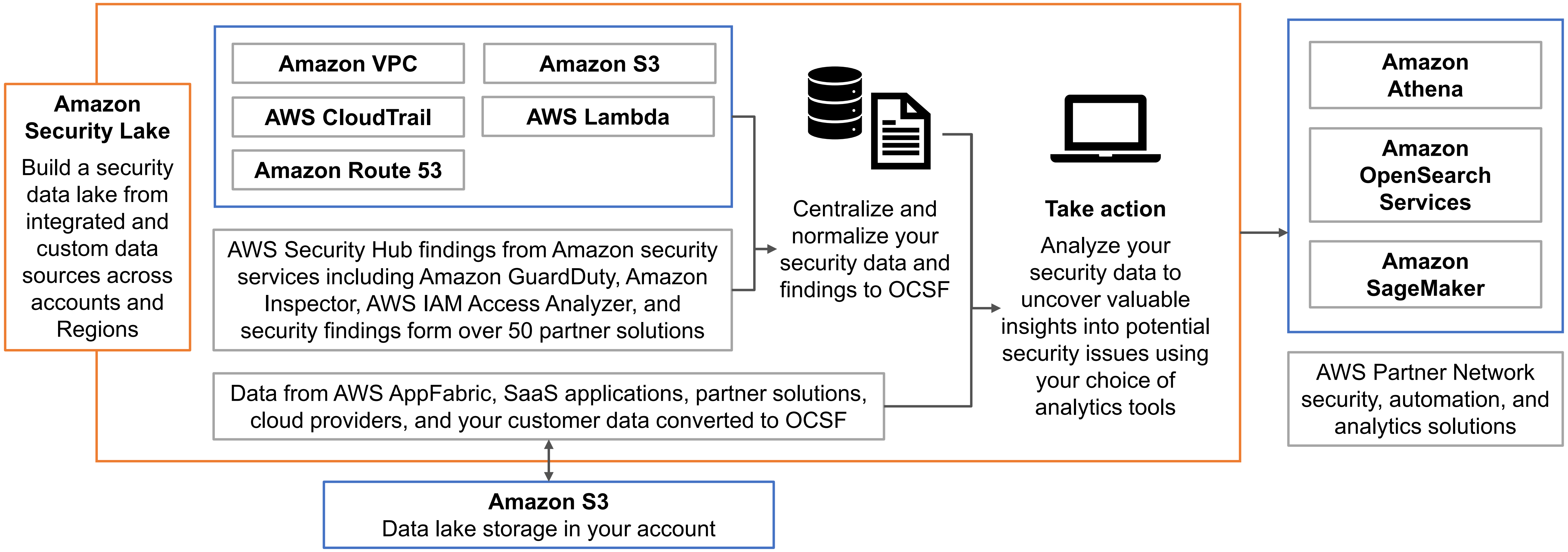
Why OCSF?
Speed up data ingestion and analysis without the time-consuming, upfront normalization tasks.

Combine data from OCSF-compliant sources to break down data silos that slow security teams.

Learn more from Splunk, which co-founded OCSF with AWS

Benefits of setting up a security lake

With its open-source schema and the fact that you own the data, Amazon Security Lake offers numerous advantages. Amazon Security Lake integrates with AWS Organizations, so you can gather logs across hundreds of accounts in a few clicks. It acts as an orchestrator based on your preferences, including the Amazon S3 tiering you use.


Amazon Security Lake
Build a security data lake from integrated and custom data sources across accounts and Regions
Amazon VPC
Amazon S3
AWS CloudTrail
AWS Lambda
Amazon Route 53
AWS Security Hub findings from Amazon security services including Amazon GuardDuty, Amazon Inspector, AWS IAM Access Analyzer, and security findings form over 50 partner solutions
Data from AWS AppFabric, SaaS applications, partner solutions, cloud providers, and your customer data converted to OCSF
Centralize and normalize your security data and findings to OCSF
Take action
Analyze your security data to uncover valuable insights into potential security issues using your choice of analytics tools
Amazon Athena
Amazon OpenSearch Services
Amazon SageMaker
AWS Partner Network security, automation, and analytics solutions
Amazon S3
Data lake storage in your account

When Amazon Security Lake receives a notification of a new Amazon S3 object, it sets up a cross-account role for direct access to Amazon S3 and manages infrastructure and permissions. You then query it in place using Amazon Athena and get support with AWS Lake Formation.

You control your data

Amazon Security Lake runs in an Amazon VPC on top of Amazon S3, so that means you control with whom you share it. You can also do analytics without moving data around, or you can send the logs to the analytics tool of your choice. You govern the log data, and you don't have to send the same data to multiple vendors. AWS subscription partners simply query them without ingesting everything. You own the data, so you know where it is and who has access to it.

Gather all the logs you need

Can you analyze all the logs you generate, or have you been having to make some hard choices? The output of some logging tools can fall in the terabyte range. For example, VPC Flow Logs can produce hundreds of gigabytes of logs—if not more—so some organizations choose the logs they think are most useful. With Amazon Security Lake, all the logs reside in an Amazon S3 bucket, so you can analyze data without wondering what you might be missing.

Govern your security data

Owning your security data preserves privacy, prevents data duplication, and reduces cost because you don't have to provide multiple vendors with the same data. Customizable retention settings help you store data for a specific period, which may help you address regulatory mandates. You can also turn Amazon Security Lake off and still retain ownership of the underlying Amazon S3 buckets. Another major advantage of Amazon Security Lake is the number of use cases it addresses—and the AWS Partners that support it.

Amazon Security Lake Partners

Third-party Amazon Security Lake integrations include solutions from source and subscriber partners.

- Source partners can send logs and security events to your security data lake in the OCSF format.
- Subscriber partners help you analyze logs in the OCSF format and address a variety of security use cases such as threat detection, investigation, and incident response.
- Service partners can help you help you build and use Amazon Security Lake.

A reservoir of valuable use cases

Your organization can use Amazon Security Lake a number of ways:

Analyze multiple years of security data quickly

Centralize petabytes of data from cloud, on-premises, and AWS source partners in your Amazon S3 buckets, and use your preferred AWS and AWS subscriber partner tools for security analytics. Amazon Security Lake integrates with security information and event management (SIEM) solutions, extended detection and response (XDR) tools, Amazon Athena, and Amazon OpenSearch Service to quickly query and analyze petabytes of data. AWS subscriber partners can help you analyze logs in the OCSF format.

Simplify your compliance monitoring and reporting

Make it easier to monitor and report on compliance across multiple log sources, AWS Regions, and accounts. With Amazon Security Lake, you can centralize security data from AWS and AWS source partners into one or more rollup Regions to simplify your compliance and reporting obligations.

Facilitate your security investigations with elevated visibility

Give your security teams the broader visibility needed to initiate thorough security investigations and rapid response to security incidents. Because the security-related logs and findings generated by AWS services and AWS source partners are centralized and in the same format, your security operations teams can more easily investigate issues.

Democratize security data management across hybrid environments

Optimize data accessibility across your organization and facilitate a more comprehensive approach to security operations. Amazon Security Lake can store security-related logs and data from various sources, including cloud, multi-cloud, and on-premises systems, making it simpler to collect and analyze security data in the OCSF format. Your security teams can query that data with AWS and AWS subscriber partner analytics tools to understand and respond to threats.

About [AWS Partner]

Subhead goes right here

[AWS Partner - use this space to talk about your solution, the associated benefits and use cases, and how it integrates with AWS] Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque semper, orci sit amet ullamcorper lobortis, lacus ex facilisis nunc, in viverra ex sem sit amet ante. Aenean consectetur facilisis nulla eget iaculis. Donec ultricies sem lacus, in vehicula orci blandit vitae. Duis non placerat est. Vestibulum lobortis auctor enim, vitae mattis justo mattis sit amet. Nunc nec pulvinar nibh. Donec id lectus tincidunt, vestibulum enim a, iaculis urna. Fusce mattis pulvinar justo id mollis. Proin dictum orci odio, a dignissim turpis semper vel. Quisque pharetra ut lacus ac congue.Mauris molestie urna et ligula condimentum vulputate. Pellentesque in congue nulla. Integer viverra nulla arcu, non cursus tortor scelerisque at. Nullam ornare neque neque, non ornare tellus hendrerit sit amet. Ut sit amet convallis turpis. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc pulvinar interdum feugiat.Vestibulum condimentum sagittis mauris sed hendrerit. Etiam ipsum sapien, posuere non elit id, convallis auctor ex. Mauris dolor mi, finibus eu faucibus nec, vestibulum sit amet nulla. Cras tempor vehicula ex, convallis laoreet libero. Donec consectetur vestibulum tempus. Vivamus sit amet luctus nisl. Praesent pulvinar nisl magna, eget molestie leo dignissim in. Phasellus dapibus, lorem ut molestie ullamcorper, orci nisl aliquam mi, id rhoncus augue lacus vel ipsum. Donec rutrum neque sodales placerat sagittis. Fusce ut convallis nisl. Duis nec tellus laoreet, mollis mi id, ornare nunc. Phasellus tincidunt quis eros malesuada. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc pulvinar interdum feugiat.Vestibulum condimentum sagittis mauris sed hendrerit. Etiam ipsum sapien, posuere non elit id, convallis auctor ex. Mauris dolor mi, finibus eu faucibus nec. Etiam ipsum sapien, posuere non elit id, convallis auctor ex. Mauris dolor mi, finibus eu faucibus nec.

Benefits of using Amazon Security Lake with [AWS Partner]

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque semper, orci sit amet ullamcorper lobortis, lacus ex facilisis nunc, in viverra ex sem sit amet ante. Aenean consectetur facilisis nulla eget iaculis. Donec ultricies sem lacus, in vehicula orci blandit vitae. Duis non placerat est. Vestibulum lobortis auctor enim, vitae mattis justo mattis sit amet. Nunc nec pulvinar nibh el. Quisque pharetra ut lacus ac congue.

Benefit 1 headline goes here

Mauris molestie urna et ligula condimentum vulputate. Pellentesque in congue nulla. Integer viverra nulla arcu, non cursus tortor scelerisque at. Nullam ornare neque neque, non ornare tellus hendrerit sit amet. Ut sit amet convallis turpis. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc pulvinar.

Benefit 2 headline goes here

Mauris molestie urna et ligula condimentum vulputate. Pellentesque in congue nulla. Integer viverra nulla arcu, non cursus tortor scelerisque at. Nullam ornare neque neque, non ornare tellus hendrerit sit amet. Ut sit amet convallis turpis. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc pulvinar.

Benefit 3 headline goes here

Mauris molestie urna et ligula condimentum vulputate. Pellentesque in congue nulla. Integer viverra nulla arcu, non cursus tortor scelerisque at. Nullam ornare neque neque, non ornare tellus hendrerit sit amet. Ut sit amet convallis turpis. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc pulvinar.

CASE STUDY

[Customer name]

Customer Logo

Challenge

[AWS Partner - use this space to briefly describe the customer’s challenge] Amet ullamcorper lobortis, lacus ex facilisis nunc, in viverra ex sem sit amet ante. Aenean consectetur facilisis nulla eget iaculis. Donec ultricies sem lacus, in vehicula orci blandit vitae. Duis non placerat est. Vestibulum lobortis auctor enim, vitae mattis justo mattis sit

Solution

[AWS Partner - use this space to briefly describe how your solution addressed the customer’s challenge] Amet ullamcorper lobortis, lacus ex facilisis nunc, in viverra ex sem sit amet ante. Aenean consectetur facilisis nulla eget iaculis. Donec ultricies sem lacus, in vehicula orci blandit vitae. Duis non placerat est. Vestibulum lobortis auctor

Benefits

[AWS Partner - use this space to briefly describe the benefits your customer saw after leveraging your solution] Amet ullamcorper lobortis, lacus ex facilisis nunc, in viverra ex sem sit amet ante. Aenean consectetur facilisis nulla eget iaculis. Donec ultricies sem lacus, in vehicula orci blandit vitae. Duis non placerat est.

Customer name here

Customer Title Here

"Lorem ipsum dolor sit amet,consectetueradipiscingelit, seddiam nonummynibheuismodtincidunt ut laoreetdoloremagna aliquameratvolutpat. Ut wisi enim adminimveniam, quis nostrudexercitation ullamcorpersuscipitlobortisnisl utaliquipex ea commodo. Ut wisienimadminimveniam, quisnostrudexercitationullamLorem ipsum dolor sit amet,consectetueradipiscingelit, seddiam nonummynibheuismodtincidunt utlaoreetdoloremagna aliquameratvolutpat. Ut wisienimadminimveniam, nonummynibheuismodtincidunt utlaoreetdoloremagna aliquameratvolutpat. Ut wisienimadminimveniam"

AWS Partner Logo

Learn more

Amazon Security Lake

[AWS Partner resource, hyperlinked]

[AWS Partner resource, hyperlinked]

[AWS Partner resource, hyperlinked]

aws PARTNER

- MSP Partner
- Saas Partner
- Training Partner
- Marketplace Seller
- Network Competency

[AWS Partner Name]; [AWS Partner Name] [Phsyical Address].