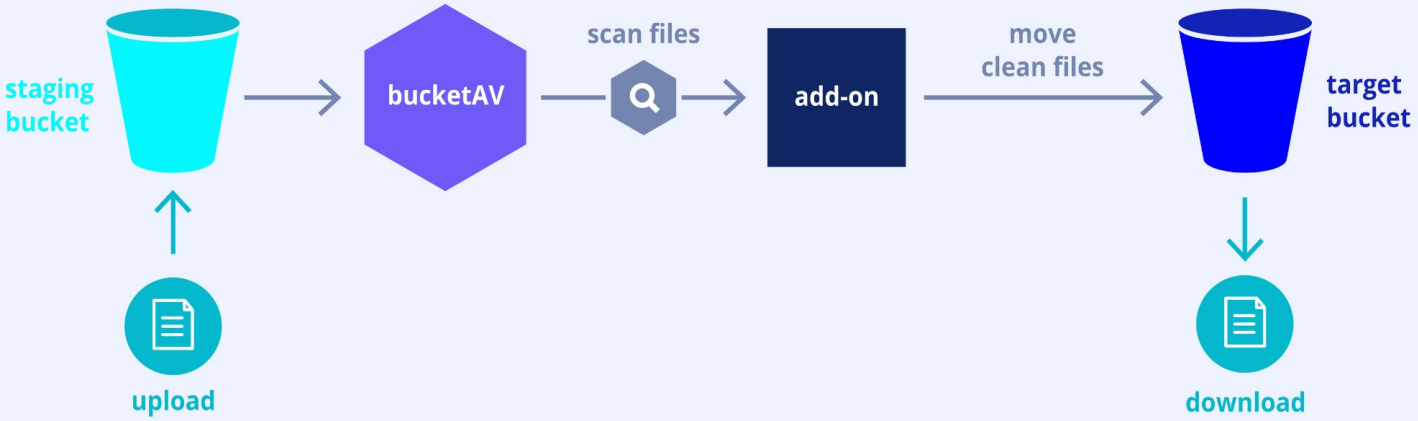
bucketAV

Antivirus protection for
Amazon S3
Cloudflare R2

Factsheet

Common approaches & use cases

Staging bucket

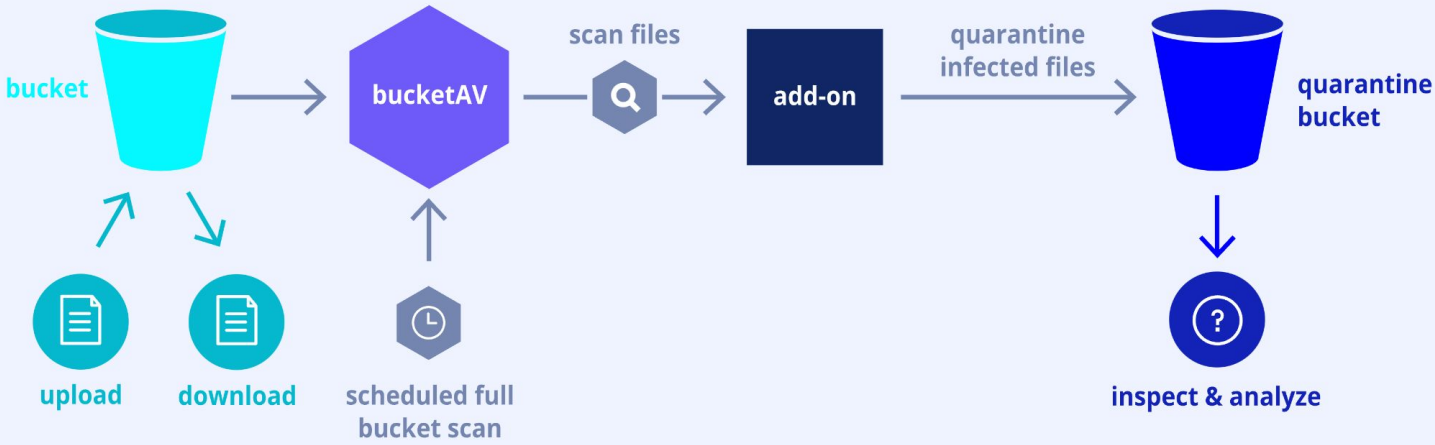


The easiest way to ensure that users can download only clean files is to use two buckets—one for uploads and one for downloads. The Move Clean Files Add-On moves clean files from the staging bucket to the target bucket.

One risk to consider is that this approach does not include a periodic full bucket scan. A file that was clean when uploaded could be detected as infected by the latest signature update. If you can tolerate infected files being removed from the target bucket, you can add the Scan bucket at regular intervals Add-On.

Use cases | **User uploads**

Quarantine infected files



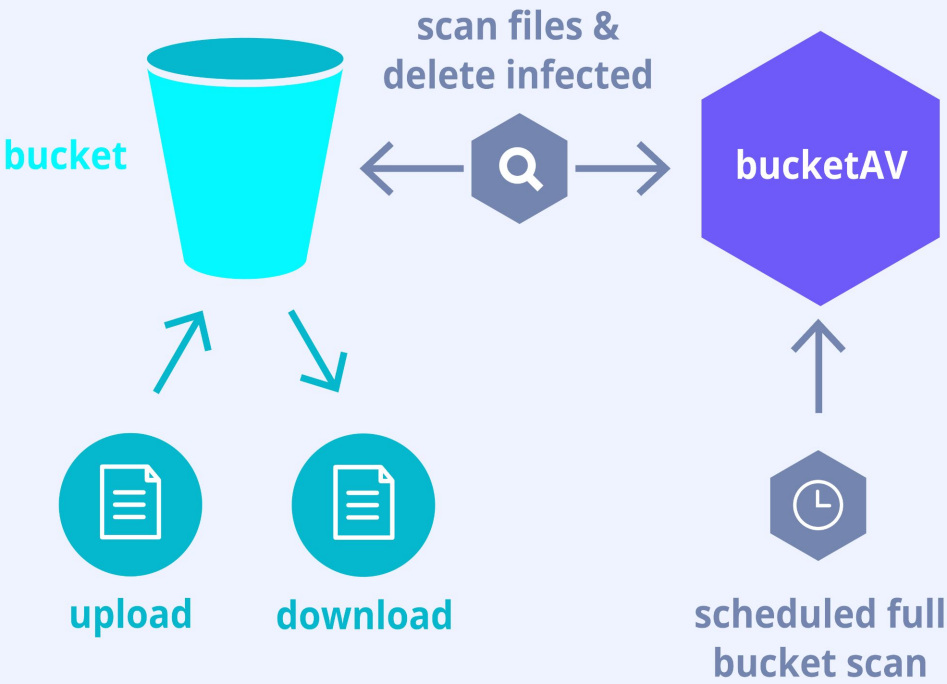
A quarantine approach is a security technique to isolate potentially harmful data to prevent it from spreading and causing damage to users. To protect a data lake using this approach, the following steps are needed:

- Data scanning
- Isolation
- Analysis

By using a quarantine approach, organizations can reduce the risk of malware infections in their data lake and maintain the security and integrity of their data.

Use cases	Date lake	Data compliance

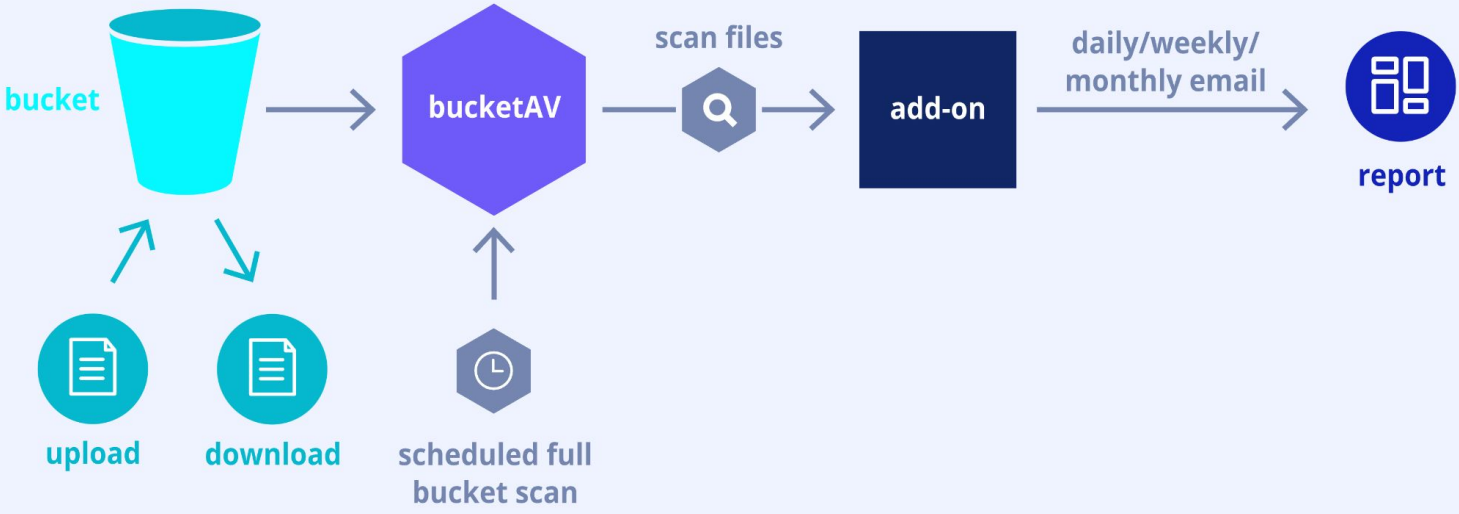
Delete infected files



Deleting infected files as soon as detected is a low-effort approach.

Use cases	Date lake	Data compliance

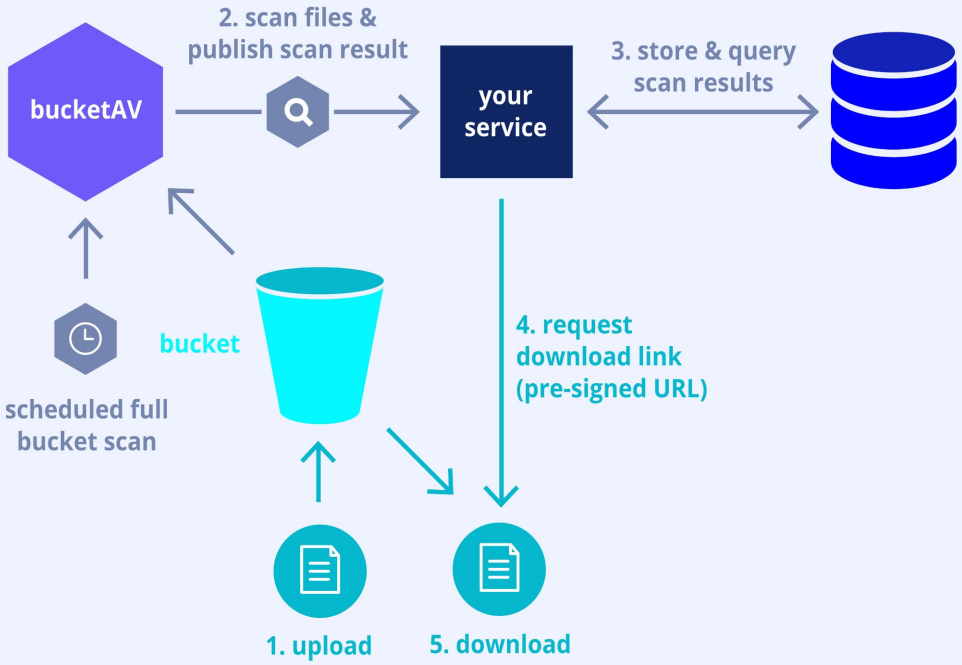
Reporting only



Instead of removing the threat, you can also minimize the impact on the data lake by only observing the data using reporting capabilities of bucketAV.

Use cases	Data lake	Content distribution	Data compliance

Application integration



If you use pre-signed URLs for sharing files, you can check the scan result before your application creates the pre-signed URL and returns it to the user.

Two common implementations:

- You can call the S3 GetObjectTagging API to get the bucketav tag with the scan result (Amazon S3 only).
- You can store the scan results in your database and check against your database. This option also allows the possibility of notifying the file owner about infections.

Use cases | **User uploads**

Block infected file download

You can allow downloads from the public only if the file is clean using an S3 bucket policy (Amazon S3 only). Therefore, you block downloads of infected and unscanned files.

Use cases	User uploads	Content distribution

Key Benefits

Data Protection

Scan your data with virtual machines running in your AWS account—no need to transfer data to an external service.

Scalable

Scan as many files as needed. bucketAV scales automatically. That's ensuring cost efficiency even for spiky workloads.

Simple

Get started within 15 minutes with the help of our setup guide and auto-installer based on AWS CloudFormation.

Fast

Uploaded files are scanned within seconds to detect malware as quickly as possible.

Up-to-date Malware Database

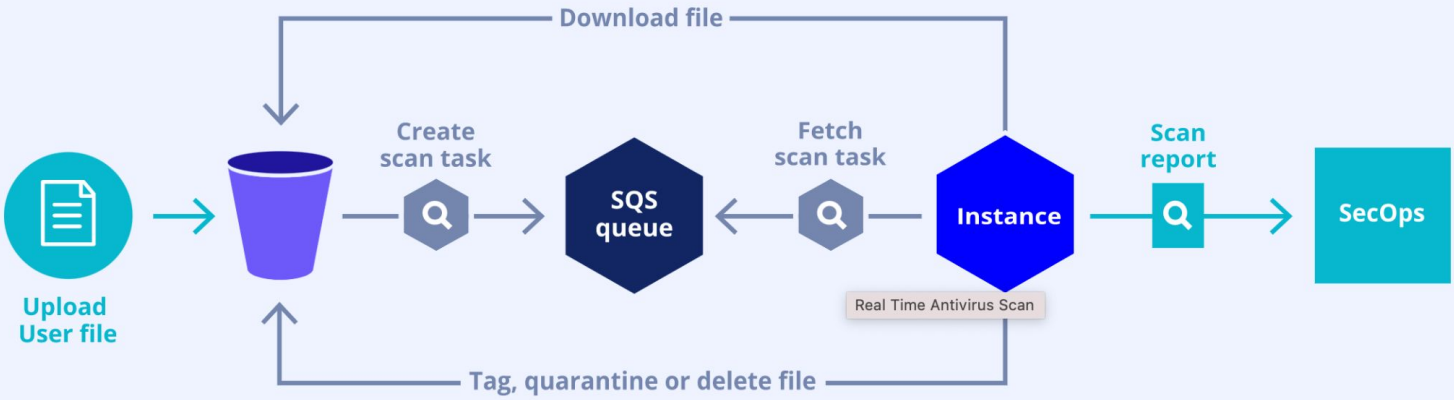
The signatures are updated continuously to protect you against the latest threats.

Automated Mitigation

bucketAV quarantines, deletes, moves, tags, and notifies about infected files. Configure the automated actions as needed.

Features

Real-time virusscan



When uploading a new file to a bucket, the bucket sends a scan job to a queue. One of the virtual machines running bucketAV picks up the scan task. The EC2 instance downloads the file from S3 or R2 and calls the ClamAV® or Sophos® antivirus engine to scan for trojans, viruses, and malware.

Afterward, the scanner sends a report with the scan result to a topic which forwards the message to an email address, Slack channel, Microsoft Teams team, or any HTTPS endpoint. On top of that, the scanner adds a tag to the scanned file and optionally quarantines or deletes infected files.

Scheduled bucket scan

On top of real-time scanning, bucketAV optionally scans your buckets regularly, such as daily, weekly, or monthly.

You know that all files are checked against the newest threat database if you scan your files repeatedly.

On-demand antivirus scan

Run an on-demand scan to ensure a secure baseline of all buckets after installing bucketAV.

On top of that, scan individual files against the latest virus signatures database at any time by submitting scan jobs manually or by integrating bucketAV into your applications using Amazon SQS & SNS or our HTTPS API.

On-access file scan

Scan files before downloading for maximum protection against the latest threats (Amazon S3 only).

The scan is transparent to the developer and user. You connect to Amazon S3 as before.

HTTPS API

Submit scan jobs to bucketAV via HTTPS and integrate scan results into your application (Amazon S3 only).

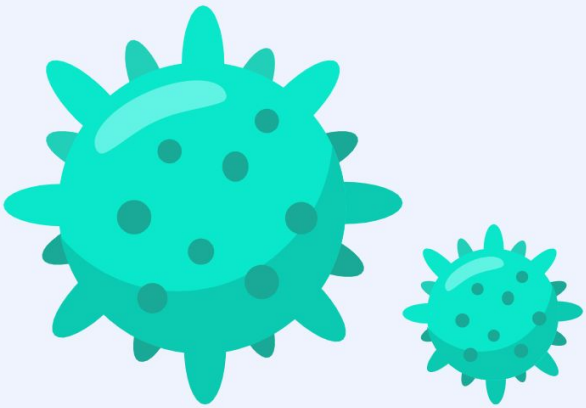
The HTTPS API uses the same engine and provides the same information as the native integration.

Reporting

bucketAV provides a daily, weekly, or monthly report via email. The report includes statistics about scanned files as well as insights into findings.

CSV files with raw data for further analysis are part of the report and can be inspected manually in Microsoft Excel.

Antivirus engines

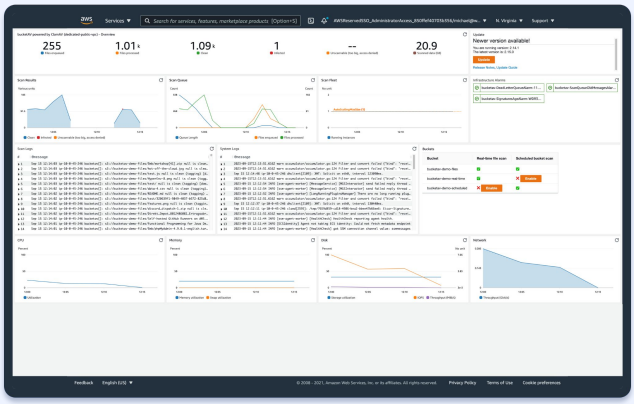


bucketAV is available in two editions: powered by ClamAV® or Sophos®.

- ClamAV® is a open-source antivirus engine.
- Sophos® is a trusted cybersecurity provider.

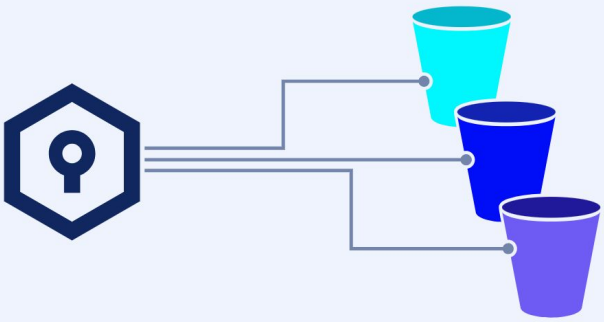
You can switch engines at any time.

Real-time dashboard



Get an overview of the scan results as well as the health of the scan queue. bucketAV also provides a detailed log of all scan results and system logs. Last but not least, the dashboard provides insights into the hardware utilization of the scanning fleet.

Automated mitigation



bucketAV quarantines, deletes, moves, and tags files based on the scan result. On top of that, you can subscribe to notifications based on scan results. You can configure automated rules to fit your needs. For example, you can quarantine infected files or move clean files into a secure bucket.

Need more help? Write us! hello@bucketav.com

Multiple AWS accounts

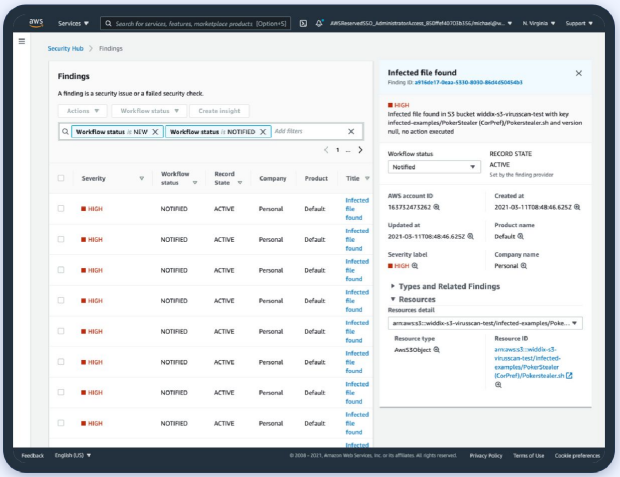
Are you making use of multiple AWS accounts to isolate different workloads? Good news! bucketAV supports scanning buckets from multiple AWS accounts.

However, we recommend running bucketAV in the same account as your S3 buckets to minimize the configuration overhead and keep the isolation boundaries in effect.

Multiple buckets

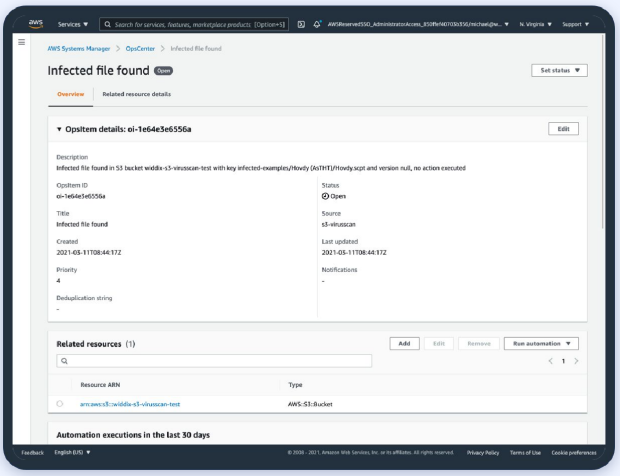
Connect one or multiple buckets to bucketAV. Our dashboard shows all your protected and unprotected buckets.

Security Hub integration



AWS Security Hub collects and displays security and compliance-related information. bucketAV integrates with AWS Security Hub. Infected files show up as security findings. Your SecOps team investigates the findings using the Security Hub workflow.

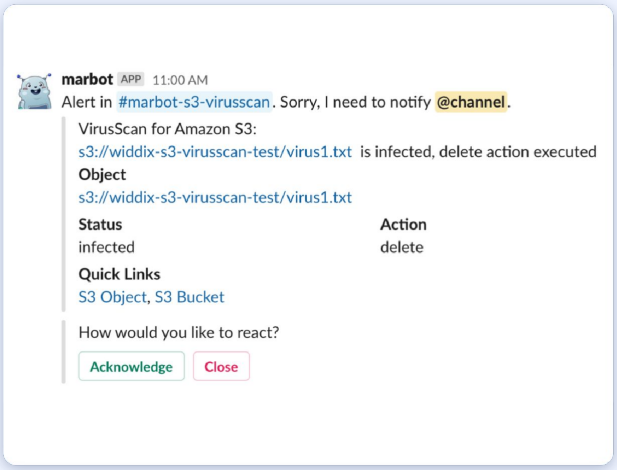
SSM OpsCenter integration



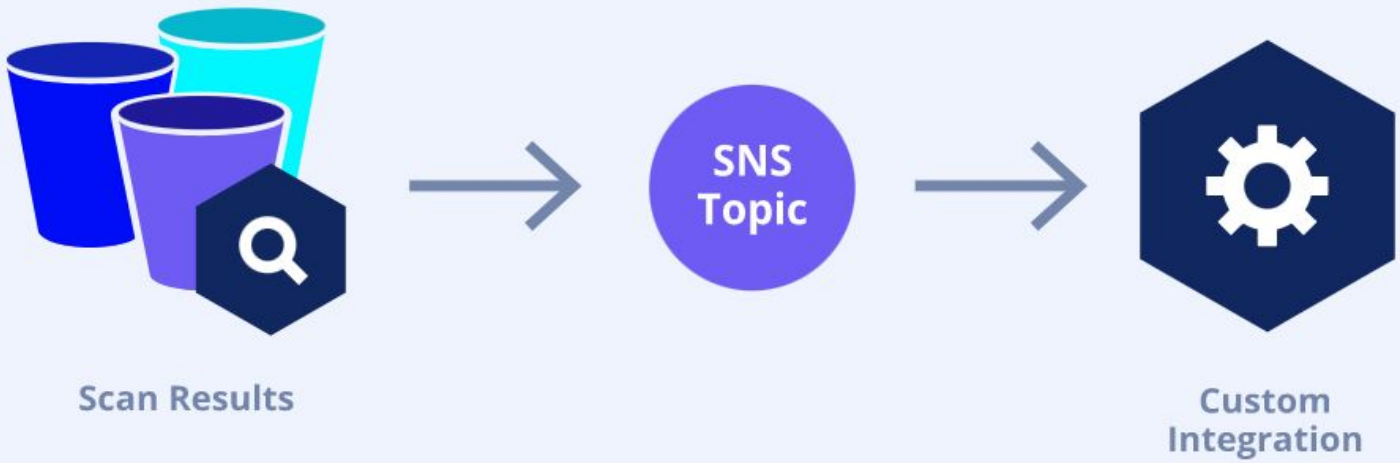
AWS Systems Manager OpsCenter provides a central location where operations engineers and IT professionals can view and investigate infected files. OpsCenter comes with a workflow engine to ensure that every finding is noticed.

Slack and Microsoft Teams integration

bucketAV integrates with [marbot - a chatbot for AWS Monitoring](). You can notify your team in Slack or Microsoft Teams whenever an infected file is found.



Custom integration



AWS is the largest cloud platform in the world. bucketAV provides a cloud-native integration point. All scan results are published to Amazon SNS. If interested in the scan results, you can subscribe to the SNS topic and react to any file scan in real time.

Integrations

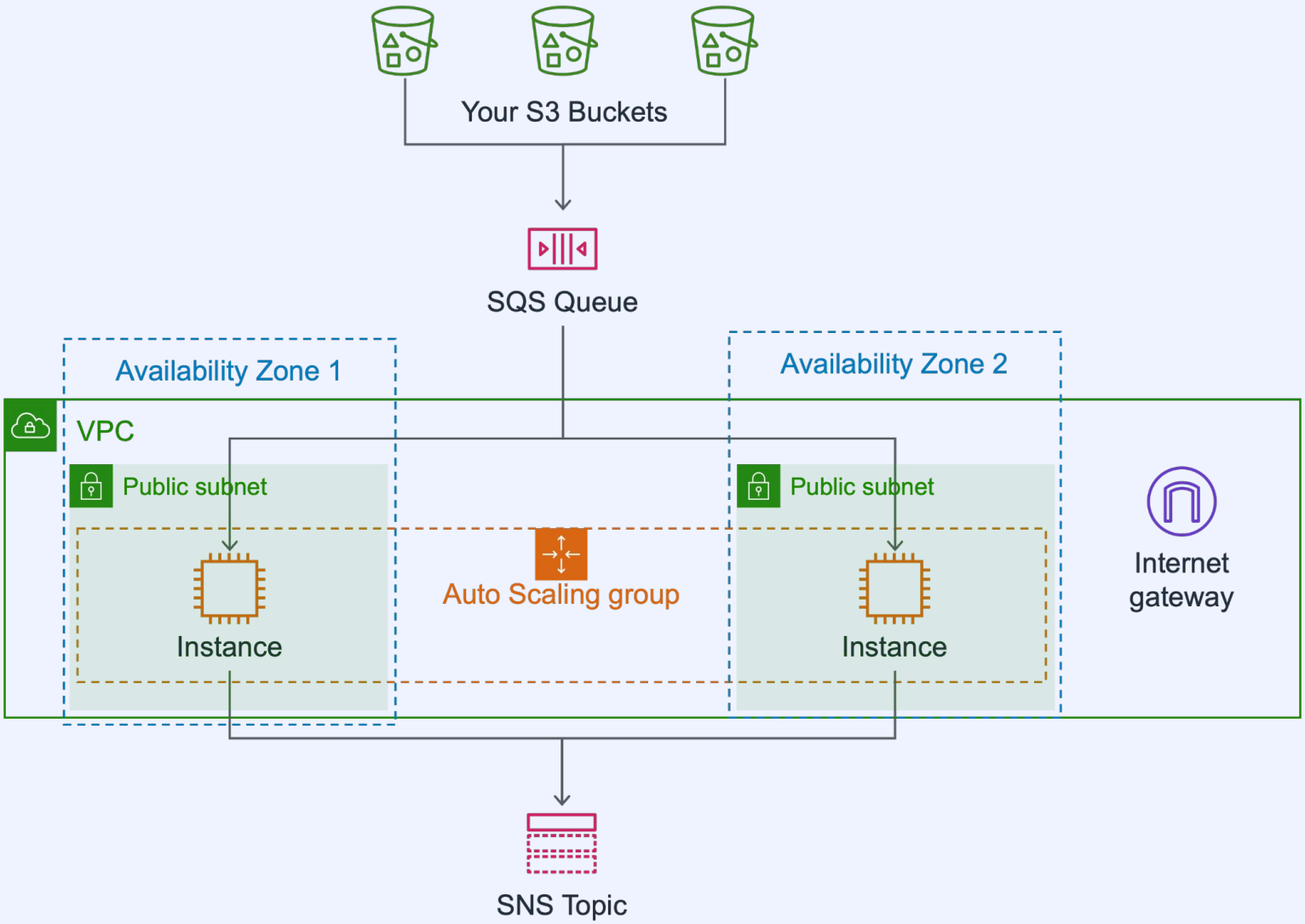
bucketAV comes with out-of-the-box malware protection for Amazon S3 and Cloudflare R2. But sometimes, you need deeper integration into specific AWS services or third-party products to implement malware scanning at the security boundaries of your architecture.

bucketAV integrates with the following products out of the box:

- Amazon Connect
- AWS Transfer Family
- Atlassian Jira
- Atlassian Confluence
- Salesforce
- WordPress

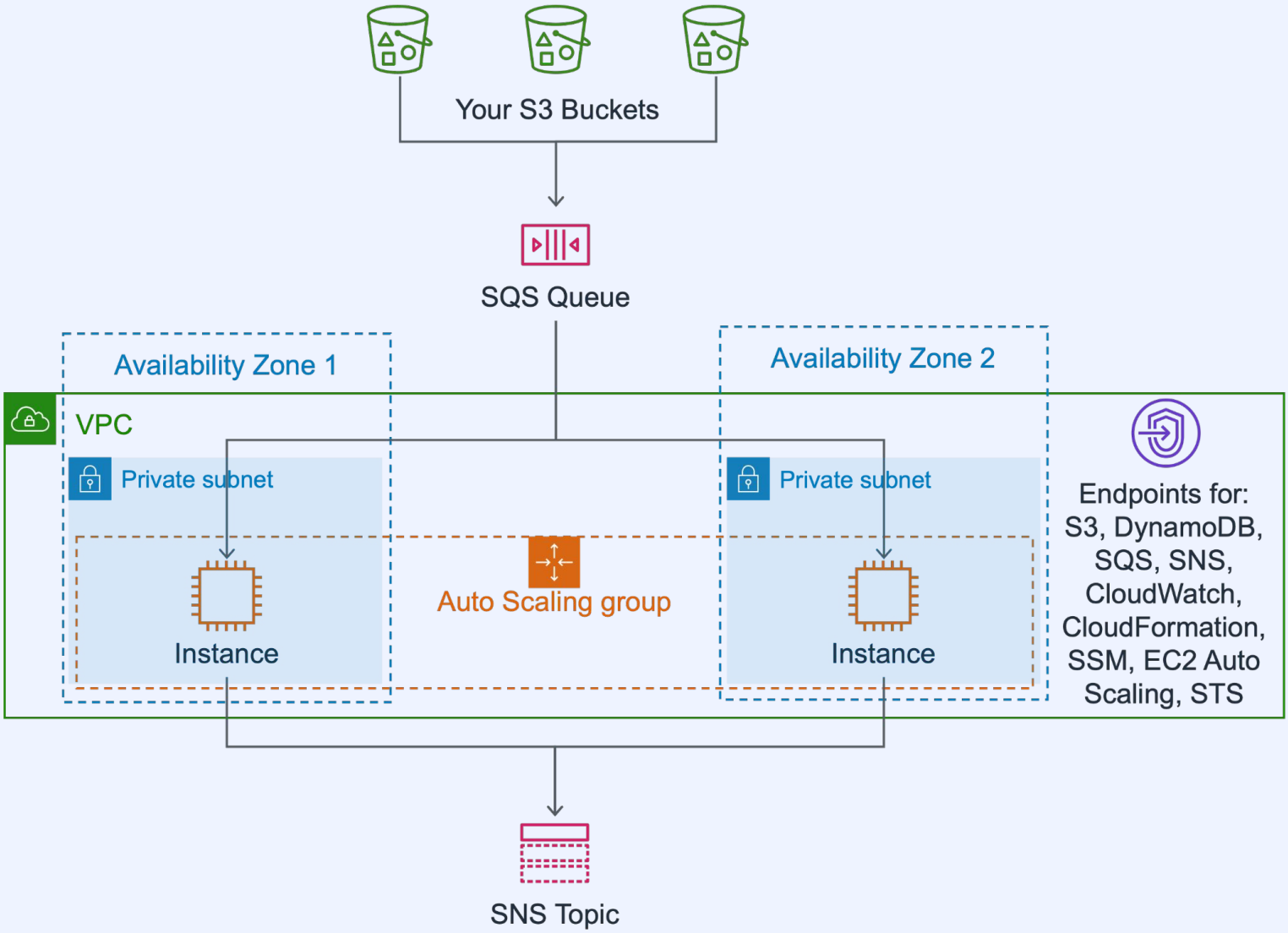
Learn more

Delivery Methods



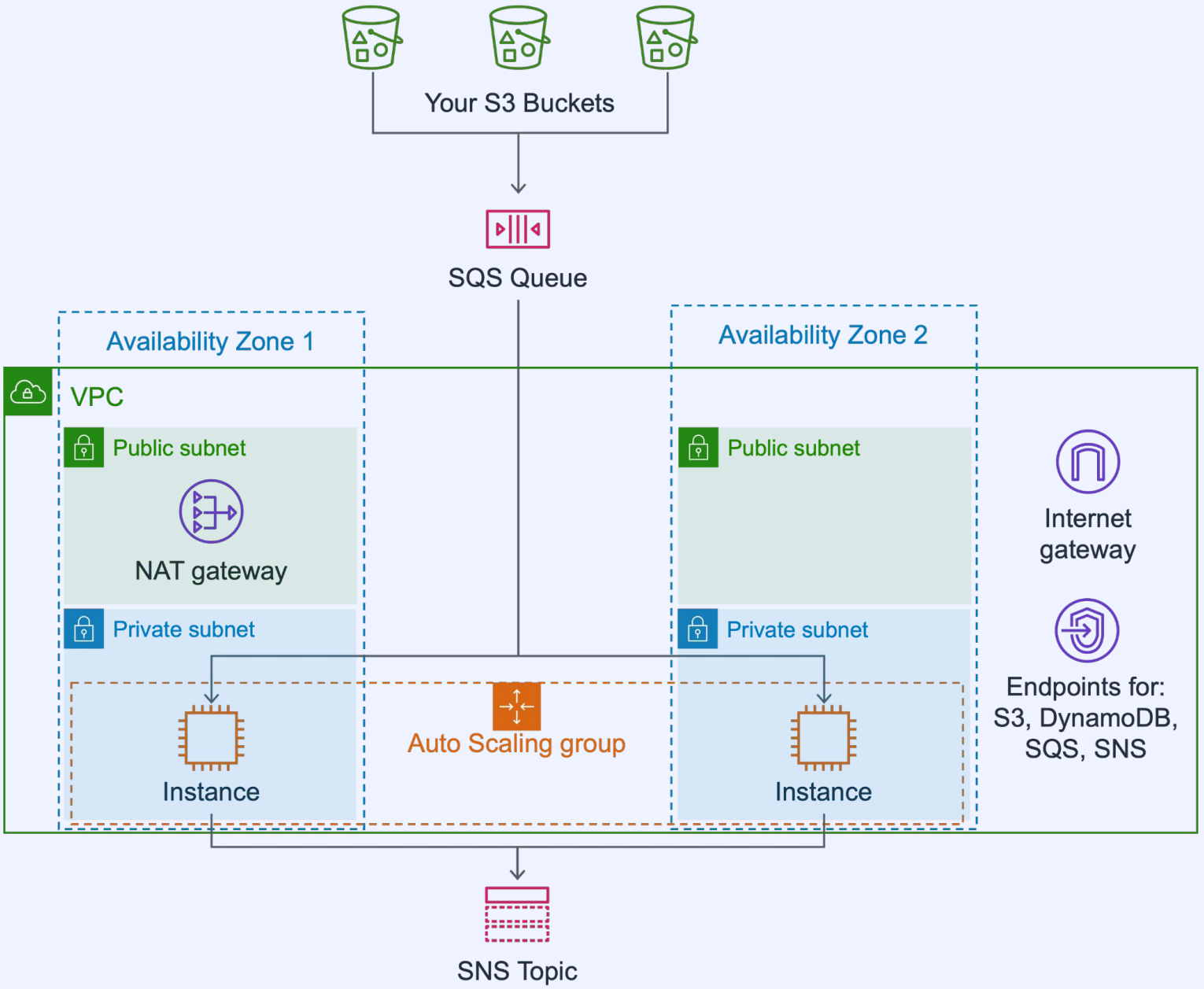
Dedicated public VPC (recommended)

- VPC (10.0.0.0/16) with Flow Logs, Internet Gateway
- Two public subnets with least privilege ACL
- EBS volume encrypted
- Least privilege IAM role
- Least privilege Security Group



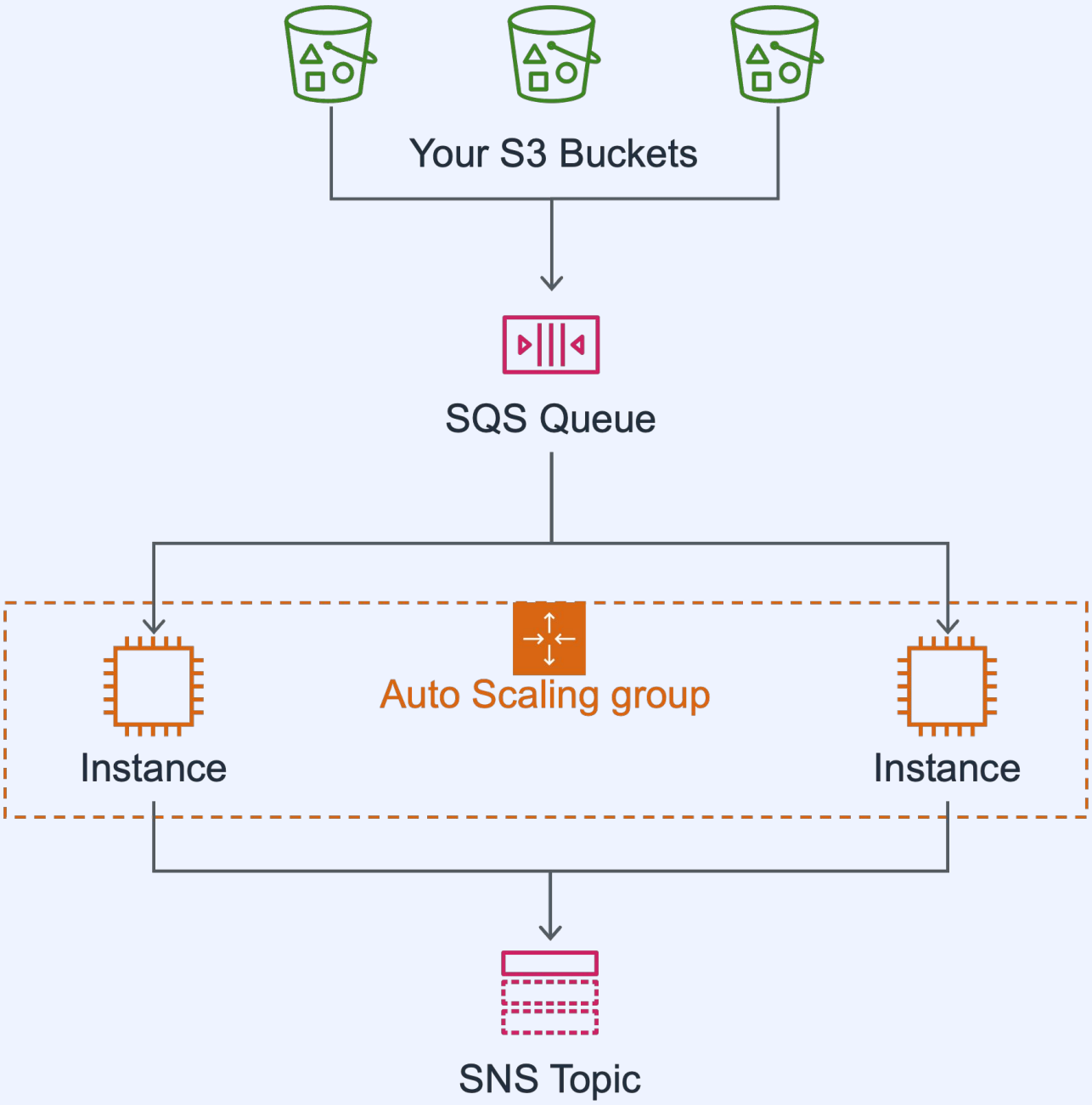
Dedicated private VPC (ClamAV)

- VPC (10.0.0.0/16) with Flow Logs
- Gateway VPC Endpoints for DynamoDB and S3
- Interface VPC Endpoints for SNS, SQS, EC2 Auto Scaling, STS, CloudFormation, CloudWatch, CloudWatch Logs, SSM
- Two private subnets with least privilege ACL
- EBS volume encrypted
- Least privilege IAM role
- Least privilege Security Group



Dedicated private VPC (Sophos)

- VPC (10.0.0.0/16) with Flow Logs, Internet Gateway, NAT Gateway
- Gateway VPC Endpoints for DynamoDB and S3
- Interface VPC Endpoints for SNS, and SQS
- Two public subnets with least privilege ACL for NAT Gateway
- Two private subnets with least privilege ACL for Scan Fleet
- EBS volume encrypted
- Least privilege IAM role
- Least privilege Security Group



Existing VPC

- EBS volume encrypted
- Least privilege IAM role
- Least privilege Security Group

Learn more about required outbound communication!

How can we help you?

You can find frequently asked questions, guides on how to install or update bucketAV and much more at https://bucketav.com/help/.

Need more help? Write us! hello@bucketav.com

bucketav.com

Antivirus protection for Amazon S3

Need more help? Write us! hello@bucketav.com