RansomStop

Architecture and Deployment Models

Overview

RansomStop supports multiple platforms and deployment options, as well as environments including on-prem, cloud IaaS and cloud PaaS. The architecture and deployment models reflect the various environments as well as the requirements and restrictions of each platform and environment.

Platforms

RansomStop, as of November 2025, supports the following platforms:

- Windows Server
- Synology NAS appliances
- AWS S3 buckets
- Google Drive / Workspace

RansomStop

Deployment Models

RansomStop has 2 different deployment models, standalone and distributed. A standalone deployment is where all the RansomStop components are hosted on the single device that is being protected, i.e. Windows Server. A distributed deployment uses a dedicated RansomStop Analyzer VM which receives events from multiple protected hosts that run the RansomStop service locally and does all ransomware detections on the dedicated Analyzer virtual machine.

Not all deployment models are available for all platforms. See platform and environment restrictions below.

On-Premise Environments

RansomStop supports Windows Servers and Synology NAS deployments on-premise.

Windows Server

These can be deployed in Standalone or Distributed models. In the standalone model, the RansomStop application runs entirely on the Windows Server that is being detected. In the distributed model, there is a service which runs on the protected Windows Server which is responsible for forwarding events and handling responses from the RansomStop Analyzer. The RansomStop Analyzer is a dedicated VM that can detect ransomware activity from multiple protected hosts.

RansomStop

Diagram: Windows Server Standalone Model

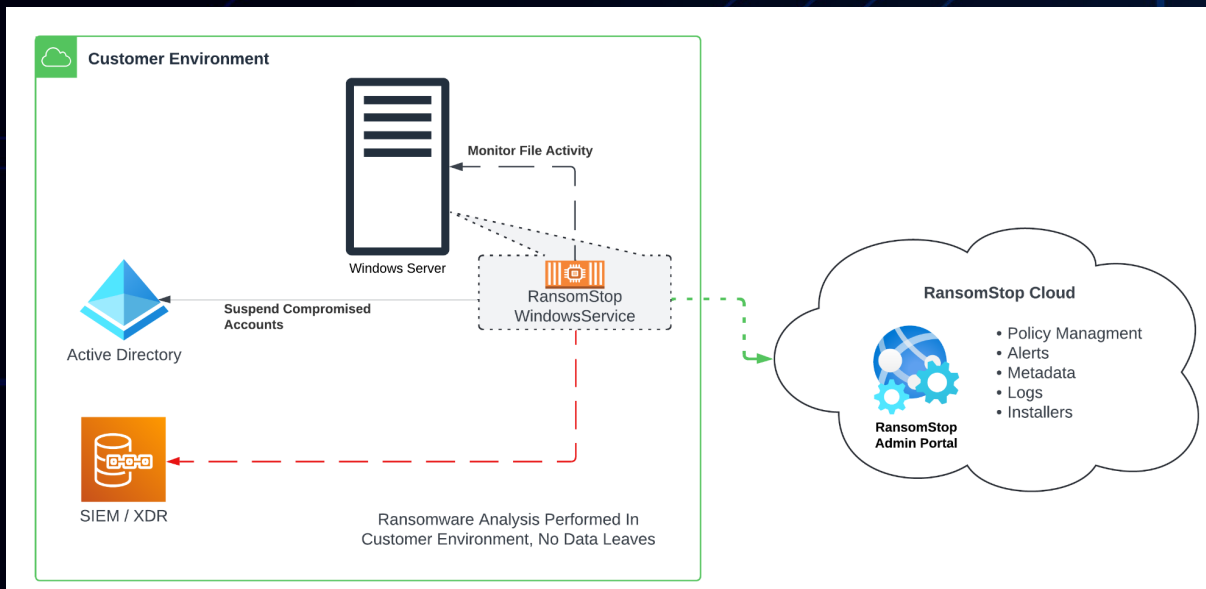
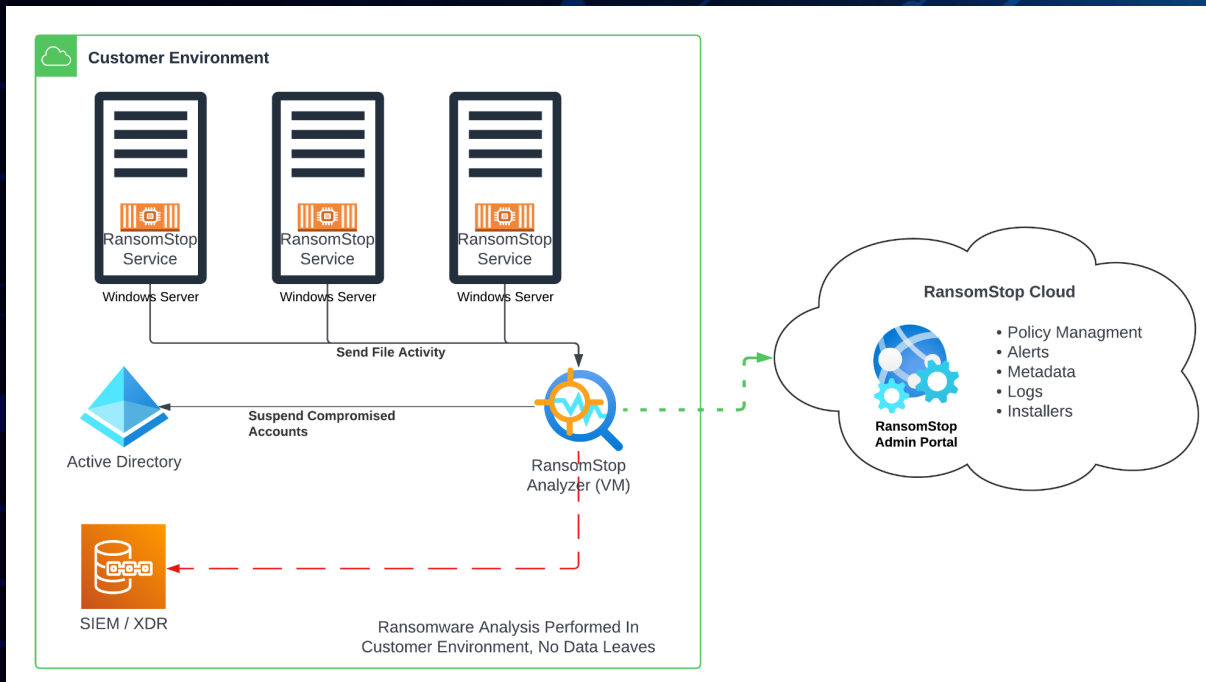


Diagram: Windows Server Distributed Model



Synology NAS

Synology NAS can only be deployed in the Distributed model. It is deployed identically to the Windows diagram above.

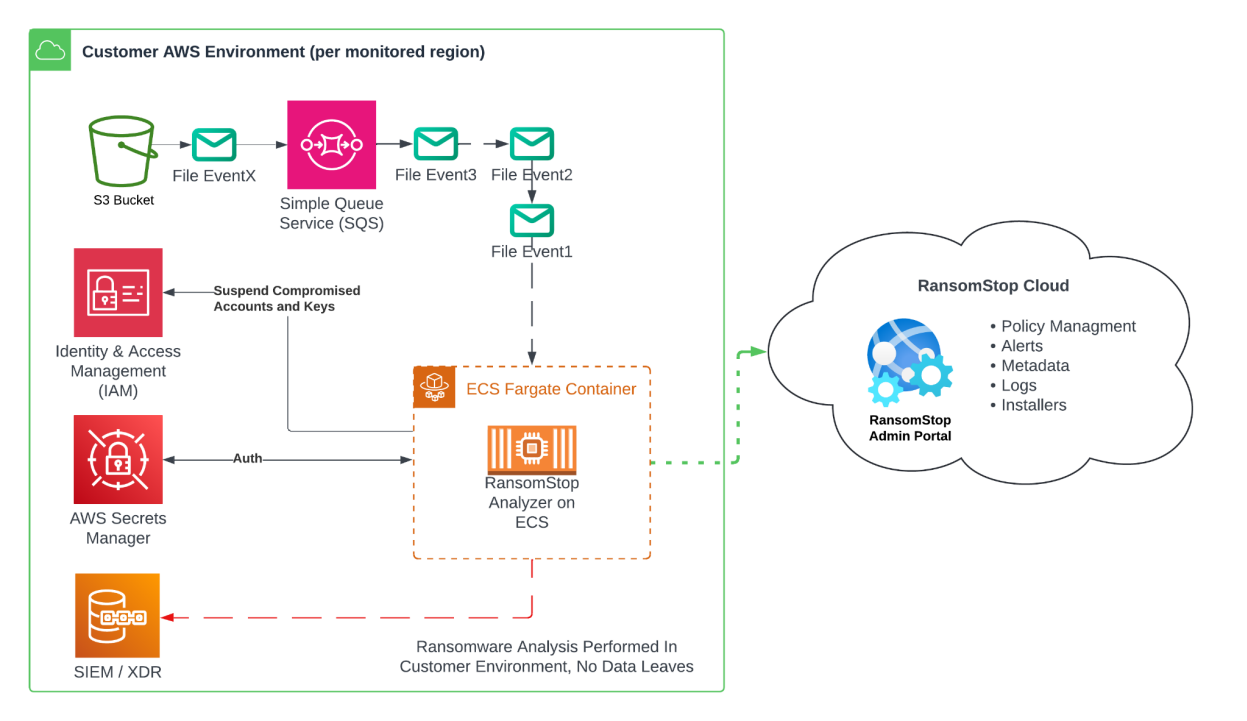
RansomStop

Cloud Environments

Amazon Web Services (AWS)

RansomStop supports detection and response for AWS S3 buckets. For AWS S3, RansomStop supports a cloud-native Distributed Model. The RansomStop Analyzer is a container that runs on Elastic Cluster Service (ECS) on Fargate (managed). It also uses SQS, Secrets Manager, and IAM services. Deployment is handled through dynamically generated CloudFront templates you can download from the RansomStop Admin Portal.

Diagram: AWS S3



Google Drive

RansomStop supports detection and response for Google Drive / Workspace. For Google Drive / Workspace, RansomStop supports a cloud-native Distributed Model. The RansomStop Analyzer is a container that runs in Google Cloud Run. There is an additional container that also runs in Google Cloud Run that provides an administrative console to configure monitored drives. It also uses Secrets Manager, FireStore, and IAM services.

RansomStop

Deployment is handled through dynamically generated bash scripts using Google CLI that you can download from the RansomStop Admin Portal.

Diagram: Google Drive