

Implementation Guide:

Alert Logic Managed Detection & Response (MDR) for AWS Control Tower

Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram.....	5
Pre-requisites	8
Deployment and Configuration Steps	9
Best Practices	13
Solution Estimated Pricing.....	13
FAQs.....	13
Additional resources.....	13
Partner contact information.....	13

Foreword

Alert Logic Managed Detection and Response (MDR) helps you identify and respond to attacks faster through seamlessly connecting an award-winning security platform, cutting-edge threat intelligence, and expert defenders.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Alert Logic MDR in an AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

Your company's security depends on being able to detect threats and respond to attacks quickly. But most organizations investigate less than 4 percent of all events they receive.

Alert Logic has a better way.

- A managed connected solution that brings an award-winning platform, cutting-edge threat intelligence, and expert defenders together
- Flexible coverage tailored to your individual business needs
- 24/7 SOC and expert remediation advice
- Simple pricing with a lower total cost than assembling your own solutions or traditional outsourcing

With Alert Logic Managed Detection and Response (MDR), you receive:

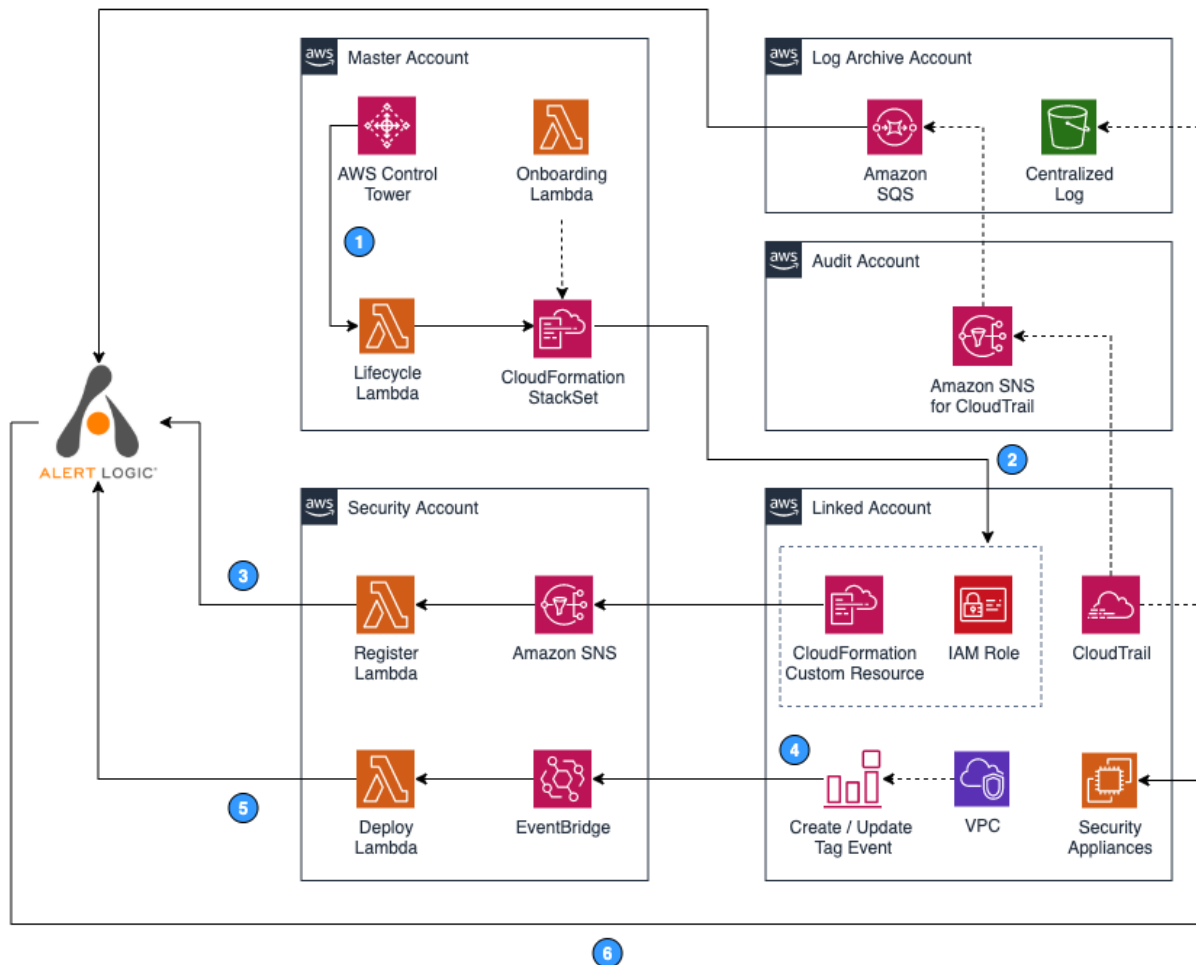
- **Threat detection** that spans the entire attack surface and operates at scale
- **Protection for your business** - including your containers and applications - with the proven combination of a network [intrusion detection system](#) (IDS), [vulnerability management](#), [log management](#), [extended endpoint protection](#) and [web application firewall](#) protection for hybrid, cloud, and on-premises environments
- **Threat intelligence based on industry data and expert security analyst research**, with machine-learning based on data analysis across thousands of customers' attack surface
- **Real-time alerting, incident verification, and remediation guidance** from experts available 24/7 with a 15-minute SLA for verified incidents.

Alert Logic MDR's integration with [AWS Control Tower](#) enables customers to automatically protect existing and newly enrolled AWS Accounts through a series of automations in response to an AWS Control Tower [LifeCycle events](#):

- Perform pre-requisite steps to setup Alert Logic MDR in the AWS account vended by AWS Control Tower [Account Factory](#)
- Register AWS account in Alert Logic MDR portal to initiate asset discovery and security assessment.
- Set up ingestion of AWS CloudTrail logs into Alert Logic MDR platform.
- Tag Amazon VPCs with Alert Logic identifiers in all AWS accounts so that they are included in the protection scope by Alert Logic MDR.
- Deploy Alert Logic MDR scanning and intrusion detection system (IDS) appliances to the target VPCs based on the protection scope.

Architecture diagram

Alert Logic MDR's AWS Control Tower Automation utilizes the following AWS Services to enable automatic protection of existing or newly enrolled AWS Accounts: [Amazon EventBridge](#), [AWS CloudFormation](#), [AWS Lambda](#), [AWS IAM](#), [AWS Secrets Manager](#), [Amazon SNS](#) and [Amazon SQS](#)



AWS Accounts presented in the architecture diagram

- Control Tower Master Account – Master account on which AWS Control Tower was enabled
- Log Archive Account – Account for centralized repository of logs including CloudTrail logs.
- Audit Account – Restricted account with read/write access to all accounts. Centralized SNS topic for security and CloudTrail notification are located here.
- Security Account – An account where Alert Logic Control Tower Automation Orchestration is deployed.

- **Linked Account** – One or more AWS Accounts protected by Alert Logic MDR. This is the account which Alert Logic Appliances and Agents are deployed into.

Overview of the Solution

The following steps are associated with numbers 1-6 indicated in the architecture diagram.

1. When a new Linked account is enrolled into AWS Control Tower, the **LifeCycle** lambda function receives a notification from AWS Control Tower and deploys AlertLogic-CT StackSet Instance to the new Linked account.
2. In the new Linked account, **AlertLogic-CT** StackSet Instance will create an IAM Role to enable Alert Logic MDR Asset Discovery. Upon completion, the stackset instance send SNS event via Custom Resource to the Security account to notify that a new deployment must be registered with Alert Logic MDR.
3. In the security account, a lambda function named **Register** is subscribed to the **ALHubTopic** SNS topic to receive new deployment registration requests from the new Linked account. Once it receives a notification request, it registers a new linked account deployment with Alert Logic MDR.
4. When user in the new Linked account tagged/untagged any VPCs with any of the following keys: "al", "alertlogic", "tm", "threatmanager", an event is published to Amazon EventBridge.
5. Lambda function named **Deploy** receives the event and updates deployment protection scope in Alert Logic MDR accordingly.
6. If 'Automatic' mode was specified during the initial setup, Alert Logic will create a security subnet in a newly protected VPC and deploy Alert Logic appliances. If 'Manual' mode was chosen, it is a responsibility of a customer to deploy Alert Logic Appliances to protect newly added VPCs. Alert Logic MDR supports two deployment mode: <https://docs.alertlogic.com/get-started/about-deployment-types.htm#Deploymenttypes>

The deployment of this solution begin with a CloudFormation stack deployed in the AWS Control Tower Master account. The stack creates 2 AWS Lambda Functions, 2 AWS CloudFormation StackSets and AWS CloudWatch Event Rule for AWS Control Tower Lifecycle. **Onboarding** Lambda are used during initial deployment to orchestrate **AlertLogic-CT** StackSets instance, creation of SQS in Log archive account and SQS to SNS subscription in Audit account. **Onboarding** Lambda also orchestrate **AlertLogic-CT-Central-IAM-Role** stackset (not shown in the diagram) to create a stackset instance in Log Archive account for CloudTrail ingestion. **LifeCycle** Lambda will be triggered by the CloudWatch Event Rule during new AWS account setup, this Lambda will deploy **AlertLogic-CT** StackSets to the new AWS account.

AlertLogic-CT stackset launches stackset instances in all AWS accounts included in the scope of deployment. In each accounts, this stackset creates an IAM role for Alert Logic MDR and CloudWatch Event rule for detecting tag changes on VPC. **AlertLogic-CT** stackset create additional resource in the Security Account including: an Amazon SNS Topic, 2 AWS Lambda Functions, and an Amazon EventBridge Event bus.

Pre-requisites

The solution doesn't require any additional resources to be enabled outside of the ones already enabled by AWS Control Tower. This guide assume you already have AWS Control Tower deployed. To get started with AWS Control Tower, check out the [Getting Started](#) documentation.

The solution requires a dedicated AWS account to be designated as Security account. The Security account must be part of AWS Control Tower managed account.

Before you implement this solution, we recommend that you become familiar with [AWS CloudFormation](#), [AWS Lambda](#), [AWS CloudTrail](#) and [Amazon EventBridge](#) services.

In addition, it is unlikely that a customer will need to increase any limits, but it is important to note that the Automation solution will create an EventBridge in the Security Account to capture tags updates in Linked Accounts.

If you are new to AWS, see Getting Started with AWS: <https://aws.amazon.com/getting-started/>.


For additional information on AWS Marketplace, see <https://aws.amazon.com/marketplace/help/about-us>.

Deployment and Configuration Steps

Step 1.1: Subscribe to Alert Logic MDR products on AWS Marketplace.

Locate the **Alert Logic MDR** in the AWS Marketplace

- [Alert Logic MDR \(US\)](#)
- [Alert Logic MDR \(UK\)](#)
- [Alert Logic MDR Professional - SaaS Contract \(US\)](#)
- [Alert Logic MDR Professional - SaaS Contract \(UK\)](#)



Alert Logic MDR Professional - SaaS Contract (UK)

Sold by: [Alert Logic](#)

Intrusion detection system, security monitoring and threat analysis, and log-based threat detection backed by Alert Logic's threat intelligence team and 24/7 Security Operation

[Show more](#)

[Continue to Subscribe](#)

[Save to list](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Product Overview

Alert Logic MDR Professional - Threat Detection and Incident Management
Includes all the capabilities in Alert Logic MDR Essentials.

Alert Logic MDR Professional provides a threat management solution that includes an intrusion detection system, security monitoring and threat analysis, and log-based threat detection. This is backed by Alert Logic's threat intelligence team and 24/7 Security Operation Centers (SOCs). Detection methods include advanced machine learning and anomaly identification, and the ability to detect AWS user behavior anomaly detection to identify potential account compromise or misuse of resources. And, Alert Logic MDR Professional works with AWS Security Hub to add additional security context with verified security incidents. This helps you quickly find unauthorized activity without having to hire your own security experts to investigate alerts, remove noise, analyze, and prioritize threats

For terms longer than 12 months, or to learn more, please contact Alert Logic at awsmarketplace@alertlogic.com

Sold by	Alert Logic
Fulfillment Method	Software as a Service (SaaS)

Highlights

- Enhance the effectiveness of AWS Security Hub, with SOC verified Alert Logic security findings.
- Streamline security in AWS by visualizing your environment with an interactive asset topology that makes it easy to drill down into your asset view to better understand your security picture.
- Discover possible issues in your deployed assets and cloud-configurations with vulnerability scanning and health monitoring.

Click on the **Continue to Subscribe** button.



Step 1.2: Guidance on Contract Duration and Renewal

In the new screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

Alert Logic MDR Professional - SaaS Contract (UK)

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

Contract Duration
 12 months

Renewal Settings
Auto Renew when this contract ends on - Thu Jun 10 2021?
 Yes
 No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services

Total Contract Price	\$0
<small>Due Today Auto Renew -Yes</small>	

Select contract Option(s)

Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.

Contract Options

25 nodes - Professional **\$31800 / Units**
25 nodes - Professional

50 nodes - Professional **\$51000 / Units**
50 nodes - Professional

100 nodes-Professional **\$75000 / Units**
100 nodes-Professional

150 nodes - Professional **\$93000 / Units**
150 nodes - Professional

Step 1.4: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button.

You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

Step 1.5: Set up Account

Once you subscribed to the solution, Alert Logic sends email validation email. Once confirmed, another email is sent to enable password reset and the access to the portal is granted.

Step 2.1: Log into Alert Logic MDR

Go to <https://console.account.alertlogic.com/#/login> to login to Alert Logic portal.

Step 2.2: Getting Started

Create API Keys to enable Automation Solution deployment. In order to do that, go to 'Manage->Users' section in the Alert Logic Portal, select existing or create new user and generate new access key id/secret in the user's Access Keys section.

Save access key id and the secret as you will need this information in order to deploy Alert Logic MDR Automation for AWS Control Tower.

For more detail, follow the user guide: <https://docs.alertlogic.com/prepare/access-key-management.htm#Generateanaccesskey>

Step 3.1: Deploy Solution in Master Account

Login in to Master account in AWS Control Tower as an Administrator. To deploy solution, select the region where your AWS Control Tower is deployed, create new CloudFormation Stack using template from:

<https://s3.amazonaws.com/alertlogic-public-repo.us-east-1/templates/ct-al-master-onboarding.yaml>

You will need to provide the following information in order to deploy CloudFormation Stack:

- AlertLogicAPIAccessKey and AlertLogicAPISecretKey generated in step 2.2.
- AlertLogicCustomerID – This can be found on the Support page in Alert Logic Portal
- OrgId – AWS Organization ID
- AuditAccount – AWS Control Tower Audit account
- LogArchiveAccount – AWS Control Tower Log Archive account
- SecurityAccount – Designated AWS security account
- IncludeOrganizationalUnits – Comma-delimited list of Organizational Units to enable Alert Logic MDR Automation for. Leave the default (ALL) to enable Automation for all Organizational units.

- ExcludeOrganizationalUnits – Comma-delimited list of Organizational Units to exclude from Automation.
- AutomationMode – Choose ‘Automatic’ if you want enable Alert Logic to automatically deploy Alert Logic MDR appliances into protected VPCs. Otherwise, select ‘Manual’ to assume responsibility of deploying Alert Logic Appliances.
- TargetRegion – List of regions to enable Alert Logic MDR Automation for.

Step 3.3: Verification Steps

Upon Cloud Formation deployment completion, you should see Shared accounts listed as deployments in Alert Logic MDR portal.

Any Stack Instances with status shown as CURRENT in AlertLogic-CT CloudFormation StackSet will be listed as deployments in Alert Logic MDR portal

Step 4.1: Validation Steps

Linked Accounts will have Alert Logic appliance automatically deployed within 15 minutes.

In addition, it is customer’s responsibility to install Alert Logic MDR Agents to protected hosts. Follow these instructions to deploy Alert Logic MDR Agents:

- <https://docs.alertlogic.com/prepare/alert-logic-agent-linux.htm>
- <https://docs.alertlogic.com/prepare/alert-logic-agent-windows.htm>

The agents will be automatically claimed and assigned to the appliances.

Step 4.2: How to use

Alert Logic MDR solution will automatically analyze network traffic, logs (CloudTrail and host logs) and scan hosts for vulnerabilities. This information can be accessed through the Alert Logic MDR Portal. Please refer to FAQ and Additional Resource sections below for more detail.

Best Practices

- AWS Cross Account Role Setup for Alert Logic MDR: <https://docs.alertlogic.com/prepare/aws-cross-account-role-setup.htm>
- Alert Logic MDR Deployment Types: <https://docs.alertlogic.com/get-started/about-deployment-types.htm>
- Configure IAM Role for AWS: <https://docs.alertlogic.com/prepare/iam-role-creation.htm>
- Create and Manage Alert Logic Access Keys: <https://docs.alertlogic.com/prepare/access-key-management.htm>

Solution Estimated Pricing

Pricing detail is available on AWS Marketplace: <https://aws.amazon.com/marketplace/pp/B07K2J16QH>

FAQs

FAQ: <https://support.alertlogic.com/hc/en-us/categories/115001241223-Frequently-Asked-Questions>

Additional resources

- <https://docs.alertlogic.com/get-started/subscriptions-addons.htm>
- <https://docs.alertlogic.com/analyze/service-status.htm>
- <https://www.alertlogic.com/managed-detection-and-response/>
- <https://www.alertlogic.com/resources/whitepapers/key-steps-in-defining-a-shared-responsibility-model-for-amazon-web-services-aws/>
- <https://www.alertlogic.com/assets/datasheets/AL-Paving-the-way-to-the-Cloud-20.pdf>
- <https://www.alertlogic.com/assets/datasheets/AL-built-for-AWS.pdf>

Partner contact information

<https://www.alertlogic.com/about-us/>