aws marketplace

Implementation Guide:

ExtraHop Reveal(x) 360- Network Detection and Response for AWS Control Tower

Table of Contents

Foreword

Defending multiple accounts on AWS requires unified visibility, threat detection, and response. With Reveal(x) 360 network detection and response (NDR) and AWS Control Tower, organizations can securely expand their presence while removing the friction caused by manually implementing guardrails or Amazon VPC Traffic Mirroring sessions for each new account.

SaaS-based Reveal(x) 360 unifies security with cloud-scale visibility, real-time advanced threat detection, and streamlined workflows to speed investigation and response from a single management pane. This unified approach eliminates the complexity of deploying and operating separate tools for each account or environment, including containerized environments such as Amazon Elastic Kubernetes Service (EKS) and AWS Fargate. Reveal(x) 360 also removes the friction caused by data silos between security and IT teams that need to collaborate closely in order to provide a safe, reliable digital experience.

Benefits of Reveal(x) 360 for AWS Security

Reveal(x) 360 unlocks network data in the cloud without the need for agents, removing deployment friction and providing elastic network detection and response (NDR) with limitless scalability. Features and benefits include:

Complete Coverage: SecOps teams can detect, investigate, and respond to threats across multiple accounts in a single management pane. Continuous monitoring and L2–L7 analysis ensure end users are always up to date and in the know.

Cloud-Scale Visibility: East-west and north-south visibility, as well as packet-level insight and out-of-band decryption of SSL/TLS 1.3 encrypted traffic at line rate, ensure that organizations always know what's happening in their AWS environment.

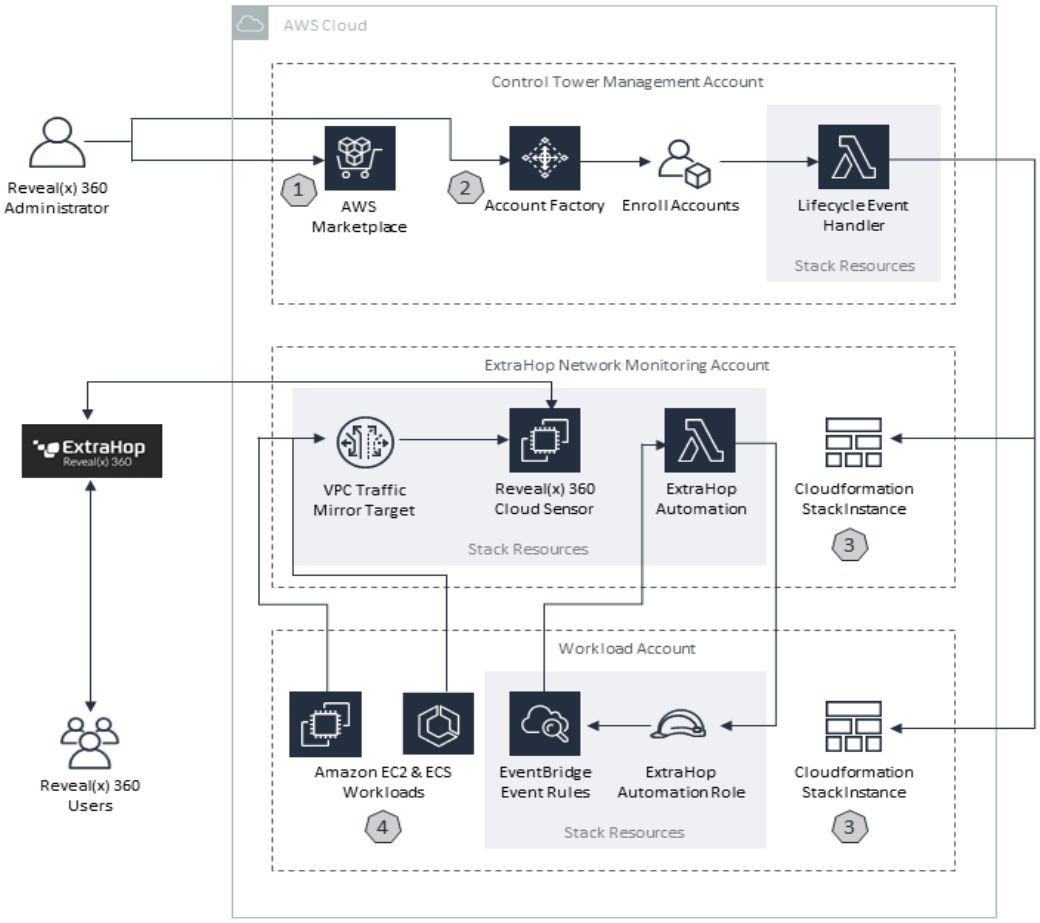
Real-Time Threat Detection: By combining machine learning-powered behavioral analysis with rules-based detection, peer group analysis, and deep learning, Reveal(x) 360 quickly identifies known and unknown threats and provides holistic coverage of attacker tactics, techniques, and procedures.

Intelligent Response: Streamlined investigation workflows enable security teams to go from alert to response in clicks, not days. For deeper context, analysts can dig into a cloud-based record store with 90-day lookback.

Low-Friction Deployment and Management: As a SaaS-based solution that doesn't require agents, instrumentation, or configuration, Reveal(x) 360 deploys quickly in public cloud and on-premises environments. For AWS environments, you can deploy on-demand sensors directly from the Reveal(x) 360 management pane.

Immediate Value: Reveal(x) 360 passively monitors network traffic across environments and starts learning complex relationships through continuous asset discovery, classification, and mapping as soon as it's deployed.

Architecture Diagram



A Reveal(x) 360 Administrator:

1. **Subscribes** to ExtraHop SaaS and BYOL Listings on AWS Marketplace.
2. **Deploys** the ExtraHop-ControlTower-Lifecycle CloudFormation Stack in the Control Tower Management Account.
3. **Enrolls** AWS Accounts in Control Tower Management which creates a CloudFormation StackSet Instance based on the type of Account enrolled.
4. Mirrored network traffic from EC2 and ECS Workloads in Workload Accounts **is automatically delivered** to the Reveal(x) 360 Sensor.

Reveal(x) 360 Users:

1. Use Reveal(x) 360 to Identify and Respond to advanced threats against cloud workloads.

Prerequisites

Below is a high-level description of each ExtraHop and AWS prerequisite required to use ExtraHop Reveal(x) 360 with AWS Control Tower. Apart from configuring your Control Tower Landing Zone, this guide's Deployment and Configuration Steps section includes detailed configuration steps for each prerequisite.

Prerequisite Summary:

1. **ExtraHop:** a Reveal(x) 360 Tenant
2. **ExtraHop**: a Reveal(x) 360 user account
3. **ExtraHop**: two sets of Reveal(x) 360 API Keys
4. **ExtraHop**: subscription to Reveal(x) Ultra Sensor listings on AWS Marketplace
5. **AWS**: AWS Control Tower Landing Zone
6. **AWS**: AWS Service Quota increase for active VPC Peering Connections
7. **AWS**: a CIDR range to use for a new VPC that does not overlap with your existing VPC CIDRs
8. **AWS**: Organizations integrations with Marketplace, License Manager, and Resource Access Manager

ExtraHop Reveal(x) 360

Marketplace Subscriptions

This guide requires an active Reveal(x) 360 subscription. Deployment and Configuration Step 1 "Complete Prerequisites" walks through initiating a Free Trial for those who do not already have an active Subscription.

Active Tenant

If you do not already have a Reveal(x) 360 Tenant, this Guide walks you through signing up for a Free Trial via the SaaS NDR AWS Marketplace Listing to get one provisioned.

User Account

Once your Tenant is provisioned, you will need to create a user account to view all packet analysis and threat detection results in the Reveal(x) 360 Console.

REST API Credentials

To provide context to SOC Analysts using Reveal(x) 360, ExtraHop Automation will synchronize EC2 inventory and detection data to/from Reveal(x) 360 using the Reveal(x) 360 REST API. Separate API credentials are needed to synchronize metadata and detection data.

Amazon Web Services

AWS Control Tower

This guide assumes you have already enabled AWS Control Tower. To get started with AWS Control Tower, check out the Getting Started documentation. Before you implement this solution, we recommend that you become familiar with AWS CloudFormation, AWS Lambda and Amazon EventBridge services.

This guide assumes you have disabled Control Tower VPC Creation for new accounts created by Account Factory.

- If you are new to AWS, see Getting Started with AWS.
- For additional information on AWS Marketplace, see About AWS Marketplace.
- Refer to Getting Started with Control Tower for a Control Tower tutorial.

IP Address Space Management

The ExtraHop Sensor in the Network Monitoring Account is an Amazon EC2 Instance that will be created in a new VPC. This ExtraHop VPC will connect to your Workload VPCs using VPC Peering Connections, which require that CIDRs between peered VPCs not overlap. This guide assumes you are able to identify a CIDR to assign the ExtraHop VPC that will not conflict with Workload VPCs in your Workload AWS Accounts.

Service Quotas

Your Reveal(x) Sensor's VPC needs connectivity to workload VPCs to enable ingestion of mirrored network traffic. While it is possible to use AWS Transit Gateway for this purpose, it is preferable to use VPC Peering Connections to optimize costs, as AWS does not charge for same-AZ traffic between two VPCs.

Because the default Service Quota for Active VPC Peering Connections is 25, this guide implements a Service Quota request template in the AWS Organizations Management Account to automatically handle raising the service quota to the maximum of 125 per VPC.

Marketplace and License Manager

To enable automatic Reveal(x) Sensor provisioning, Control Tower Member Accounts must be entitled to use the AWS Marketplace Subscriptions entered into by the Control Tower Management Account.

Your ExtraHop Network Monitoring Account is entitled to deploy Reveal(x) Sensors via a Distributed Grant from AWS License Manager. Integrating AWS Organizations with both AWS Marketplace and AWS License Manager will enable the ExtraHop-ControlTower-Lifecycle Lambda Function to create and activate the needed Grants.

Organizations and RAM

This guide will use AWS Resource Access Manager (RAM) to ensure your ExtraHop Traffic Mirror Target is properly shared to all Workload Accounts. Verify you have enabled RAM sharing with AWS Organizations.

Deployment and Configuration Steps

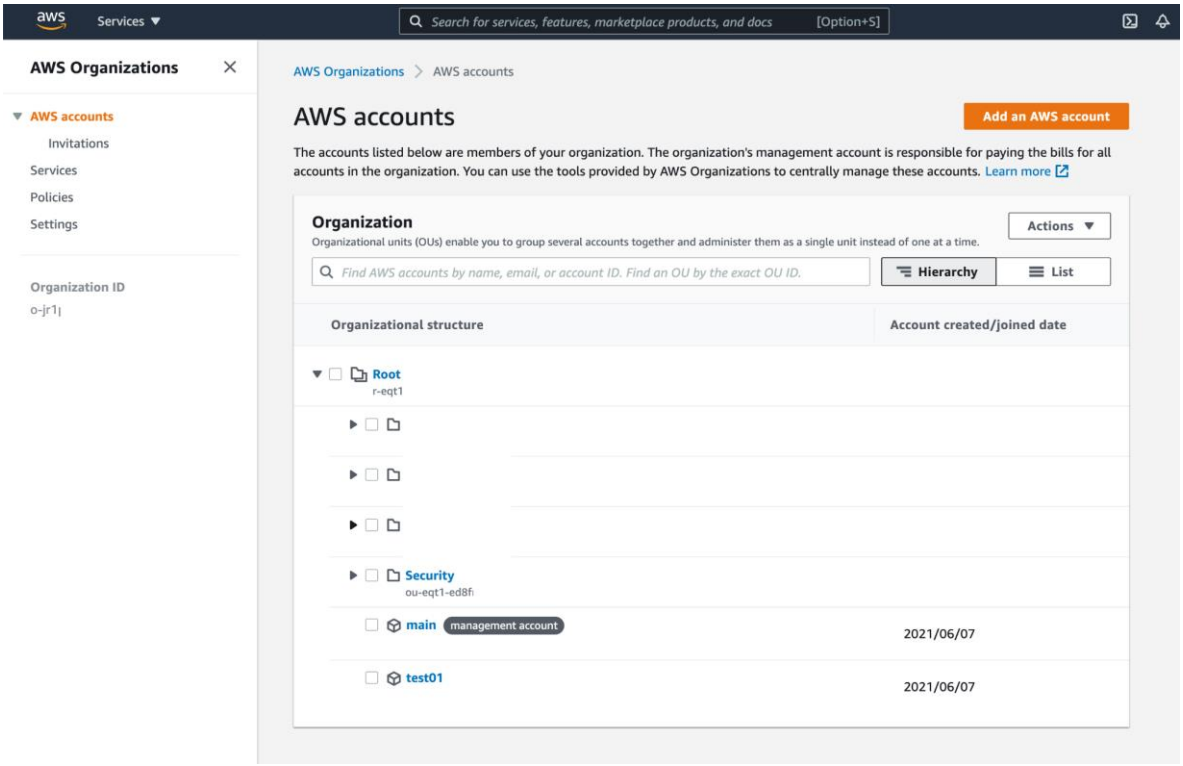
You will complete the following steps:

- Complete Prerequisites
- Prepare and Create Accounts
- Configure Reveal(x) Sensor
- Validate Deployment

1. Complete Prerequisites

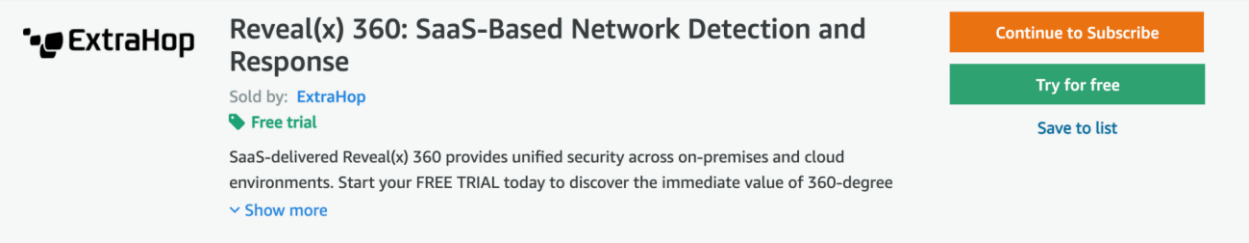
Step 1.1: Subscribe to ExtraHop Reveal(x) 360

Sign into the AWS Console using your Control Tower Management Account. To confirm which Account is designated the "Management" Account, search for the **AWS Organizations** service and view the **Accounts** page.

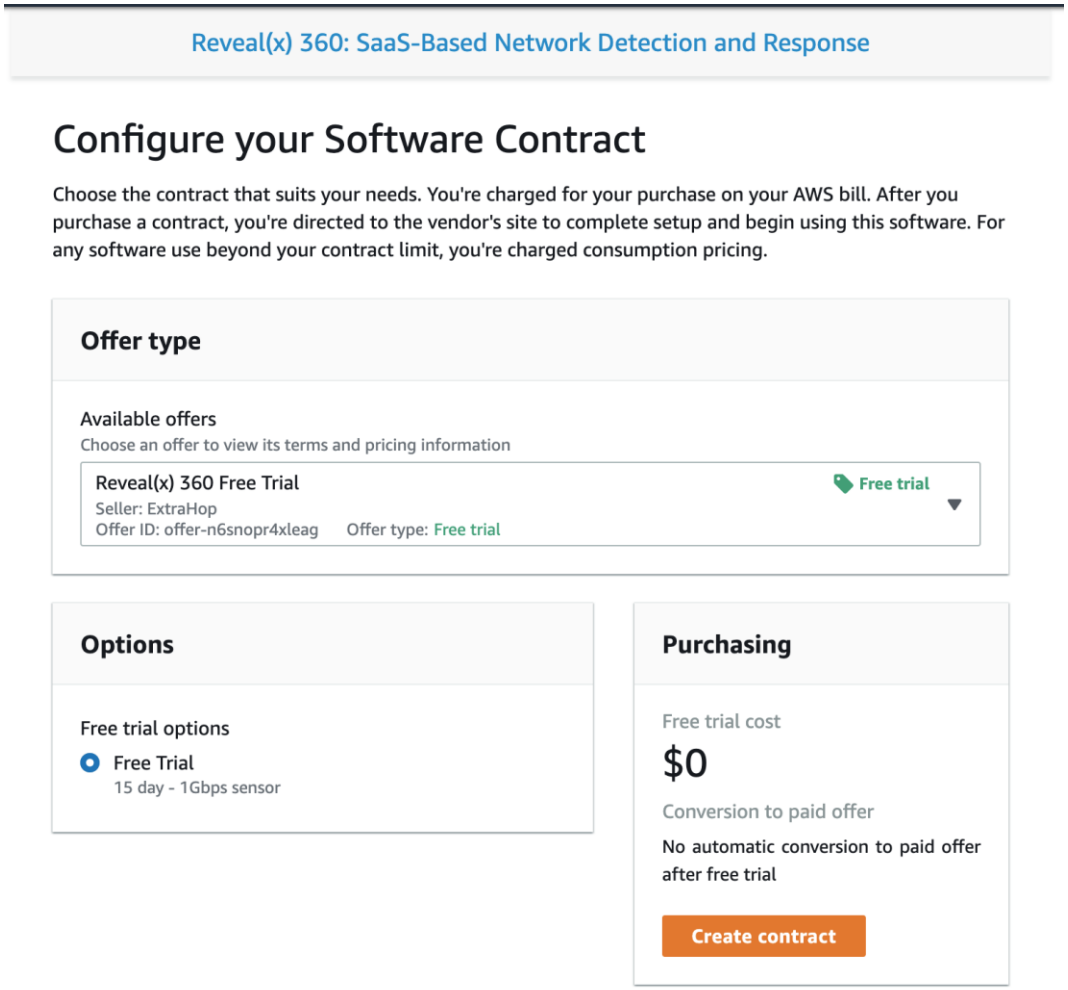


Locate Reveal(x) 360: SaaS-Based Network Detection and Response in the AWS Marketplace.

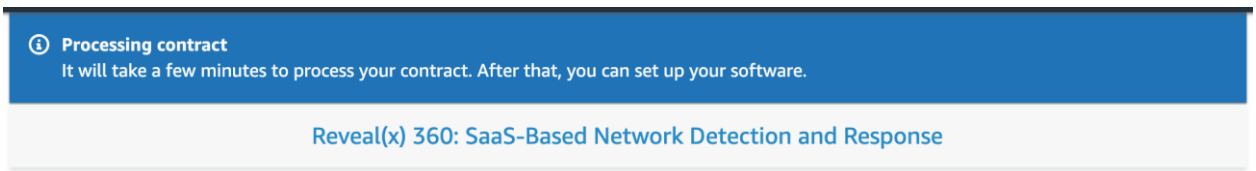
Click **Try for free**.

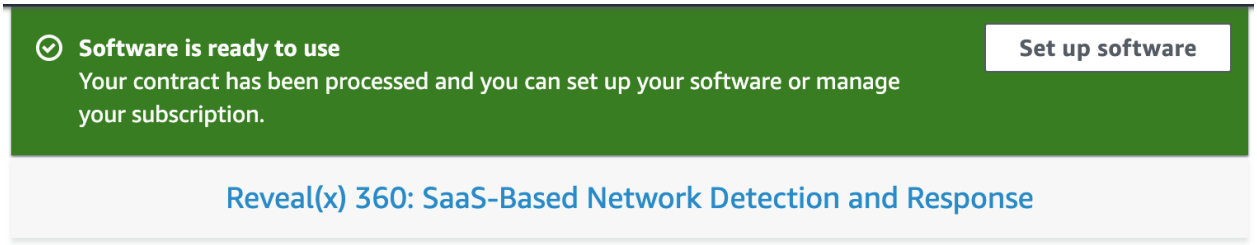


Click **Create contract**. On the subsequent screens, click **Accept the contract**, and **Close.**



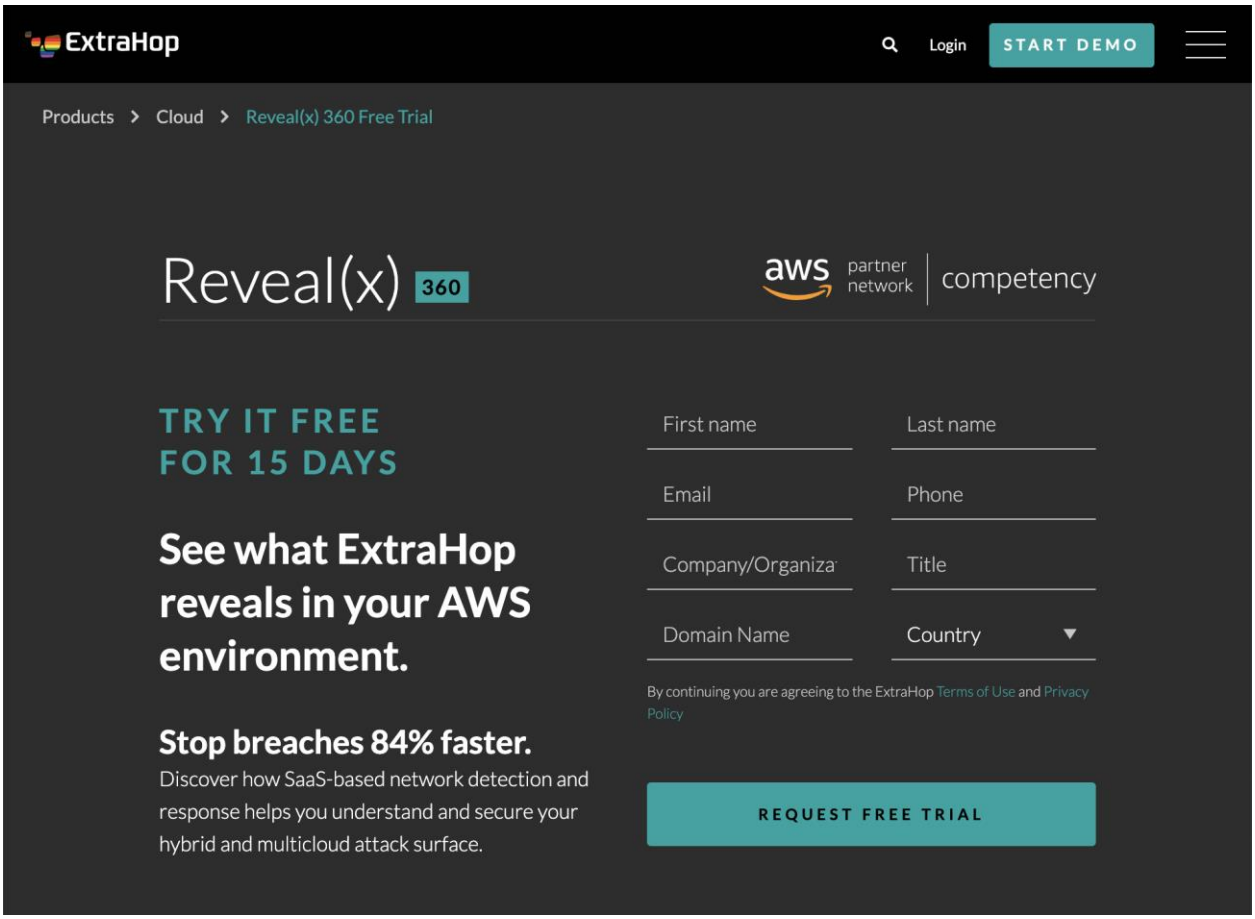
Stay on the "Configure your Software Contract" page until the notification at the top changes from "Processing contract" to "Software is ready to use". Then click **Set up software.**





You will be directed to: **https://www.extrahop.com/products/cloud/free-trial/**

Enter the following information to initiate your Tenant Provisioning:



NOTE: For **Domain Name**, enter an shorthand abbreviation for your company/organization. The **Domain Name** you select will appear as part of your unique Reveal(x)360 Console URL, which takes the form: `https://<customername>.cloud.extrahop.com`

Note the value you use. You will supply this **Domain Name** as a CloudFormation parameter in Step 2.1 below.

After Subscribing to the SaaS listing, ExtraHop will create a unique Reveal(x) 360 Tenant and send a "Welcome" email to the AWS Account's primary email address with instructions on how to log in to the new Tenant.

> NOTE: It may take up to two business days for you to receive the Welcome email.

Step 1.2: Create Reveal(x) 360 User Account

Once your Tenant is provisioned, complete the initial setup steps to add at least one user who can log into the Reveal(x) 360 Console with **ApplianceAdmin** or **FullWrite-FullPacketsWithKeys** privileges. This is required to view any packet analysis and detected threats from your AWS environment.

Step 1.3: Create Reveal(x) 360 API keys

Log into your Reveal(x) 360 Console at `https://<customername>.cloud.extrahop.com` and enable the REST API.

Create two sets of API Credentials: one called `MetadataSync` and the other called `DetectionSync` with permissions configured as follows:

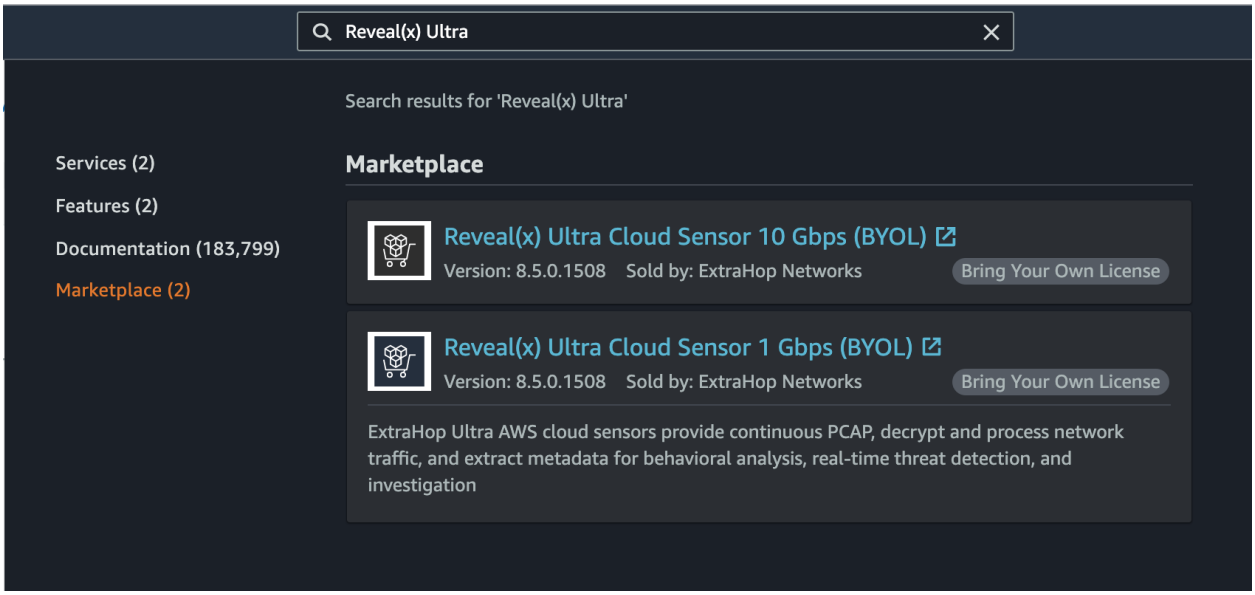
Reveal(x) 360 API Credentials:

Name	Permission Level	Packet Access	Detection Access
`MetadataSync`	Full write privileges	No access	No access
`DetectionSync`	Full read-only privileges	No access	Full access

> NOTE: Record the API ID and Secret at creation time. The API Secret cannot be retrieved afterwards.

Step 1.4: Subscribe to Sensor Listings

Sign into the AWS Console of your AWS Control Tower Management Account, and search for the **Reveal(x) Ultra Sensor** listings on AWS Marketplace.



Subscribe to both Reveal(x) Ultra Cloud Sensor listings (1 Gbps and 10 Gbps). Subscribing to all BYOL Sensor Listings at the outset of your deployment enables flexibility to change sizes as your network traffic analysis needs change over time.

Search for the **AWS Marketplace Subscriptions** service and review the **Manage subscriptions** page to confirm both Sensor size listings appear.These subscriptions can take a few minutes to become available.

Step 1.5: Disable Control Tower New VPC Creation

Remain signed in to your Control Tower Management Account and search for the AWS Organizations service. On the Account Factory page, click the **Edit** button in the **Network configuration** section.

Uncheck the boxes for all Regions to ensure that Control Tower does NOT create a default VPC for any new accounts. Click **Save**.

Step 1.6: Confirm All Organizations Features Enabled

Remain signed in to your AWS Control Tower Management Account and search for the AWS Organizations service. Review the Settings page and verify that **"Your organization has all features enabled."** The 'all features' setting is enabled by default in AWS Control Tower environments.

> NOTE: This AWS User Guide provides instructions for Enabling all Features in AWS Organizations.

Step 1.7: Enable Resource Access Manager

Remain signed in to your AWS Control Tower Management Account and follow the steps to Enable resource sharing with AWS Organizations to enable the Resource Access Manager service.

NOTE: Resource Access Manager must be enabled from the RAM Service. Do NOT Enable trusted access via the AWS Organizations Service.This will result in the needed Service Role not being properly created, which will prevent Resource Shares from being created later.

Step 1.8: Increase PCX Service Quota

Remain signed in to your AWS Control Tower Management Account and search for the **Service Quotas** service. To enable Quota request templates, you will need to change your Region to **us-east-1 (N. Virginia)**, even if this is not your Control Tower "home region".

On the **Quota request template** page, click the **Enable** button and **Add quot**a as follows:

Quota Request Template Values:

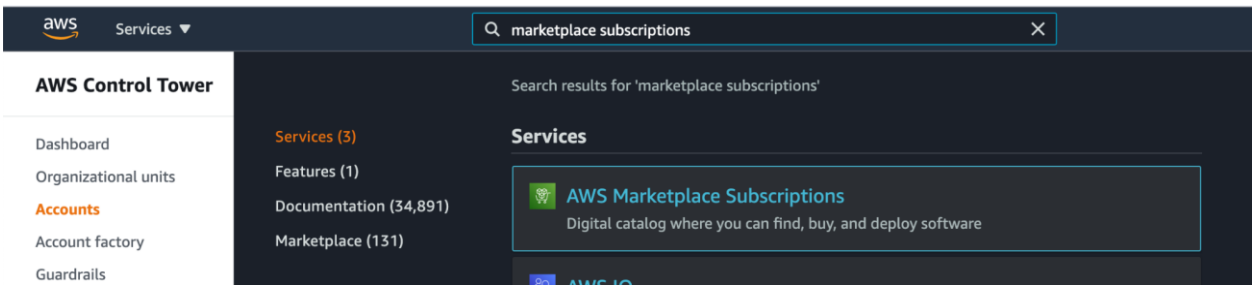
Region	Your Control Tower Home Region
Service	Amazon Virtual Private Cloud (VPC)
Quota	Active VPC peering connections per VPC
Desired quota value	125

NOTE: You must submit a separate quota request template for each Region where you plan to deploy a Reveal(x) sensor.

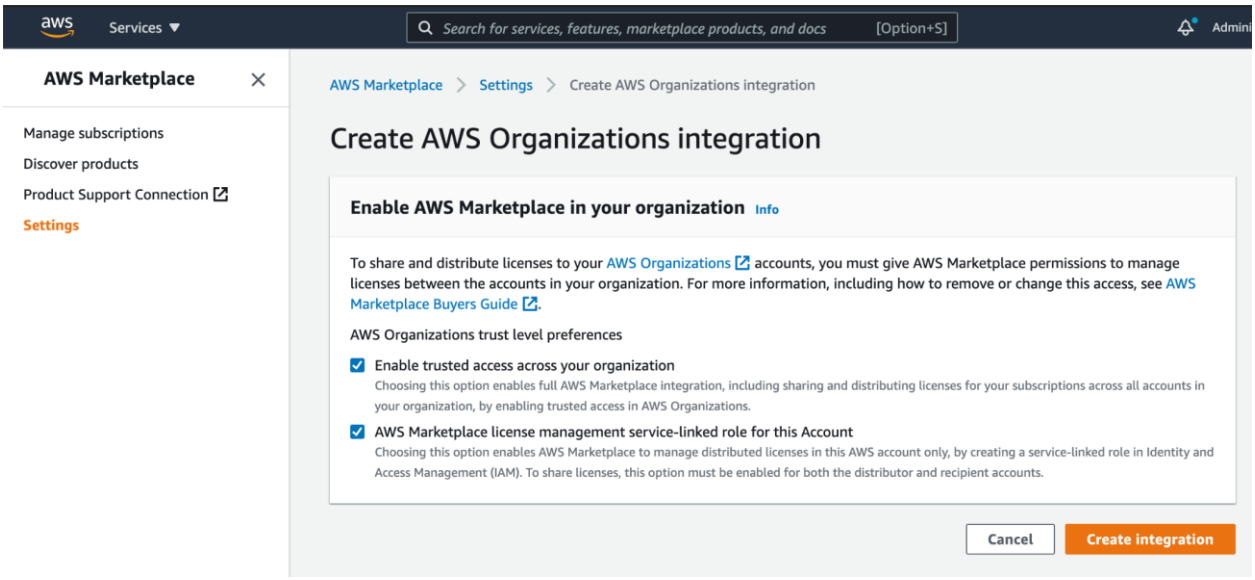
NOTE: After taking effect, this Service Quota increase will apply to newly created Accounts in this Organization. This will be required for the ExtraHop Network Monitoring Account you will create in Step 2 below.

Step 1.9: Integrate AWS Marketplace with AWS Organizations

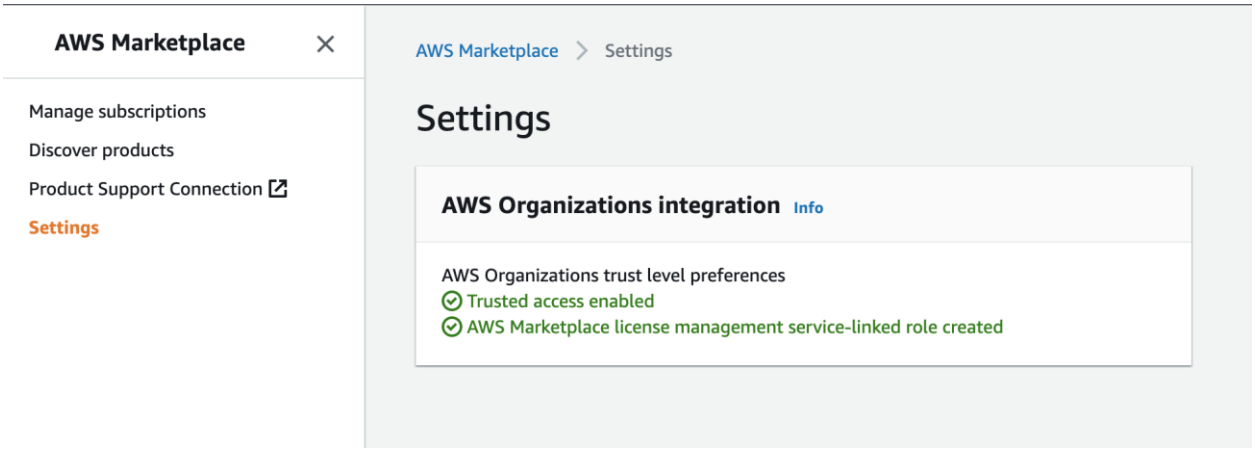
Sign into the AWS Console using your Control Tower Management Account and search for the **AWS Marketplace Subscriptions** service.



On the Settings page, click **Create Integration.** On the subsequent screen, check the two boxes to **Enable AWS Marketplace in your organization**, and click **Create Integration**.



Review the Settings page to confirm Marketplace-Organizations Integration is complete:



Step 1.10: Enable AWS License Manager

Remain in the AWS Marketplace service, and navigate back to the **Manage subscriptions page**.

Follow the steps for Sharing subscriptions in an organization to enable AWS License Manager to distribute entitlement Grants to your Organization's AWS accounts for your Reveal(x) AWS Marketplace subscriptions.

Step 1.11: Integrate License Manager with Organizations

Sign into the AWS Console using your AWS Control Tower Management Account and search for the **AWS License Manager** service. Click the Settings page and note that the status for **Link AWS Organizations accounts** is **Not completed**. Switch your Region to **US East (N. Virginia)** and **Edit** your account settings to enable the link between Organizations and License Manager.

NOTE: You must complete this step in **US East (N. Virginia)** even if your AWS Control Tower Home Region is elsewhere. The us-east-1 Region is the "Home Region" for the AWS License Manager service, which handles replicating grant status to all Regions in the background when you subscribe to AWS Marketplace Listings from your AWS Control Tower Home Region.

2. Prepare and Create Accounts

In this step, you will:

- Deploy a CloudFormation stack in your AWS Control Tower Management Account
- Use the Account Factory to create two new AWS Accounts.

The CloudFormation stack you deploy in the AWS Control Tower Management Account includes a Lambda Function which will act on Accounts created using Account Factory, creating the necessary resources to onboard them to your Reveal(x) 360 deployment.

Step 2.1: Create the ExtraHop-ControlTower-Lifecycle Stack

In this step, we will use CloudFormation to deploy the ExtraHop-ControlTower-Lifecycle stack, which lays the foundation for your Reveal(x) 360 deployment. This stack includes a Lambda which will process the AWS Control Tower lifecycle events, as well as two CloudFormation StackSets which create the relevant AWS resources in your Network Monitoring Account and Workload Accounts. Refer to the Architecture Diagram for a high-level overview of these AWS resources and how they interact with each other.

Sign into the AWS Console using your Control Tower Management Account and search for the CloudFormation service. Click **Create stack** and select **With new resources (standard)**.

To **Specify template**, enter the following **Amazon S3 URL**:

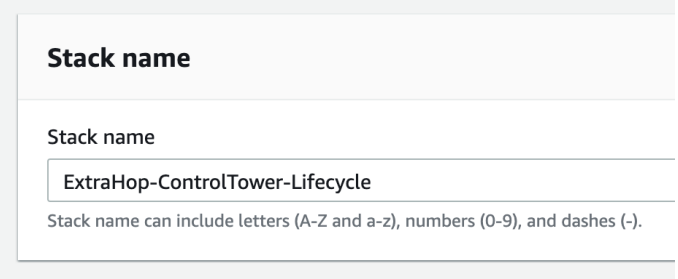
`https://extrahop-onboarding-<region-name>.s3.<region-name>.amazonaws.com/public/controltower-management-account.yaml`

NOTE: Substitute your Control Tower "home Region" name for **<region-name>** in the S3 URL. For example: `https://extrahop-onboarding-us-west-2.s3.us-west-2.amazonaws.com/public/controltower-management-account.yaml`

Currently supported Regions include:

- `us-east-1`
- `us-east-2`
- `us-west-1`
- `us-west-2`

Click **Next** and to review **Stack Details**. Give your Stack a name such as **ExtraHop-ControlTower-Lifecycle.**



Most users should use the suggested default Parameter settings.

Configure the Stack Parameters as Follows:

Parameter Group: Reveal(x) 360

Parameter	Value
Tenant Name	Must match the **Domain Name** selected in Step 1.1
MetadataSync API Id	Must match the ID for the **MetadataSync** credential created in Step 1.3 with **Full Write** privileges
MetadataSync API Secret	Must match the Secret for the **MetadataSync** credential created in Step 1.3 with **Full Write** privileges
DetectionSync API Id	Must match the ID for the **DetectionSync** credential created in Step 1.3 with **Full Read Only with Detections Access** privileges
DetectionSync API Secret	Must match the Secret for the **DetectionSync** credential created in Step 1.3 with **Full Read Only with Detections Access** privileges

Parameter Group: Network Monitoring Account

Parameter	Value
Notification Recipient	Must be an email address that can receive SNS notifications

Parameter Group: ExtraHop VPC

Parameter	Value
VPC CIDR	Must be a CIDR that does not overlap with existing VPC CIDRs
Public Subnet CIDR	Must be a subnetwork of the VPC CIDR Parameter
Private Subnet CIDR	Must be a subnetwork of the VPC CIDR Parameter
Sensor Ingest Subnet CIDR	Must be a subnetwork of the VPC CIDR Parameter

Parameter Group: Reveal(x) Sensor

Parameter	Value
Sensor Model	Must match the Sensor Model of your BYOL License
Sensor Elastic IP	true
Remote Access CIDR	The IP address range from which you will log in to the Sensor via HTTPS. Common values include a VPN CIDR or a work-from-home user's public IP address expressed as a /32.

Click **Next** to **Configure stack options**. No custom stack options are needed. Click **Next** to review selections.

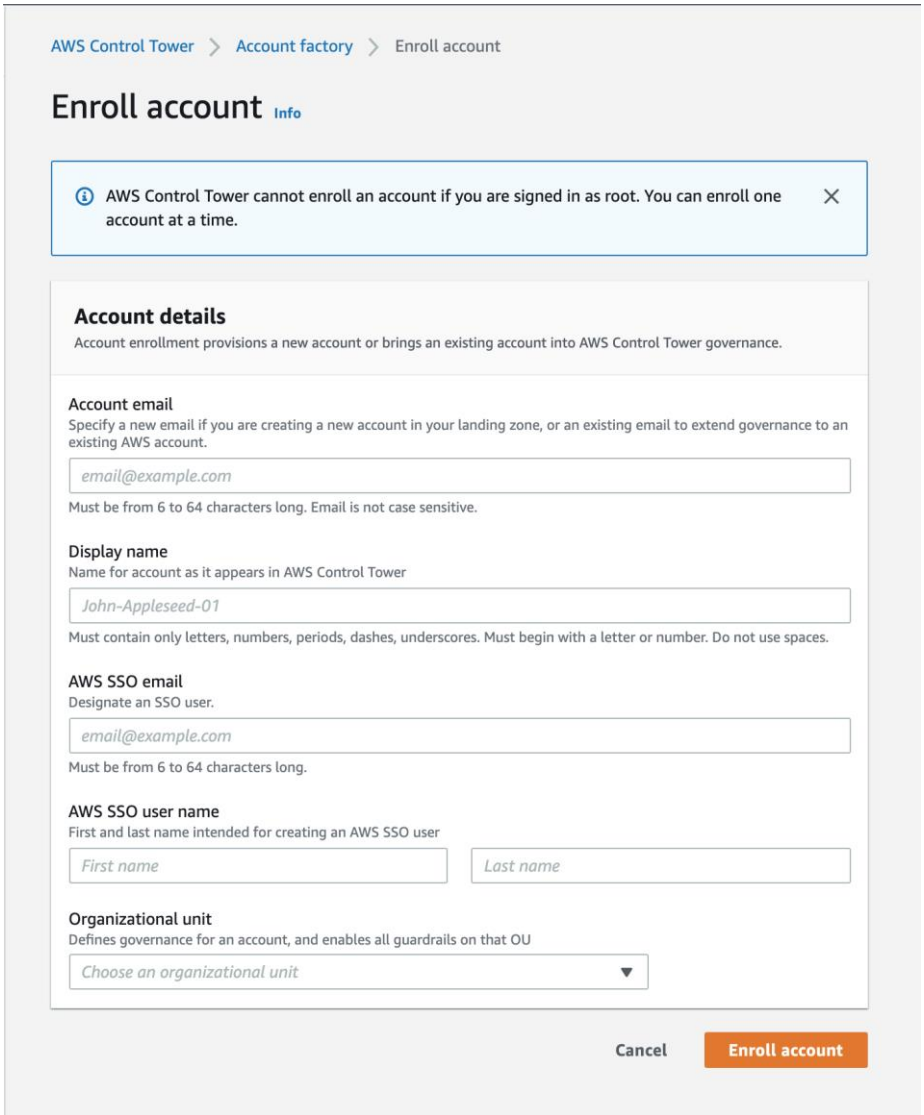
> NOTE: While reviewing selections, you have the option to save a Quick Create link that contains your Parameter selections.

Review the selections and scroll down to accept **I acknowledge that AWS CloudFormation might create IAM resources with customer names** and choose **Create stack.**

A successful stack creation will show a status of **Create Complete**.

Step 2.2: Use Account Factory to Vend a New Network Monitoring Account

Sign into the AWS Console using your Control Tower Management Account and search for the Control Tower service. On the **Account factory** page, click **Enroll account**. Provide details for this dedicated ExtraHop Network Monitoring Account.



Recommended new Account Parameters:

Parameter	Value
Account email	An email address like user+netmon@company.com (see NOTE below)
Display name	Must be **ExtraHop-NetworkMonitoring**
AWS SSO user email	The AWS Control Tower Management Account SSO user's email address
AWS SSO user name	The AWS Control Tower Management Account SSO user's first and last name.
Organizational unit	Must be an OU that is already enrolled in AWS Control Tower.

NOTE: This AWS Root Account email should be a new distribution list or shared mailbox, never a single individual's mailbox. This Root user is separate from the SSO user you will specify below. This Root user will get a randomly-generated 25+ character password by default which can be reset via the "Forgot Password" process if necessary.

NOTE: Specifying the SSO user email and user name of the AWS Control Tower Management Account user will let Account Factory automatically assign this user AdministratorAccess in the newly created account.

NOTE: Account Factory can take up to 30 minutes to finish creating a new Account. Refer to Create or Enroll an individual account for more information.

This Guide will refer to this account as your "ExtraHop Network Monitoring Account" or "Network Monitoring Account".

During this enrollment process, the ExtraHop-ControlTower-Lifecycle Lambda Function processes the `CreateManagedAccount` event and creates the Extrahop-NetworkMonitoring-Account CloudFormation StackSet in the Network Monitoring Account.

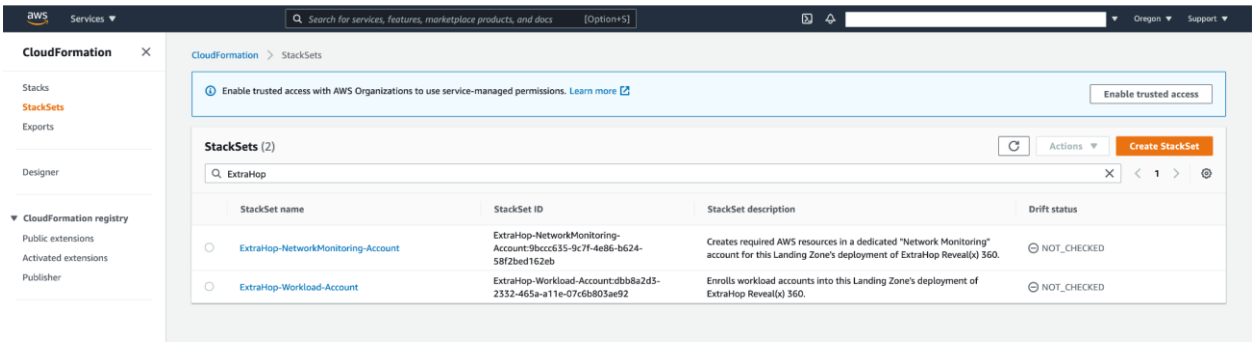
Step 2.3: Use Account Factory to Vend a New Workload Account

Sign into the AWS Console using your Control Tower Management Account and search for the **Control Tower** service. On the **Account factory** page, click **Enroll account**. Provide details for this new Workload Account.

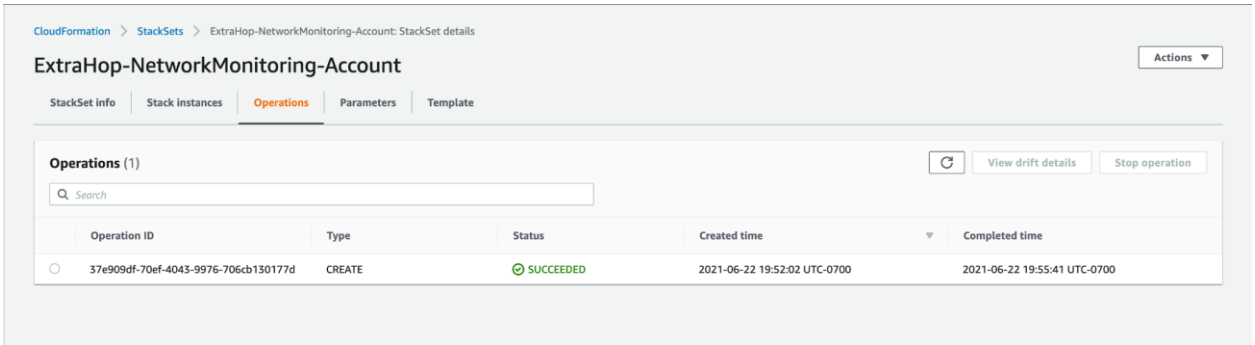
NOTE: It can take up to 30 minutes for Account Factory to complete new Account creation and Enrollment, during which time Control Tower applies Guardrails and the ExtraHop-ControlTowerLifecycle Function creates the ExtraHop-Workload-Account StackSet.

Step 2.4: Validate the Network Monitoring Account Resources

To validate the StackSet creation was successful, search for the CloudFormation service, and view the **StackSets** page.



Click on the name of the ExtraHop-NetworkMonitoring-Account StackSet and view its **Operations**. You should see a **SUCCEEDED** Status for the most recent Operation Id, similar to the below:



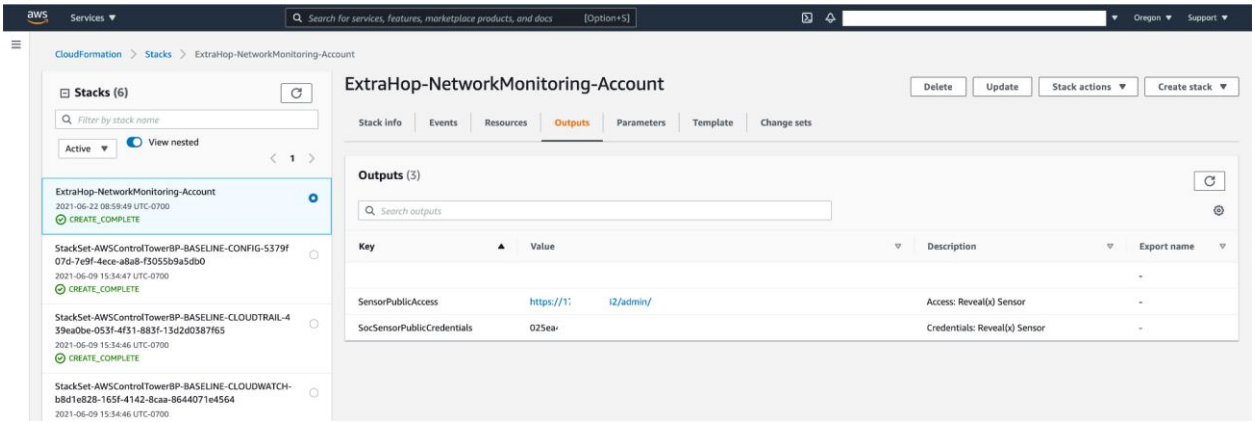
Log into the Network Monitoring Account and search for the **EC2** service. You should have one running Instance in your Control Tower Home Region: your Reveal(x) Sensor.

3. Configure Reveal(x) Sensor

Step 3.1: Configure Sensor Interfaces

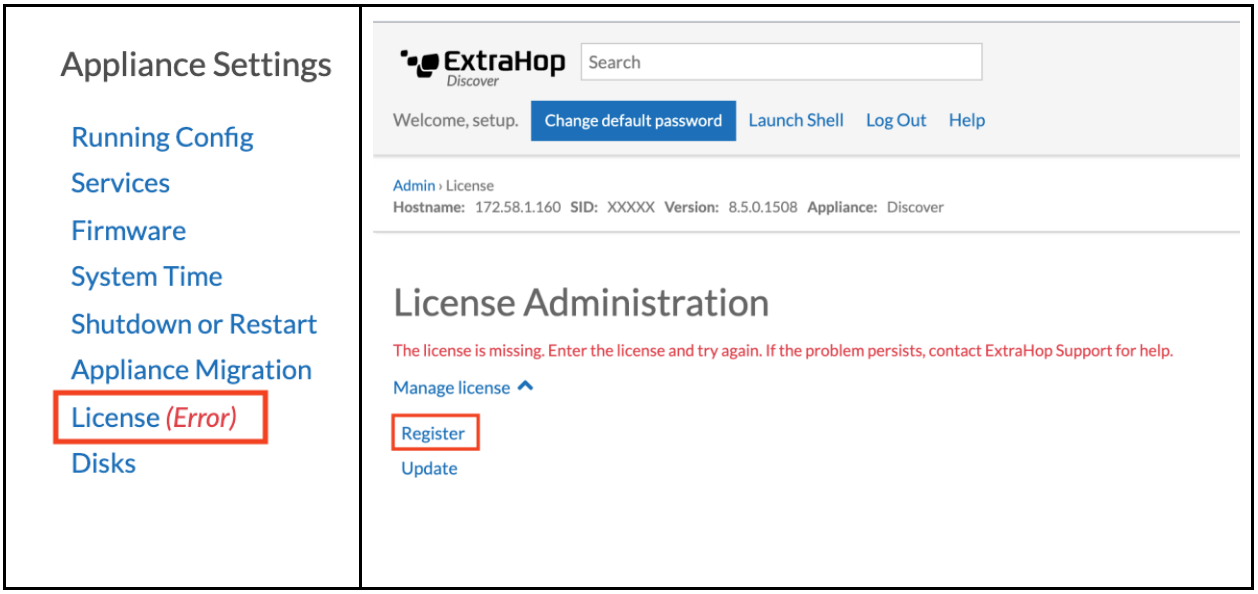
Sign into the AWS Console using your Network Monitoring Account and search for the **CloudFormation** service. Identify the **ExtraHop-NetworkMonitoring-Account** Stack and view its **Outputs**.

> NOTE: both your Sensor's unique password and the URL of the Reveal(x) Sensor's Management Interface.



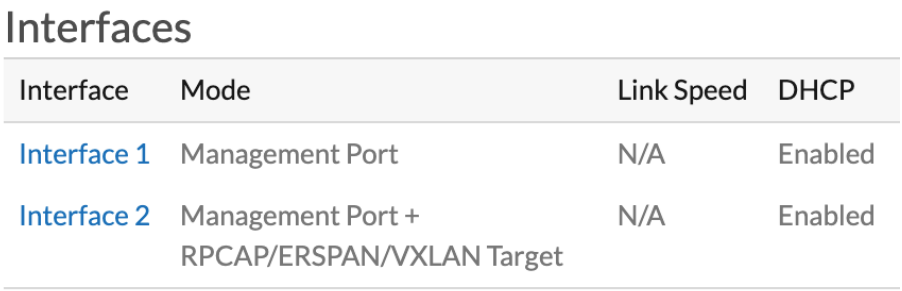
Log in to the Sensor with the username **setup** and register your Sensor.

From the System Settings Gear Icon, click **Administration**. Click **License**, click **Manage License**, enter your product key, and click **Register**.



Remain in the Sensor's Admin UI**.** On the Admin UI page, click **Connectivity** and update the Network Interface settings as follows:

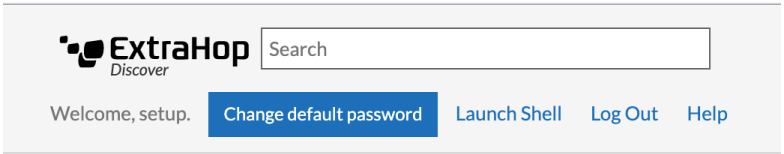
- Interface 1: Set Mode to **Management Port.** Leave **DHCP Enabled**.
- Interface 2: Set Mode to **Management + RPCAP/ERSPAN/VXLAN Target** and **Enable DHCP**.



View and Save the **Running Config** from the prompt.

Step 3.2: Connect to ExtraHop Cloud Services

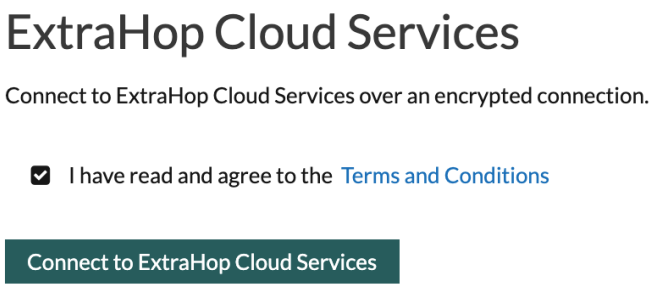
Remain in the Sensor's Admin UI at `https://<sensor_ip_address>/admin`**.** Follow the prompt to change the default passwords for the **setup** and **shell** accounts.



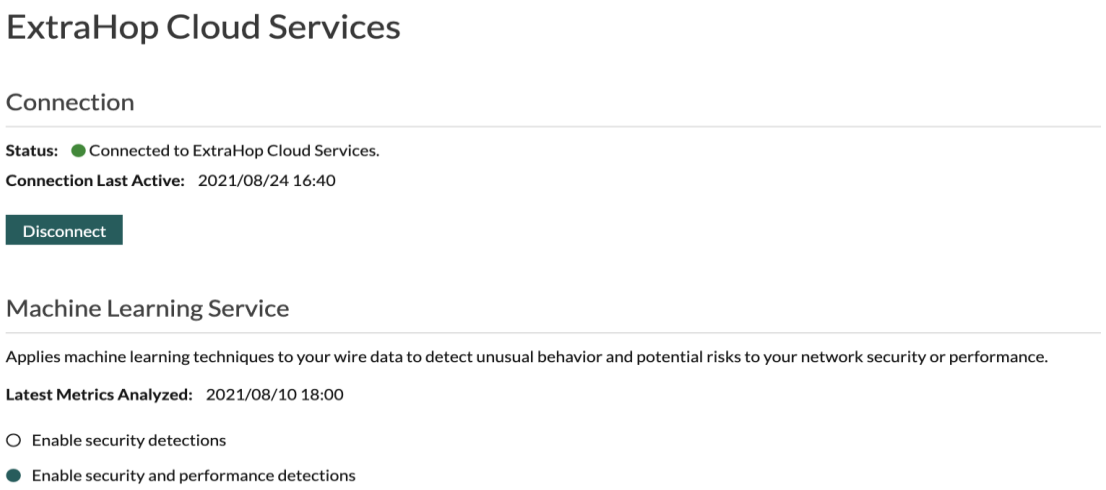
NOTE: the "old" password for the Setup user can be found in the CloudFormation Outputs for the ExtraHop-NetworkMonitoring-Account Stack referenced in Step 3.1.

NOTE: If you do not see a prompt to **Change default password**, You can navigate to `https://<sensor_ip_address>/admin/pass` to change the password for the **setup** and **shell** accounts.

Remain in the Sensor's Admin UI at `https://<sensor_ip_address>/admin/`. On the Admin UI page, click **ExtraHop Cloud Services**, review the Terms and Conditions, and click **Connect to ExtraHop Cloud Services** and Enable **Performance** and **Security** Detections

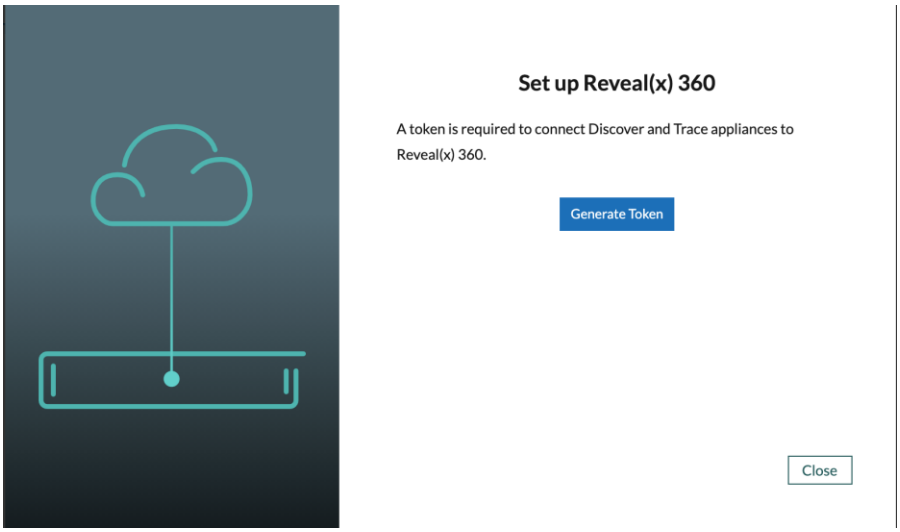


Refer to Connect to ExtraHop Cloud Services for more information.When successfully connected to ExtraHop Cloud Services, the page should look like this:



Step 3.3: Connect Sensor to Reveal(x) 360

Log into your Reveal(x) 360 Console at `https://<customername>.cloud.extrahop.com` and click the System Settings Icon to access the **Administration** page. Click **Connect Appliances** and Generate a pairing Token.



Log into your Sensor's Admin UI**.** On the Admin UI page, click **Connect Command Appliances**. Click **Add Appliance** and paste in the pairing token you generated from the Reveal(x) 360 Console. Add a **Discover Appliance Nickname** and click **Connect**.

Refer to Connect to Reveal(x) 360 from self-managed sensors for more information.

4. Validate Deployment

Step 4.1: Confirm Network Monitoring Account StackSet Deployment

Sign into the AWS Console using your Network Monitoring Account, and search for the **CloudFormation** service. Find the Stack for your **ExtraHop-NetworkMonitoring-Account** and confirm it's status is "Create Complete".

> NOTE: The Stack name will be similar to: `StackSet-ExtraHop-NetworkMonitoring-Account-2c85e3fe-bd59-4a01-8924-ee8d48dcbb0c`

Step 4.2: Confirm Workload Account StackSet Deployment

Sign into the AWS Console using your Workload Account, and search for the **CloudFormation** service. Find the Stack for your **ExtraHop-Workload-Account** and confirm it's status is "Create Complete".

> NOTE: The Stack name will be similar to: `StackSet-ExtraHop-Workload-Account-2c85e3fe-bd59-4a01-8924-ee8d48dcbb0c`

Step 4.3: Create Workload Account Resources

ExtraHop Sensor deployments are Regional. To validate that your deployment's ExtraHop Automation components are working as intended, you will create a temporary VPC and EC2 Instances in the same Region as your Sensor. Refer to the Architecture Diagram to see how ExtraHop Automation uses cross-account Event delivery and Lambda invocation to maintain your ExtraHop data feed.

When you create the temporary Workload VPC, you will see it is automatically peered to the ExtraHop VPC in the Network Monitoring Account, and a Route to the ExtraHop VPC's CIDR is automatically added to the Workload VPC's route tables that references the new VPC Peering Connection. Similarly, when you create temporary EC2 Instances (your 'monitored workloads'), you will see Mirror Sessions automatically forward a copy of their network traffic to the ExtraHop Sensor's Traffic Mirror Target.

After you have observed the automatically generated Peering Connection, Route, and Mirror Sessions, you will decommission the temporary EC2 Instances and VPC.

Download the `tasks.zip` archive with AWS CLI scripts which you'll use to create and delete a VPC and EC2 Instance for testing purposes:

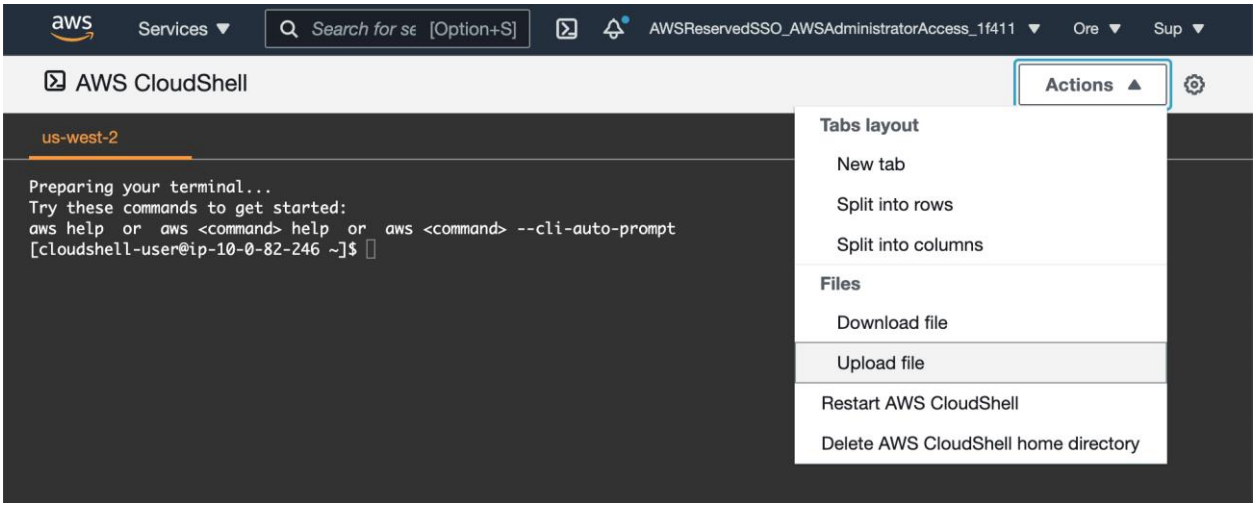
`https://extrahop-onboarding-`**`<region-name>`**`.s3.`**`<region-name>`**`.amazonaws.com/public/tasks.zip`

> NOTE: Substitute your Control Tower "home Region" name for **`<region-name>`** in the S3 URL.
>
> For example: `https://extrahop-onboarding-us-west-2.s3.us-west-2.amazonaws.com/public/tasks.zip`
>
> Currently supported Regions include:
>
> - `us-east-1`
> - `us-east-2`
> - `us-west-1`
> - `us-west-2`

Sign into the AWS Console using your Workload Account, and launch the **AWS Cloud Shell** in the same Region where your Sensor is deployed.

> NOTE: The Network-Monitoring-Account StackSet will typically deploy the Sensor in the Region's first Availability Zone, alphabetically, by AZ Name. For example, `us-west-2a` for the `US West (Oregon)` Region.

Upload `tasks.zip` from the **Actions** menu.



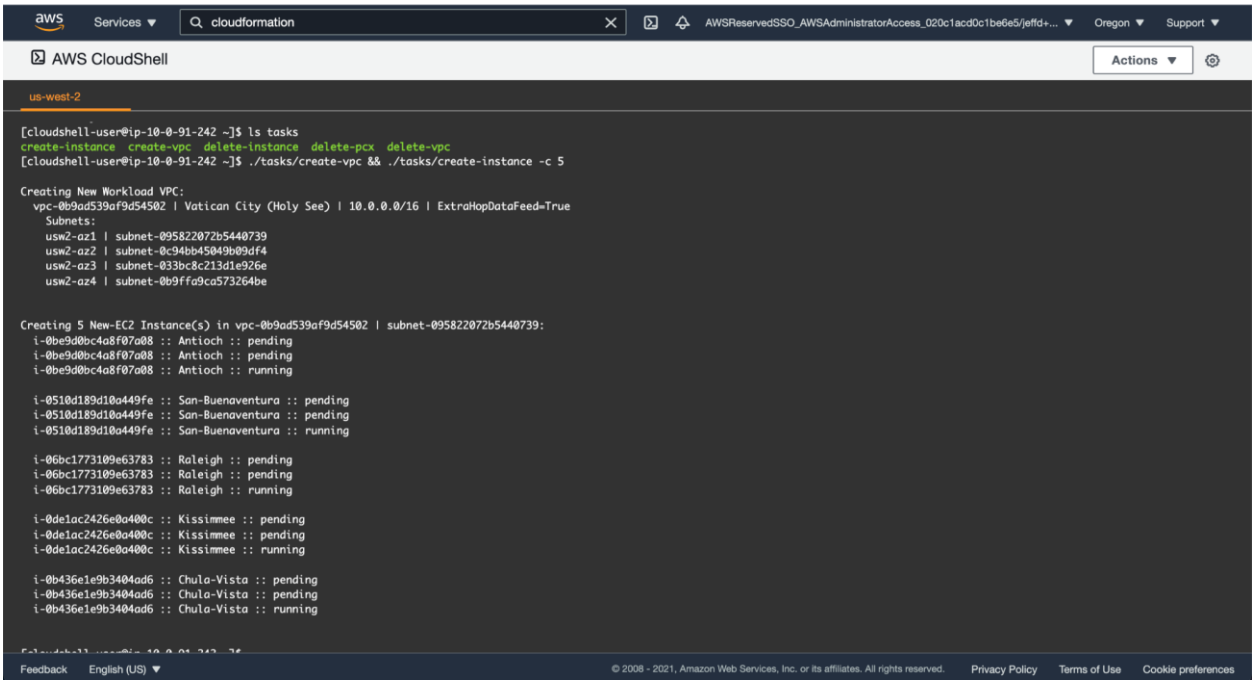
Extract and initialize the individual task scripts using this command:

```
unzip tasks.zip && files=$(ls tasks) && for file in $files; do chmod +x tasks/$file;  done;
```

Create a new Workload VPC and 5 new EC2 Instances using the following command:

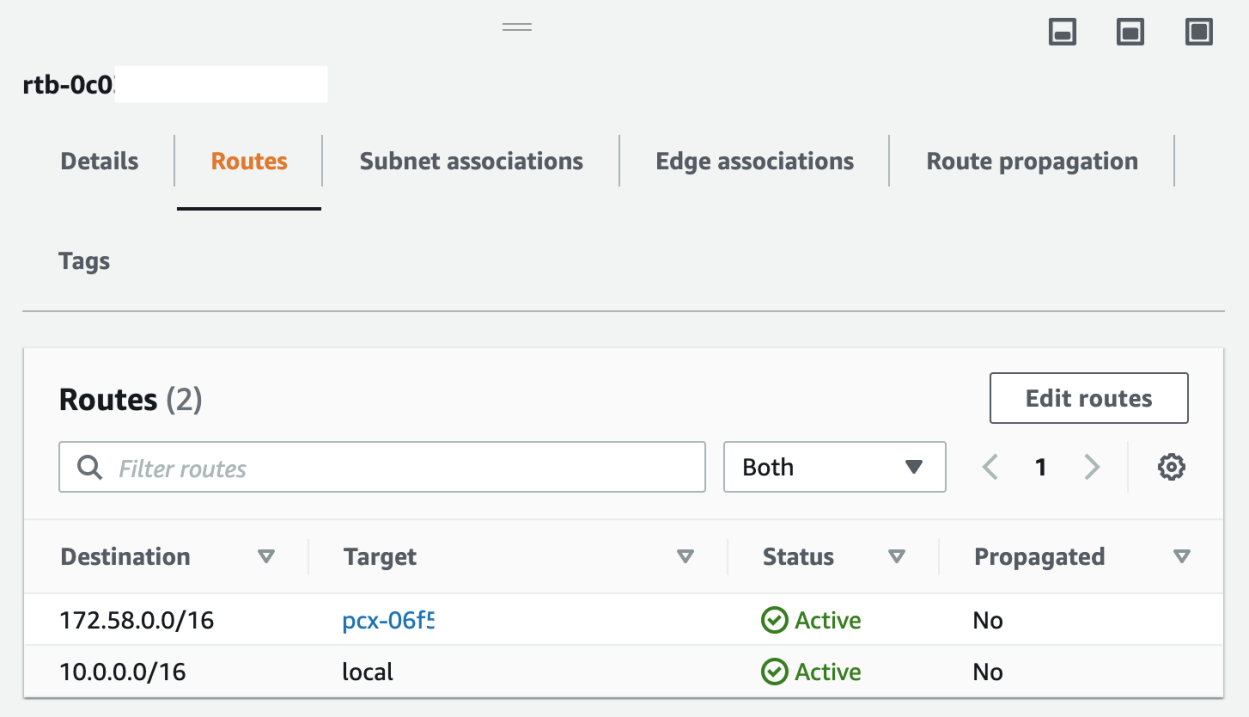
```
./tasks/create-vpc && ./tasks/create-instance -c 5
```

You should see output similar to the following:



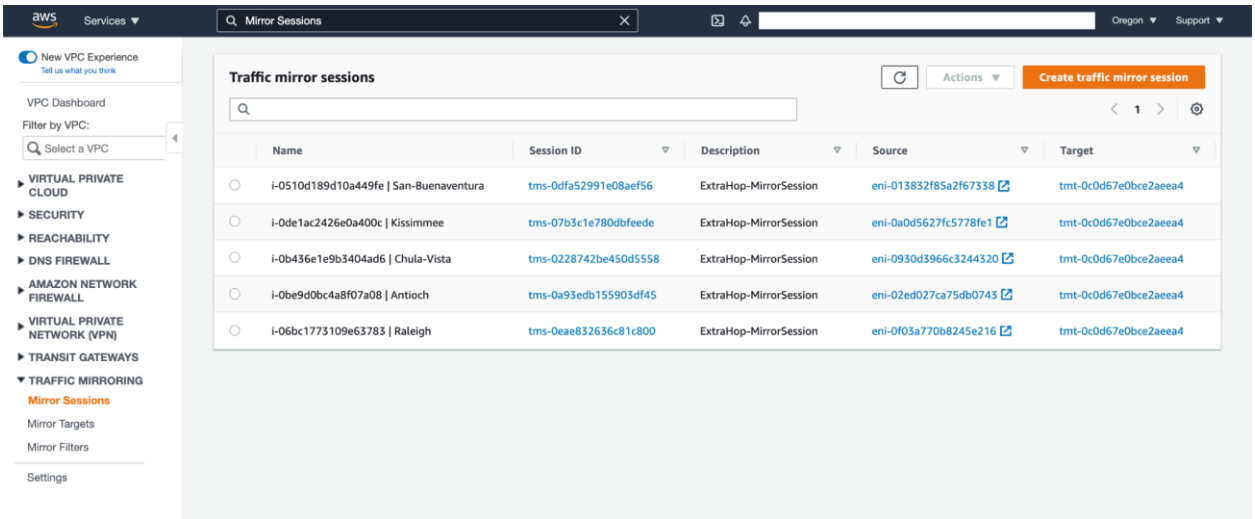
Search for the **VPC** Service and Review your Workload VPC's **Route Table**.

Confirm your Workload VPC's Default Route Table has a Route to the ExtraHop VPC that references a VPC Peering Connection. A Peering Connection and Route were automatically created for your Workload VPC. If you Delete the Workload VPC, the Peering Connection and Route(s) will be automatically removed.



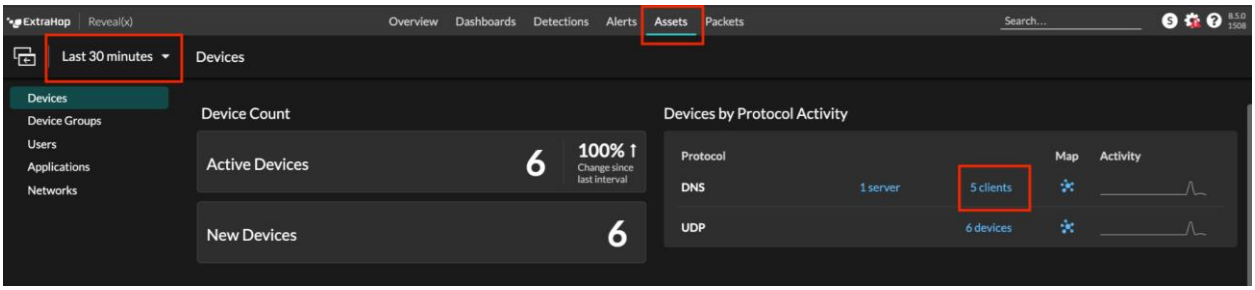
NOTE: The IP address range **172.58.0.0/16** is the default ExtraHop VPC CIDR. You may have selected a different CIDR to use. If needed, refer to the **VpcCIDR** parameter in the Network-Monitoring-Account Stackset reviewed in Step 4.1.

Review the **Mirror sessions** page in the VPC service. Confirm an **ExtraHop-MirrorSession** Traffic Mirror Session was automatically created for each EC2 Instance you created. When you delete these EC2 Instances, the Traffic Mirror Sessions will be automatically removed.



Step 4.4: View Analyzed Traffic

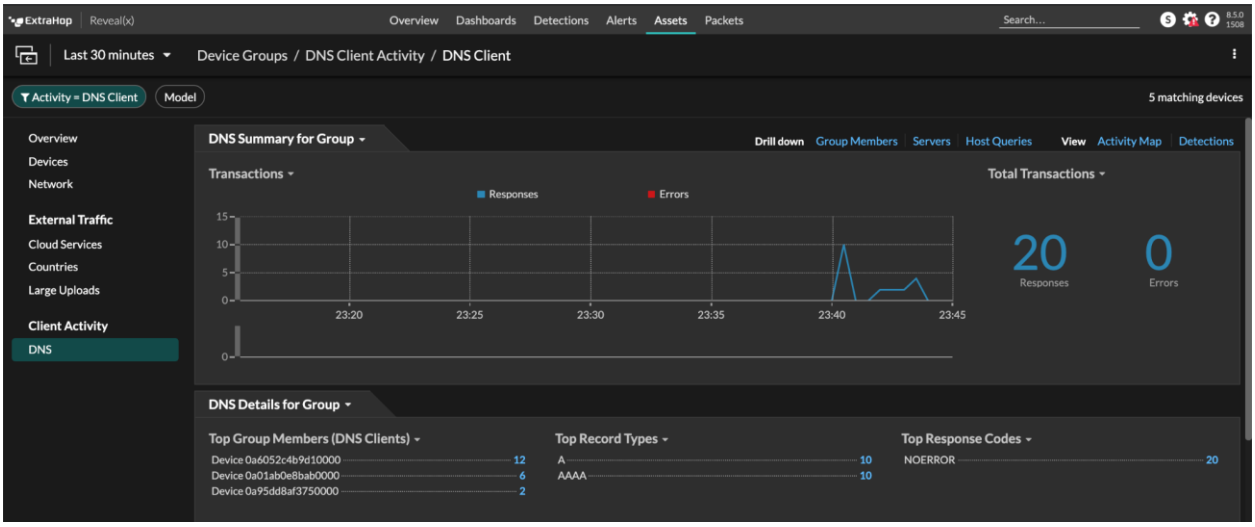
Log into your Reveal(x) 360 Console at `https://<customername>.cloud.extrahop.com` and select **Assets** from the navigation bar at the top of the page. Your Assets page should look similar to this:



Note the new Devices your Reveal(x) sensor has automatically discovered from receiving mirrored network traffic from your workloads. Note your Sensor has also automatically discovered the VPC Router that is acting as a DNS server.

> NOTE: See the VPC User Guide for more information about DNS resolution with a VPC's default ".2" Route 53 resolver.

Change your Time Selector to **Last 30 Minutes** and click the link for **5 DNS Clients** to view DNS transaction data for the **DNS Client Activity Group**.

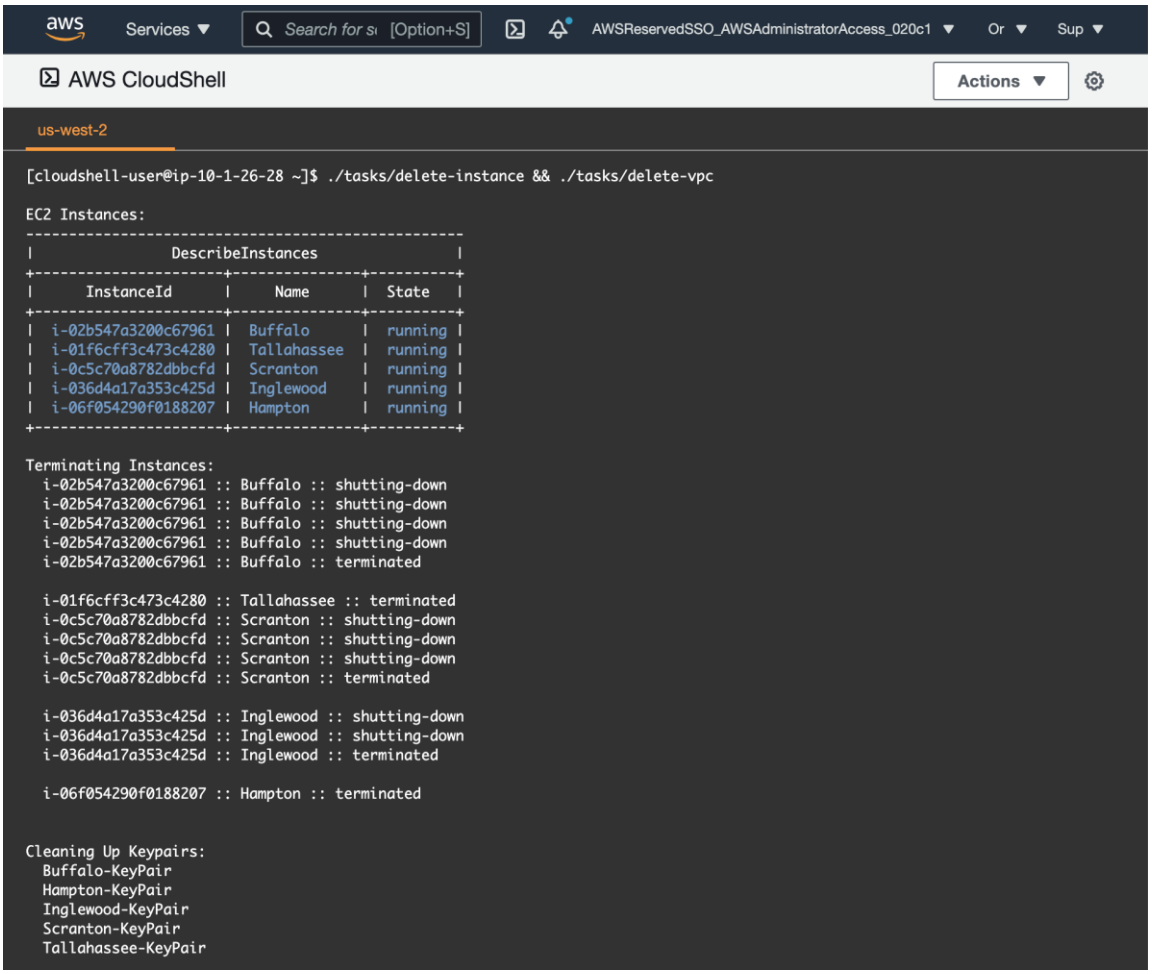


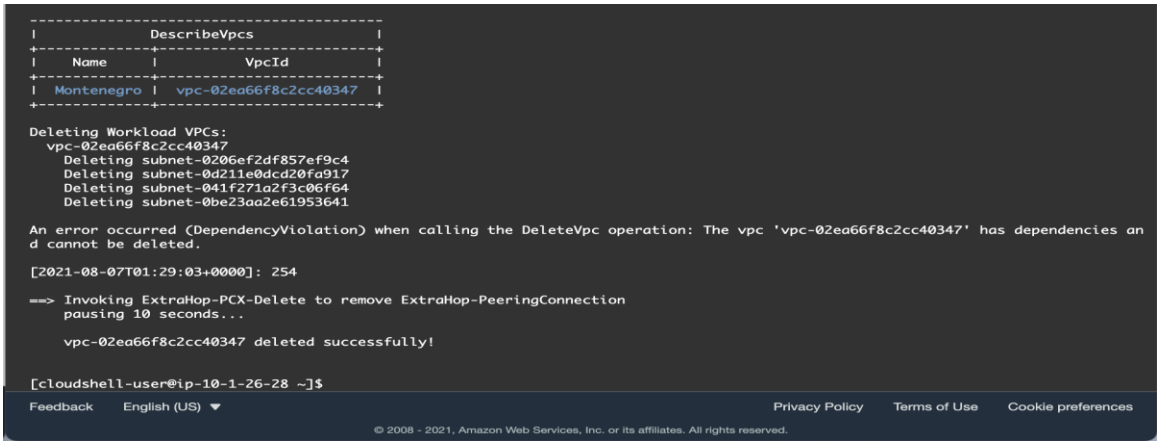
Step 4.5: Decommission Test Workloads

When finished, remove the test Workload VPC and EC2 Instance using the following command:

```
./tasks/delete-instance && ./tasks/delete-vpc
```

You should see output similar to the following:





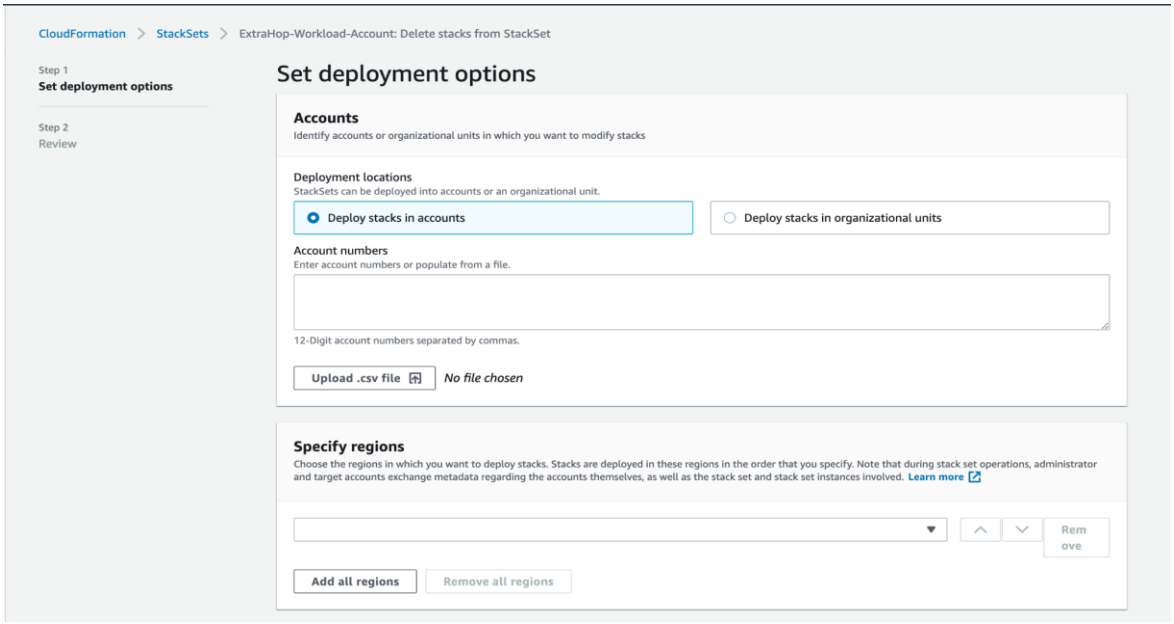
5. Solution Cleanup

Step 5.1: Delete StackInstance from Workload Account

Sign into the AWS Console using your Control Tower Management Account and search for the CloudFormation service. Select the StackSets page and select the **ExtraHop-Workload-Account** StackSet.

Review the **Stack instances** tab and note the Account IDs of the Accounts where the Stack instance is deployed.

From the **Actions** menu, click **Delete stacks from StackSet**, and enter the Account numbers.



Specify your AWS Control Tower home Region, and click **Next** to Review your selected Deployment options, and click **Submit**.

Click the StackSet's **Operations** tab to see the DELETE operation and it's status. Proceed to the next step when it's Status changes to SUCCEEDED.

Step 5.2: Delete StackInstance from ExtraHop-NetworkMonitoring Account

This step repeats the instructions from Step 5.1 to remove the ExtraHop-NetworkMonitoring-Account Stack instance.

Remain signed in to your Control Tower Management Account and remain on the CloudFormation StackSets page. Select the **ExtraHop-NetworkMonitoring-Account** StackSet. Review the **Stack instances** tab and note the Account ID of the Account where the Stack instance is deployed.

From the **Actions** menu, click **Delete stacks from StackSet**, and enter the Account number.

Specify your AWS Control Tower home Region, and click **Next** to Review your selected Deployment options, and click **Submit**.

Click the StackSet's **Operations** tab to see the DELETE operation and it's status. Proceed to the next step when it's Status changes to SUCCEEDED.

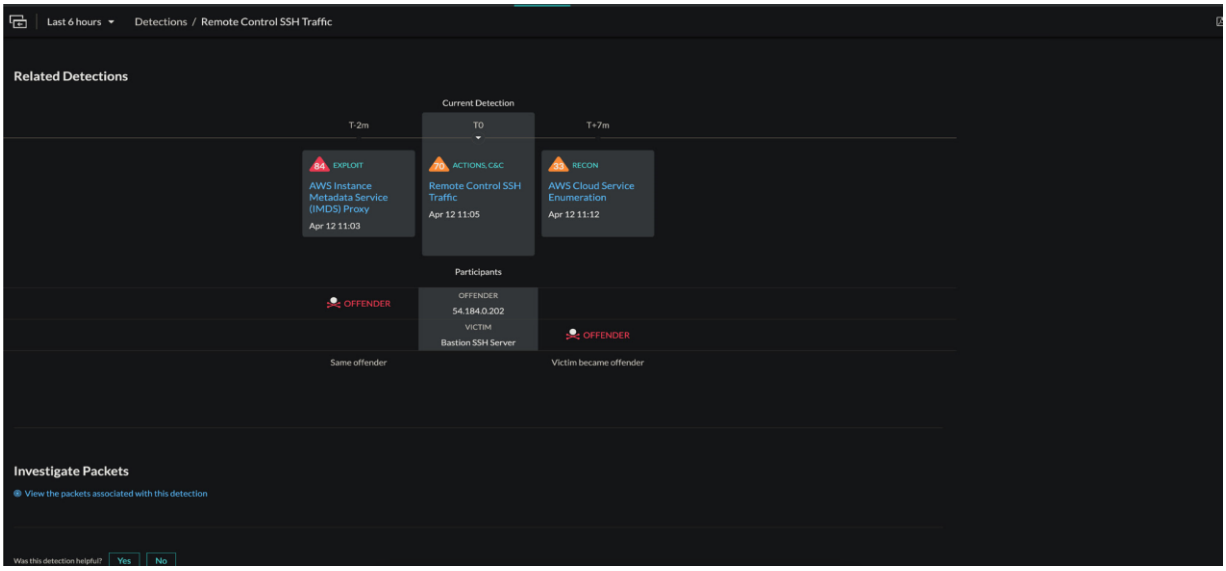
Step 5.3: Delete Stack from Control Tower Management Account

Remain signed in to your Control Tower Management Account and in the CloudFormation Service. On the **Stacks** page, select the **ExtraHop-ControlTower-Lifecycle** Stack and click **Delete stack**.

When the ExtraHop-ControlTower-Lifecycle Stack is finished deleting, you will have removed all resources created in this Implementation Guide.

Use Cases

Reveal(x)360 users secure their AWS workloads from a variety of advanced and everyday threats by eliminating cloud blind spots, discovering supply chain attacks, detecting lateral movement, and responding faster to threats.Eliminate Cloud Blind Spots



Gain continuous visibility into sensitive cloud workloads and data through passive monitoring, even in encrypted traffic.

How do you monitor access to sensitive data in the cloud?

Do you have visibility into encrypted traffic and up to Layer 7?

How do you detect unauthorized movement of large quantities of sensitive data in the cloud?

Understanding which cloud services are sending and receiving data is critical to securing sensitive data. With complete coverage across hybrid and multi-cloud deployments, Reveal(x) 360 enables security teams to monitor sensitive workloads no matter where they live.

With Reveal(x) 360 you'll be able to:

- View cloud workload activity and identify anomalous behavior automatically.
- Trace data transfers inside the VPC and to external endpoints, APIs, and cloud services.
- Automatically provides the context of data flows: which users are sending and receiving, where data is going, and what the data contains.

Discover Supply Chain Attacks

Monitor AWS services through a dedicated pane in the Reveal(x) 360 user interface.

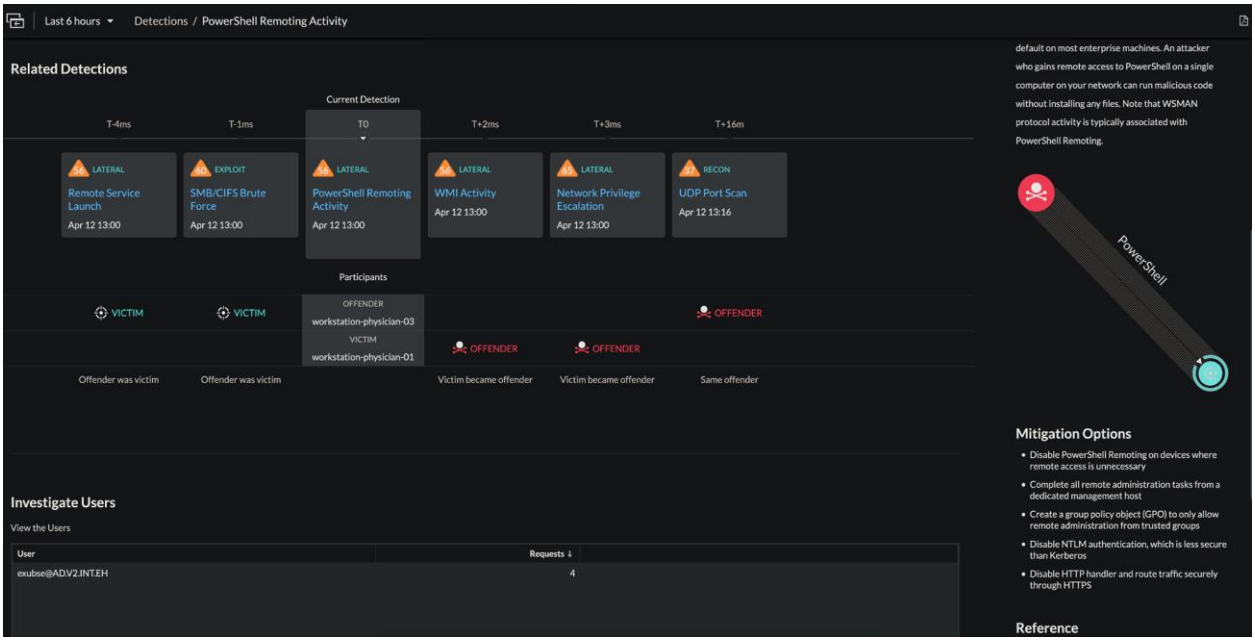
How do you monitor and secure your workloads and container deployments in the cloud?	**What processes do you have in place to assure that new dependencies introduced in production are secure?**

To effectively secure supply chains, you need the ability to monitor cloud workloads for unexpected changes or communications with untrusted or unknown entities. Reveal(x) 360 decreases risk and helps you manage the attack surface to reduce potential damage from supply chain attacks.

Reveal(x) 360 provides:

- Continuous monitoring to quickly surface unexpected changes to cloud workloads.
- Machine learning infers which assets house critical data and makes forensics instantly available for data leakage.
- Detects whether production workloads are pulling updates when they shouldn't in real time.
- Quickly identify and examine unknown or unexpected communications.

Detect Lateral Movement



Detect and investigate communications between cloud workloads and outside entities.

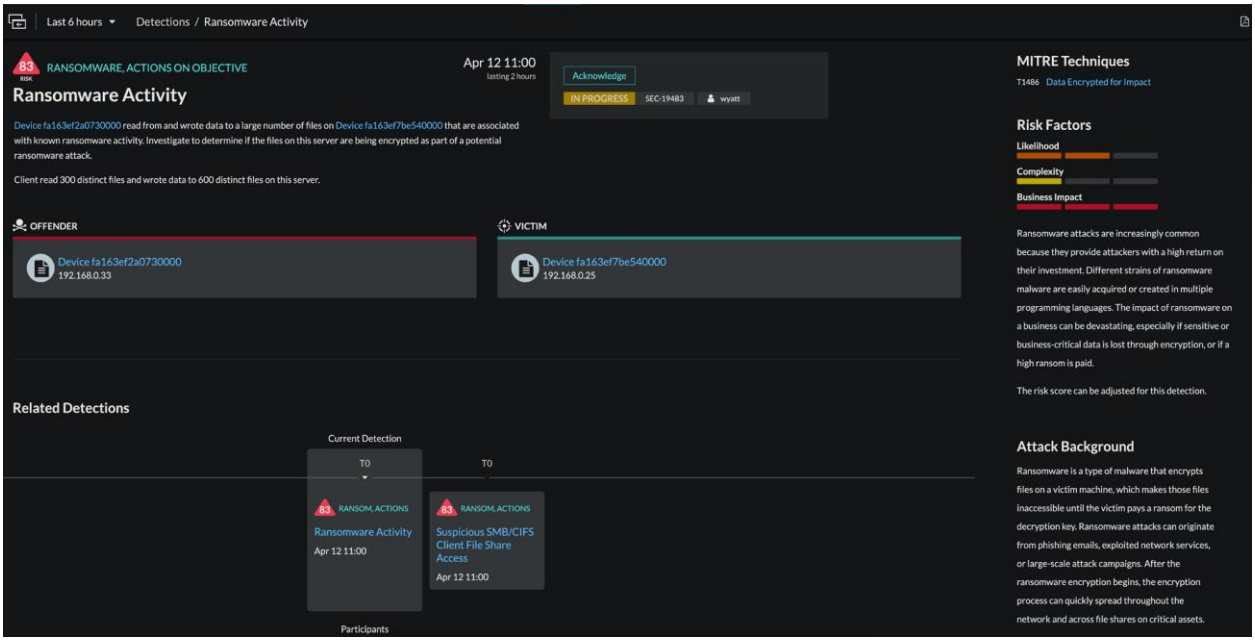
Do your existing security controls provide real-time detection of threats?	**Can your network controls detect suspicious activity over encrypted channels?**	**How do you track normal and abnormal service account activity?**

Lateral movement is a necessary stage in every breach, and on average, there are 10 lateral movements in every attack. The ability to detect post-compromise recon and lateral movements is essential for securing critical data and cloud workloads. Although attackers can hide evidence of their tactics from logging tools, lateral movement between cloud workloads always generates network artifacts.

Reveal(x) 360 enables you to:

- Track privileged account activity and monitor anomalous communication across segments.
- Detect payload attacks using machine learning to identify behaviors such as “low and slow” data staging and exfiltration.
- Gain necessary context that streamlines investigations to speed response via the intuitive user interface.

Respond Faster to Threats



Conduct faster triage of cloud security alerts with accurate, high-context detections.

Are your tools causing alert fatigue and increasing your MTTR?	**Do your current tools provide context and associate disparate cloud security events?**
What information do you need during an investigation?	**How many tools do you use to gather data?**

Privacy regulations have strict disclosure rules that require IR teams to conduct investigations quickly and accurately. And yet, attacks can go undetected for weeks or months. With Reveal(x) 360, security teams can improve time to respond by up to 84%.

With Reveal(x) 360 you can:

- Accurately determine the scope of incidents for implementing appropriate response, internal assessment, and regulatory reporting.
- Instantly access automatically curated cloud asset information, network metadata, and forensic evidence in one solution.
- Go from detection to context and forensic evidence in clicks with intuitive investigation worklfows.

Solution Estimated Pricing

ExtraHop Licensing Costs

Reveal(x) 360 SaaS Subscription

Below are the total costs for these different subscription durations.
Additional taxes or fees may apply.

Reveal(x) 360: SaaS-Based Network Detection and Response

Units	Description	12 MONTHS	24 MONTHS	36 MONTHS
Free Trial/Pay-as-you-go	$0 up front (Optional 15 day Extra Small Sensor FREE TRIAL w/opt out)	$0	$0	$0
Extra Small Sensor	1 Gbps continuous traffic analysis and 20GB of daily record capacity.	$41,799	$83,598	$112,860
Medium Sensor	10 Gbps continuous traffic analysis, 200GB of daily record capacity.	$105,550	$211,100	$284,985
Large Sensor	25 Gbps continuous traffic analysis, 500GB of daily record capacity.	$255,699	$511,398	$690,384
50GB Record Capacity	Add 50GB of additional record capacity daily to tenant.	$30,800	$61,600	$92,400
100 GB Record Capacity	Add 100GB of additional record capacity daily to tenant.	$51,300	$102,600	$153,900
200 GB Record Capacity	Add 200GB of additional record capacity daily to tenant	$92,500	$185,000	$277,500
500 GB Record Capacity	Add 500GB of additional record capacity daily to tenant.	$184,800	$369,600	$554,400
1 TB Record Capacity	Add 1TB of additional record capacity daily to tenant.	$308,000	$616,000	$924,000

Additional usage fees

You will be billed monthly for additional usage costs if your usage exceeds your contract. Your additional usage costs will be determined by the number of units you use above your contract.

Description	Fees
On-demand record capacity (per GB)	$1.69/unit
On-demand Extra Small 1Gbps Sensor (per hour)	$5.04/unit
On-demand Extra Small 1Gbps Sensor + PCAP (per hour)	$8/unit

AWS Resource Costs

EC2 (ExtraHop Sensor)

The table shows current software and infrastructure pricing for services hosted in **US East (N. Virginia)**. Additional taxes or fees may apply.

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Reveal(x) Ultra Cloud Sensor 1 Gbps (BYOL)

	EC2 Instance type	Software/hr	EC2/hr	Total/hr
◉	c5.2xlarge ★*Vendor Recommended*	$0	$0.34	$0.34

Additional Resources

AWS Resources

Learn more about VPC Traffic Mirroring

Launch Announcement

Deep Dive

Non-Nitro Support

Pricing Change for VPC Peering

ExtraHop Resources

Learn more about ExtraHop:

ExtraHop on APN

ExtraHop website

See more ExtraHop AWS Marketplace listings:

ExtraHop on AWS Marketplace

Learn more about ExtraHop Reveal(x) 360 SaaS-Based NDR:

Product

ExtraHop Reveal(x) 360 product page

ExtraHop Reveal(x) 360 solution brief

ExtraHop Reveal(x) 360 eBook

Customers

Wizards of the Coast customer story

MAPCO customer story

Try it

ExtraHop Reveal(x) 360 online demo

ExtraHop Contact Information

For questions regarding product sales ...

Email: michaelg@extrahop.com

For product and technical information ...

Email: jeffd@extrahop.com

For additional information ...

Website: https://www.extrahop.com/company/contact/