DEPLOYMENT GUIDE

Infoblox Threat Defense™ Security Asset Workspace

Table of Contents

Introduction

The new Security Assets Workspace offers a clean, centralized view designed to make it easier for your team to monitor threats, investigate incidents, and manage assets—all in one place. This redesigned UI is purpose-built to streamline the way security teams monitor threats, investigate incidents, and manage associated assets. With improved navigation, contextual insights, and a more responsive layout, the updated interface empowers users to quickly identify high-risk assets, understand their threat exposure, and take informed action—all from a single, unified workspace.

Key Benefits of the New Interface

Streamlined Navigation: A more intuitive layout that allows users to quickly locate and assess relevant security data.

Improved Visibility: Clear, organized views of threat-related assets to support faster decision-making.

Enhanced Troubleshooting: Tools and features that facilitate efficient investigation and resolution of security incidents.

These features allow users to confidently navigate the Security Assets UI and leverage its capabilities to strengthen threat detection and response workflows.

Asset Discovery for Infoblox Threat Defense™

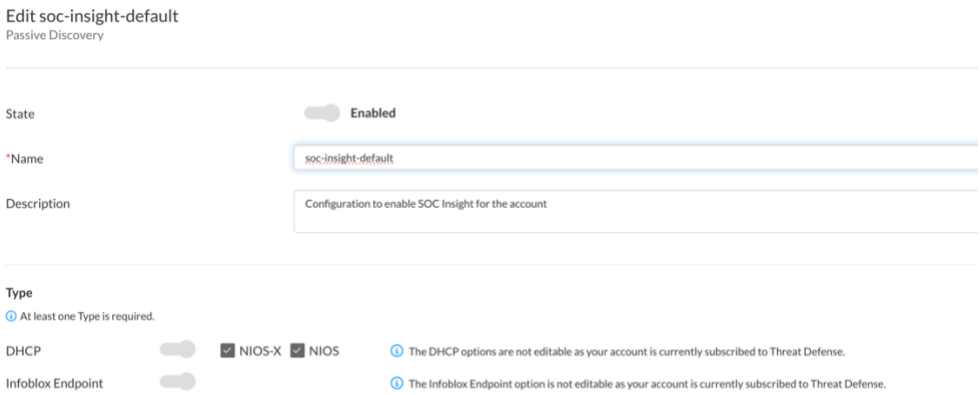
Infoblox Threat Defense uses industry-standard protocols to collect asset data from your network infrastructure. Data sources include, but are not limited to, on-prem NIOS-X servers, NIOS Grids, Infoblox Endpoints, and cloud platform and third-party providers.

Passive Discovery

Passive discovery is turned on by default, so you do not need to configure anything manually. The Infoblox Portal automatically starts collecting asset data to help you get up and running quickly.

Data Sources:

- DHCP NIOS-X
- DHCP NIOS
- Infoblox Endpoint



NIOS Grid Connector

With the NIOS Grid Connector, you get a clear view of assets across your on-prem NIOS Grid setup—making it easier to track DNS, DHCP, and IP address management (IPAM) data in one place. If you have configured NIOS Grids to communicate with Infoblox Universal DDI™, you can enable the NIOS Grid Connector service on the respective service instances (Grid Manager, Grid Manager Candidate, or standalone appliance) to import certain DNS, DHCP, and IPAM data from the Grids or members to Universal DDI.

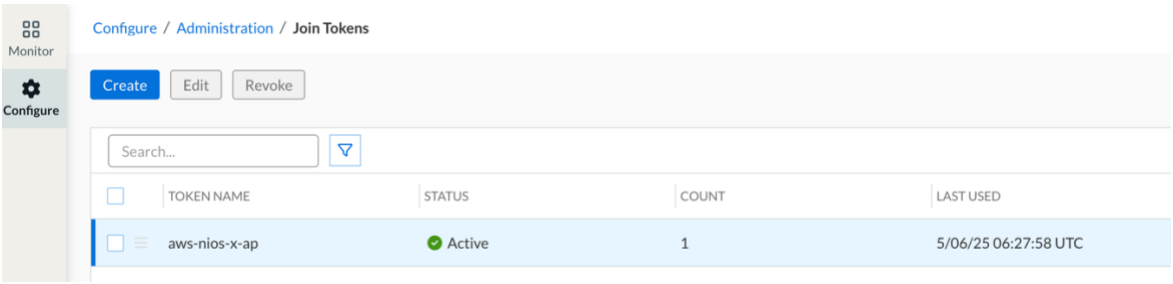
The NIOS Grid Connector enriches Infoblox SOC Insights with authoritative IPAM and configuration data—networks, zones, host records, and asset relationships. It helps SOC Insights gain additional topology and ownership context.

To establish connectivity between the Infoblox Portal and your NIOS Grid so NIOS Grid Connector can pull networks/zones/hosts and push them to the cloud, ensure your NIOS Grid is healthy and reachable.

Complete the following steps to establish connectivity:

- Create a **Join Token** in the **Infoblox Portal** or use an existing one.
- To create a **Join Token**, navigate to *Configure* > *Administration* > *Create Token* and click on *Create*.
- Copy the **Join Token** from the **Infoblox Portal**.

Note: A join token in Infoblox is a secure, time-bound credential generated in the Infoblox Portal that allows an on-prem NIOS Grid or connector (like NIOS Grid Connector or NIOS-X) to securely register with the Infoblox Cloud. It ensures authenticated pairing between the local grid and the cloud tenant without exposing permanent credentials.

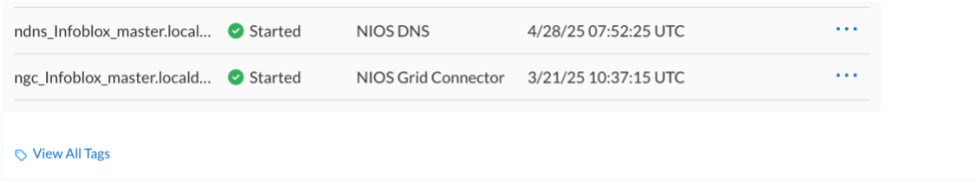


- Sign in to **NIOS**.

1. Navigate to the *Grid* > *Grid Manager*.
2. Select a single device in NIOS. This device must be a Grid Manager, Grid Manager Candidate, or standalone appliance. It is recommended to select the Grid Manager Candidate.
3. Click *Edit*.
4. Click *CSP Config*.
5. Configure the following in the **Basic** tab.
    a. **Join Token:** Paste the **Join Token** you copied from the Infoblox Portal here.
    b. **CSP Resolver:** Specify the IP address of the Infoblox Portal.
    c. **HTTPs Proxy:** Specify the HTTPS proxy. If your network environment does not allow direct HTTP or HTTPS communication with the internet through a firewall from a secure location in which the Grid Manager or standalone appliance resides, you can configure your appliance to use a proxy server.
    d. Click *Save & Close*.

To enable the NIOS Grid Connector service, complete the following:

1. From the **Infoblox Portal**, click *Configure* > *Servers*.
2. On the **Servers** page, select the **NIOS Server** you added
3. Click on *Create Service* and select *NIOS Grid Connector* to enable the service.

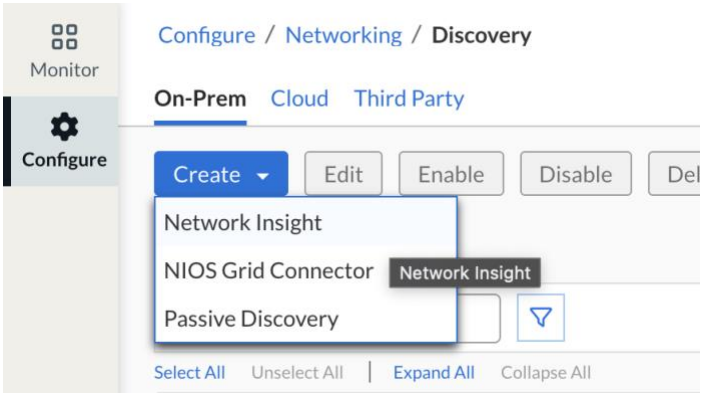


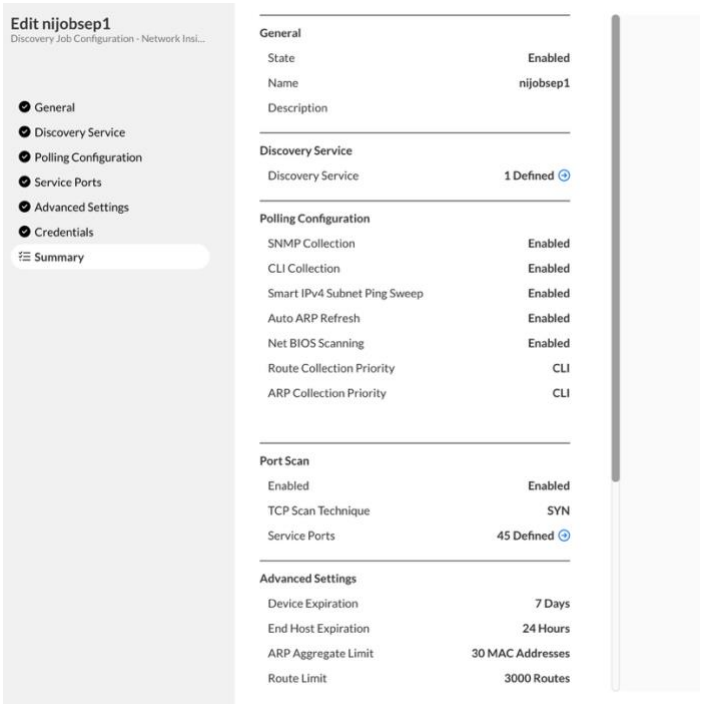
Network Insight Discovery

Enabling Network Insight Discovery enhances Threat Defense with deep, automated visibility into every networked device and connection. By continuously identifying infrastructure components and endpoints across distributed and virtual environments, it enriches threat data with real asset context. This allows Threat Defense to correlate security events with specific devices, detect rogue assets, and prioritize threats based on network relevance—turning visibility into actionable, context-driven protection.

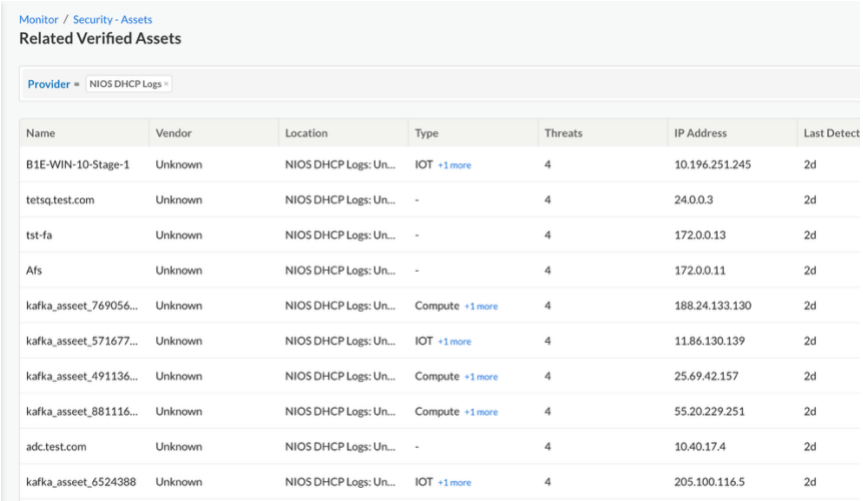
Complete the following steps to enable network insights discovery for your networks:

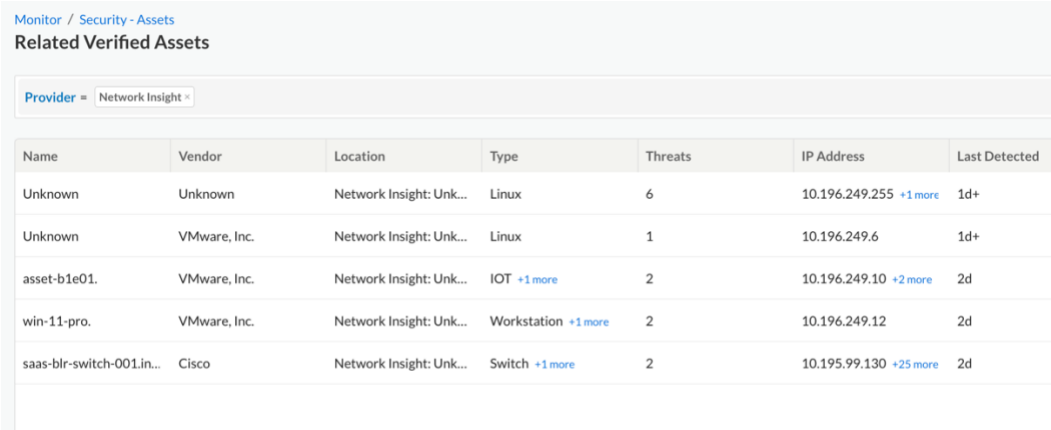
1. Log in to the **Infoblox Portal**.
2. Onboard the **NIOS-X Server**, enable the **Discovery Service** and provide the details of networks to be scanned.
3. Go to *Configure* > *Networking* > *Discovery* > *On-Prem*.
4. Click *Create* > *Network Insight*.
5. Select the created **Discovery Service**.
6. Configure the **Polling Configuration** and provide the required credentials for access.
7. Click on *Save and Close*.





Once assets are discovered and have generated any security events, they become visible within the Security Assets sub-workspace.





Cloud Data Connector

Infoblox Data Connector enables seamless integration between your on-premises NIOS deployment and the Infoblox Cloud by securely collecting and forwarding IPAM and DHCP logs. This centralized log aggregation allows organizations to gain comprehensive visibility into all network-connected assets, including IP addresses, devices, and lease activity.

1. Log in to the **Infoblox Portal**.
2. Go to *Configure* > *Service Deployment* > *Protocol Service*.
3. Click *Create Service*.
4. From the drop-down menu, select *Data Connector*.

In the **General Info** step of the **Create Data Connector Service** wizard, specify the following:

- **Name** (required field): Provide a name for the service instance.
- **Description**: Provide a description for the service instance.
- **Service State**: Set the toggle switch to start or stop the service.

- **Server** (required field): Do the following to select a NIOS-X server on which you want to run this service:
    a. Click *Select Server* and choose a server from the drop-down list. Only available NIOS-X servers are listed. Alternatively, use the **Search** tool to locate and select a server.
    b. Click *Select* to add the server to the configuration.

The server status may momentarily change to "Degraded" when a new service is added to the server.

Cloud Sources

AWS

Infoblox AWS Discovery allows for automatic discovery of resources in your AWS environment. This enables organizations to extend their on-premises IPAM and network visibility into their public cloud infrastructure.

Prerequisites

Actions required on your AWS Account to allow discovery:

- Create an **IAM Policy** based on the permissions you want to provide to Infoblox to receive information from AWS. (Sample Policy for Discovery Sync).
- Attach the policy to a specific **IAM User** or a **Role** (the role must trust Infoblox's AWS Account ID).

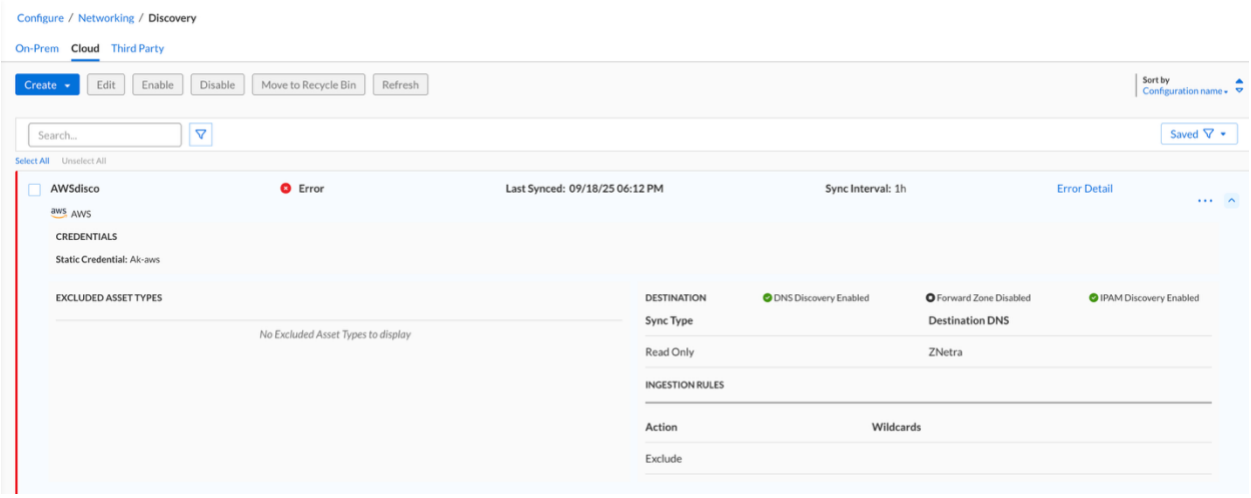
To create a network discovery configuration for AWS, complete the following:

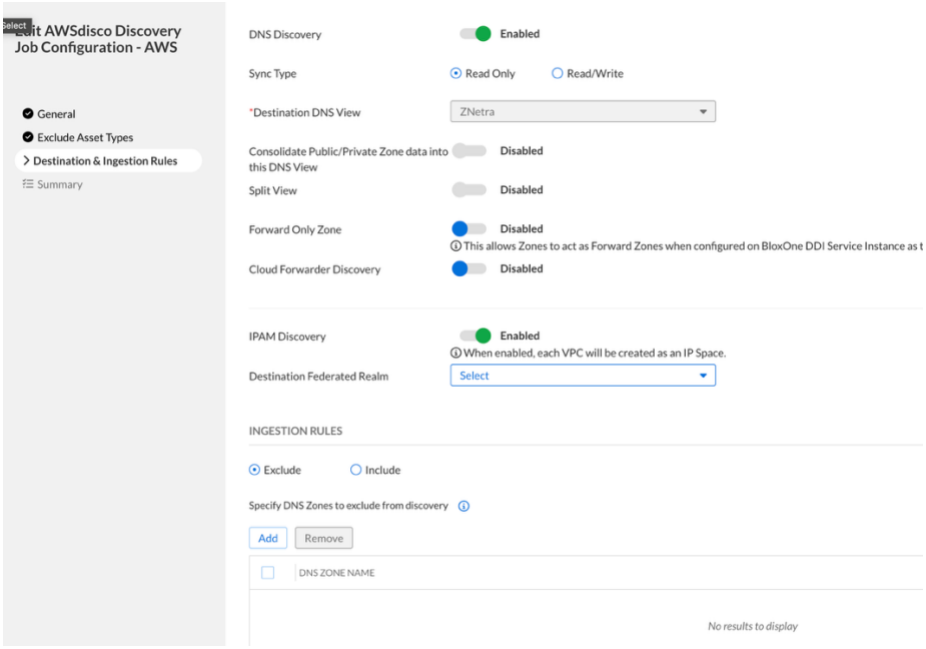
1. Go to *Configure* > *Networking* > *Discovery* > *Cloud*.
2. Click *Create* > *AWS*.
3. In the **General** step of the Create Discovery Job Configuration wizard, configure the following:
    - **State:** Toggle *Enabled* (green) or *Disabled* (blue). AWS discovery is enabled by default.
    - **Name:** Specify a name for the network discovery configuration. The name should only contain alphanumeric characters and underscores.
    - **Description:** Specify a description for the network discovery configuration.
    - **Sync Interval:** Choose the sync interval from the drop-down. Choose *Auto* if you want the Infoblox Portal to choose the sync interval automatically. The default sync interval is 15 minutes.
    - **Credentials:** The following settings are configured in the Credentials pane:
        - **Account Preference:** Select the account preference from the drop-down. Choose *Single* or *Auto-Discover Multiple*.
        - **Type of Access:** Select the type of access from the drop-down. There are three options:
            - **Principal ID + Role ARN:** If you choose this option, you must specify the Principal ID and the Role ARN:
                - **Principal ID:** For Principal ID-based authentication, choose *Principal ID* to grant access for permission

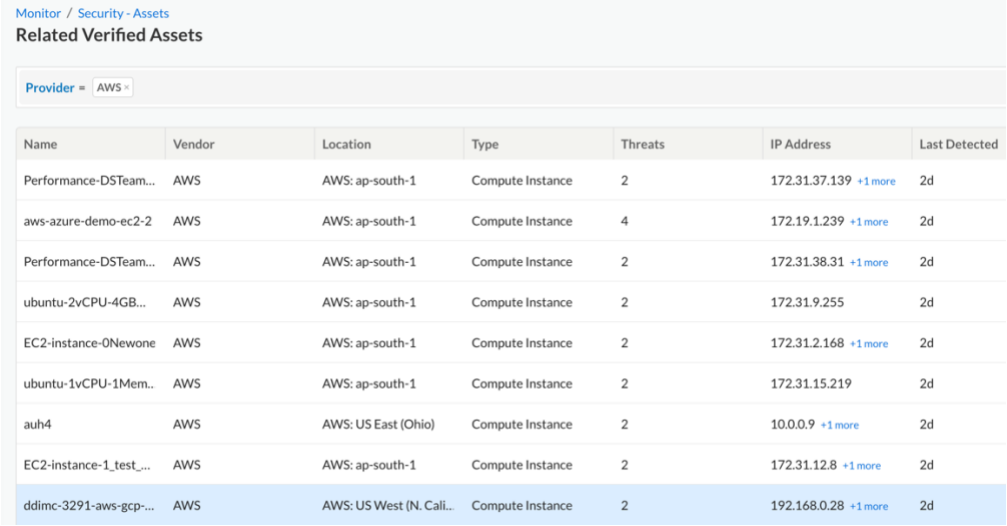
and *External ID*. The Principal ID and External ID will be required for configuring permissions in your AWS Account.
        - **AWS Role ARN:** Specify the AWS Role ARN. The AWS Role ARN cannot be edited once it is created.
    - **Static Credentials:** If you choose this option, you must select the credentials from the drop-down or create new credentials.
    - **Static Credential + Role ARN:** If you choose this option, you must choose the Credentials and the Role ARN:
        - **Credentials:** Select the credentials from the drop-down or create new credentials.
        - **AWS Role ARN:** Specify the AWS Role ARN. The AWS Role ARN cannot be edited once it is created.
- Provide the **Account ID**.

4. Click *Next*.
5. In the **Destination and Ingestion Rules** step of the Create Discovery Job Configuration wizard, configure the following:

    - **DNS Discovery:** Toggle *Enabled* (green) or *Disabled* (blue). DNS discovery is disabled by default. When enabled, all the DNS objects are discovered.
    - **Sync Type:** The following options are available:
        - **Read Only:**
            - The periodic synchronization from the cloud provider takes place.
            - Users cannot write/update Zones and Records objects on the cloud provider through the Infoblox Portal
        - **Read Write:**
            - Users can read and write from/to the cloud provider from the Infoblox portal.
    - **Destination DNS View**: Select the DNS view from the drop-down. The discovered objects will be copied to the selected DNS view.
    - **Consolidate Public/Private Zone data into this DNS View:** If you enable this option, public and private zone data will be copied into this view.
    - **Split View:** All private hosted zones are placed into a DNS view that is automatically created by the Universal DDI platform during synchronization.
    - **Forward Only Zone:** This allows Zones to act as Forward Zones when configured on Universal DDI Service Instance as the Authoritative DNS Server.
    - **Cloud Forwarder Discovery:** If you enable this option, you can sync DNS resolver endpoints into a DNS view. If you enable Consolidate Public/Private Zone data into this DNS View, the DNS resolver endpoints are synced to the selected DNS view. Otherwise, the DNS resolver endpoints are synced to a separate view with the format discovery_job_name.resolver-rules.
    - **IPAM Discovery:** When enabled, IP address information will be synchronized with IPAM. When disabled, IP address information will not be synchronized with IPAM.
    - **Ingestion Rules:** Discovery automatically imports all DNS zones from the source. However, if you wish to synchronize only specific zones, you can configure the discovery process to include or exclude designated DNS zones.


Configure / Networking / Discovery
On-Prem
Cloud
Third Party
Create
Edit
Enable
Disable
Move to Recycle Bin
Refresh
Sort by
Configuration name
Search...
Saved
Select All
Unselect All
AWSdisco
Error
Last Synced: 09/18/25 06:12 PM
Sync Interval: 1h
Error Detail
AWS
CREDENTIALS
Static Credential: Ak-aws
EXCLUDED ASSET TYPES
No Excluded Asset Types to display
DESTINATION
DNS Discovery Enabled
Forward Zone Disabled
IPAM Discovery Enabled
Sync Type
Destination DNS
Read Only
ZNetra
INGESTION RULES
Action
Wildcards
Exclude


Edit AWSdisco Discovery Job Configuration - AWS
General
Exclude Asset Types
Destination & Ingestion Rules
Summary
DNS Discovery
Enabled
Sync Type
Read Only
Read/Write
*Destination DNS View
ZNetra
Consolidate Public/Private Zone data into this DNS View
Disabled
Split View
Disabled
Forward Only Zone
Disabled
This allows Zones to act as Forward Zones when configured on BloxOne DDI Service Instance as t
Cloud Forwarder Discovery
Disabled
IPAM Discovery
Enabled
When enabled, each VPC will be created as an IP Space.
Destination Federated Realm
Select
INGESTION RULES
Exclude
Include
Specify DNS Zones to exclude from discovery
Add
Remove
DNS ZONE NAME
No results to display



Note: The DNS queries from the AWS environment will have to be forwarded to Infoblox for resolution in order to utilize the Security Assets workspace feature.

Asset Discovery from Third-Party Integrations

CrowdStrike

Infoblox Universal Asset Insights™ integrates seamlessly with CrowdStrike to deliver comprehensive asset discovery across on-premises, hybrid, and multi-cloud environments. This integration enables near–real-time visibility and creates a centralized, infrastructure-wide repository of assets and their connectivity details.

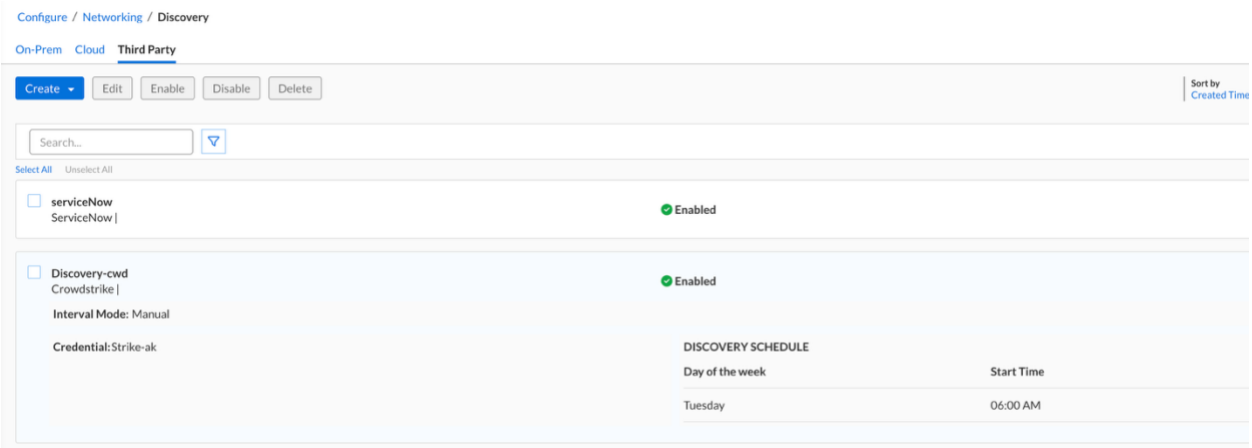
By combining endpoint security insights from CrowdStrike with the network intelligence of Universal DDI, organizations gain a more complete view of their infrastructure. This enhanced visibility improves operational efficiency, strengthens contextual awareness, and supports streamlined workflows—ultimately helping to bolster your organization's security posture.

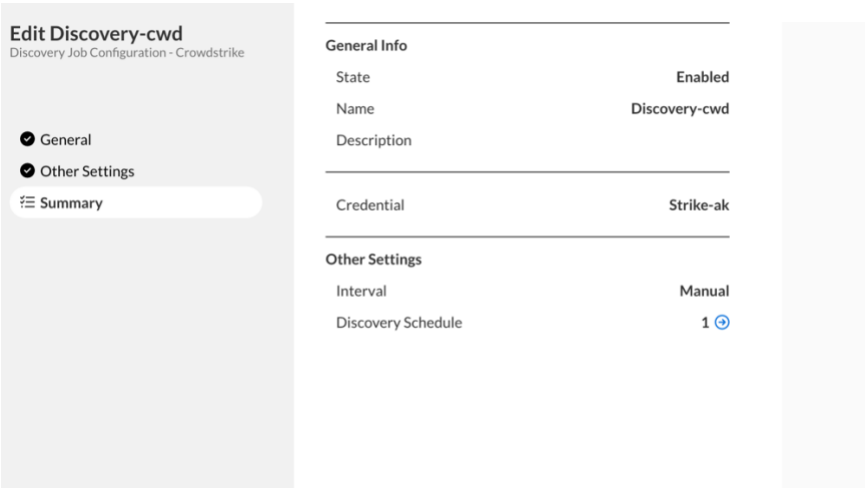
Complete the following steps to create a network discovery configuration for CrowdStrike:

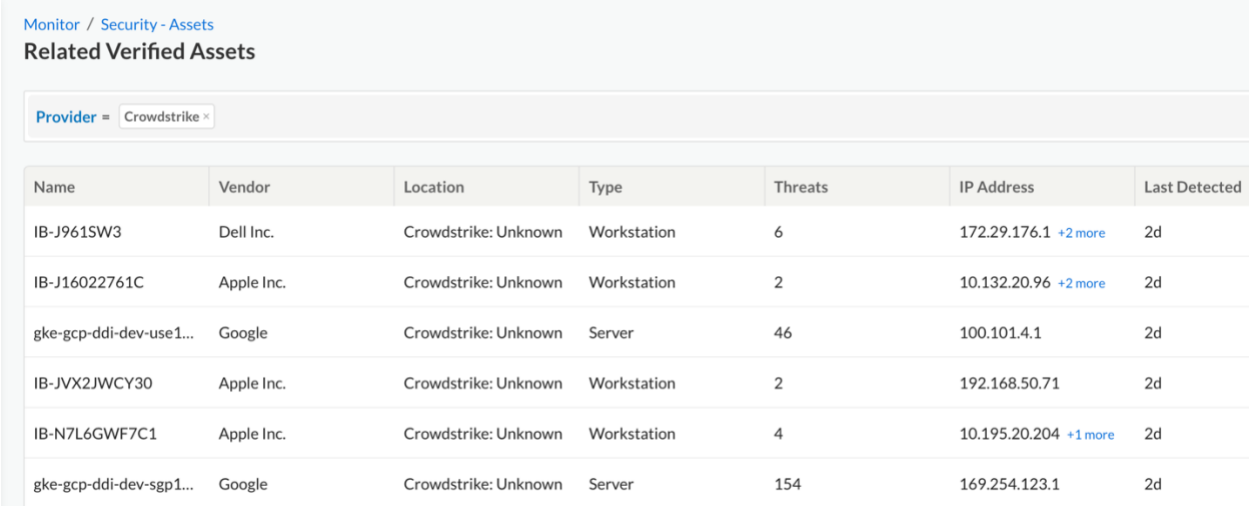
1. Go to *Configure* > *Networking* > *Discovery* > *Third Party Data Providers*.
2. Click *Create* > *Crowdstrike*.
3. Configure the following in the **General** pane:
    - **State:** CrowdStrike discovery is disabled by default.
    - **Name (required):** Specify a name for the network discovery configuration.
    - **Description:** Specify a description for the network discovery configuration.
    - **Credential (required):** Select a pre-existing credential from the drop-down. Alternatively, select *New Credential* from the drop-down and configure the following:
        - **Credential Name (required):** Specify a name for the credential.
        - **Credential Description:** Provide a brief description for the credential and click *Next*.
    - Specify the following third-party credentials:
        - **Access Key ID (required):** Specify the access key ID to connect to CrowdStrike.

    - **Secret Access key (required):** Specify the secret access key to connect to CrowdStrike.
    - **Temporary Session Token:** Specify the temporary session token for CrowdStrike and click *Next*.
4. Review the summary for the new credential and click *Save*.
5. Click *Next*.
6. Configure the following settings in the **Other Settings** pane:
    - **Timer Setting (required):** Select *Auto* to allow network discovery to occur automatically. No schedule is required when *Auto* is chosen. Alternatively, you can choose *Manual* and configure the **Discovery Schedule**.
    - **Discovery Schedule:** Click *Add*. Configure the following:
        - **Day of the Week:** Select the day of the week when discovery should occur.
        - **Start Time:** Specify the start time for discovery to occur.
7. Click *Save and Close*.

Note: To utilize the Security Assets workspace, ensure that DNS queries from all endpoints are forwarded to Infoblox. This forwarding is necessary for generating security events within the workspace.





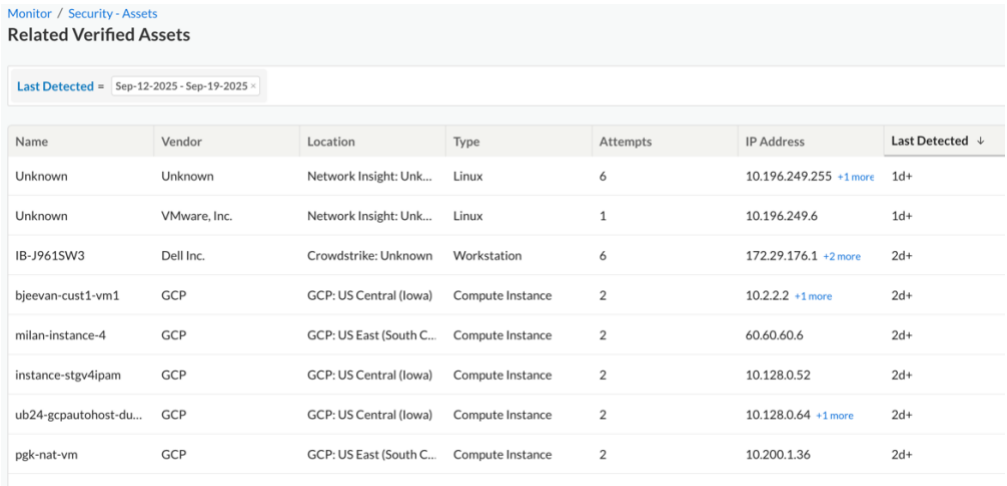


Monitoring Discovered Asset Data on Infoblox Portal

For Threat Defense, asset monitoring is available in the **Security Workspace** of the Infoblox Portal:

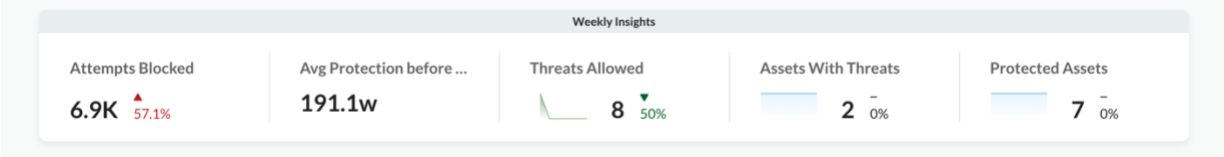
- *Monitor > Security Workspace*
  - *Security > Threats* sub-workspace
  - *Security > Assets* sub-workspace

You can view the list of all the verified assets by clicking on the option in the top right and selecting *View Verified Assets* from the drop-down. This page provides a consolidated list of all the identified assets along with several filter options to identify specific assets based on your requirement.

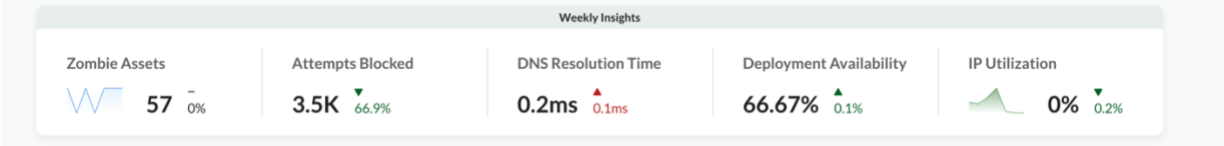


KPI Ribbon

The **Weekly Insights** ribbon at the top displays business KPIs giving an overview of the health of the organization and impact of Threat Defense in securing your network.



The KPI Ribbon will differ if you have both the Threat Defense and UDDI licenses.



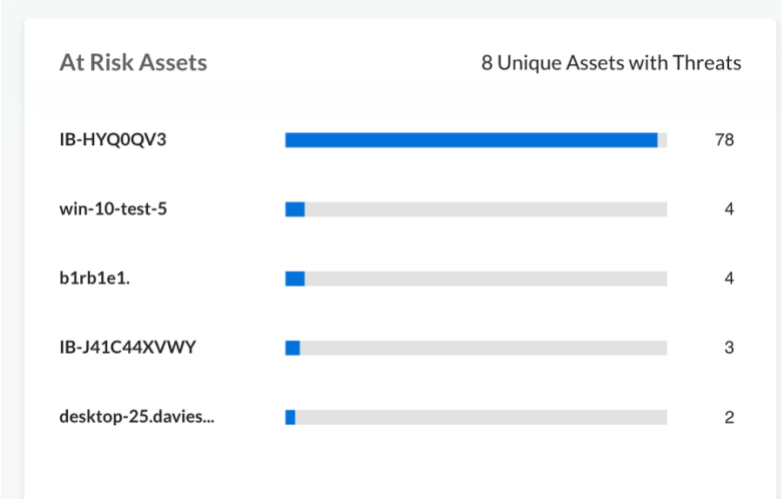
Percentage Change Formula (Trend Analysis)

To determine the **percentage increase or decrease** across the week, the following formula is used:

$$\text{Percentage Change} = \left(\frac{\text{Value}_{\text{Last Day}} - \text{Value}_{\text{First Day}}}{\text{Value}_{\text{First Day}}}\right) \times 100$$

At Risk Assets

The **At Risk Assets** tile provides the top five unique assets based on number of events identified by Threat Defense that are currently associated with active threats. This feature enables users to quickly assess which assets may be compromised, supporting faster prioritization and response.

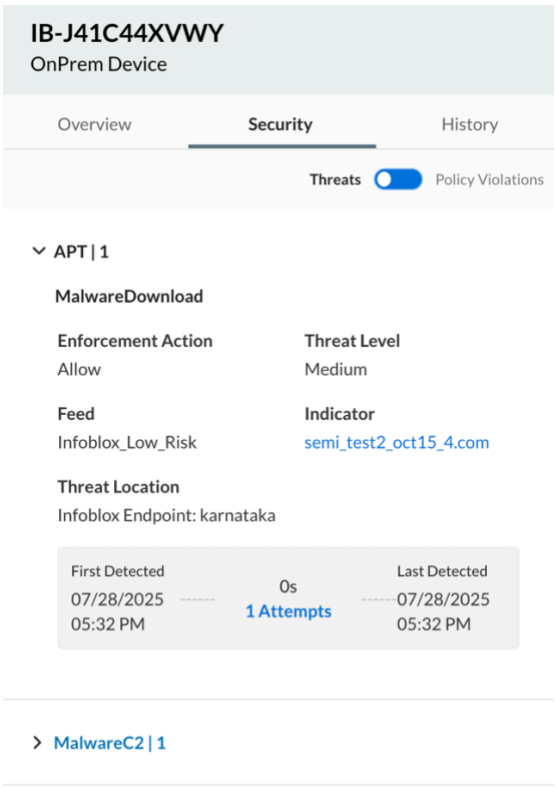


Asset Name	IP Address	Threat Location	Type	Vendor	Attempts	Last Detected
IB-HYQ0QV3	10.120.251.196 +36 m...	Infoblox Endpoint: kar...	Workstation	Dell Inc.	25	2d+
desktop-25.davies-br...	77.111.181.25	Infoblox Endpoint: cali...	Workstation	Unknown	2	5d+
IB-J41C44XVWY	192.168.1.24	Infoblox Endpoint: kar...	Workstation	Apple	3	9d+

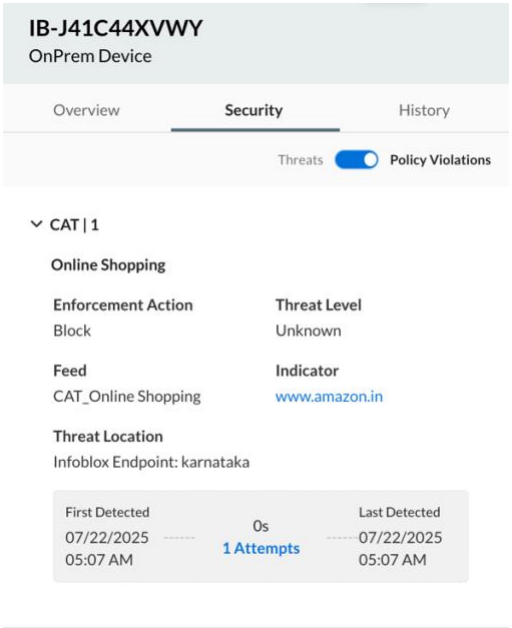
You can easily filter the results based on the specific attributes you are looking for. You can select a specific asset or the action applied on the events. Other available filter options are **Threat Class**, **Threat Location** or the **Threat Type**.

Clicking on a specific asset provides more details into the risk and options to investigate further.

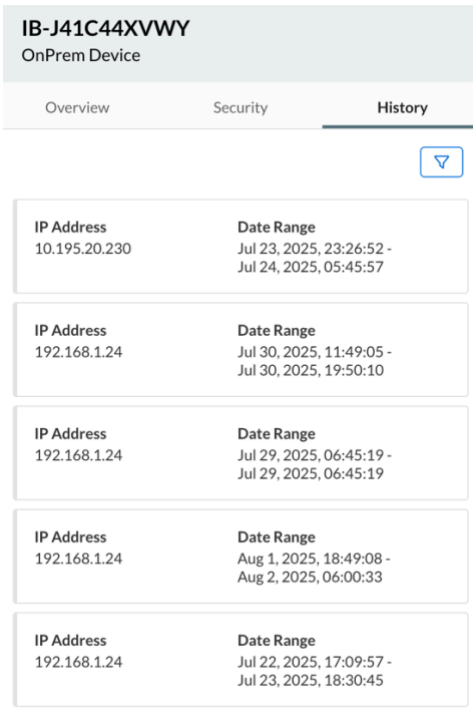
The **Security** tab lists the threats triggered by the assets in a detailed format.



The toggle button allows you to view the **Policy Violations** triggered by the asset for further analysis.

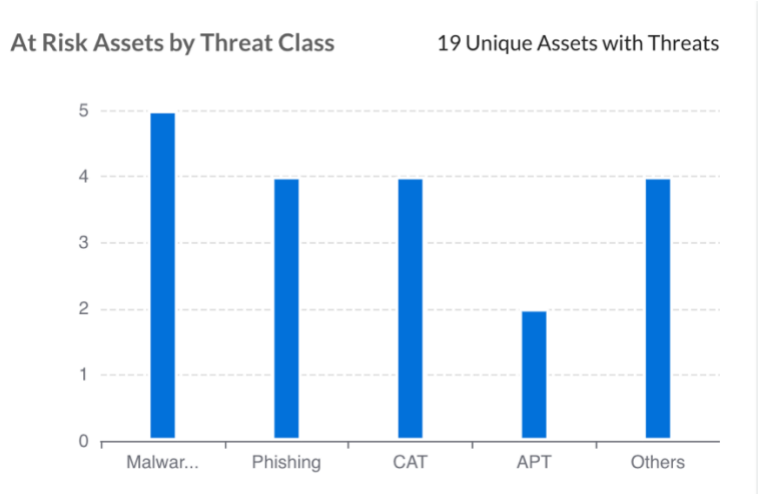


The **History** tab will give a trail of the different IP addresses associated with the asset over time for audit purposes.

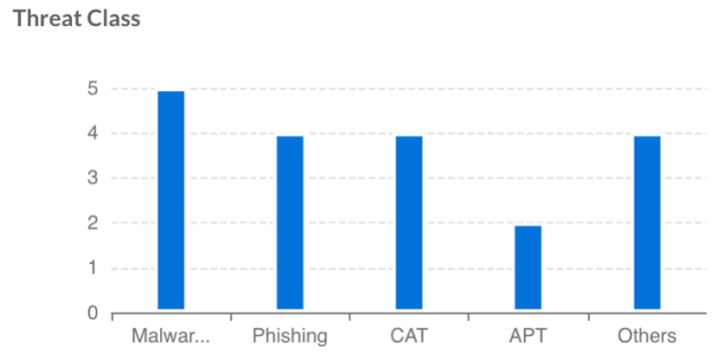


At Risk Assets by Threat Class

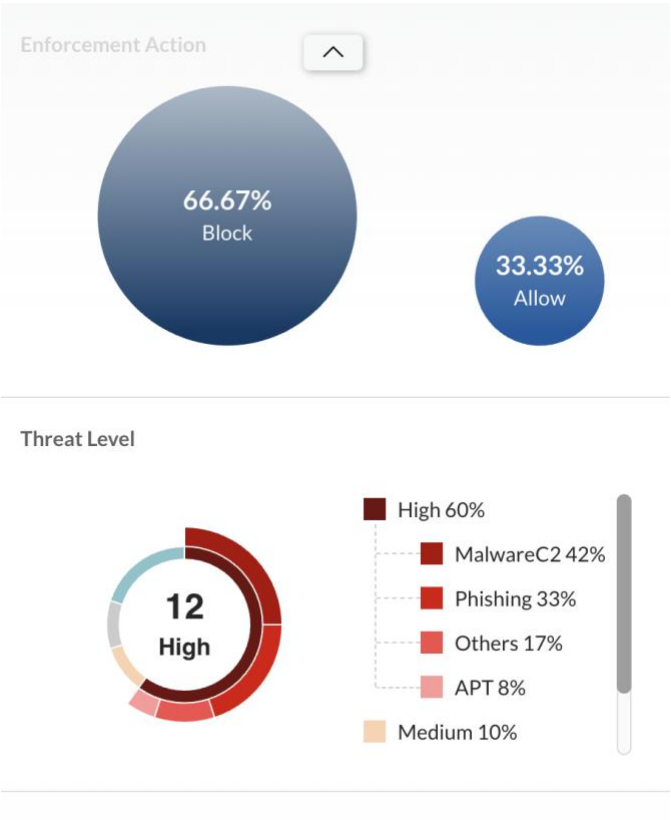
The **At Risk Assets by Threat Class** tile presents the top five threats identified with the option to view all the assets with threats in detail.



The different threat classes identified are displayed in this section and you can select the threat class for the assets you want to view.

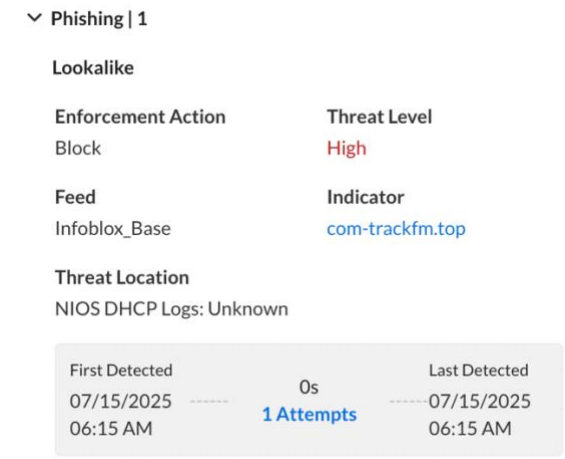


Additionally, other options like the action enforced on the events associated with the asset or the threat level can be used to further drill down.

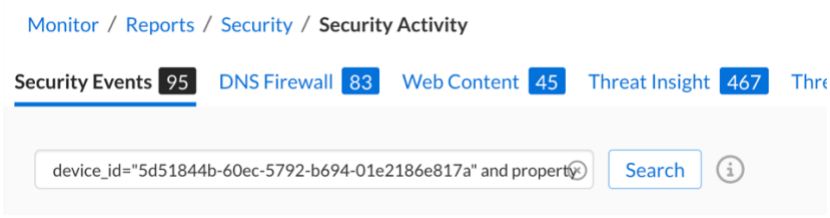


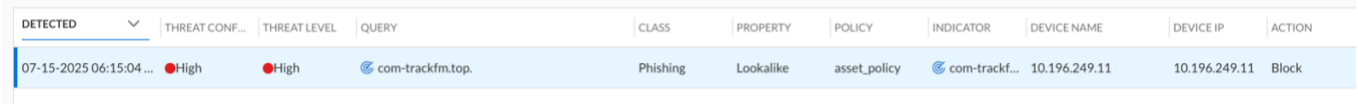
After selecting a specific asset, the **Advanced** tab lists the network interface details of the asset.

In the **Security** tab, you can click on the link to list the related security events. It will redirect you to the **Security Activity** page.



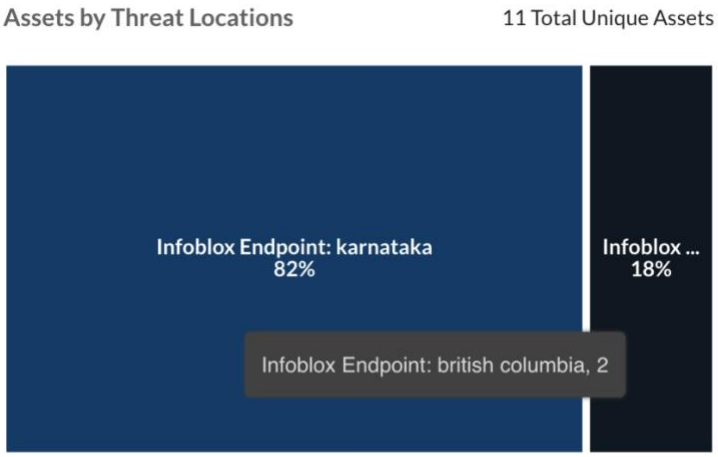
Filtered **Security Events** for the selected asset and threat property type are listed on this page for further analysis.



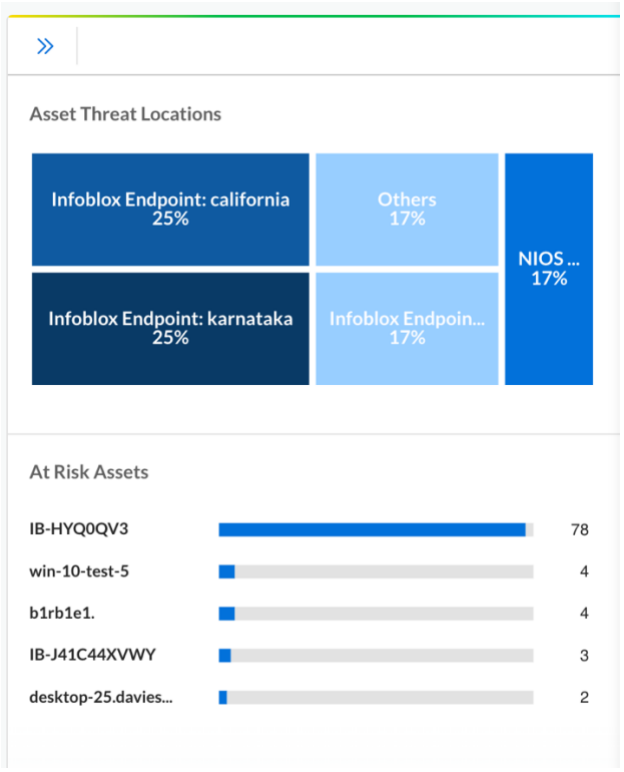


Assets By Threat Locations

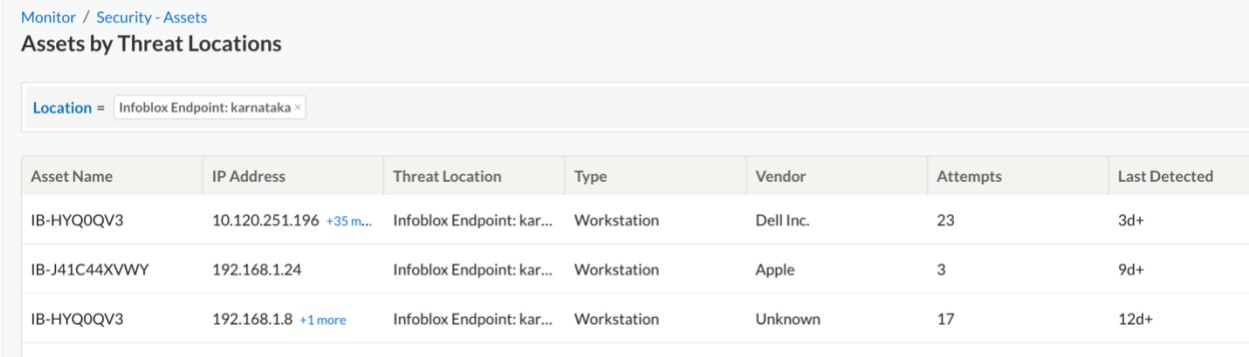
The **Assets by Threat Locations** tile presents the top five threat locations identified, with the option to view all the assets with threats.



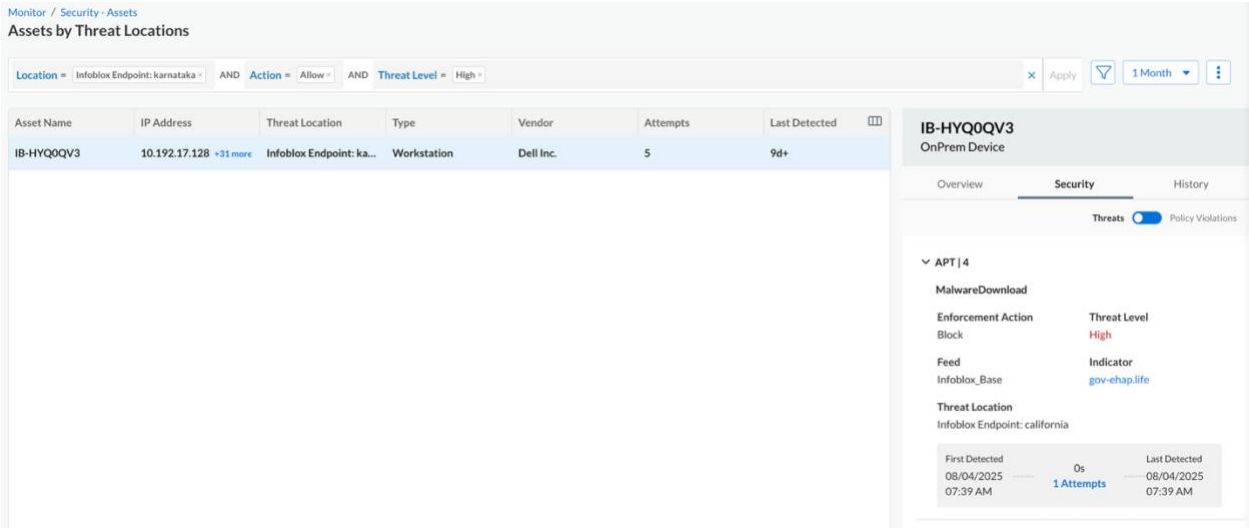
After navigating to the page, the filter section allows you to easily filter the assets based on different parameters, such as **Location**, **Policy Action**, **Asset Type**, etc.



You can filter assets based on a specific location. In this case, only the assets with threat location as “Karnataka” are listed to ease the investigation.

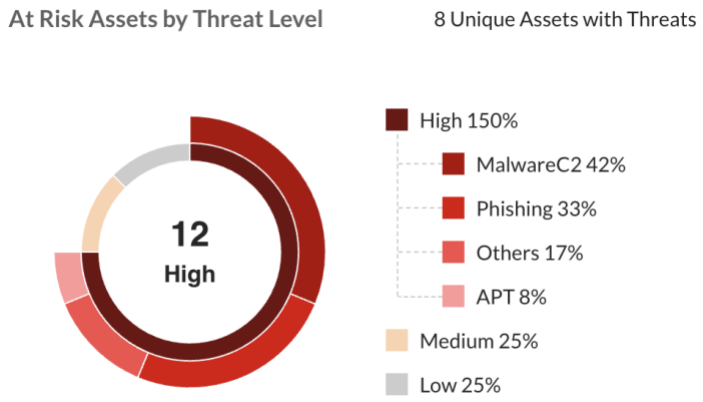


All the threats and policy violations associated with the asset are listed in the **Security** tab which can be used to further investigate the identified security events.

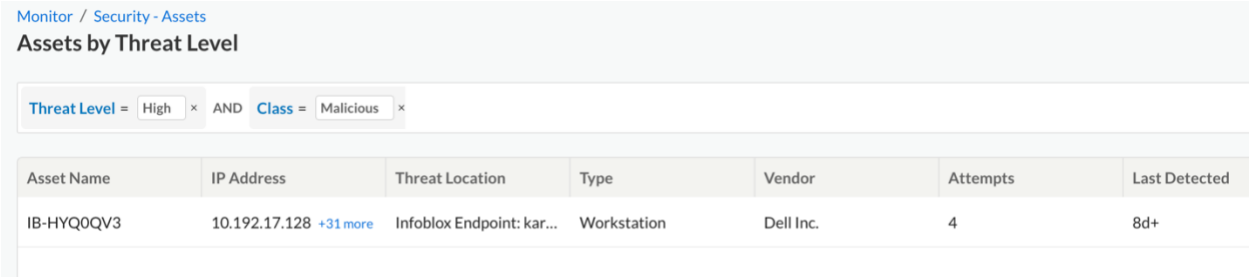


At Risk Assets by Threat Level

The **At Risk Assets by Threat Level** tile presents a consolidated view of different types of threats identified, categorized by threat level and threat property. Upon navigating to the page, you have the option of filtering the identified assets based on the severity of the associated threats.

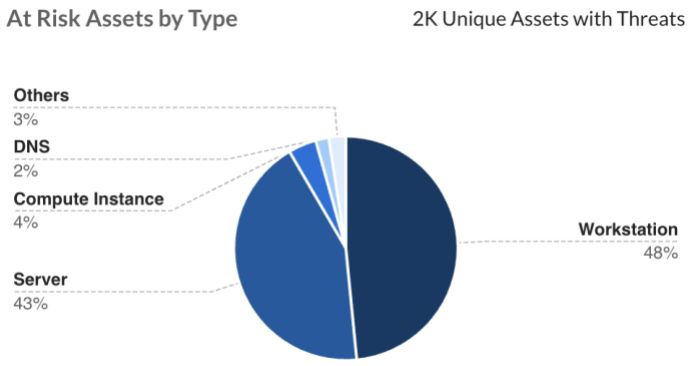


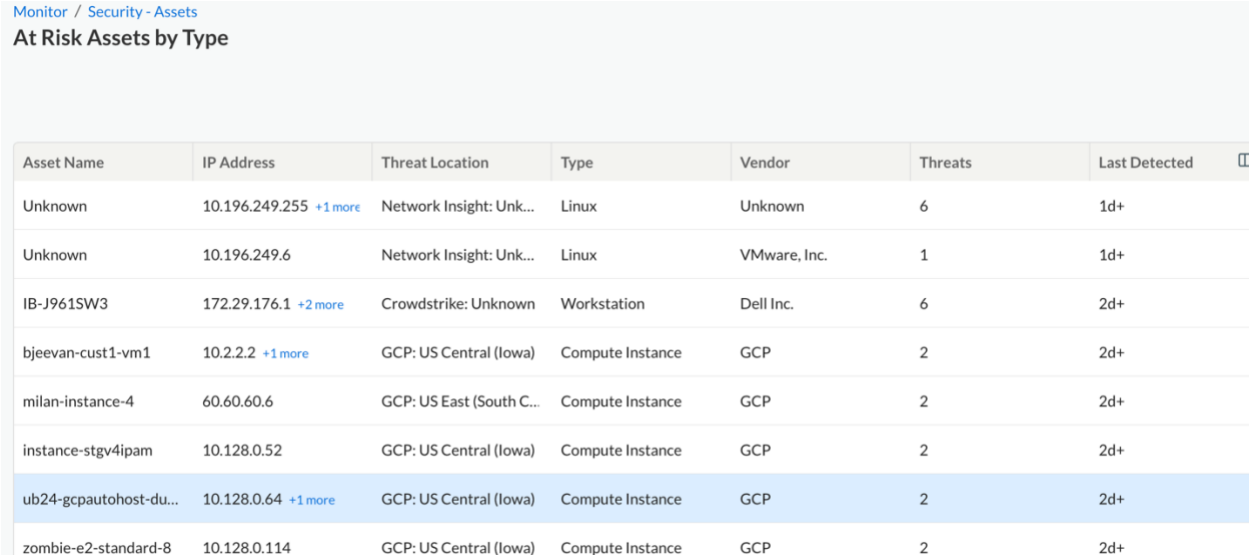
Simply click on the *Threat Level*, or specifically on the threat property, to apply the filter.



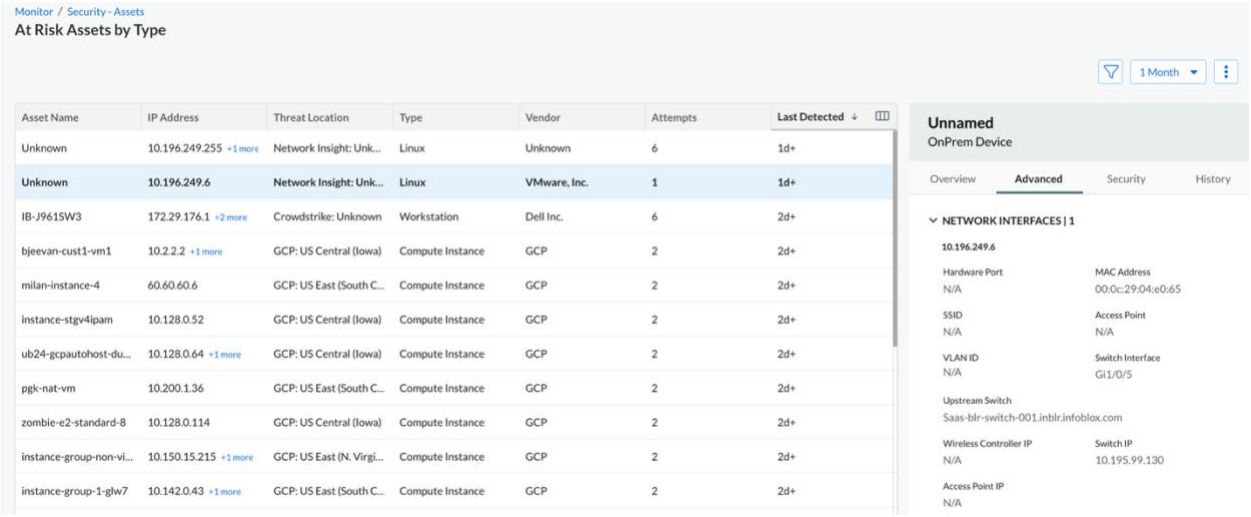
At Risk Assets by Type

The **At Risk Assets by Type** tile provides a consolidated view of the top five asset types that have been identified with associated threats, helping prioritize remediation efforts.

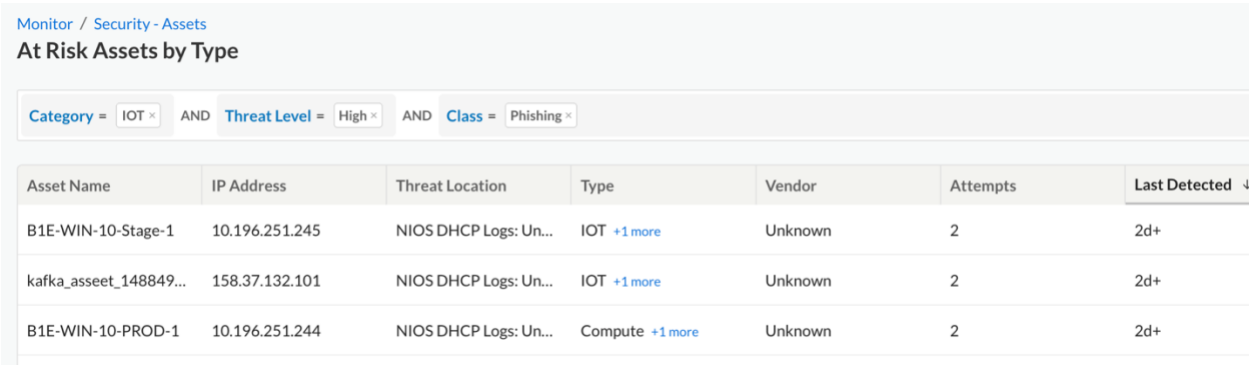




Additional details about the asset can be obtained by selecting the specific asset. Details include information about the asset's network interfaces, connected upstream switch, and ports.

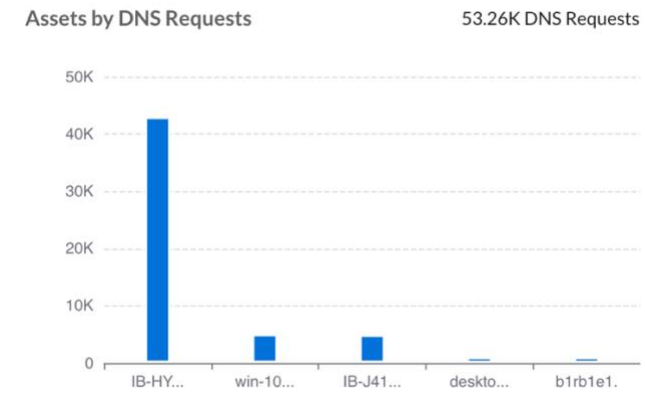


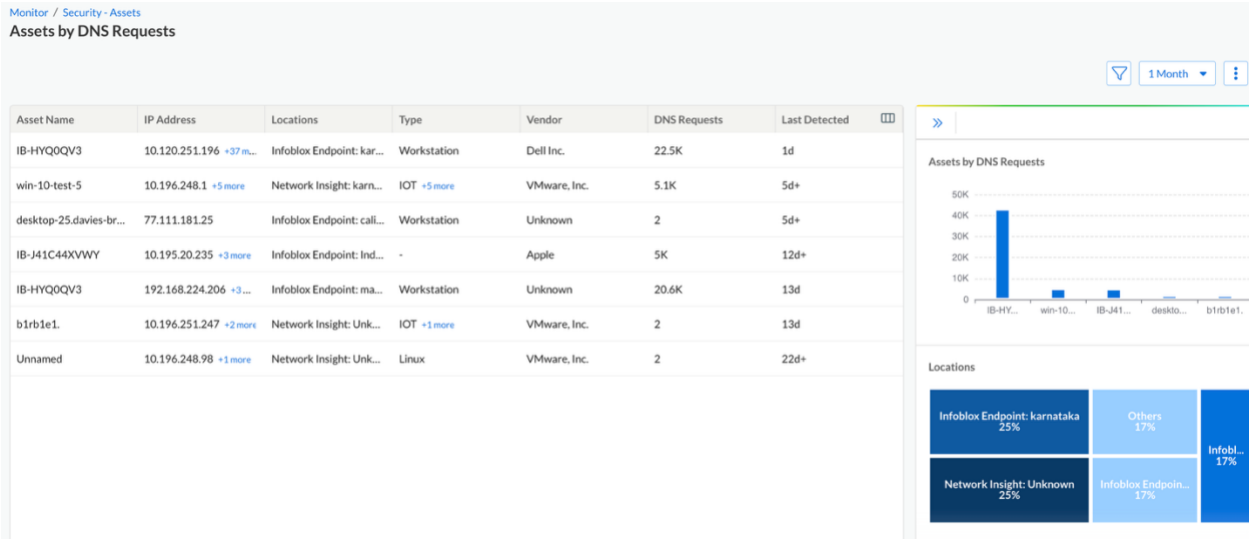
You can easily filter to identify specific asset types and the level of threats that need to be prioritized for safety. This helps reduce the noise and lets you focus on specific assets and their associated threats.



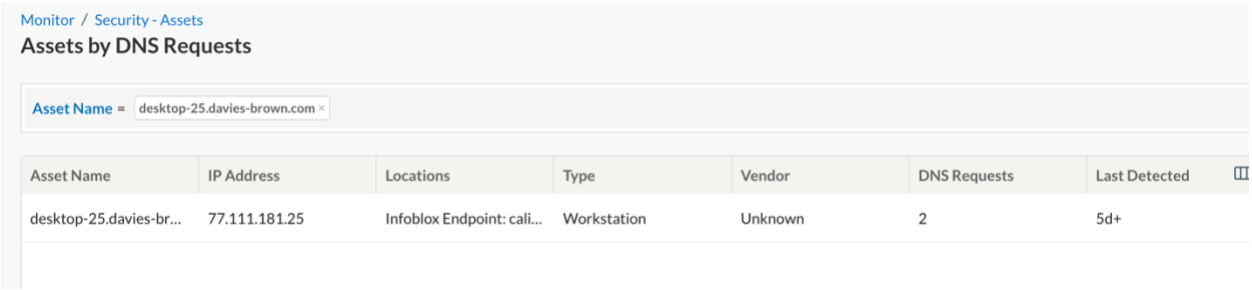
Assets by DNS Requests

The **Asset by DNS Requests** tile presents a consolidated view of the top five assets identified based on the number of DNS requests initiated, with an indication of number of DNS requests initiated by the assets. Upon navigating to the page, it lists all the identified assets along with the number of DNS requests made.

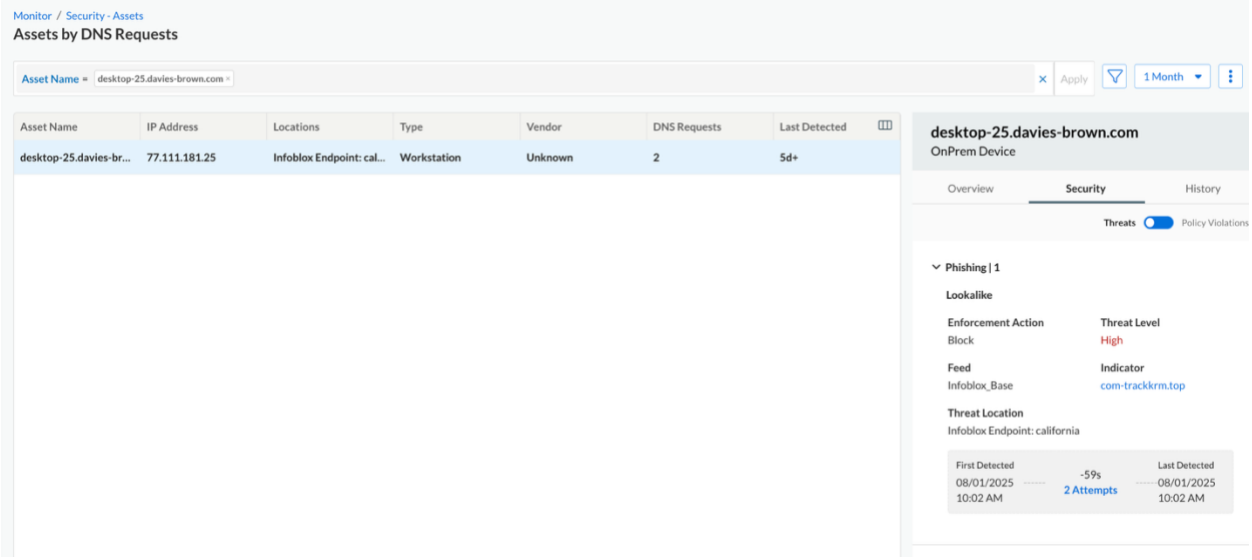




You can filter specific assets based on different attributes to pinpoint to specific assets for easier navigation.

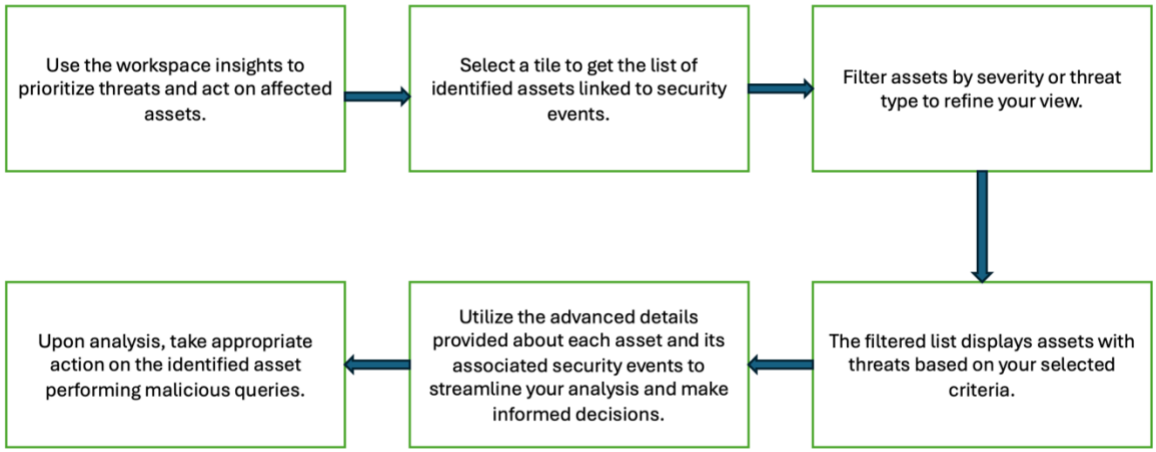


Once filtered, you can view all the threats associated with the asset, making it easier to navigate to the related security events.



Workflow

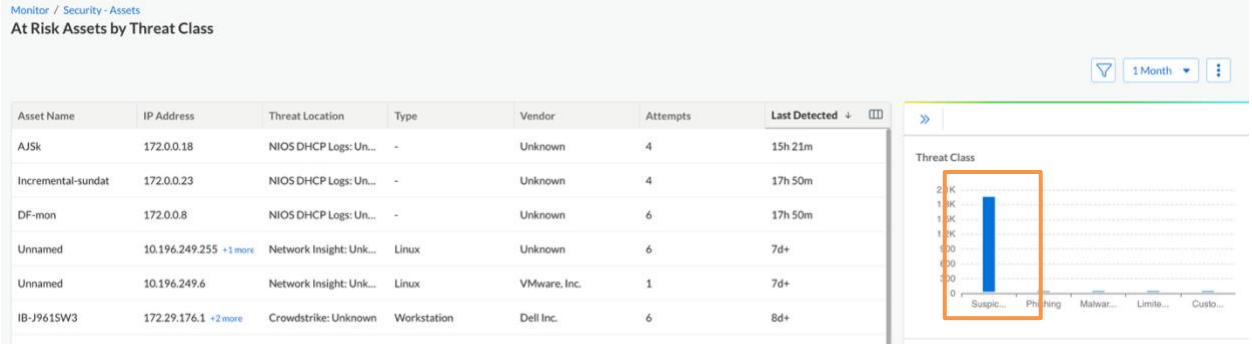
Below is a high-level workflow designed to help assess reported threats efficiently. It enables quick identification of associated assets, including their details and locations, so you can take appropriate action to protect the network.



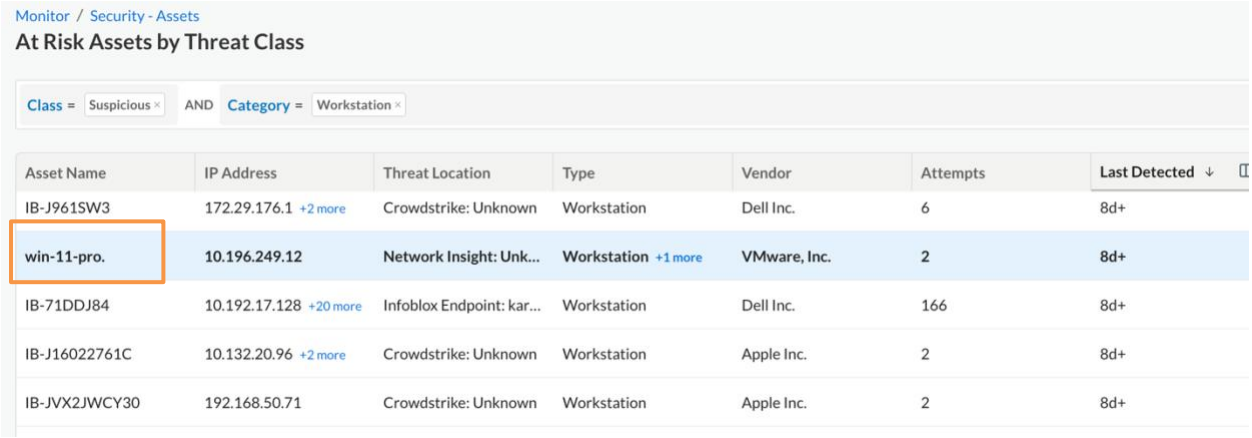
Deployment Use Cases

Assets Connected to Wired Network Generating Suspicious Lookalike Type DNS Queries

By navigating to the **Security Assets** workspace and selecting the *At Risk Assets By Threat Class* section, you can view the list of assets along with the option to easily filter assets based on the threat class. This view helps prioritize response efforts by highlighting which assets are linked to which type of threats, enabling faster triage and investigation.

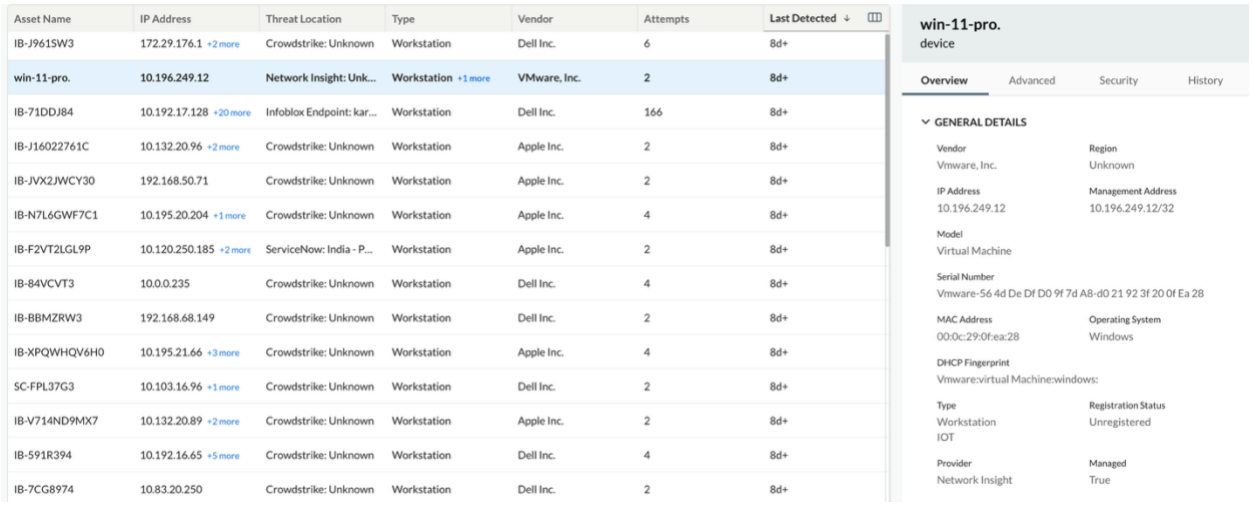


By clicking on the *Lookalike* option in the **Threat Class** section you will be shown only the assets associate with this threat type.



To carry out further investigation of the threat event, you can select a specific asset, and you will get additional details about the asset and its associated events.

Note: Certain additional information will be available if **Network Insights Discovery** has been enabled for the networks from where assets are discovered.

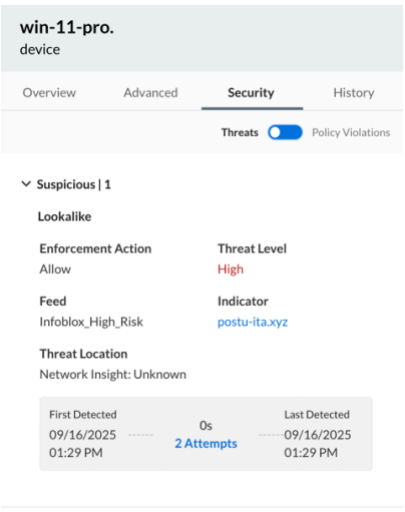


This includes details of the asset, such as:

- IP Address
- MAC Address
- Asset Type
- Operating System
- Connecting Switch Hostname
- Connecting Switch IP Address
- Connected Interface

This same section also provides the details of the threat identified, providing insight into the type of threat, its severity level, action applied, etc.

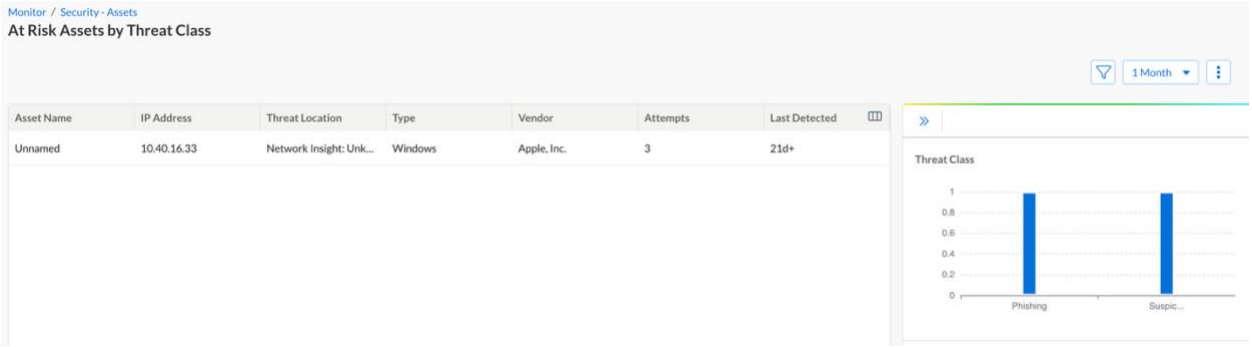
You can also investigate further on the related security events generated for deeper analysis using effective tools like Dossier.



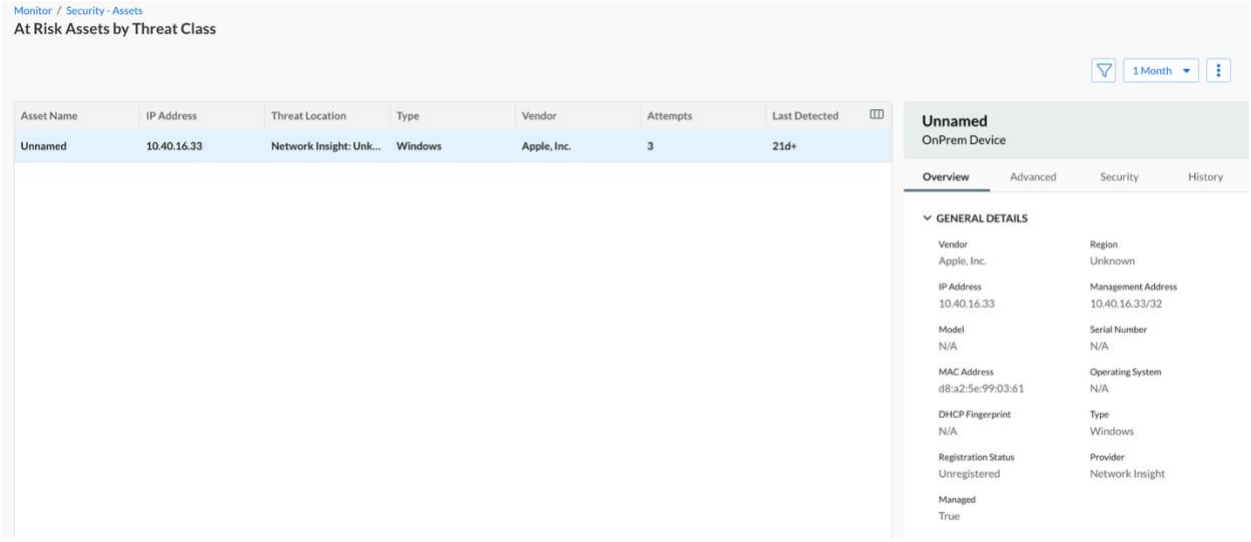
Assets Connected to Wireless Network through an Access Point Generating Suspicious Lookalike Type DNS Queries

In this scenario, we will explore a setup where a wireless endpoint connects to the network through an access point that is centrally managed by a wireless LAN controller. The malicious DNS query is initiated from this discovered endpoint, and we will see how the Security Assets workspace can be effectively utilized to investigate the threat and identify the specific asset and its related information to take appropriate action.

By navigating to the **Security Assets** workspace and selecting the *At Risk Assets by Threat Class* section, you can view the list of assets along with the option to easily filter assets based on the threat class. This view helps prioritize response efforts by highlighting which assets are linked to which type of threats, enabling faster triage and investigation.



By clicking on the *Lookalike* option in the **Threat Class** section you will be shown only the assets associated with this threat type.



To carry out further investigation of the threat event, you can select a specific asset, and you will get additional details about the asset and its associated events.

Note: Certain additional information will be available if **Network Insights Discovery** has been enabled for the networks from where assets are discovered.

This includes details of the asset, such as:

- IP Address
- MAC Address
- Asset Type
- Operating System
- SSID
- Access Point Hostname
- Access Point IP Address
- VLAN ID
- Upstream Switch Hostname
- Upstream Switch IP Address
- Wireless Controller IP Address

This same section also provides the details of the threat identified, providing insight into the type of threat, its severity level, action applied, etc.

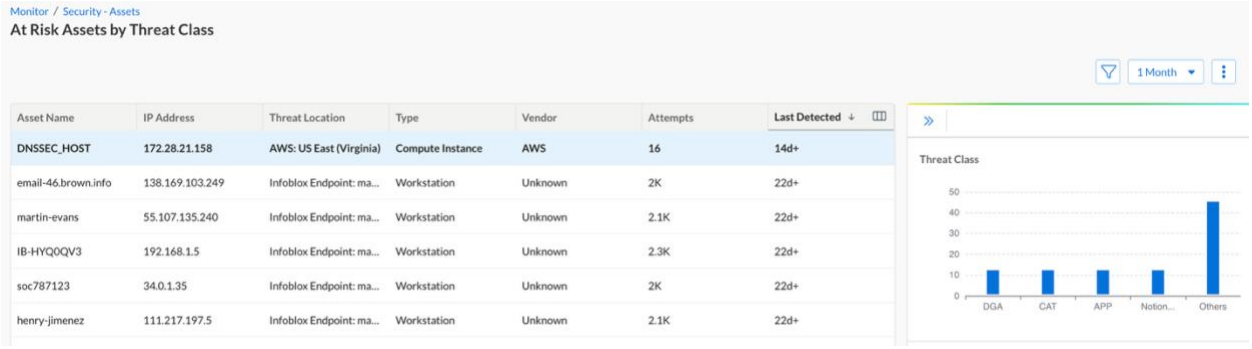
You can also investigate further on the related security events generated for deeper analysis using effective tools like Dossier.

Compromised Assets Deployed in Public Cloud (AWS) Attempting Data Exfiltration

In this scenario, we will explore a setup where an asset deployed in your AWS account is discovered by Infoblox and is forwarding its DNS queries to Infoblox for resolution.

DNS exfiltration is attempted from this discovered endpoint, and we will see how the Security Assets workspace can be effectively utilized to investigate the threat and identify the specific asset and its related information to take appropriate action.

By navigating to the **Security Assets** workspace and selecting the *At Risk Assets By Threat Class* section, you can view the list of assets along with the option to easily filter assets based on the Threat Class. This view helps prioritize response efforts by highlighting which assets are linked to which type of threats, enabling faster triage and investigation.

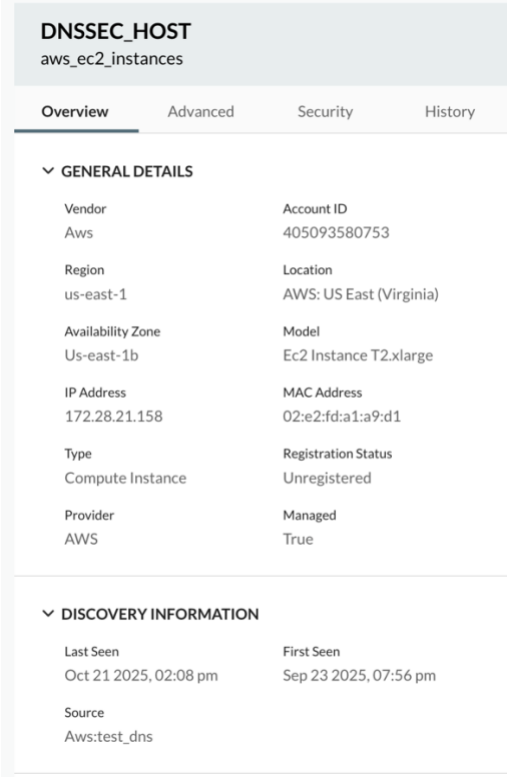


To carry out further investigation of the threat event, you can select the specific AWS asset, and you will get additional details about the asset and its associated events.

This single pane will provide details about the AWS asset to easily identify it in your AWS account to decide upon the appropriate action.

The details include:

- Account ID
- Region
- Availability Zone
- Instance Type
- Source of the Discovered Asset



There are additional AWS-specific details provided in the same section under the **Advanced** tab.

This includes details of the asset, such as:

- Private DNS Name
- Subnet ID
- Instance ID
- Security Group

This same section also provides the details of the threat identified, providing insight into the type of threat, its severity level, action applied, etc.

You can also investigate further on the related security events generated for deeper analysis using effective tools like Dossier.

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com