IronNet

# The IronDefense App for Phantom

## Overview

IronDefense, IronNet's flagship product, delivers cyber analytics and integrated hunt to a variety of public and private sector enterprises. Designed by national security analysts and top intelligence data scientists, IronDefense provides machine-speed detection at scale to identify advanced threats that are often missed by existing commercial cybersecurity solutions. IronNet's collective defense platform, IronDome, shares these behavior-based detections with communities of similar risk profiles to create a defensive fabric across companies, sectors, and nations.

The IronDefense App for Phantom enables security teams to manage alerts more efficiently by integrating teams, processes, and tools together through the automation of tasks and orchestration of workflows. Data ingestion from IronDefense allows users to capitalize on Phantom's ability to automate security actions through playbooks and rapidly triage IronDefense events and alerts in an automated, semi-automated, or manual fashion. Users can also utilize Phantom's mission control feature to access IronDefense events, alerts, and IronDome community activity for investigation, decision, and action.

## How It Works

In IronDefense, an alert is the result of multiple events. Each event is associated with an alert. IronDome provides collective defense information with correlations for each alert and notifications that highlight significant findings from IronDome communities. Events, alerts, and IronDome community information are all available through the IronDefense App for Phantom.

To use the IronDefense App for Phantom, you must first enable IronAPI, IronNet's RESTful API (application programming interface). IronAPI enables IronDefense and Phantom to send and receive the data they need without a graphical user interface. IronAPI is a RESTful API, meaning it conforms to the REST (representational state transfer) web architecture which is designed to provide optimum performance, scalability, simplicity, and reliability. Actions available via our RESTful API include:

- CommentOnAlert
- SetAlertStatus
- RateAlert
- GetEvent
- GetEvents
- GetAlerts
- GetAlertNotifications

- GetDomeNotifications
- GetAlertIronDomeInformation
- GetEventNotifications
- ReportObservedBadActivity

## Core Features

The IronDefense Phantom app provides the ability to leverage the following IronAPI endpoints, each of which provides the ability to seamlessly integrate IronDefense into existing cybersecurity ecosystems.

| Feature | Description |
|---|---|
| CommentOnAlert | Allows a client to comment on any given alert, with the option to send to IronDome (if enrolled). The default request rate limit on this endpoint is 10 requests per second. |
| SetAlertStatus | Allows a client to change an alert's status to progress it through the review process. The default request rate limit on this endpoint is 10 requests per second. |
| RateAlert | Allows a client to rate an alert as part of the review/triage process. The default request rate limit on this endpoint is 10 requests per second. |
| GetEvent | Allows a client to retrieve details for an IronDefense event including the event context. The default request rate limit on this endpoint is 10 requests per second. |
| GetEvents | Allows a client to retrieve IronDefense events for a particular IronDefense alert. Event context information is not included in these event objects. The default request rate limit on this endpoint is 10 requests per second. |
| GetAlerts | Allows a client to retrieve IronDefense alerts in an environment. The response can be filtered based on the alert field parameters and limited to a given number of alerts. The default request rate limit on this endpoint is 10 requests per second. |

| Feature | Description |
|---|---|
| GetAlertNotifications | Allows a client to retrieve alert notifications from IronDefense without pulling duplicate messages that have already been ingested. The default request rate limit on this endpoint is 10 requests per second. |
| GetDomeNotifications | Allows a client to retrieve IronDome notifications from IronDefense without pulling duplicate messages that have already been ingested. The default request rate limit on this endpoint is 10 requests per second. Default is set to Disabled. |
| GetAlertIronDomeInformation | Allows a client to retrieve community IronDome correlation information for an alert. The default request rate limit on this endpoint is 10 requests per second. |
| GetEventNotifications | Allows a client to retrieve event notifications from IronDefense without pulling duplicate messages that have already been ingested. The default request rate limit on this endpoint is 10 requests per second. Default is set to Disabled. |
| ReportObservedBadActivity | Allows a client to submit a domain and/or IP of observed bad activity for the creation of a Threat Intelligence Rule, an event or alert, and IronDome correlations. The default request rate limit on this endpoint is one request per 10 minutes. This limit is imposed as the goal of this endpoint is to ingest malicious activity discovered by other security tools within the enterprise network. It is not intended to provide a means to integrate third-party threat intelligence feeds or to query IronDome for information about indicators of compromise (IoC). |

# Use Cases

The following are four example scenarios that illustrate potential uses of the IronDefense App for Phantom.

## Scenario One:

After ingesting IronDefense data into Phantom, users can share analyst assessments with IronDefense to enable collective defense via the IronDome platform. Other participants in IronDome will be able to use the information to improve their security posture.

## Scenario Two:

After ingesting IronDefense data into Phantom, users can take proactive measures on next-generation firewall (NGFW) and endpoint detection and response (EDR) tools to prevent further attacks. These measures include creating blacklists to alert on or block additional malicious activity and quarantining devices. Employing strategies like these permits IronDefense Phantom app users to expand the utility of IronDefense and increase the ROI of other products integrated with Phantom.

## Scenario Three:

Users can update existing NGFW and EDR alert workbooks to submit observed malicious IoCs to IronDefense to look for correlations across the IronDome community. By sharing these discoveries with IronDome, IronDefense Phantom app users are able to understand the trends of attackers by receiving information on whether the same malicious activity has been observed by other IronDome participants.

## Scenario Four:

IronDefense data within Phantom can also be used to drive analyst workflow automation, such as IT service management (ITSM) ticket creation. By leveraging the IronDefense Phantom app, users can eliminate the manual and tedious process of creating tickets to initiate remediation efforts, allowing Security Operations Center (SOC) analysts to focus their attention on analyzing alerts.

# Download the IronDefense App for Phantom

Existing IronNet customers who have deployed IronDefense can download the IronNet App for Phantom from the Phantom App Store by visiting https://my.phantom.us/apps/ and searching for IronNet. Instructions on how to install and configure the Phantom app will be provided by your IronNet Customer Success representative.