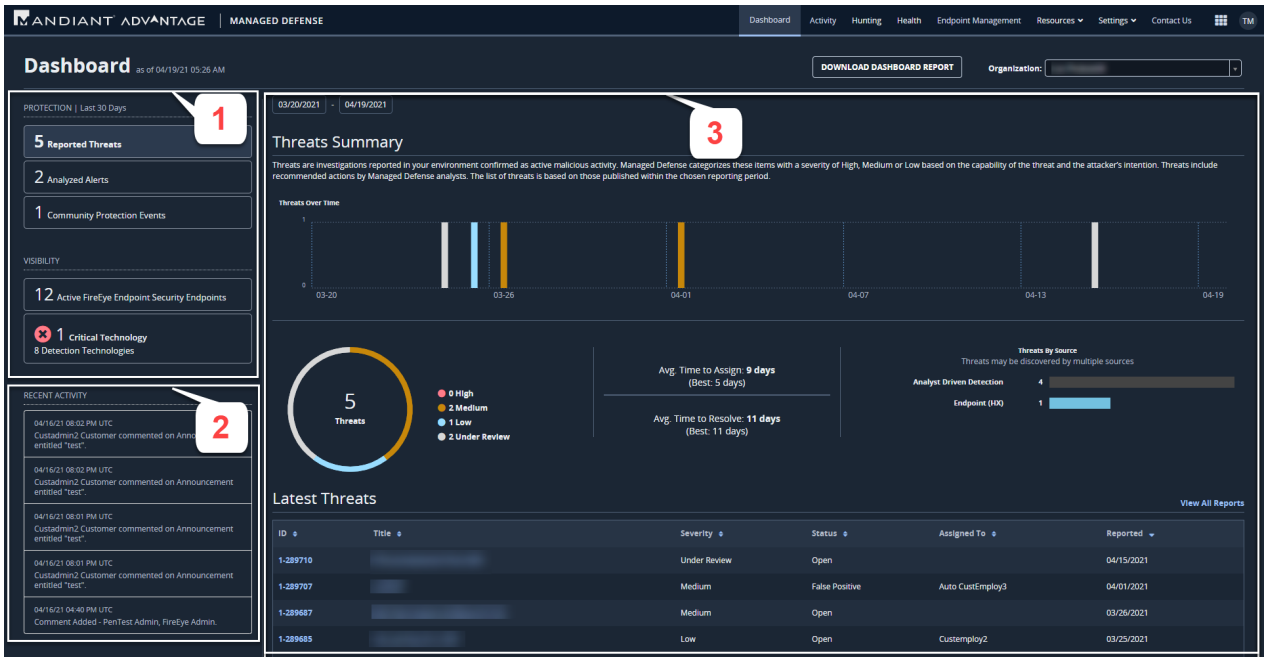
WORKING WITH MANAGED DEFENSE DASHBOARDS

When you first log in to the MD Portal, you will see the Dashboard. The Dashboard provides real-time threat information, protection status, and coverage information for all your network and endpoint devices. The Dashboard page is divided into three sections:



1. MD Portal Dashboard Menu
2. Recent Activity
3. Selected Dashboard View

Dashboard Views

The MD Portal Dashboard menu, located in the left panel, has a number of dashboard views. The Dashboard menu shows summary information related to threats to your network or endpoints by default for the last 30 days. You can change this default filtering by date (see **Filtering Views by Date** for more details). The dashboards are grouped into three areas:

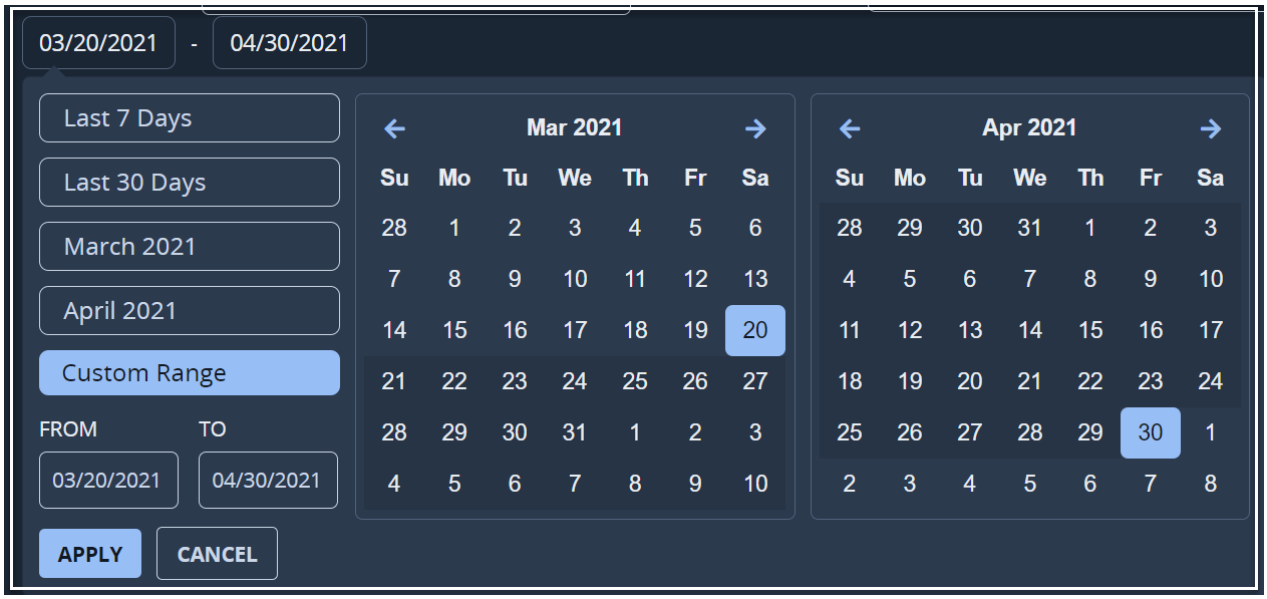
- PROTECTION,
- VISIBILITY, and
- RECENT ACTIVITY

The **Protection Dashboards** allow you to drill down and review information about any reported and attributed threats to your network or endpoints, threat alerts, and analyst-driven investigative activities. The **Visibility Dashboards** provide information on the system health for your connected appliances. The **Recent Activity Dashboard** displays a summary of last five user activity events on your MD service such as compromise reports including Investigation and Incident alerts.

NOTE: Your MD service components, portal views, and dashboards depend on your MD subscription and service type. Contact your MDC if you need to upgrade your subscription type in order to access a specific service component or dashboard option.

Filtering Views by Date

Use the Date Range Selector to filter the information provided in the dashboards such as **Reported Threats Dashboard**, **Analyzed Alerts Dashboard**, and **Community Protection Events** and display activities within a specific time frame. You can also select a fixed date interval that occurs in the past (for example, the last 7 days, last 30 days, the current month, or the previous month) or you can select a specific look-back period. Modified dates only affect the summary information and dashboard charts. The *Latest Threats* table and *Latest Alerts* table shown in the **Reported Threats Dashboard** and **Analyzed Alerts Dashboard** only display the last five reports. Similarly the **Recent Activity Dashboard** displays a summary of last five user activity events on your MD service.



NOTE: The Date Range Selector's default range is **Last 30 Days**.

Protection Dashboards

The Protection Dashboards are designed to provide you with real-time threat protection information for your network and endpoints. In this category you have three dashboards:

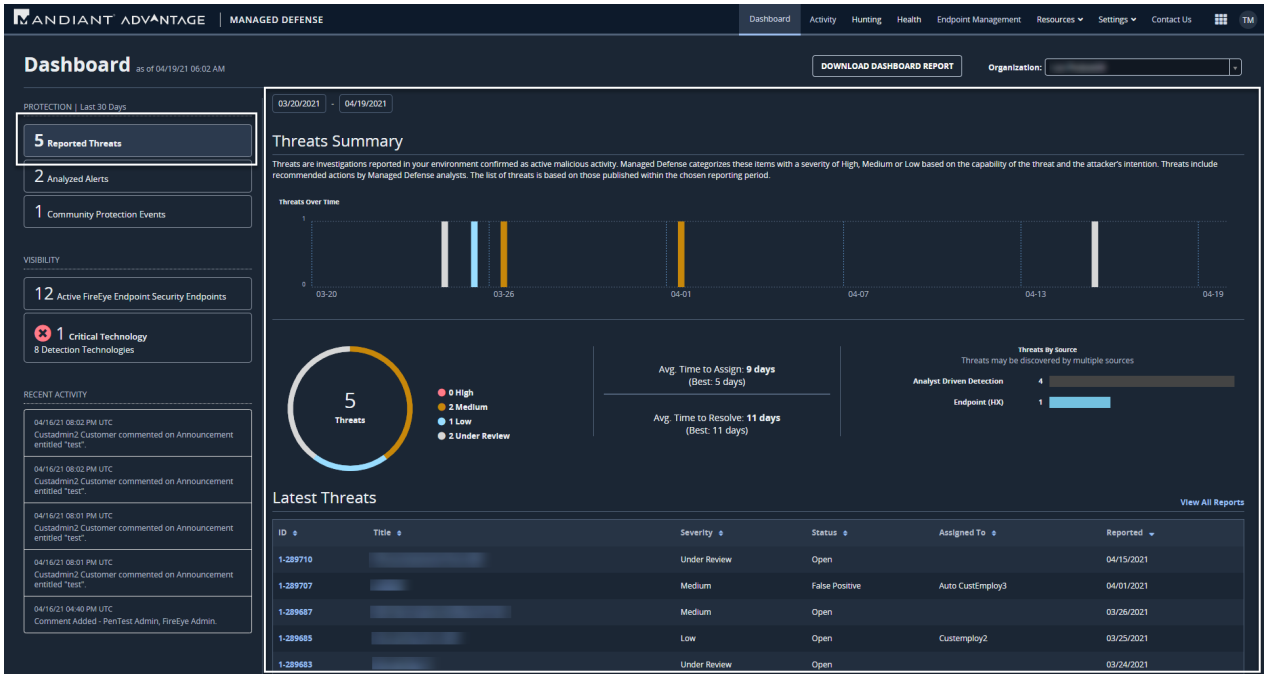
- ***Reported Threats Dashboard***,
- ***Analyzed Alerts Dashboard***, and
- ***Community Protection Events***

Reported Threats Dashboard

The Reported Threats Dashboard displays a summary of all threat activity on your network or endpoints that has been detected and validated by MD. This dashboard view displays two critical threat metrics for your network and endpoints:

- ***Threats Summary***, and
- ***Latest Threats***

You can filter the information by using the Date Range Selector at the left-top of the dashboard.



Threats Summary

The Threats Summary panel displays the following key metrics for detected threats in your environment:

- A graph of high, medium, low severity, and under review compromise reports published within the date range.
- The number of high, medium, low severity, and under review compromise reports published within the date ranges.
- The average efficiency and response time of your security team.
- The number of security threats uncovered by each technology and by *Analyst Driven Detection* in your environment.

Latest Threats

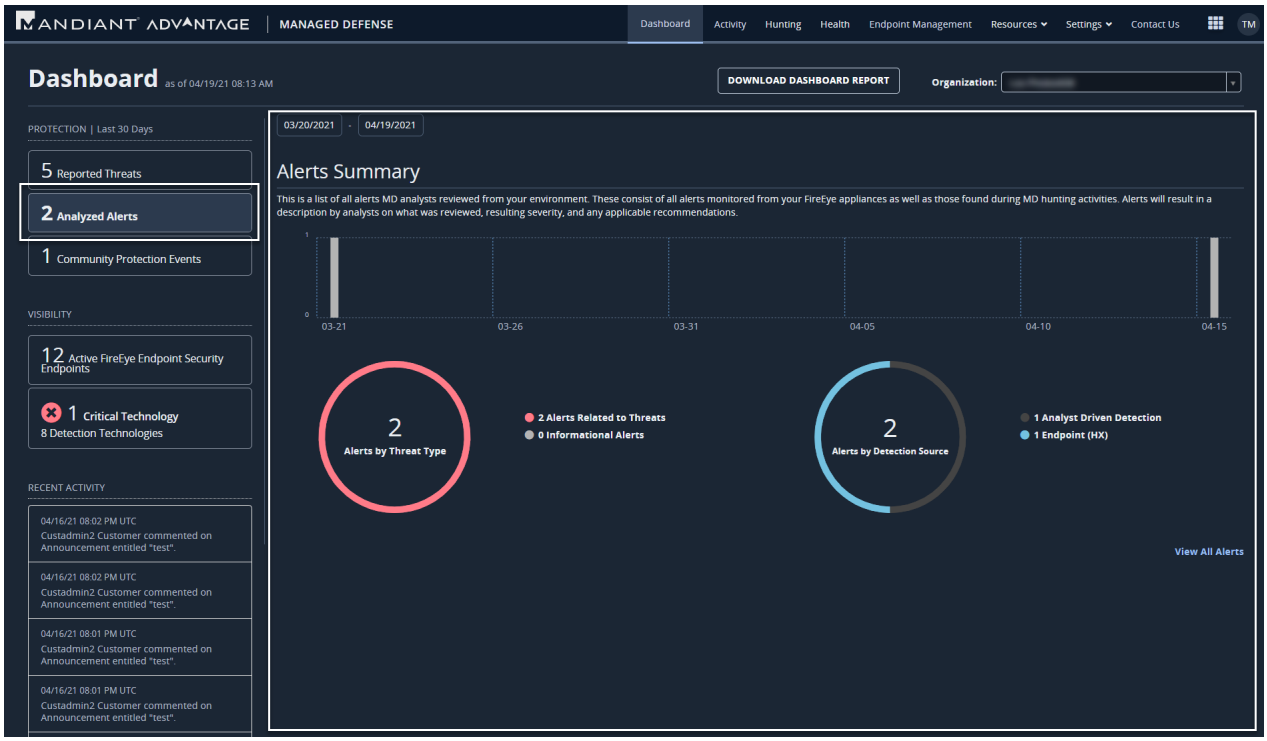
The Latest Threats table displays critical information about the last five compromise reports. You can also drill down into each compromise report by clicking on the specific report link provided in the columns ID or Title. You can view the entire Investigation reports by clicking *View All Reports* link located on the right (see **Reviewing Alerts and Reports (https://docs.mandiant.com/home/reviewing-alerts-and-reports)**).

Report Elements	Description
ID	Unique identifier given to each compromise report
Title	Report name
Severity	Threat level assigned to the report
Status	Report Status • **Open** - the report is still under Investigation • **Resolved** - threat remediation has occurred

Report Elements	Description
	• **False Positive** - the threat is not a true threat
	• **Disputed** - the threat status is being determined
Assigned To	Staff member within your organization currently working on the Investigation
Reported	Report publish date

Analyzed Alerts Dashboard

The Analyzed Alerts dashboard provides key metrics for alerts in your environment through the ***Alerts Summary*** and a link to *View All Alerts* (see **Reviewing Alerts and Reports** **(https://docs.mandiant.com/home/reviewing-alerts-and-reports)**). This is a list of all alerts MD analysts reviewed from your environment. These consist of all alerts monitored from your appliances as well as those found during MD hunting activities. Alerts will result in a description by analysts on what was reviewed, resulting severity, and any applicable recommendations. Filter the data shown by using the Date Range Selector at the top of the dashboard.



Alerts Summary

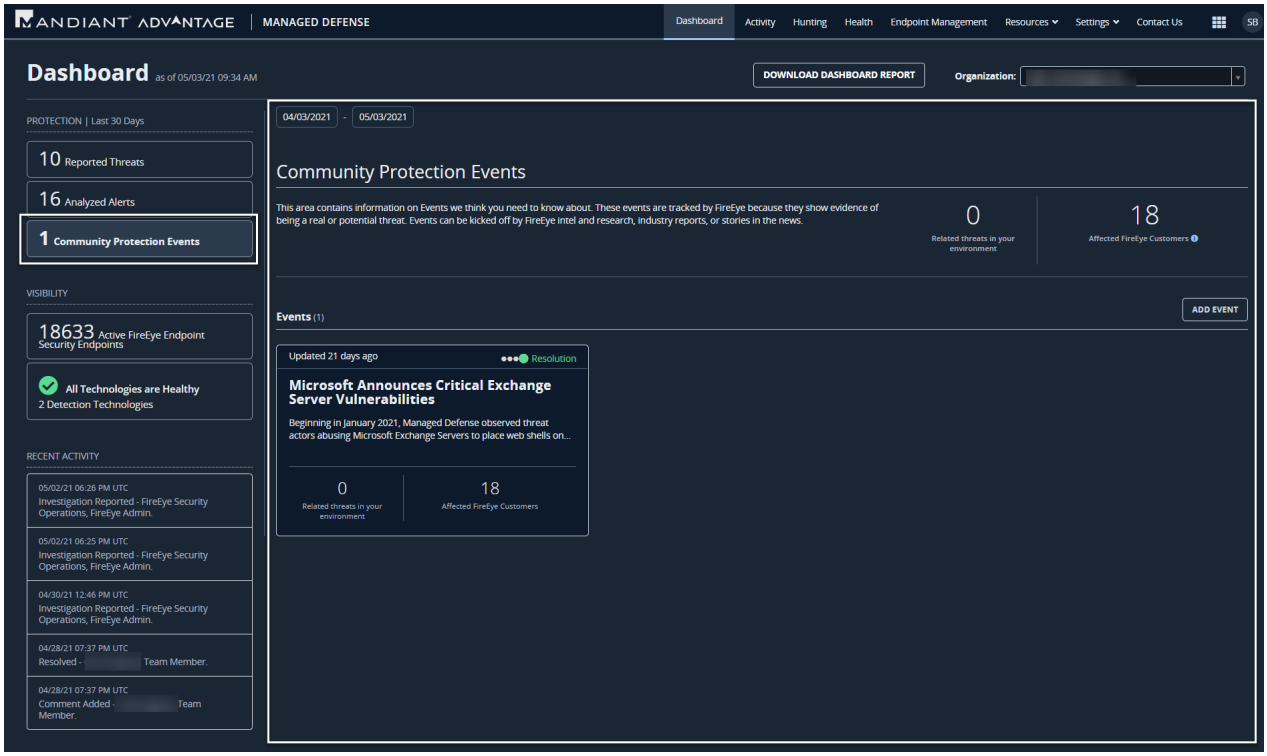
The *Alerts Summary* panel displays the number of alerts within your environment that have completed the MD analyst review process, grouped by alert type and detection source. The *Alerts by Threat Type* graph displays the total number of validated threat alerts and the total number of Informational Alerts.

NOTE: Informational alerts are alerts for any endpoint activity that is not related to a compromise. For example, the legitimate use of administrator tools on an endpoint would trigger an Informational Alert.

The *Alerts by Detection Source* graph displays the number of all alerts detected by your appliances and the number of alerts triggered by a MD analyst during analyst-driven Investigations.

Community Protection Events

Mandiant highlights activity that is of specific interest or has the potential to affect MD clients with *Community Protection Events*. These events are tracked by Mandiant because they show evidence of being a real or potential threat. Events can be kicked off by Mandiant Threat Intelligence and Research, industry reports, or stories in the news. Use this dashboard to drill down and review detailed information on *Community Protection Events*, affected customers, and deployed detections. Filter the events by using the Date Range Selector at the top of the dashboard.



Accessing Community Protection Events

Each individual event can be expanded providing detailed information on the threat, status of detections in your environment, and IOC(s) if available.

Visibility Dashboards

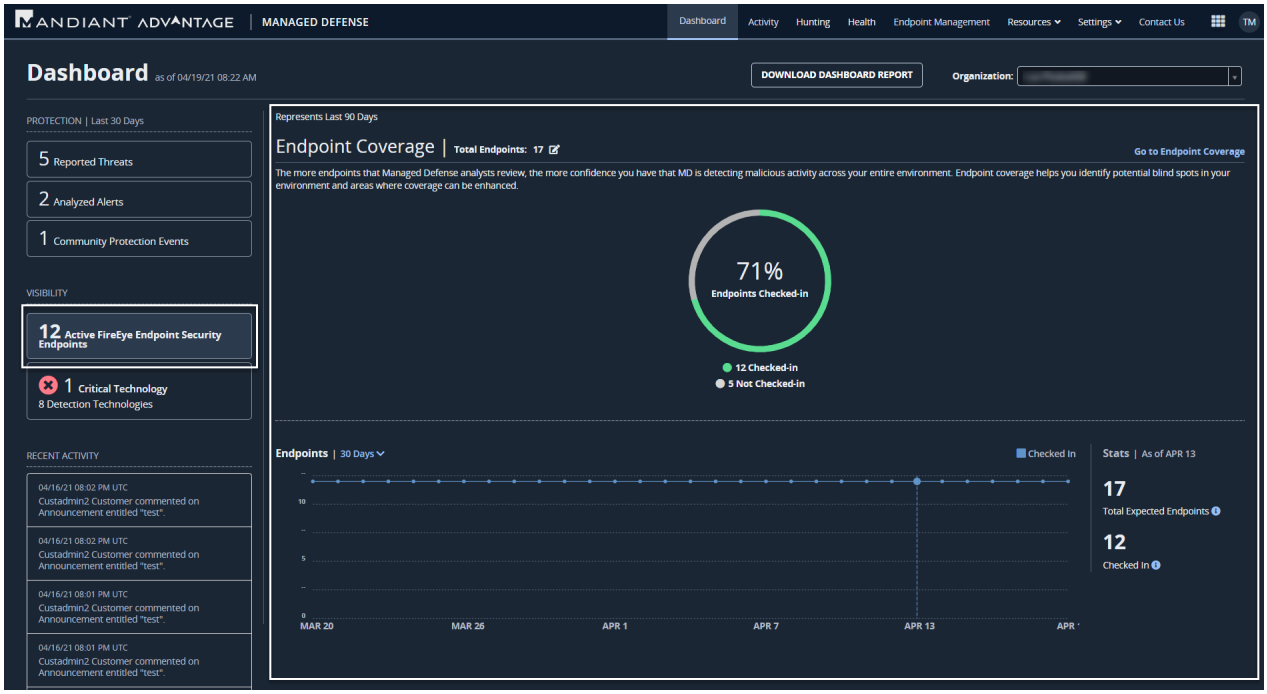
The Visibility Dashboards provide the information about the service coverage, health information you need to ensure all of your endpoints and networks are protected. In this category you have two dashboards:

- ***Endpoint Coverage Dashboard***, and
- ***Detection Technology Health Dashboard***

Endpoint Coverage Dashboard

Endpoint coverage is a critical visibility metric that is essential to reducing security vulnerabilities and breaches across your network. The more endpoints that MD analysts review, the more confidence you have that MD can detect malicious activity across your environment. Endpoint coverage helps you identify potential blind spots in your environment and areas where coverage can be enhanced.

The Endpoint Coverage Dashboard gives you instant visibility into how many endpoints you have connected to your MD service and your endpoint service status in real-time.



Endpoints

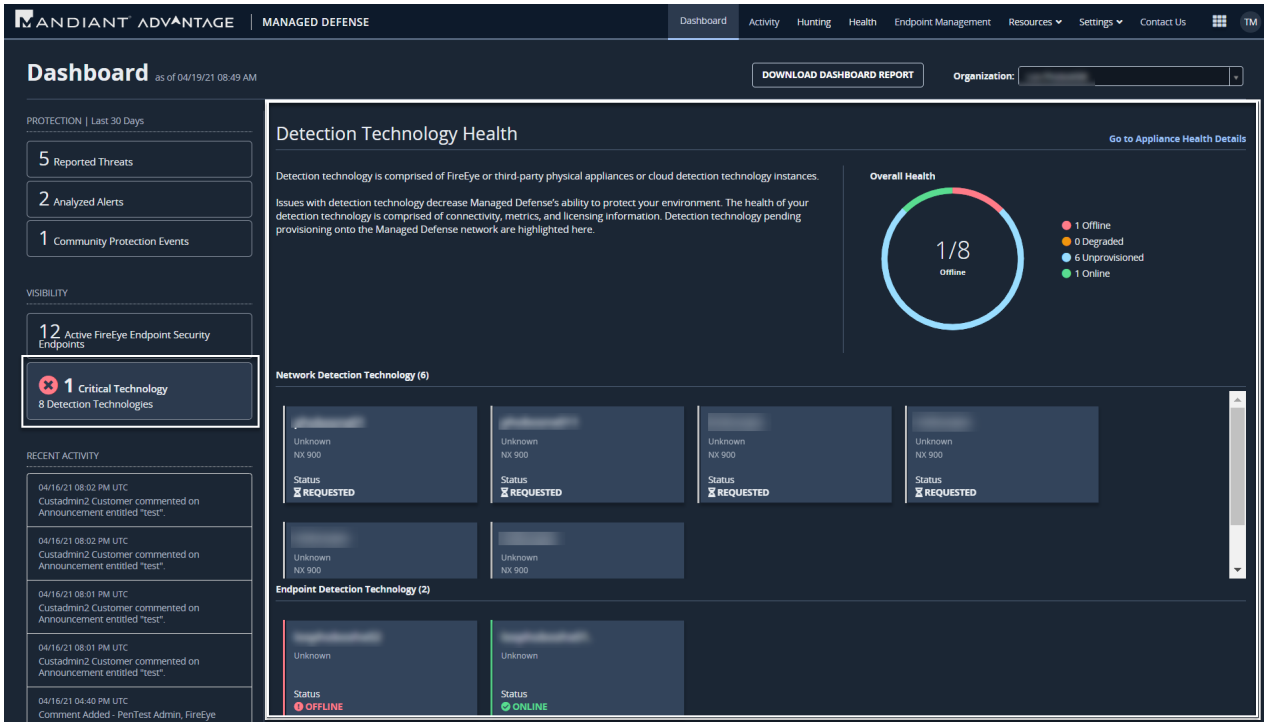
This section allows you to see the total number of endpoints in your environment and exactly where your endpoints stand through Endpoint Check-ins. The Endpoint Check-ins shows a count and percentage for the total number of checked-in endpoints and a count of the total number of endpoints not checked in. Contact your MDC to change the total number of endpoints expected.

To see more details about your endpoint health, click the **Go to Endpoint Coverage** link at the top right corner of the dashboard. See **Monitoring Endpoint Health** **(https://docs.mandiant.com/home/monitoring-endpoint-health)** for more details about endpoint coverage and the Endpoint Health dashboard.

> **NOTE:** The Endpoint Coverage dashboard will be present for customers with Trellix Endpoint Security technology. This dashboard does not exist for customers with only Microsoft Defender for Endpoint technology, but FireEye Endpoint Security metrics will be displayed for customers that use both endpoint technologies.

Detection Technology Health Dashboard

Detection technology is comprised of Trellix or third-party physical appliances or cloud detection technology instances. Potential appliance problems can create vulnerabilities in your network and increase exposure to threats and attacks. Appliance issues also decrease MD service visibility into your environment and create blind spots in your network. The health of your detection technology is comprised of connectivity, metrics, and licensing information. Detection technology pending provisioning onto the Managed Defense network are also highlighted here. The *Detection Technology Health* dashboard provides system health information on all of your appliances grouped by technologies such as *Network Detection Technology*, *Email Detection Technology*, and *Endpoint Detection Technology*. Click on the *Go to Appliance Health Details* link to navigate to Monitoring Appliance Health **(https://docs.mandiant.com/home/monitoring-appliance-health)**.



Recent Activity Dashboard

The Recent Activity Dashboard displays a summary of the last five events on your MD service, including the date and time stamp, the user interacted, and a description of their recorded action.