# ExtraHop Addy User Guide

For more documentation, see https://docs.extrahop.com/.

Published: 2017-04-19

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

# Contents

# About the Addy service

The ExtraHop Addy™ service is a cloud-based service that applies machine learning techniques to automatically determine what is normal behavior and what is unusual behavior in your IT environment without any user configuration. Unlike other machine learning solutions that rely on logs or agent data, the Addy service applies machine learning technology to wire data. When the Addy service is activated, you can browse and investigate anomalies from the **Metrics** section of the Web UI on the Discover appliance.

Overall, the Addy service offers the following types of help:

- Uncover potentially hidden issues
- Collect high-quality, actionable data to identify root causes of anomalies
- Find previously unknown performance issues, security issues, or infrastructure quirks
- Gain deeper insight into your network

**Important:** The Addy service does not analyze sensitive information and data types.

The Addy service provides you with high-quality, actionable data about anomalies—but does not replace decision-making or expertise about your network. The following best practices explain how to determine which anomalies are worth further investigation and when to take action.

### Investigate anomalies in the Discover appliance

Anomalies are displayed in the **Metrics** section of the Discover appliance. When you click on **Metrics**, the Anomalies page loads with a list of anomalies for the selected time interval.

When you click on an anomaly title, you navigate to the Device or Application page that contains the anomalous metric data observed at the time of the anomaly. This page also contains metrics related to the anomaly, which gives you a big picture view of what is happening on your network. You can then drill down on specific URIs, clients, and servers to find the source of the anomaly, and then decide how to act.

For example, if you see an FTP server error anomaly detected for a server, you can navigate to view metrics for that server in the Discover appliance, and then drill down on the anomalous error by user or client IP address to identify who is generating the error.

### Investigate anomalies by changing the time interval

By changing the time interval, you can view anomalies that might have occurred during a reported problem. For example, does the time frame of the anomaly coincide with a reported issue, such as slow load times or login times? You can also change the time interval to compare anomalies from the past month to the current date, which gives you a sense of whether the occurrence or severity of anomalies is changing over time.

### Investigate anomalies by protocol

Certain protocols might be more important to your organization because of their role in security, commerce, or communication processes. By filtering by protocol, you can quickly monitor real-time anomalies associated with critical protocols.

For example, an FTP 530 error anomaly might indicate that someone is trying to gain unauthorized access to information on your network. Or Citrix server and client latency anomalies might indicate that clinicians cannot access patient information in a timely fashion. Selecting different protocols can also show you how anomalies correlate to each other.

Or, for example, an anomalous HTTP response time followed immediately by an anomalous CIFS server processing time might suggest that web servers are dependent on how quickly CIFS storage can send and receive files.

# Get started with the Addy service

The following sections explain how to connect to the Addy service and how to navigate anomaly detection in the Discover appliance.

Before you begin

You must meet the following requirements before you can detect anomalies with the Addy service:

- An Addy service license
- Ability to connect to ExtraHop Cloud Services, which requires full system privileges and might require access through any firewalls
- A Discover appliance with at least four weeks of stored wire data metrics
- If you want to receive email notifications, contact ExtraHop Support for configuration assistance

## Connect to ExtraHop Cloud Services

After you acquire a license for the Addy service, the license status and ExtraHop Cloud Services settings are automatically updated on your Discover appliance.

**Before you begin**
You must have ExtraHop administrator (full system) privileges to access the ExtraHop Admin UI and to connect to Cloud Services.

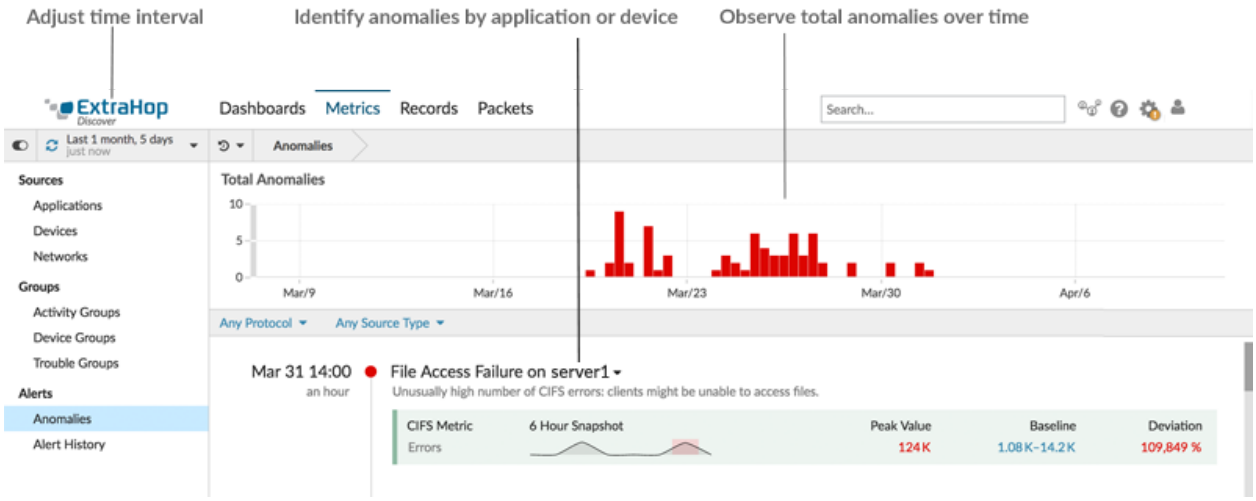
1. Log into the ExtraHop Admin UI.
2. In the Network Settings section, click **ExtraHop Cloud Services**.
3. Click **Terms and Conditions** to read this content.
4. After becoming familiar with the Addy service terms and conditions, select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

**Next steps**
If you cannot connect to ExtraHop Cloud Services, check your firewall rules. The Discover appliance must be configured to connect to ExtraHop Cloud Services through a transparent proxy. If the problem persists, contact ExtraHop Support for help.

## Navigating anomaly detection

After connecting to Cloud Services, the Addy service automatically begins to calculate baselines from stored Discover appliance metrics and detect anomalies. To browse anomalies, log into the Web UI on the Discover appliance and select **Metrics**. The Anomalies page appears, which displays the following information about anomalies detected from your wire data.

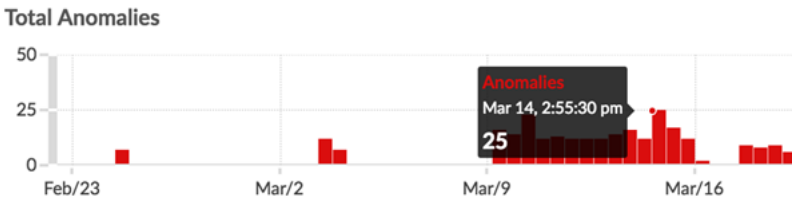
- The time interval, which shows you the time period for the anomalies you are seeing. You can adjust the time to view previously-detected anomalies. To see active, ongoing anomalies in your environment, change the time interval to **Last 30 minutes**.
- The Total Anomalies chart, where you can view the number of concurrent anomalies that occurred for specific time periods.
- Anomalies by application or device, where you can find details including the anomaly description and metric values for the anomalous behavior. Anomalies are sorted by their start time. The anomaly that started the most recently is listed first.




## Explore the Total Anomalies chart

The Total Anomalies chart provides a summary of detected anomalies (y-axis) over time (x-axis). Each bar in the chart represents the total number of concurrent, active anomalies that were detected during a specific time period. Look for the tallest bar to determine when the most anomalies occurred in a time period.

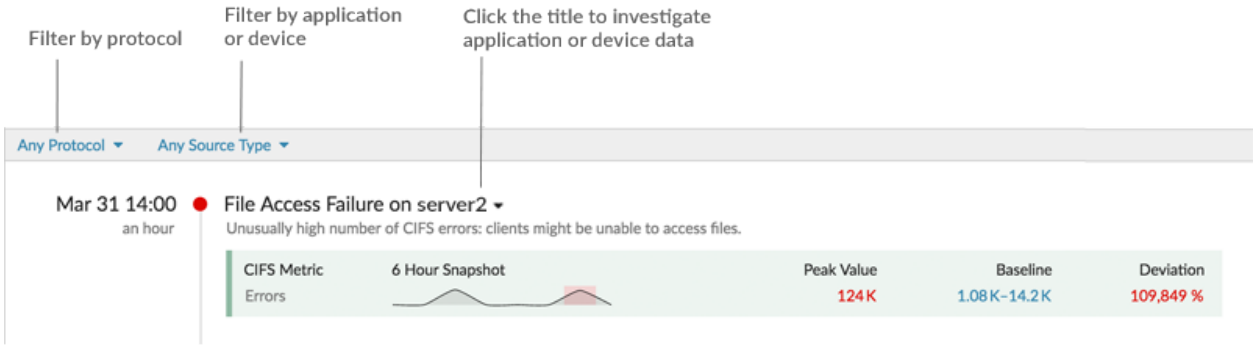
- Hover over a bar to view information, such as date, time, and the number of detected anomalies for a specific time period.



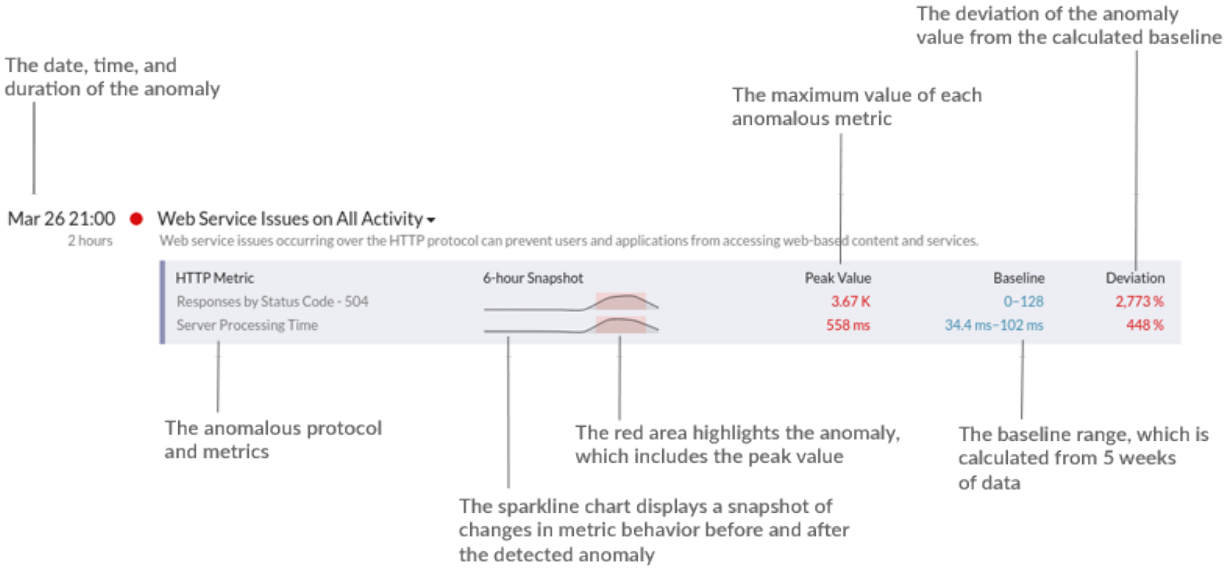

- Click and drag across an area on the chart (which will become highlighted in green) to zoom in on a specific time period. The time interval dynamically updates in the Discover appliance, and details about each anomaly that occurred in the updated time period are displayed below.


## Explore anomalies by application or device

You can filter anomalies by protocol and source type and then navigate to an Application or Device page in the Discover appliance to investigate anomalies in the context of overall network activity (as shown in the following figure).




Details about each anomaly are described in the following figure. These details provide information about each anomalous metric observed for a single application or device.




Because more than one anomalous metric can be associated with a single application or device, you can evaluate how concurrent anomalies, which occurred at the same time, might contribute to an issue. For example, when browsing anomalies through the Addy service in the ExtraHop Web UI, you might notice an anomaly for one of your web servers, where HTTP server processing time and status code anomalies occurred at the same time. You could then investigate by clicking the anomaly title to navigate to the Device page for that web server.

### Sparklines and values

Sparklines are simple line charts that help you learn about the metric behavior that has lead up to the anomaly. The sparkline charts displays a snapshot of metric data from the time frame around the duration of the detected anomaly (such as 6 hours), and not the overall time interval from the top of the page (such as the last 7 days).

The red area on a chart highlights the anomalous metric values, which includes the peak value, on the sparkline. The peak value, baseline, and standard deviation of the anomalous metric values from the baseline are calculated by the machine learning engine of the Addy service.

**Duration**

The duration of the anomaly, listed below the date and time, indicates how long the anomalous value was detected by the Addy service. The minimum duration of an anomaly is one hour, because the Addy service detects anomalies by analyzing metric data with 1-hour granularity.

If the duration value is displayed as **ONGOING**, the anomalous metric is in the process of being detected.

# Working with anomaly detection

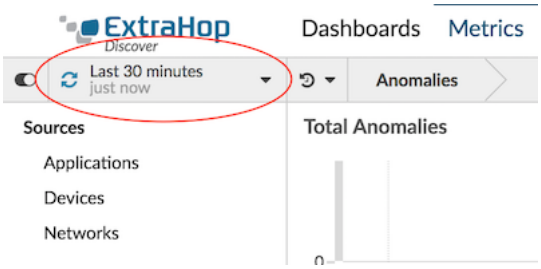
The following procedures describe how to filter and investigate anomalies in the Discover appliance.

## Change the time interval

The Anomalies page displays all of the anomalies that were detected within the time interval that is set for the Discover appliance. You can change the time interval with the global time selector.

The Addy service detects anomalies by analyzing metric data with 1-hour granularity. This means that anomalies are detected through the Addy service by the hour.

1. Log into the Web UI on the Discover appliance and click **Metrics**.
2. In the top left corner of the page, click the time interval as shown in the following figure.




3. From the Time Interval tab, select one of the following options:

| Option | Description |
|---|---|
| **Last 30 minutes** | Displays the last 30 minutes of detected anomalies, and filters active ongoing anomalies to the top of the page. |
| **Last 6 hours** | Displays the last six hours of detected anomalies. |
| **Last day** | Displays the last 24 hours of detected anomalies. |
| **Last week** | Displays the last seven days of detected anomalies. |
| **Last** | Displays the anomalies detected within a customized unit of time.<br>1. Type the number for the unit of time.<br>2. Click the drop-down list and select **minutes**, **hours**, **days**, **weeks**, **months**, or **years**.<br>3. Click **Save**. |
| **Custom time range** | Displays the anomalies detected within a fixed date and time range.<br>1. Click the drop-down field. A calendar dialog box opens.<br>2. Click a day to specify the start date for the range. One click specifies a single day. Clicking another day specifies the end date for the range. Click the back and forward arrows on the calendar to change the month displayed on the calendar. |

4. Click **Save**.

   The global time interval includes a blue refresh icon and gray text that indicates when the Web UI last refreshed the page. To refresh the Anomalies page for the specified time interval, click the refresh icon.

## Filter anomalies by protocol

By default, anomalies for all protocols are displayed. You have the option to filter anomalies by protocol.

1. Log into the Web UI on the Discover appliance and click **Metrics**.
2. Below the Total Anomalies chart, click **Any Protocol**. All protocols are selected by default.
3. Click **Select All** to deselect all the protocols. Select one or more protocols from the drop-down list.
4. Click anywhere outside of the drop-down list. A filtered list of anomalies appears.

## Filter anomalies by source type

By default, anomalies for both applications and devices are displayed. You have the option to filter anomalies by source type.

1. Log into the Web UI on the Discover appliance and click **Metrics**.
2. Below the Total Anomalies chart, click **Any Source**.
3. Select **Application** or **Device** from the drop-down list.
4. Click anywhere outside of the drop-down list. A filtered list of anomalies appears.

## Share an anomaly by URL

You can access the URL for an individual anomaly, which you can then share with other ExtraHop users.

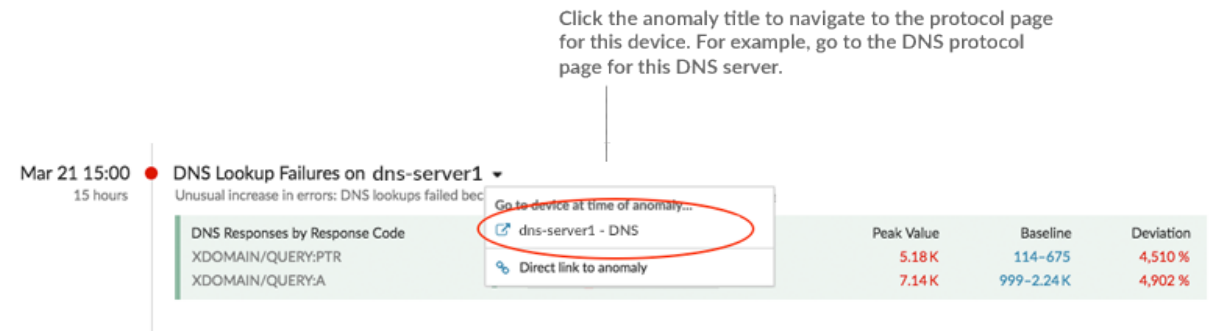
1. Log into the Web UI on the Discover appliance and click **Metrics**.
2. Click the title of an anomaly that you want to share, and then select **Direct link to anomaly**.
   An anomaly page with the selected anomaly appears.
3. Copy the URL from the browser window.

   The URL links directly to the anomaly in the Discover appliance with the same time interval.

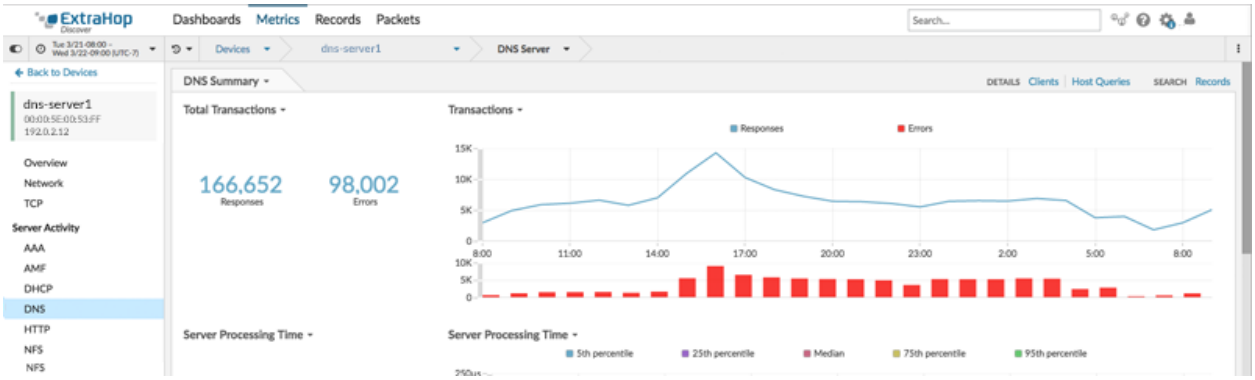
## Investigate an anomaly from a protocol page

On the Anomalies page, you can find high-level information about what type of unusual behavior occurred, when the behavior occurred, and the application or device name that is associated with the behavior. You can then jump from the anomaly into the Application or Device page in the Discover appliance to find specific details and context about how the unusual behavior is affecting your network.

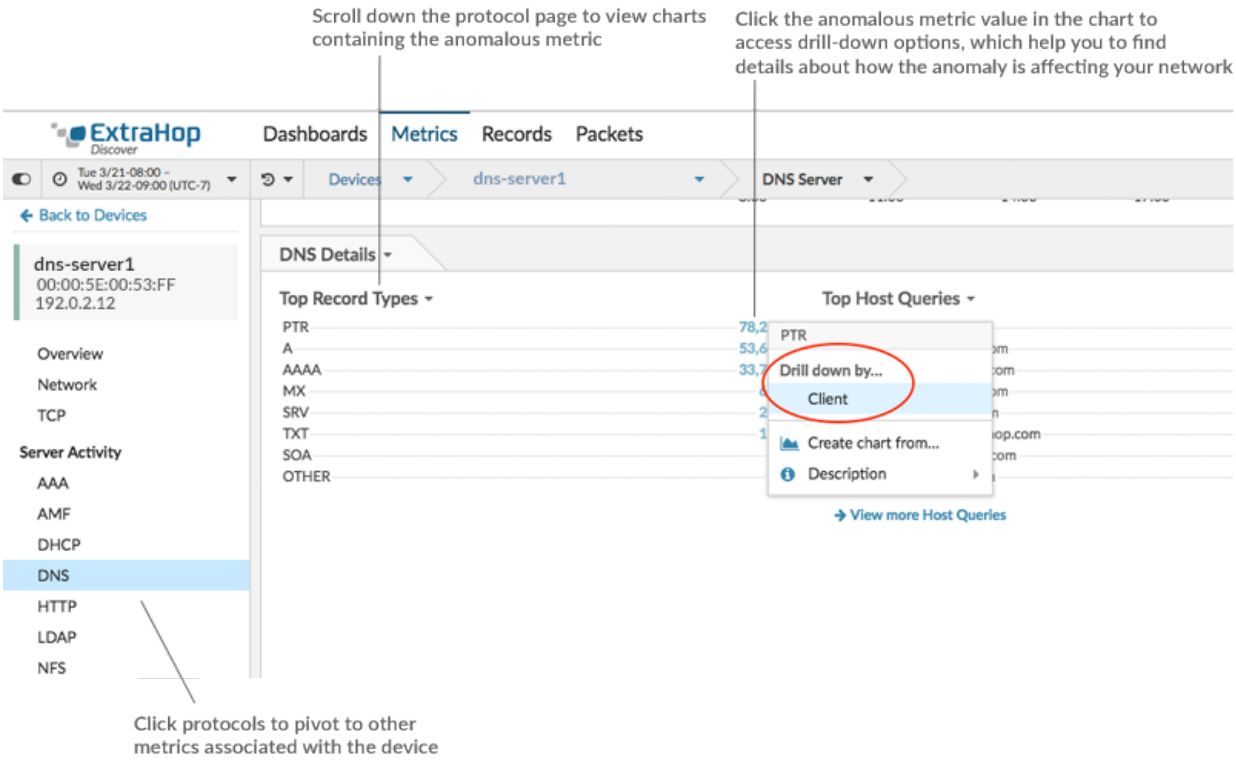
1. Log into the Web UI on the Discover appliance and click **Metrics**.
2. Find the anomaly that you want to investigate.
3. Click the anomaly title and then select the application or device name from the drop-down, as shown in the figure below.




A protocol page for the device or application appears, which displays all of the metric data associated with that specific device or application, as shown in the figure below.




4. From a protocol page, you can then drill down on metrics to find specific details, and pivot to other protocols to find related metrics, as shown in the figure below.



**Next steps**

- Drill down on metrics from a device protocol page
- Drill down on metrics from an application page

# Appendix

The following sections contain reference information about the Addy service.



## How the Addy service works

This section explains how the Addy service identifies anomalies.

Anomalies are unexpected deviations from normal patterns in device or application behavior. By detecting an anomaly as soon as it happens, you can identify and resolve a potential issue before it becomes a larger problem. You can also review historical anomaly data to investigate issues related to known security or network outage events.

In most network monitoring tools, anomalies are detected through manually-configured alerts and trend models for individual devices. However, as your network changes—because of hardware reconfigurations or the addition of applications to your network—these types of alerts and models can become quickly outdated and potentially inaccurate. Addy automatically delivers consistent and accurate results about anomalous metrics and protocols without requiring manual configuration for individual devices. The Addy machine learning engine analyzes historical baseline behavior of individual devices, and automatically adapts to each device across time when there are changes to baseline data in your network.

Here is how Addy anomaly detection generally works: the metrics that the Addy machine learning engine analyzes come from wire data that is collected by your Discover appliance. The Discover appliance processes this data, generates metrics, and associates the metric data with protocols, devices, and applications. Addy retrieves a subset of protocol metrics from the Discover appliance to analyze and report results about detected anomalies.

The algorithm that drives the machine learning engine in Addy calculates baselines and adapts to changing variations in protocols and metric data to determine patterns of normal network behavior. Outliers, or anomalies, are then detected based on three variables:

- Observed data, collected in real-time by the Discover appliance
- Baseline data, calculated from 5 weeks of historical data collected by the Discover appliance
- Threshold value, which is automatically adjusted by the algorithm based on historical metric data and heuristics defined by IT networking domain experts at ExtraHop

> **Note:** If you need to define a specific threshold value for an anomaly, which might be associated with a service level agreement (SLA) for example, we recommend manually configuring an alert in the Discover appliance.

Essentially, an anomaly is detected when observed data deviates from baseline data by a significant amount. You can then view analysis results about anomalies on the Anomalies page in the Web UI of the Discover appliance. For each anomaly, Addy provides the measured deviation (which is the difference between the observed value and the baseline), the anomaly value, and the baseline value (which contains a range that is considered as normal) at the time of the anomaly.

Addy also provides anomalous 50th percentile or 75th percentile values for a subset of metrics that account for server processing time.

## Glossary for Addy Service

The following section defines terminology for the Addy service.

**Anomaly**

Metric activity that deviates from what is standard, normal, or expected.

**Application**

In the ExtraHop system, applications are user-defined containers for metrics that are associated with multiple devices and protocols. These applications can be created through the ExtraHop Trigger API. By default, an All Activity application is available for all users, which provides metrics for all devices and protocols seen by the ExtraHop appliance.

**Atlas Remote Analysis**

Atlas Remote Analysis is an ExtraHop service that provides monthly reports created by analysts. The Atlas team of analysts perform an unbiased analysis of network data and identify areas in IT infrastructure where improvements can be made.

**Baseline**

A baseline is a range of values that represent a normal background level of activity, which is calculated based on 5-weeks worth of data. The baseline is the basis for comparison with observed values to detect changes in metric activity.

**Deviation**

A quantity calculated to indicate the extent of change from a baseline.

**Device**

Devices are objects on your network that have been automatically discovered and classified by the ExtraHop system. Metrics are available for every discovered device on your network.

**Discover appliance**

The ExtraHop Discover appliance provides the ability to analyze and visualize all of your network, application, client, infrastructure, and business data. The Discover appliance passively collects a copy of unstructured wire data—all of the transactions on your network—and transforms this data into structured wire data.

**Protocol**

A protocol defines the format and the order of messages exchanged between two or more devices, as well as the actions taken on the transmission or receipt of a message or other event.

**Machine learning**

Machine learning is a data analysis method where algorithms are designed to iteratively and independently learn from previous computations and adapt to new changes in data.

**Metric**

A metric is a measurement of observed network behavior. Metrics are generated from network traffic, and then each metric is associated with a protocol.

**Sparkline chart**

Sparkline charts are small line charts that help you learn about the metric data behavior that led to an anomaly. The dotted line represents the baseline or expected value at each time point, and the solid line represents the deviation or observed value. The duration of the anomaly is highlighted in red in the chart.