Anomaly Detection FAQ

Published: 2018-07-17

Here are some answers to frequently asked questions about anomaly detection by the ExtraHop Addy service.

- How are anomalies detected by the ExtraHop system?
- How secure is Addy?
- What data is sent from the Discover appliance and ExtraHop Reveal(x) to the Addy service?
- What type of anomalies are detected?
- Which security anomalies does Addy detect in ExtraHop Reveal(x)
- Which IT operations anomalies does Addy detect?
- After connecting Addy, how far back can an anomaly be detected?
- How quickly can an anomaly be detected?
- How do I see ongoing anomalies?
- Can I get an email alert for detected anomalies?
- Can Addy help me detect chronic network issues?
- Does Addy support Discover appliance and ExtraHop Reveal(x) connections through a proxy?
- Is anomaly detection available on the ExtraHop Command appliance?
- Does Addy detect anomalies associated with custom metrics?
- After the Addy license expires, can I still view my previous anomalies?

How are anomalies detected by the ExtraHop system?

After you apply your Addy license and connect your Discover appliance or ExtraHop Reveal(x) appliance to ExtraHop Cloud Services, Addy begins to apply machine learning technology to your wire data automatically. Addy evaluates 4-weeks of data to calculate a range of expected network and user behavior that spans hundreds of metrics and several protocols. Addy determines what is normal with the Addy machine learning engine, which includes a proprietary algorithm that combines time series decomposition, unsupervised learning, heuristics, and domain expertise to evaluate data. Addy then detects deviations from the expected data range of metric values. Addy is always learning about changes to your network's traffic patterns and does not require additional configurations.

You can view and interpret anomalies on the Anomalies page in the Web UI.

For more information, see How the ExtraHop Addy service works.

How secure is Addy?

The cloud-based Addy service is designed to be secure from end-to-end. Unlike a typical SaaS solution, Addy does not ingest payloads, filenames, strings, or other data categories that could contain sensitive information. Sensitive data remains on-premise and under your control. ExtraHop received SOC 2, Type 1 compliance certification for the Addy service.

For more information, see the ExtraHop Addy: Security Overview datasheet.

What data is sent from the Discover appliance and ExtraHop Reveal(x) to the Addy service?

Addy takes advantage of the unique processing capabilities of the Discover appliance and ExtraHop Reveal(x) appliance to "pre-process" wire data for hundreds of metrics on-premise. These appliances encrypt metric values and IP addresses that are sent to Addy. Addy does not receive sensitive data such as filenames, strings, or payloads from these appliances. Custom metrics are not sent to Addy.

For more information, see the ExtraHop Addy: Security Overview datasheet.

What type of anomalies are detected?

Anomalies are unusual deviations from normal network behavior. Depending on the type of Addy license you purchased, Addy detects several categories of security and IT operations anomalies.

Which security anomalies does Addy detect in ExtraHop Reveal(x)

With the ExtraHop Reveal(x) license, Addy detects anomalies associated with several security risks, including the following scenarios:

- Command and control activity
- Brute force attacks
- Reconnaissance activity
- Remote login attempts
- Lateral movement activity
- Data exfiltration
- Rogue DHCP servers

For more information, see ExtraHop Reveal(x) Security anomalies.

Which IT operations anomalies does Addy detect?

Addy detects anomalies associated with several network infrastructure and performance use cases, including the following scenarios:

- Failed login or authorization attempts
- Database errors and performance issues
- Poor user experience associated with Citrix sessions
- Infrastructure performance issues, such as DHCP configuration or network congestion
- Email service degradation
- File storage access issues
- Web application errors

Note that you will not see these anomalies if you have ExtraHop Reveal(x). For more information, see IT operations anomalies.

After connecting Addy, how far back can an anomaly be detected?

After you first connect to Addy, you can look for anomalies starting one week back. Addy then detects all new anomalies moving forward. Addy anomalies are displayed on the Anomalies page in the Web UI.

Note that Addy requires four weeks (28 days) of data to calculate an expected range of metric values. The expected range represents normal network behavior. Data processing is typically completed within a few hours.

How quickly can an anomaly be detected?

Currently, Addy analyzes data every hour. Addy then sends any identified anomalies back to the appliance within minutes.

How do I see ongoing anomalies?

Change the time interval to the **Last 30 minutes** and then visit the Anomalies page in the Web UI. Ongoing anomalies are listed at the top of the page.

Can I get an email alert for detected anomalies?

Yes. First, you must configure an anomaly alert from the Alert page in the Discover appliance or ExtraHop Reveal(x). An anomaly alert lets you specify which device name, application name, security

anomaly category, IT operations category, or metric you want to receive an email for. You can also assign a severity level to the alert. Then, configure email notification settings for your anomaly alert.

Can Addy help me detect chronic network issues?

Addy focuses on detecting anomalies for new abnormal deviations from four weeks of historical behavior.

To help you determine whether an anomaly is a chronic issue instead of an occasional deviation, we recommend that you continuously monitor your environment for trends in network behavior. The ExtraHop Atlas report service is another good way to identify chronic issues, such as constant DNS lookup failures or a high number of errors, and receive a recommended remediation an issue.

Does Addy support Discover appliance and ExtraHop Reveal(x) connections through a proxy?

In ExtraHop 7.0, Addy and ExtraHop Cloud Services support implicit and explicit proxies. The proxy requires that DNS resolve all *.extrahop.com domains, and the outbound 443 port is open to all IP addresses on the internet. These settings are implemented on the firewall for the proxy's source IP address.

For more information on configuring an explicit proxy, see Troubleshoot your connection to the Addy service.

Is anomaly detection available on the ExtraHop Command appliance?

Yes, you can view anomalies from each of the Discover appliances connected to the Addy service on the Anomalies page of a Command appliance. You can also create anomaly alerts on the Command appliance.

Keep in mind that anomalies are stored on the Discover appliance. You cannot view anomalies that were detected on a Discover appliance from a different Discover appliance.

You may also view security anomalies on a Command appliance that is connected to an ExtraHop Reveal(x) appliance. However, a Command appliance can only connect to either Discover appliances or ExtraHop Reveal(x) appliances.

Does Addy detect anomalies associated with custom metrics?

Not at this time.

After the Addy license expires, can I still view my previous anomalies?

Yes, previous anomalies are available in a Discover, ExtraHop Reveal(X), or Command appliance.