ANATOMYIT

Frequently Asked Questions for EDR & SOC Implementation

What is EDR?

Endpoint Detection and Response (EDR) is a security solution that monitors workstations and servers (endpoints) for cybersecurity threats and responds in real-time to help mitigate the situation. EDR helps the Security Operations Center (SOC) to respond quickly to threats and minimize the potential impact. With built-in machine learning and AI, the EDR solution will perform some threat containment, and also suggest to the SOC ways to stop the issues and restore any affected solutions more quickly than a human could.

How is EDR different than Antivirus?

A legacy antivirus solution is software that is installed directly on individual devices that protects against malicious programs. It required individual management and updating, that notified the end-user who was then tasked with notifying someone else in IT to investigate the situation. EDR is a solution that detects and halts all kinds of cybersecurity threats, providing notification and centralized visibility and control over all the devices on the network to the SOC, which is a 24x7 operation. EDR addresses the speed to identification and resolution, which is critical in any cybersecurity incident.

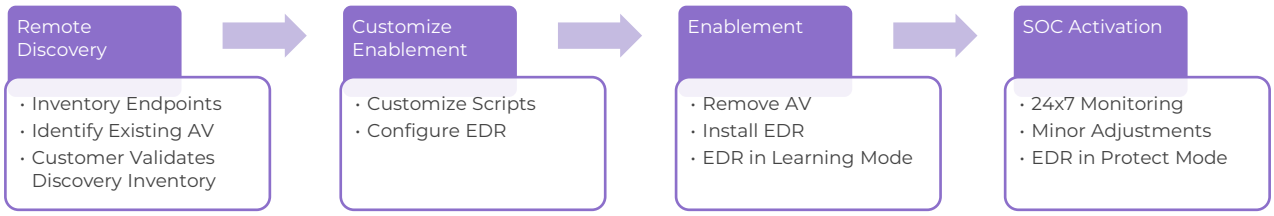
What happens during the EDR implementation?

The Anatomy IT team will perform all the enablement activities for you in a way that does not disrupt your daily activities. This is a low-touch type of implementation, which is typically done over a couple weeks. The first week is for handling of pre-

requisites and the second week is focusing on the enablement. The enablement occurs during non-business hours.

The SOC is activated at the end of the EDR enablement. They will be monitoring the EDR 24x7 starting at this point. Over the first week or so the EDR provides protection while it learns the applications, user routines, and system behaviors. During this time the SOC may make minor adjustments behind the scenes to tailor the EDR solution to your specific environment. At the end of the learning period, the SOC will finalize the activation and place the EDR in the production mode called Protect.

The overall implementation process has four steps:



What do end-users need to do?

Almost nothing. You will be asked to leave your workstation/laptop powered on for a couple evenings during the implementation. This will allow the Anatomy IT team the ability to perform the remote discovery and then a few days later the enablement.

Once EDR is enabled, you simply contact the support team as usual if you have any IT issues. There is nothing specific that you need to do regarding EDR.