FireEye
SECURITY REIMAGINED

Understanding the FireEye Proof of Value Program

HERE'S WHAT YOU CAN EXPECT

FireEye POVs only analyze real-time network traffic and report on live incidents that are present in your environment. There are never any "pre-baked" objects to trigger positive results. So everything you see is based on actual threats that your organization faces.

This POV will help you understand:

- How the appliance fits within your security infrastructure and workflow
- How it will perform in your network
- What it will take to operate/support the appliance
- The existence of any previously unknown threats in your environment

As the POV progresses, your Sales Engineer (SE) and Account Manager (AM) will guide you through the installation and each of these steps:

Step 1: Setting the stage

You should have already established three to five POV success criteria to measure whether the POV is a success. These criteria will vary, depending on your security goals, but should be measureable, repeatable, controlled and sensible.

Working with your SE and AM, you should have identified critical stake holders and established agreements on POV milestones and deadlines. These agreements ensure that everyone involved with the POV is working together to create the best possible outcome.

Step 2: Understanding your alerts

After defining success criteria and installing your device you may start to see alerts. Your SE may reach out to you to perform an in-depth malware analysis review of any alerts. During this review they will address any questions or issues pertaining to malware analysis, integration and architecture in your environment.

FireEye devices are designed to detect advanced malware and targeted attacks. FireEye data suggests that static defenses are becoming less and less effective against these forms of modern malware. If you do receive alerts you may consider adjusting your organization's approach to security by:

- Evolving to a different security architecture that isn't based on signatures or whitelisting.
- Investing in rapid endpoint-response capabilities to validate and contain attacks that get through your defenses.
- Developing your incident-response capabilities by hiring or outsourcing to experts.
- Reducing spending on those traditional defenses that were unsuccessful at detecting these advanced threats.

Because FireEye appliances are specifically designed to detect targeted, advanced attacks, there is the possibility that the POV may not yield any live results. In this case your AM or SE will discuss the steps for "Active Testing".

Step 3: Review your results

Next, it will be time to review your results. Your SE and AM will provide additional context around the alerts that you have seen, measure those results against your success criteria, and after the agreed upon timeframe, prepare to have the appliance shipped back to FireEye. Your SE will work through these final steps with you to ensure testing and review of the results goes smoothly.

FireEye is committed to providing you with a worthwhile POV experience. If you have any questions, please reach out to your account manager or sales engineer. Thank you again for engaging in a FireEye POV, and look out for more emails from this team on how to make this POV experience as smooth as possible.

For more information on our recent study of FireEye POV evaluators, please download our report, "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model".