# Blocker FAQ

**Q: How does Blocker differentiate itself from other security features in the market, and what specific threats does it aim to address?**

**A:** The Blocker feature in AutoElevate can block 200+ native Windows applications, binaries, and .dll files that are typically used as LOTL attack vectors.

**Q: How does AutoElevate ensure that Blocker stays up-to-date with evolving cyber threats and maintains its effectiveness over time?**

**A:** We rely primarily on sources like Microsoft, community projects (such as the LOLBAS project), and our own research to keep the product to date. That said, please note that Blocker is focused on "malware-free" aka "Living off the Land" attacks. These tend to exploit known applications and tools that have been in Windows for a very long time - a subset of which have been deprecated and only remain there for backwards compatibility.

**Q: Is Blocker a separate product from AutoElevate?**

**A:** It is not a separate product. Blocker is a new process blocking/allowing tool within AutoElevate.

**Q: Can you provide insights into the user interface and user experience of Blocker, particularly in terms of ease of use for non-technical users?**

**A:** AutoElevate and Blocker, are designed to be configured by system administrators and technical staff. That said, we do aim to make it as user friendly and easy to use as possible. Someone with limited technical knowledge should be able to configure Blocker when utilizing our recommendation engine after an appropriate audit period.

**Q: Does the Blocker feature block applications at a network level?**

**A:** AutoElevate's Blocker tool blocks at a process level.

**Q: When setting up blocking rules, is it necessary to change all endpoints back to Audit mode or can it work safely without disruptions in Live mode?**

**A:** Only new endpoints that you wish to utilize the Blocking feature on would need to be placed in Audit mode. This allows us to identify the applications, processes, and .dll's being used on the machine so the recommendation engine can suggest rules that will reduce threat vectors.