300 Cyber Security

APPLICATION ALLOWLISTING (APAL) (AKA APPLICATION WHITELISTING OR APPLICATION ZERO TRUST)

Sometimes the simplest solutions are the best ones. If systems are harmed by malicious software, why not just stop it from executing? Although it sounds easy, the practical application isn't that straightforward. There are several means to prevent programs from running, but admins are often worried about causing network chaos. Dealing with angry users isn't worth the security tradeoff. It's why almost every network we encounter has no restrictions on what software can execute.

The key to this defensive tactic is minimizing unintended consequences. Moving to a deny-by-default posture without disrupting employees' workflow requires significant planning and diligence. Luckily an effective tool exists to make this transition nearly painless. It's called ThreatLocker, and after its 100 million dollar series 'C' funding, it may be the biggest security company you've never heard of.

ThreatLocker software learns about the applications running in your environment and allows you to create allowlists based on your specific company's requirements. When launched in 'learning mode', you get a very good idea of the effect blocking certain software will have before you go ahead and block it. Users continue to work without interruption while you compile your dataset, and by the time you set policy, you've handled any unintended consequences. Also, ThreatLocker has the intelligence to know that an updated "allowed" application is still the same "allowed" application. So updates don't wreak havoc on your users.

ThreatLocker creates true defense in depth. It delivers protection when a malicious piece of software has slipped by your EDR solution, or an employee has been tricked into short-circuiting your perimeter defenses and has run malicious code. One of the private equity firms involved in the $100 million investment in April of 2022 referred to it as a "ransomware killer." It's hard to run encryption software when it's not allowed to run. ThreatLocker interacts at the kernel level and is very difficult to tamper with.

As an extra added protection, their Ringfencing feature limits how programs can interact with each other, delivering protection against supply chain-type attacks. For example, Powershell is on the allowed list, and Word is on the allowed list; however, Ringfencing can prevent Word from calling Powershell, thereby preventing an exploit in Word from being used further to infect systems.

ThreatLocker makes deny-by-default a practical defensive tactic, enabling a small IT team to adopt the policy without worrying about degrading the efficiency of their workforce. It's exactly the defense in-depth type approach demanded in the age of industrialized cybercrime.

SUMMARY

- ↗ Prevents all applications except those explicitly allowed from running
- ↗ Ensures user efficiency isn't negatively impacted by when moving to deny by default
- ↗ Application updates don't change their allowed status
- ↗ Stops what your EDR misses and what your employee attempt to unwittingly install
- ↗ Ringfencing helps prevent supply chain attacks by preventing risky software interactions

---

Why We Chose ThreatLocker

ThreatLocker was a very easy choice for APAL software because no one really does it like them. If you Google ThreatLocker competitors, you will get either EDR tools or RMM tools. EDR tools don't operate as ThreatLocker does. RMM tools would be an extremely convoluted way to create allowlists and come with various unrelated core features. Instituting this security safeguard makes tremendous sense, as it is cost-effective and, with the help of skilled technicians, relatively easy.

SUMMARY

- ↗ ThreatLocker owns the category. No one else does what they do.