DEDAUB

WHAT'S SO SPECIAL ABOUT THE IMMUNEFI FIREWALL (POWERED BY DEDAUB)

RUNTIME PROTECTION

SECURITY THAT EVOLVES WITH YOUR PROJECT

Smart contract security does not end at audits—even the most rigorously reviewed protocols can be compromised in production. The Immunefi Firewall introduces an adaptive, post-deployment defense layer that allows protocols to dynamically adjust their security posture and prevent entire classes of real-world attacks—without sacrificing DeFi composability.

dedaub.com/firewall/

Smart contract security, yadda, yadda ... you know the story.

If you think you can solve the security problem by ensuring that your smart contract code is correct, then more power to you! We love your optimism, we love your ethos, and everything that you stand for! And if you get hacked, we'll do our best to help.

But you and we both know that you may get hacked.

You may have amazing programmers. You may commission 7 audits by top experts. You may formally verify all the properties you can think of that can be verified. And you may still get hacked or may find a critical in production and get narrowly saved after suffering a reputation hit. If you think otherwise, then you think you are better than the teams of Euler, Balancer, Liquity, Yearn, and so many more. Newsflash: you are not. These are excellent teams, process- and talent-wise. You may match them or even narrowly surpass them, and we certainly hope that you do. But you won't be substantially better thn them on security, or code quality practices. Nobody is.

The problem is that you have a single line of defense. You can make it strong. But a determined attacker may find a way through.

So, here's where the Immunefi Firewall comes in. It does something different. Two things really, one kind of obvious, one completely new.

The first principle of the Immunefi Firewall is that you may want different protection at different times during the lifetime of a deployed protocol. At launch, you can lock down the protocol a bit more. Later, you can relax the protection, emphasizing integrations. Then, at some point, you find out that a similar protocol got hacked by a novel attack vector. Or that one of your invariants breaks under fuzzing. The devs say "it's Low severity". But you may still want to dial up security a bit for a month until you investigate. Then you dial it down again.

Ok, a firewall that lets you adjust its restrictiveness is the "kind of obvious" part. But it's made seamless and easy in the Immunefi Firewall. You can have the protection mode be "none"; or simple blacklisting of highly suspicious callers; or "only allow vetted callers"; or "scrutinize every single transaction" (which will hinder composability); or "let everything through as long as my invariants are preserved"; and more.

So, now let's get to the "completely new" part.

The new part is a firewall mode that can offer extremely high protection without sacrificing DeFi composability and integrations. We call this "caller vetting" or "global whitelisting". When you set this protection mode (which can be completely temporary, activated when at higher risk), the protocol only accepts calls from contracts (or EOAs running code, per EIP-7702) that have been pre-approved by the firewall. Anyone who wants to call your protocol programmatically (be it a bot, or another DeFi protocol that wants to build on top of your protocol) has to submit their code for vetting and can only call the protocol once vetted.

Wait, that sounds horrible, doesn't it? *I'm paying for a firewall service that will turn away my users?! Where are your decentralization principles? When did you abandon the idea that contracts and wallets should be treated the same, and that smart contract automation is the future of finance?*

This is a valid concern. But here's the neat part: in the vast majority of cases, this vetting will be done *entirely automatically*. Off-chain, sure. But promptly and automatically. Using algorithms that will analyze the caller contract (in bytecode form--no need to share source) as well as its provenance, and will vet, once and for all, that it is not a hack contract, nor can it be used as a pass-through component of hack contracts. We are aiming for a minimum-95% rate of automatic vetting: 19 out of 20 times, your bot users or integrators will be just one more transaction away from being able to call your protocol, forever.

And what about the 20th of these 20 times, when automated algorithms cannot vet the caller contract? In that case, there will be a bit more delay: a human (from a network of affiliated Immunefi security researchers) will need to inspect the contract code, perhaps communicate with the deployer/operator, before finally vetting the integration.

The advantages of the approach are clear: the vast majority of complex hacks simply cannot be perpetrated, at least not without fooling an advanced security system that is completely independent of the correctness of the core protocol. Integrations can still take place, with minimal friction. It is trivial for a derivative DeFi protocol (e.g., Yearn or DeFi Saver or any of many) to get vetted and to call a fully-firewall-protected protocol, with no further hurdles. It is perhaps less trivial, but still easy, for trading bots, deployed without source, to be vetted and to start operating over the protected protocol.

If you are skeptical, then let's try to capture your possible arguments and respond:

- *I don't believe that you can get to 95% automatic vetting of binary code, while preventing the majority of hacks*: The Dedaub decompilation and static analysis technology can produce a high-confidence result by examination of the binary code alone. In addition, if one includes the provenance of the code (i.e., the deployer, their past patterns, whether funded by exchanges that collaborate with law enforcement in cases of hacks) eliminating doubt in the vast majority of cases is certainly possible. Our statistics on past hacks and legitimate contracts comfortably clear the 95% bar, although future attacks may, of course, be much sneakier. Certainly someone can try to fool the vetting service by submitting small, seemingly innocuous, contracts that will later be combined into an attack. But it will be pretty tricky for such an attacker. By even submitting their code for vetting, they are inviting scrutiny, drawing attention, potentially warning of the upcoming attack. There's a whole community of bounty hunters that will be more than eager to recognize the attack potential, once the protocol and a partial mechanism of attack is posted.

- *Even if you get to 95% automatic vetting, the remaining 5% will instill enough doubt that people won't write bots over a protected protocol*: First of all, it is very likely that the author of a trading bot will have no problem identifying themselves and getting assurances that their bot will be vetted. It is the trading logic and mechanisms that they need to protect, not any information that will convince the vetting service that they are legitimate traders and not blackhat hackers. So, it is realistic to expect that bots will be happy to go through the vetting process, if they are to access a protocol with high TVL and trading opportunities. Second, the *worst* case scenario is simply the current status quo: either the protected protocol can switch off the protective caller-vetting mode, or the protocol itself can vet, on a protocol-specific basis, this particular trader.

That's pretty much it! That's the high-level story of the Immunefi Firewall. We hope you will agree with us that it can offer significantly higher protection while preserving the ease of integration and composability of DeFi. We welcome the opportunity to discuss the technical specifics and are prepared to address any further questions you may have via this form.

About Dedaub

Dedaub is an innovative security technology and audit pioneer, merging academic insights with practical white-hat hacker skills. Since 2018, it has secured major protocols and infrastructure within the Ethereum ecosystem, safeguarding billions in Total Value Locked (TVL). With over 300 security audits for top Web3 protocols and collaborations with organizations like the Ethereum Foundation and Chainlink, Dedaub has established security standards across the Web3 space.

Who We Are

We are a team of security researchers, engineers, and cryptography experts with deep experience in program analysis and real-world smart contract exploitation. Known for our rigorous audits, we also build tooling that enables large-scale analysis of smart contracts — even without verified source code. Our researchers regularly participate in security war rooms and disclose critical vulnerabilities across the Web3 ecosystem.

Our Mission

Our mission is to raise the security baseline of Web3 by setting new standards in smart contract safety. Through advanced technology, rigorous research, and close collaboration with ecosystem leaders, we work to build trust and resilience across decentralized systems. By making security precise, continuous, and production-ready, we help ensure that critical Web3 infrastructure can evolve safely at scale.

Our Values

Integrity: The highest standards of honesty and trust in every engagement.

Knowledge: Advancing blockchain and code analysis through continuous innovation.

Future: Empowering the next generation of blockchain experts.