

# How Syncplify.me Server! prevents SSHPsycho attacks

According to the [SANS ISC](#) nearly 80% of all SSH-based brute force attacks are caused by [SSHPsycho](#) or one of its variants. This seems to be confirmed by the LongTail honeypot real-time report provided by the Marist College. So, yes, SSHPsycho is a big deal, and it's a problem. And traditional blacklisting mechanisms (simply banning certain "well known" IP addresses and networks) have proved to be inefficient against it.

“LongTail shows that Cisco and Level 3's recent announcement about blocking sshPsycho's 4 class C IP ranges (also known as "Group 93" and the "Hee Thai Campaign") has done nothing to stop their brutal attacks. [Source: SANS ISC]"

Syncplify.me Server!'s intelligent and automatic blacklist (called "[Protector](#)"), though, shows to be **extremely effective at preventing** such type of attack. Its real-time dynamic attack pattern identification and prevention technology can quickly recognize SSHPsycho attacks (and the like) and **proactively stop them** as soon as they begin. Even at its "Normal" sensitivity threshold, Protector already identifies and blocks all types of SSHPsycho attacks, in most cases **before they even get to try the password authentication**.

Of course, not even Protector can keep you safe if you have a user whose username is "test" and its password is "123456", so it's strongly recommended to read the LongTail report and **avoid using the most common username/password combinations** that would make your SSH/SFTP server inherently vulnerable, not only to SSHPsycho but pretty much to any known and unknown attack. But again, Syncplify.me Server! helps you by **enforcing password complexity rules** that prevent users from using passwords that would be too easy to guess.

---

Revision #1

Created 22 July 2023 14:25:35 by DevTeam

Updated 28 January 2024 16:52:13 by DevTeam