Atomhid’s free process firewall and intrusion-prevention system (I.P.S.) can prevent malicious software introduced either in person, or activated remotely on a client device by a hacker, and it can stop it within a reasonable amount of time like an ideal I.P.S. Unlike other security software, the firewall for this is coded differently: instead of relying on malicious-code signature detection or a large database of known-malicious code, Atomhid’s I.P.S. stops the process, which would not be a bad trade off. Would your ideal security system stop malware from communicating with a server somewhere but have an insufficient and breakable firewall, allowing permission-granted software susceptibility to **in-the-middle-man attacks** and **code-injection**, or would you rather deploy a reliable firewall that will not guarantee malware from taking hold of a system, like Norton Security? Ideally, you would want both forms of security.

As a supplementary security application, this software only allows certain software on a list to operate on an operating system (0.S.) if and only if it accesses the session’s layer; and, it can do it on minimal installations of Linux kernels, too. Once an unknown malware passes by typical security-software scans and its passive detection algorithms, when it is detected by Atomhid’s I.P.S., the malware’s process and sub processes will no longer function or if it does run again, it will be stopped, but only if it is not on the pre-approved list. An added benefit of using the GUI-less version of Atomhid’s I.P.S. is that if you are on a minimal installation of a Linux kernel, this software can run and be configured to work in the background.

How Atomhid’s i.p.s. works

By common computer-nerd nomenclature—an ideal intrusion prevention system (I.P.S.) prevents unauthorized users, or hackers, from accessing, modifying, deleting, and reading your files without your knowledge—but, the malware first must access the network before the I.P.S. can defend. In the meantime, before malware accesses the web/**L.A.N.**/**W.A.N.**, malware can still damage your data and “prepare” it for later acquisition/confiscation/modification. Malicious software that does the aforementioned include: **ransomware**, **rootkits**, **keyloggers** (a sub-classification of **spyware**,) **viruses**, and **heuristic viruses**, those of which can take control over the **application layer** of the **O.S.I. seven-layer model** of a vulnerable network, and even change behavior of the underlying o.s. Atomhid’s free process-firewall system is not intended as a replacement from buying an expensive router with firmware that includes an I.P.S., rather, it is an added protection in case malware communicates with the WLAN/internet if it is central to its runtime when data is disguised well enough. The prevention of this happening is exactly what Atomhid’s I.P.S. promises, but on a higher application layer instead of the **link layer** where traditional router-based i.p.s.’ detect and defend against these attacks. As this software’s maker, I recommend using this software as a substitution to **routers** that come with business-level security or computer security software that operate as aforementioned. And as always, two layers of protection is better than one, especially when your main security software becomes compromised.

Since hackers, nowadays, have access to many hacker kits with preassembled malicious code that can be easily modified, and thus, **they can creep stealthily by without detection by the most sophisticated security system**. So, it is the job of the intrusion prevention system to prevent it and report it to the system administrator: you; this software will do exactly that. Once the malware starts its process, if it is already stopped once, it is immediately stopped again, and again, etc. Malware used by the hacker would have a tough time accessing a server from where the hacker can send malicious commands to the host, or your device.   
  
Of the many malware languets, or types of malware, the system administrator must prevent any of them from attacking vulnerable data. But, do you ever notice that in the most well-defended systems, security holes are easily punched through? On encrypted databases, news sources often narrate stories about data breaches happening to top companies, like Google; do you know what causes these breaches usually? Usually, it is a trusted person who happens to be at the site, but also, it can be a man-in-the-middle making the attack. In these nightmarish scenarios, failure is often the result of malware that was not stopped, because it did not fit any known malicious code signature.

A possible success scenario, as an example:

Let’s say you are in control of an important project—all file permissions are correct, but—you failed at preventing physical access to your computer’s terminal. A supposed friend uses your computer and gives himself permission to remotely access it with administrative priveleges, writes down your ipv4 address, and disables certain security protocols and alerts. This friend goes home to his computer and gains access to your computer through a program with known vulnerabilities of which also happens to be on a pre-approved list generated by your atypical computer security software, but he does not know that you are using Atomhid’s IPS. He already made sure that the program has access from an atypical security application running on the computer by giving, for instance, a SSH client complete read, write, update, and delete control privileges rendering his attack undetectable by passive scans. Additionally, packet scans by the security software detect nothing wrong with packets sent from the hacker’s server, ordering and commanding additional clientware he wants to run passively on your computer while you use it; this, he thinks, will go by undetected. Now, right before you are about to make that big presentation, of which your supposed “friend” wants to see fail utterly, this person sends a command to delete your project with administrative privileges. But unbeknownst to your “friend,” he loses communication with the backdoor, and you are able to have a great day, succeeding at a public presentation. Also, all data on your computer has not been accessed post intrusion. In effect, you were running Atomhid’s IPS, which had succeeded at securing your computer by scanning the session layer for pre-approved software, and if an application was not on the list, it was stopped.