

## Host IPS and Firewall

New forms of attack are constantly being developed, and relying solely on signature-based security is no protection against the many new virus variants or against the sheer volume of new malware types. StormShield's integrated Host Intrusion Protection System (HIPS) complements the integrated signature-based anti-virus/anti-spyware service and addresses this challenge through a unique combination of proactive methods to combat unknown attacks

System Hardening | Intrusion Prevention | Behavioral analysis | Rule-Based Protection

**Rule-Based Protection** StormShield enables the network administrator to define security rules based on Access Control Lists to allow or deny access to files, registries, sockets, processes, ports, and other system resources. Built into the kernel to permit the highest level of security privileges, StormShield's administrative policies automatically take priority over any other proactive or automatic protection mechanism.

For instance, administrators can define whether Internet browser plugins can be installed, which applications are allowed to access the network, which system panels can be accessed by the users, etc., as well as which applications can be launched automatically when the PC is started.

StormShield enables the IT admin to apply fine-grained rules on:

- Executable files, such as application, plug-ins and script files
- System resources, such as files, folder, system panels and registries
- Wired and wireless network connectivity
- Trusted applications, enabling the elimination of false positives