

Application Control

StormShield's Application Control protects your network from unapproved applications, which may pose serious risk to your systems and data. Unauthorized applications expose you to new vulnerabilities, compliance risks, data loss, and intellectual property theft. StormShield's Application Control can also ensure that required applications/processes are running, ensuring system compliance with your internal and regulatory policies.

To control applications, StormShield gives administrators the ability to create whitelists for approved applications or blacklists for applications that pose known risks. This also allows you to control application installations with a range of settings. You can allow new installations, block all new installations, allow only with approval, or allow the application to run on the endpoint but without network access. Important security applications such as anti-virus services can also be forced to run before other types of network and system access are granted.

Control goes beyond the application level. Access is no longer the all-in or all-out scheme of the past. Administrators can control network access rights, file access rights, download rights, registry access rights, and more – all while also controlling the access to system panels. For remote and mobile workers, administrators can enforce VPN usage before granting network rights.

These controls can be tailored to meet each organization's needs. Those needing stringent control can create whitelists that allow only approved applications to run, while those wishing to grant more flexibility can set up rules to block only known problems, such as P2P applications.

Application control provides:

- The ability to control via both blacklists and whitelists
- Control over installation of applications
- Control by file type, enabling the administrator to protect sensitive files or ban unauthorized file access or transfers
- Control over network access rights, file access rights, and registry access rights
- Control user access to system panels
- Enforcement of applications that must run, such as VPNs upon remote connections – a policy which can be dynamically applied if necessary