



4 Reasons You Need Native Linux Virus Scanning

In today's connected environments, Linux IT professionals can no longer claim that viruses are only a Windows threat.

The biggest excuse people make for forgoing virus protection is that they scan their client PCs and therefore no virus would make it to the server. However, effective malware defense requires multiple layers. This brings us to the importance of native virus scanning.

The following infographic highlights the four main reasons security experts give for using anti-virus software that runs natively on your Linux system.



1. PC-Based Virus Scanning Creates Security Concerns

- ▶ Scanning a Linux server from a PC creates security vulnerabilities. The process requires leaving a work station to be logged on throughout the scanning process, which compromises the security and integrity of the server, and leaves it visible to a virus or malicious code.
- ▶ Native virus scanning doesn't require a work station or a file share.

2. PC Scanning Isn't Very Reliable

- ▶ Some parts of Linux servers are impossible for a PC-based anti-virus solution to scan and can cause non-native scans to fail, making for an incomplete and time-consuming process
- ▶ Native anti-virus solutions can automatically remove all detected threats with no additional hardware.

3. Native Anti-Virus Scanning Eliminates Stability Problems

- ▶ A number of problems with PC-based scanning solutions, such as a lost connection to the server or a pop-up warning message, cause the scanning process to stop entirely.
- ▶ Stability concerns simply aren't an issue with native software.

4. Virus Scanning From a Pc Creates Performance Problems

- ▶ PC-based scanning is incredibly slow and increases the network load dramatically.
- ▶ A native scanning program performs much faster, doesn't increase the network load, doesn't reset a file's "last access time," and allows for more frequent scanning.