Written by Marco Attard
04 September 2015

Security vendor Check Point claims to stop unknown malware, zero-day and targeted attacks from infiltrating networks with SandBlast, a solution based on new CPU-level exploit detection technologies.

SandBlast uses both sandboxing and emulation technologies to secure enterprises from known and unknown threats. It also has a CPU-level detection engine to pick up on Return Oriented Programming (ROP), an evasion technique able to beat the protection offered by Data Execution Prevention (DEP).

Another feature is Threat Extraction, a means to provide safe versions of content immediately (by converting Word documents to PDFs) while emulation takes place in the background.

"Check Point SandBlast Zero-Day Protection identifies more malware, and actively blocks it with minimal impact on user delivery times," the company says. "SandBlast offers cutting edge sandboxing capabilities to detect threats before evasion techniques can be used, making this solution the best line of defense against undiscovered exploits, zero-day and targeted attacks."

SandBlast is available now as both an on-premises and cloud service, with initial support for Microsoft Office 2003-2015 (Word, PowerPoint and Excel) and PDF files. More document formats will be added in the future.

Go Check Point SandBlast