

DATA SHEET

APPGUARD SERVER

Overview

AppGuard Server is designed from the ground up with server defense in mind, not just an adaptation of endpoint protection for workstations. The technology protects the system from infected applications, while also protecting applications from any system infection. AppGuard defense delivers dynamic isolation and containment of critical system processes without any reliance on software or hardware sandboxing.

AppGuard for Servers Protections Include:

- Prevents adversaries or surrounding undefended vulnerable systems from gaining a foothold on the server to gain lateral infiltration into enterprise
- Delivers unmatched “pass the hash” and “pass the ticket” defense
- Halts multi-stage attacks that prey on privilege accounts stored in-server memory
- Prevents SQL Injection advanced stage from ever taking control of the server
- Prevents zero-day exploits prevalent in Web Application Servers and Database Servers from taking over exploited critical processes for nefarious purposes such as altering integrity of critical server configuration or stealing critical data from the server.
- Protects servers against memory scraping of critical processes, file-less in-memory malware, instantiating command shells to open backchannels, and uncontrolled command usage
- Patented trusted enclaves allow for segregated information, delivering “walls” of defense amongst server processes for information segregation.

AppGuard offers field-tested policies that are rapidly deployable. Using granular and manageable policies augmented by trusted publisher information and file location, AppGuard delivers application control that is both practical and effective. Additional runtime protections further establish boundaries around processes, and prevent unauthorized code or system configuration changes, preventing malware becoming persistent.

AppGuard is the only preventive technology that stops breach attempts in servers at the earliest stages of attack. Without detonating the malware, without scanning, without reliance on signatures or IoCs (Indicators of Compromise), AppGuard stops the attack and generates IoAs (Indicators of Attack) event data.

AppGuard for Servers Supported Platforms:

- Cloud-based and local server hardware
- Windows 2008 R2 through Windows Server 2016
- Linux Red Hat 7.5 (Available Q2 2019)