Nyotron PARANOID - Better Application Control

Whitelisting or application control is an important tool for an organization's ability to strike the necessary balance between the traditional Negative Security model and a Positive Security approach. However, the management of these tools is HARD.

Additionally, application whitelisting was designed and intended to control end-user's behavior, rather than stop modern attacks. The following attacks are able to bypass whitelisting controls:

1. In-memory attacks (e.g. DLL hijacking)
2. Script-based attacks (e.g. MS Office macros, PowerShell)
3. "Living off the land" attacks (using whitelisted admin tools for malicious purposes)

Nyotron's PARANOID not only provides protection against fileless malware, script-based attacks and exploitation of vulnerabilities in whitelisted applications, but also solves the whitelist management overhead problem.

	Protection against fileless attacks	Protection against application vulnerabilities & zero-days	Management overhead
APPLICATION WHITELISTING	✗	✗	↑
NYOTRON'S PARANOID	✓	✓	↓

How did we do it? Instead of whitelisting applications, we have whitelisted known-good operating system behavior and hence can enforce zero-trust model at the kernel level. No baselining or whitelist updates needed. Moreover, PARANOID provides an EDR-like visibility into malicious activity and associated root cause. Learn more about our approach HERE.

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive, Ste. 237
Santa Clara, CA 95054
1.408.780.0750
www.nyotron.com