The Nyotron Advantage

Nyotron’s PARANOID, the industry’s first OS-Centric Positive Security, acts as your last line of defense to strengthen endpoint security. PARANOID focuses on operating system behavior to stop new, never-seen-before and fileless threats that antivirus and next-generation antivirus solutions tend to miss. Our solution does not require a rip and replace approach, but rather complements your existing anti-malware solution (including Windows Defender).

You cannot win against infinite odds. According to AV-Test.org, almost 120 million new malware samples were submitted in 2017. Even at 99.9% detection rate, this would leave 120,000 undetected threats, and this is just for known file-based malware. It is time for a new approach!

PARANOID is based on a Positive Security model that understands a finite set of legitimate system sequences at the OS system call level. When activity sequence isn’t following a normative path, PARANOID prevents it from executing, no matter what attack vector or method is being used. This is what we call Threat-Agnostic Defense.

PARANOID BOOSTS THE PROTECTION OF ANTIVIRUS AND NEXT-GENERATION ANTIVIRUS SOLUTIONS:

Protection from known and unknown threats without hashes, indicators of compromise or databases of malware signatures and blacklists
Malware authors have learned to produce new variants of their malware that have deliberate changes in their signature and behavior to evade antivirus programs.

Deterministic run-time defense without the need for AI/ML models or behavior baselining
Security solutions powered by artificial intelligence (AI) or machine learning (ML) mostly focus on the malware pre-execution step and, thus, look at files written to disk. These types of products are trained on known malware samples and have trouble recognizing attacks that are completely different from anything they have seen before. Moreover, the pre-execution focus of these tools is ineffective against fileless malware that is now being used in nearly 50% of attacks.

No cloud or server connectivity is needed to block attacks (air-gapped network support)
Traditional antivirus vendors require a connection to on-prem or cloud infrastructure for frequent antivirus definition or behavioral model updates, threat intelligence feeds as well as sandbox detonation of previously unseen files. This leaves endpoints unprotected when not connected to the network.
Real-time protection from damage (data deletion, encryption, exfiltration and sabotage)
PARANOID focuses on the final phase of the attack - preventing intended damage. It understands all the ways the integrity of the operating system, data and the movement of data can be compromised, and stops these malicious activities from executing.

Fewer false positives
PARANOID has fewer false positives than AL/ML-based solutions since what constitutes legitimate system behavior is more readily understood than millions of unknown malware samples and attack vectors.

Lightweight protection
PARANOID does not need to scan files and folders, update AV definitions or perform other resource-draining activities. Instead, the solution watches state transitions and compares them to a relatively small, finite set of normative transition sequences, resulting in no noticeable performance degradation.

Protection of already infected endpoints
PARANOID is fully preventative: it will block any attempt to cause damage to a system or data even if an endpoint was compromised prior to the installation of the product. And by the way, even unpatched (e.g. out of support) systems will be protected.

ABOUT NYOTRON

Nyotron provides the industry’s first OS-Centric Positive Security to strengthen laptop, desktop and server protection. By mapping legitimate operating system behavior, Nyotron’s PARANOID understands all normative ways that may lead to damage, such as file deletion, data exfiltration, encryption, sabotage and more. Focusing on finite “good” actions allows PARANOID to be completely agnostic to threats and attack vectors. PARANOID works seamlessly with antivirus and next-generation antivirus solutions to provide the last line of defense from modern state-level attacks. Nyotron (nyotron.com) is headquartered in Santa Clara, CA with an R&D office in Israel.