DATA SHEET

Nyotron's ENDPOINT PREVENTION AND RESPONSE

TURNING DETECTION INTO PREVENTION

The proven inadequacy of existing endpoint protection technologies has fueled the rise of Endpoint Detection and Response (EDR) products. While helpful in providing better visibility and post-breach investigation, traditional EDR tools have significant trade-offs.

First, unfiltered event capture produces data deluge, resulting in additional staffing requirements and ultimately poor visibility. More critically, EDR by definition is a post-breach technology, meaning that the damage has already been done. Organizations require both visibility and protection.

Nyotron provides threat-agnostic protection for laptops, desktops, and servers while delivering precise visibility into the attack. Using OS-Centric Positive Security, our solution - PARANOID - automatically whitelists trusted OS behavior and rejects everything else. We call this approach Endpoint Prevention and Response (EPR).

PARANOID SUCCEEDS WHERE EDR FAILS IN TWO KEY AREAS:

PRECISE VISIBILITY

Provides granular visibility into the attack timelines, origin, TTPs and what the attackers attempted to accomplish.

REAL-TIME PROTECTION

Prevents the damage from occurring. No manual threat hunting or costly infrastructure or cloud connectivity required.

CAPABILITY	NYOTRON'S EPR	TRADITIONAL EDR
Detection of threats	✓ Yes (automatic)	◐ Yes (semi-automatic)
Protection from threats	✓ Yes	✗ No
No additional staffing needs	✓ Yes	✗ No
Support for air-gapped and off-line systems	✓ Yes	✗ No
Eliminates the need to collect, store and manage large volumes of data	✓ Yes	✗ No

NYOTRON
SECURING THE WORLD

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