NYOTRON
SECURING THE WORLD

"From the perspective of breadth and depth of analytical capability, it is one of the best, if not the best, displays of its type that we have seen."

Nyotron

PARANOID

This interesting product operates on malware at the endpoint. However, it is one of the behavior-based systems that we have seen work well. Just about all behavior analysis tools use behavior analysis in conjunction with other functionality, but PARANOID uses what the company calls Behavior Patterns Mapping (BPM) to look for anomalistic behavior at the endpoint. ***The system starts out by mapping all system calls that are operating correctly and uses that as a baseline. It then watches for behavior that is outside of the baseline. This makes the tool threat-agnostic because it does not care what the threat is.*** It only cares about the anomalistic behavior. Since PARANOID operates at Ring0, it can watch both user mode and kernel mode behavior. To accomplish this, Nyotron has developed its own proprietary language.

PARANOID is deployed in a client-server architecture with agents as the clients and the server deployed either on a physical host or in a virtual server. Even when the agents cannot see the server – as when traveling outside of the enterprise – the level of protection remains good. Response requires that the threat take some action. Since this action will be outside of the baseline behavior of the agent, it will be stopped before it can cause harm to the endpoint device.

One thing with which we were concerned was that it appeared to us that all of this activity on the endpoint suggested high overhead. Since that is one of the problems next-generation systems seek to solve, we asked about it. The answer is deceptively simple: The agent is a state machine. All it needs to do is save the state of the correctly operating endpoint environment and look for a state change. This implies that the correct operating state is 'save very granularly,' and it is.

In addition to the PARANOID system, there is an optional War Room module that provides an excellent and very detailed 3D display. This allows granular tracking of events from their sources outside to the details of how the malware behaved – or attempted to behave – once it entered the endpoint. ***From the perspective of breadth and depth of analytical capability, it is one of the best, if not the best, displays of its type that we have seen.***

The Nyotron website is comprehensive and the support package is very good. Standard eight-hours-a-day/five-days-a-week support is included and there are higher level support packages available for an additional fee. Pricing is at the high end of the range and, as with most of the products of this type, we believe that pricing should be a bit more aggressive since large enterprises will take a hefty hit to cover – as they should – all endpoints. It's likely, of course, that increasing competition will start to bring prices down, but for now we suggest you be prepared to work with the vendor to establish a realistic budget.

– Peter Stephenson, technology editor

DETAILS

Vendor Nyotron

Price $54 per endpoint subscription license.

Contact nyotron.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★¾

OVERALL RATING ★★★★★

Strengths Solid behavior-based endpoint anti-malware with a history of very low false positives and negatives.

Weaknesses As with many similar products, a bit pricey, especially for large enterprises.

Verdict Don't pass this one by if you are looking at anti-malware. In our view, it certainly ranks in the top five such products we've seen over the past couple of years.

Nyotron
2880 Lakeside Drive, Suite 237
Santa Clara, CA 05054
+1 408-708-0750
www.nyotron.com