DATASHEET

PARANOID

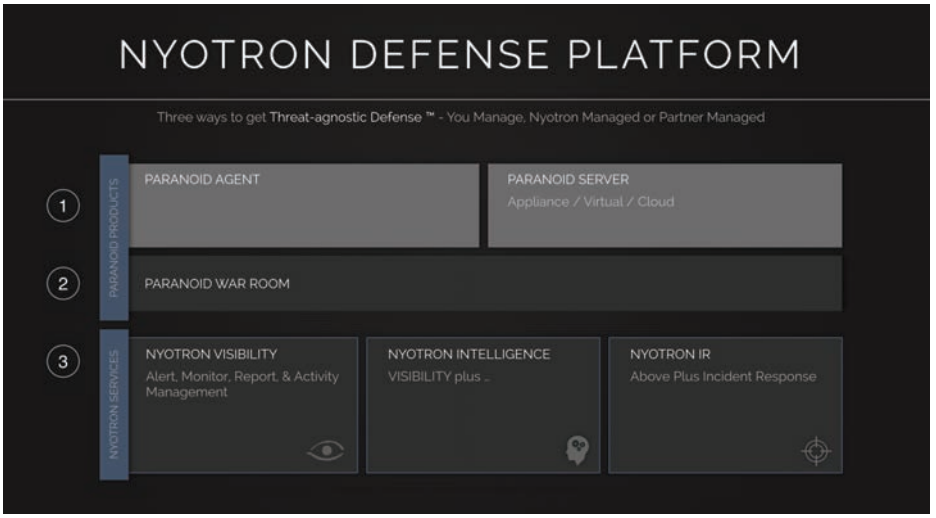
Threat Agnostic Defense™: Protection From Tomorrow's Threats Today

In today's digital era, your biggest cyber security challenge is differentiating between safe computer activity and malicious acts. Traditional security defenses such as firewalls, secure email gateways, IPSs, signature based solutions, and next generation endpoint protection platforms play a key role in your defense-in-depth strategy but fall short on protecting you against advanced threats and targeted zero-day attacks.

Approaches such as behavioral analytics, sandboxing, mathematical algorithms, machine learning, and artificial intelligence are limited in their ability to detect and mitigate threats. These methodologies often impose a heavy burden on humans and computers and only focus on detecting a particular type of threat, often a known threat, or provide data about threats that have already caused harm. Now, there is a better way to protect your assets.

THREAT-AGNOSTIC DEFENSE: CYBER SECURITY FOR THE FUTURE

At Nyotron, we realize there are infinite types of exploits – making it simply impossible to predict the next tactic attackers will use to gain access to your assets. To protect your assets, you need a defense solution that is threat-agnostic and can proactively detect, prevent and analyze threats, known or unknown, regardless of the type of attack, who generated the attack, or how, where or when the attack penetrated the organization. To prevent attacks others cannot detect, you need PARANOID, Nyotron's threat-agnostic endpoint protection platform.



NYOTRON
SECURING THE WORLD

Nyotron Security
2880 Lakeside Drive
Suite 237
Santa Clara, CA 95054
+1.408.780.0750
www.nyotron.com

PARANOID: Unprecedented Break-Through Cyber Defense

PARANOID is a game-changing data protection solution that provides you a radically different approach to thwart attacks. Acting as the last line of defense – after threats bypass all perimeter and endpoint security layers – PARANOID protects your data regardless of the type of threat or attack vector, and does not require any prior knowledge about the threat to be effective. Delivering the first-ever Threat-Agnostic Defense technology, PARANOID distinguishes between legitimate activities carried out by a program or user and threatening activities being carried out by attacks.

PARANOID consists of an agent at the endpoint, a server on the backend, and a central management console. It can be deployed apparent or transparent to the user – depending upon security policy – and can operate in detect or prevent mode to thwart the final phase of an attack and prevent actual damage.
PARANOID enables cyber analysts to immediately respond to uncovered threats using PARANOID's powerful policy actions.

PARANOID Benefits

- » Threat-Agnostic Defense
- » All in One Solution: Detect, Prevent, Respond, Analyze
- » Fast and Easy to Deploy, Low TCO
- » Real-Time Visibility
- » Advanced Forensic-Analysis

"Nyotron's solution works very well with the multiple defense systems that El Al Airlines has in place and adds significant capabilities in terms of identifying and preventing unknown and targeted threats."

- Ofer Tsabary, CEO, El Al Airlines

PROTECT YOUR DATA AND YOUR ENTERPRISE

Operating System Behavior Mapping: The Secret to Securing Your Assets

Leveraging Nyotron's patented operating system Behavior Pattern Mapping (BPM) programming language, normative operating system call flows are mapped. PARANOID agents, residing on endpoint devices, operate in real-time within the operating system's kernel to analyze system calls before they are executed. The BPM detects system calls that present behavior that is not normative and stops the execution of the call. Detecting threats at the OS level allows PARANOID to protect against threats that infiltrated the network prior to PARANOID installation. Using an agent at the kernel level to detect threats eliminates the need for scanning, gathering, and maintaining huge volumes of data – saving organizations both time and money and eliminating any concerns regarding performance degradation.

Understanding the Attack with Rich Forensic Data

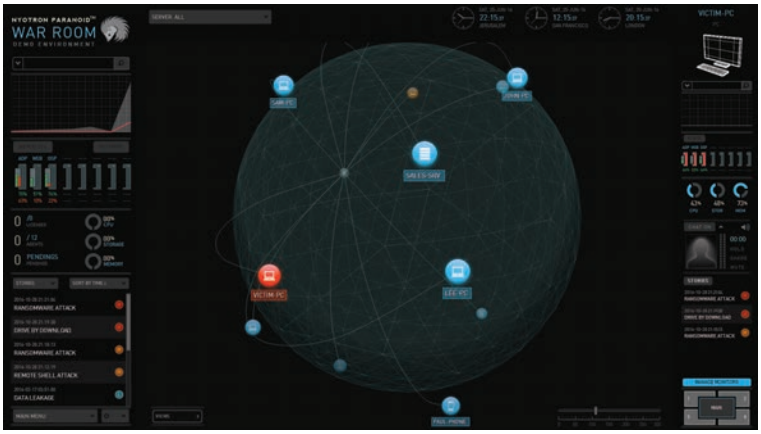
Monitoring OS system call activity, PARANOID captures meaningful, actionable forensic data, enabling security analysts to fully understand the attacker's steps (when, where and how the attack happened), as well as who on the network was affected.

PARANOID War Room: Sophisticated Monitoring, Alerting and Activity Management

For enterprises that employ cyber security experts or run a Security Operations Center, our PARANOID War Room product provides you unlimited real-time visibility into your endpoints' security status.

Leveraging a sophisticated 3D presentation, the PARANOID War Room allows you to view your endpoints according to your desired classifications – by geo location, by network grouping, etc.

Whether in DETECT or PREVENT mode, the PARANOID War Room provides you in-depth details about an attack as it happens: where the attack is happening, if it is spreading to other endpoints, what the nature of the threat is, how it got in, and how it spread.



Flexible Deployment Options

PARANOID is available on premise or as a service, called Nyotron Managed Defense Services. For MSSP's, we also offer a Managed Defense Services package for you to deliver on behalf of your customers

Nyotron Security

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