WHITE PAPER

PARANOID: Threat-Agnostic Defense™

A NYOTRON WHITE PAPER

The current challenge in cyber security is: how can vendors deliver a higher level of security to protect organizations from today's sophisticated unknown attacks?

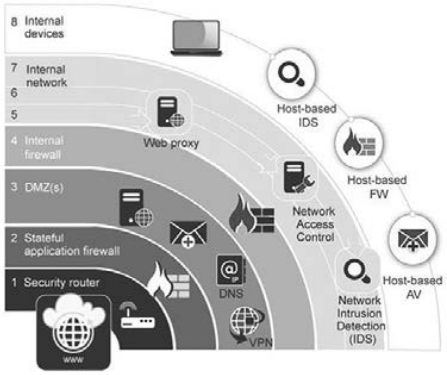
As many cyber attacks are targeted, security teams should behave as if the organization is already under attack. In addition, the emphasis today is on corporate resilience to cyber attacks, which means that we must achieve rapid recovery with minimal damage.

This white paper provides insights into a new threat-agnostic paradigm. This methodology is a necessity for all types of organizations that are struggling with the biggest challenge in today's digital era - how to effectively detect and prevent zero-hour threats while actually knowing nothing about them?

The Evolution of Security

Traditional security vendors are dependent on signature-based technology. Their research teams explore cyberspace, catalog threats, attack vectors, vulnerabilities, signatures, and other techniques to learn how attackers think and design their attacks. Then, vendors push regular updates our to their customers that are designed to alert when they recognize a familiar threat pattern. This concept of "blacklisting & shipping" is, in fact, a losing war, as it cannot deal with what is unknown.

Next came the next-generation technologies - decoy honeypots, containment, behavioral detection, machine learning and artificial intelligence. Additional technologies focused on detecting threats via their attack vector. Yet the threats continue to get through - bypassing security technologies layer by layer, until reaching their final destination - endpoints and servers. Once the malware reaches their destination, the damage stage of the attack begins: deleting files, altering data, data exfiltration or data encryption.



The attacker's ultimate goal will always be your assets - your sensitive data. A persistent threat will always find a way to bypass all endpoints and perimeter security means.

All other security technologies - whether at the perimeter or at the endpoint - ultimately act as gates, that you know will be bypassed. You need a technology that provides a last line of defense concept.

NYOTRON
SECURING THE WORLD

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

The Challenge of Unpredictable Future

Today's evolving Ransomware attacks such as TeslaCrypt, CHIMERA, PETYA and the latest PowerWare are a great example of how new types of threats are causing us to lose again. The sheer number of these attacks and the variants of those attacks that are being created is simply impossible to keep up with. And what about tomorrow's threat? No one can predict the new attack vectors or methodologies. This is why a new security paradigm is needed to evolve in order to prevent any future threats, without actually having to know anything about the threat in order to prevent it.

The Paradigm Shift – Protect Against Today's and Tomorrow's Threats

Nyotron is a privately-held cyber security company based in Silicon Valley. Nyotron offers a game changing security paradigm to cope with designated APT's and Zero-hour attacks. PARANOID, the company's flagship product, delivers unprecedented protection for high profile organizations and national-level institutions. As the attacker's ultimate goal is to get inside the endpoints and servers, where the data is, PARANOID acts as a 'Last Line of Defense' - which focuses on the final phase of the attack - preventing the actual damage.

PARANOID technology was designed under these assumptions:

1. The attacker will eventually find a way to bypass all security means
2. The threats are already inside, undetected.

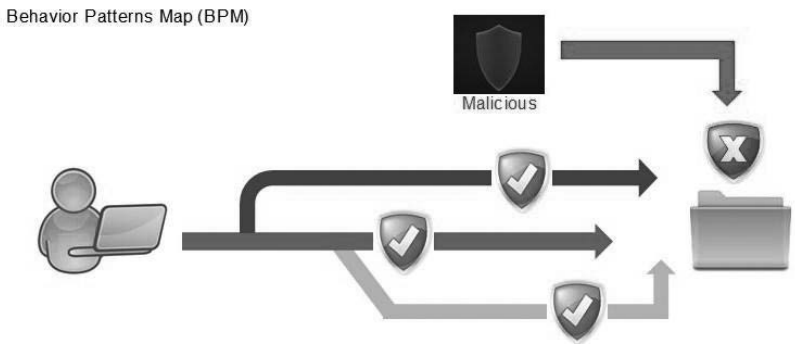
PARANOID Technology

Nyotron's technology relies on a completely different security paradigm. Rather than exploring the wild and limitless attack possibilities, Nyotron is focused on what is always consistent: attacker's final damage stage. This stage consists of finite damage, such as file deletion, data exfiltration, malicious encryption, and more. Relying on the operating systems behavioral patterns map, Nyotron mapped all the normative ways that may lead to damage. This way, PARANOID distinguishes between "good" and "bad" actions, detecting and preventing any malicious activity – regardless the threat type, attack vector and origin.

Example: Malicious File Deletion

All normative OS patterns related to file deletion are mapped. This ensures detection of illegal patterns leads to deletion of same file.

Malicious Deletion



Differentiators

Traditional signature-based anti-virus vendors identify "known threats". Next- generation vendors claim to predict the "unknown", but typically analyze files for KNOWN components that have already been identified and attempt to predict or guess if the file is malicious. Additionally, other solutions claim to protect against specific exploitation methods or types of threats or known application vulnerabilities (e.g. Java, Adobe). This results in enterprises buying multitudes of point products to feel protected.

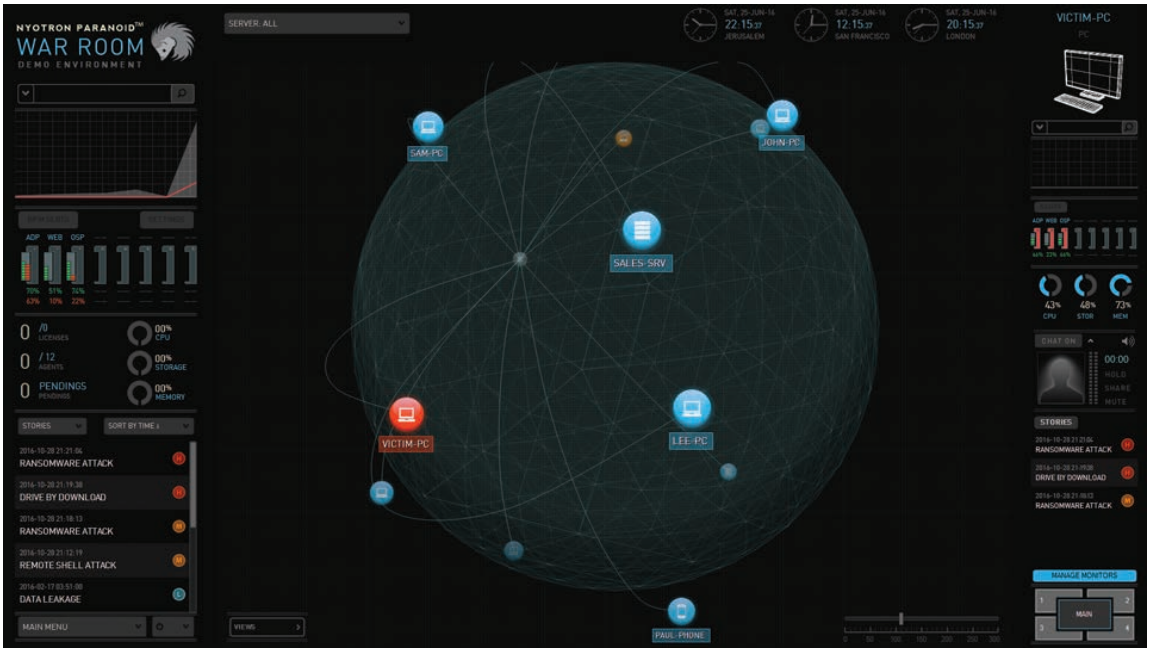
Delivering the first-ever 'threat agnostic' technology, PARANOID differentiator is clear - PARANOID is immediately effective against threats from the outside and those that are already inside the network as well as upcoming unknown threats, without the need to learn about their structure, their nature, their attack vectors, method or technique, as required of any of the machine learning, artificial intelligence or mathematical-based techniques.

A True Zero-Hour Solution: PARANOID Key Benefits

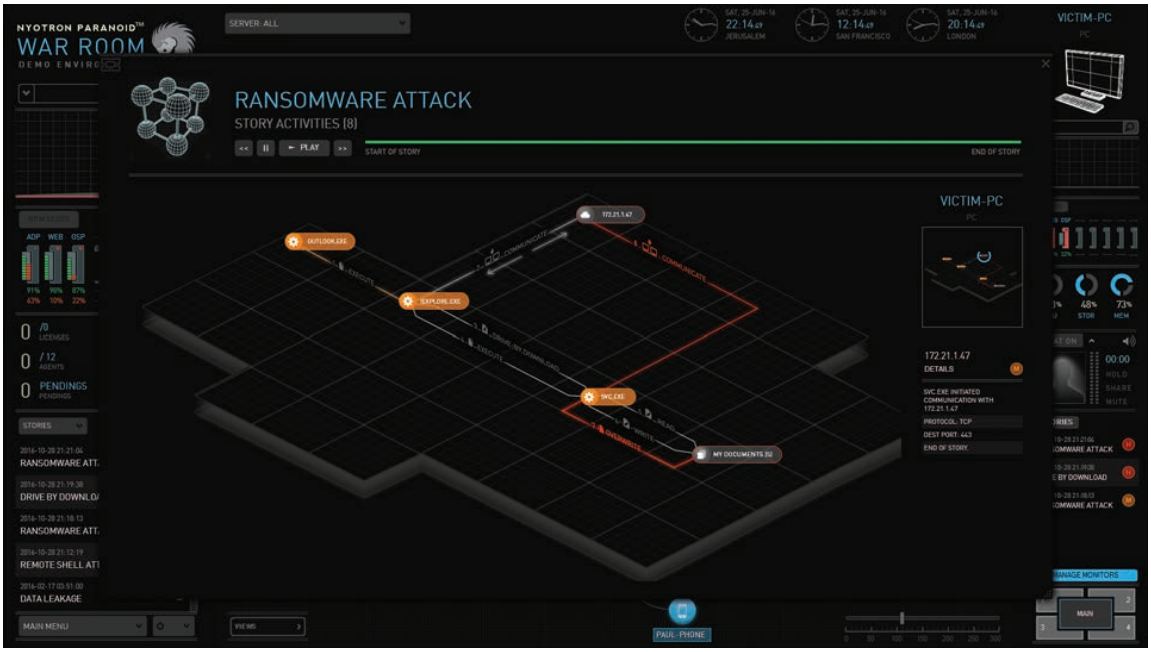
PARANOID provides a comprehensive actionable solution – Detect, Prevent, Respond and Analyze. PARANOID changes the traditional paradigm from aftermath damage handling, to a real-time prevention to ensure business continuity.

Real Time Detection/Prevention - any suspicious activity considered potential 'damage-related activity' is detected or prevented in real-time (dependent upon your security policy). The entire set of malicious activities are displayed in the central management system.

Nyotron War Room – A 3D representation of your endpoints are displayed in the management console that offers full network and attack spread visualization. The War Room can represent multiple networks or geo location views, simplifying the way to view, analyze and respond to cyber attacks.



Step-by-step forensics story line view – watching every OS activity, PARANOID offers valuable actionable incident information with extensive and meaningful forensic capabilities and scoring. Security analysts can now easily understand what happened and when, as they are exposed to a recording of the attacker's steps and their impact.



PARANOID New Generation Story-Line Forensics View

Managed Defense Services

Nyotron Managed Defense Services (MDS) for end-user customers and MSSPs – Nyotron offers flexible anti-APT solution utilization based on organization needs and nature. PARANOID may be delivered as a service, through Nyotron's 24/7 Global War Room (GWR) Center. The GWR is operated by Nyotron's top analysts and research teams, providing SLA-based proactive and actionable alerts, as well as forensics and mitigation services to its global customers. Combines technology and human expertise to deal with the most advanced threats.

Minimal TCO and easy operations - PARANOID is NOT a learning technology. As soon as it is silently deployed, it starts to immediately protect– whether the asset is inside or outside the actual network.

Zero business interruption – PARANOID's light footprint client does not rely on any database frequent updates. Setting its own industry record of less than 1% footprint and no reboot deployment, PARANOID performs silent installation. A special covert mode implementation is also available.

Advantage for SIEM and Cyber Centers - PARANOID enables full integration with SIEM and other event management systems. PARANOID dramatically narrows the "unknown threats gap", as well enabling Cyber analysts to respond immediately using the PARANOID powerful policy actions.