PARANOID. Threat-Agnostic Defense.

A NYOTRON WHITE PAPER 2016

The challenge in cyber-security is: how can we differentiate between a simple computer activity generated by a safe program and the same activity generated by a threat?

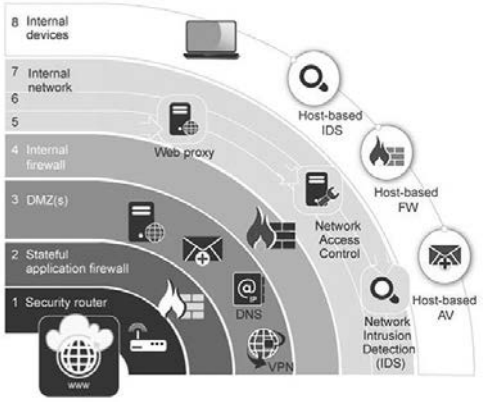
As many cyber-attacks are targeted attacks, security teams should behave as if the organization is already under attack. In addition, the emphasis today is on corporate resilience to cyber-attacks, means that we must achieve rapid recovery with minimal damage.

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

The Evolution of Security Technology

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 periodically ship their customer's regular updates, which are designed to alert when they recognize a familiar threat pattern. This concept of "blacklisting & shipping" is now in fact a losing war, as it cannot deal with what is unknown.

Then came the next-generation technologies - decoy honeypots, containment, behavior detection and algorithmic approaches. Different technologies also 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 threat objective kicks in to cause the actual damage - deleting, altering exfiltration or encrypting information (Ransomwares) that is stored on these assets.



Attacker's ultimate goal will always be the asset, where the information is. A persistent threat will always find a way to bypass all endpoints and perimeter security means.

A powerful defense layer needs to be applied on endpoints, as 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. 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 – generically 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-day 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 information is, PARANOID acts as a 'Last Line of Defense' - focuses on the final phase of the attack - preventing the actual damage.

PARANOID technology was designed under these assumptions:

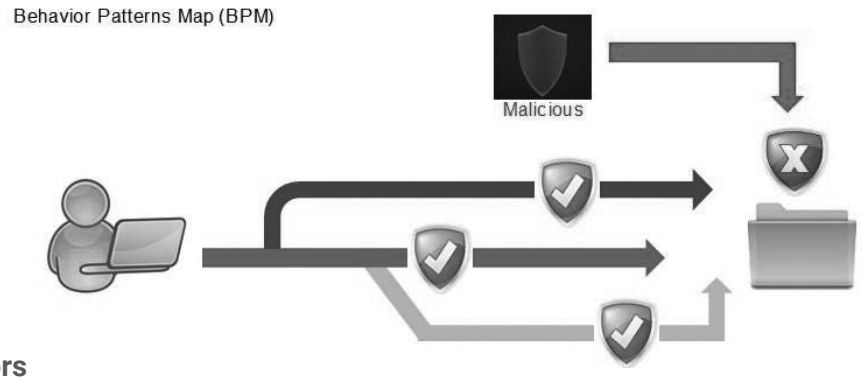
1. The attacker will eventually find a way to bypass all security means
2. The threats are already inside, undetected.

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 on a final number of possible damages, such as file deletion, data exfiltration, malicious encryption, and more. Relying on the operating system behavioral patterns consistency, Nyotron mapped all the normative ways that may lead to a damage. This way, PARANOID distinguishes between the computerized terms of "good" and "bad", 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

First generation Anti-Virus traditional vendors, match with "known threats". Next- generation advanced cyber solution ("cyber- X" vendors) can match some of the "unknown", but typically cover just a specific angle of the entire threat landscape or attack campaign. For example, some solutions rely on known exploitation methods or known application vulnerabilities (e.g. Java, Adobe), while others rely on big-data or statistical machine learning of the network and user behavior. Similar to the antivirus solutions, the effectiveness of these second-generation technologies depends on how they learn or know about the threat, attack vector, or user behavior.

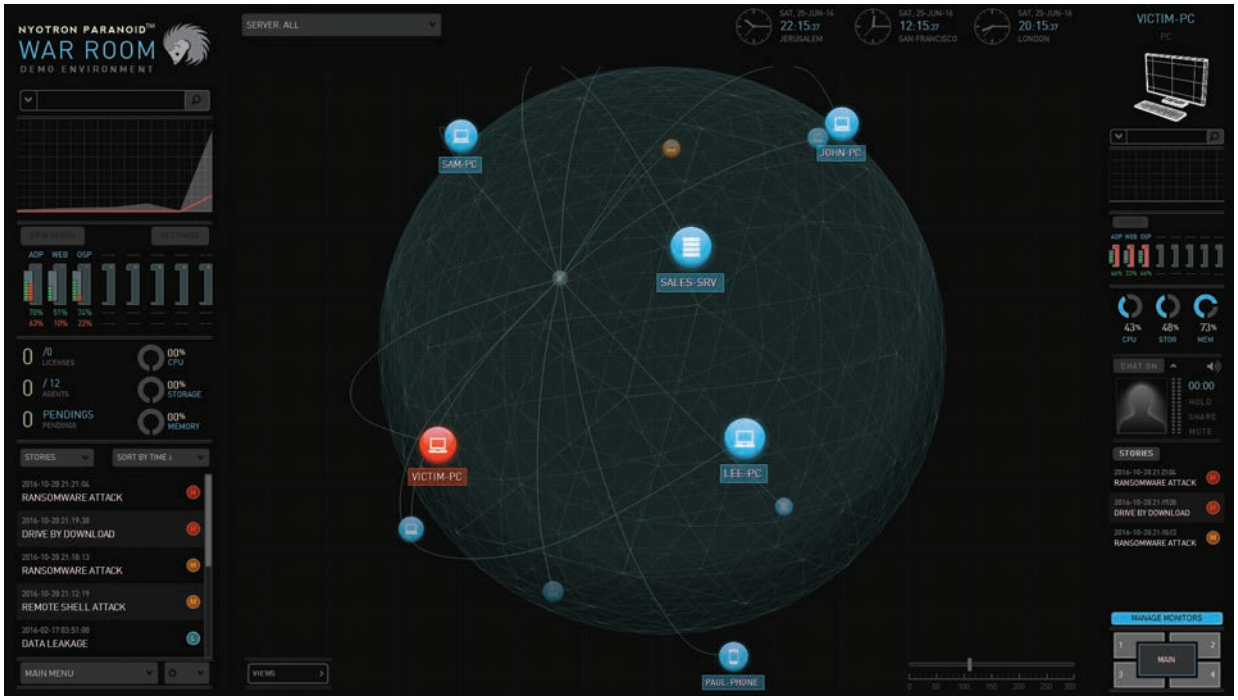
Delivering the first-ever 'threat agnostic' technology, PARANOID differentiator is clear - PARANOID is immediately effective against threats that are already inside the network and upcoming unknown threats, without the need to learn about the threats structure, their nature, their attack vectors, threat origin, or any other of the "machine learning" or mathematical-based techniques.

A true Zero-Day solution: PARANOID key benefits

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

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

PARANOID War Room – A 3D management console offers full network and attack spread visualization. The War Room can represent multiple networks or geo-locations 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 when and what happened, as they are exposed to all recorded attacker's steps and their impact.

PARANOID New Generation Story-Line Forensics View

Nyotron Managed Defense Services (MDS) for end-customers and MSSP's – 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 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.

Managed Defense Services

Combines technology and human expertise to deal with the most advanced threats.

Minimal TCO and easy operations - PARANOID is a non-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.