The Challenge of an Unpredictable Future

The sheer number of attacks, such as ransomware and other advanced threats are impossible to keep up with. What about tomorrow’s threats?

This is why a new security paradigm is needed to protect organizations from any future threat without having to know anything about it today.

PARANOID is Designed Based on These Assumptions

An attacker will eventually find a way to bypass all defensive measures.

OR

Undetected threats are already inside the environment.

The Paradigm Shift—Protect Against Today’s and Tomorrow’s Threats

PARANOID offers a game changing security paradigm to cope with advanced attacks. Rather than exploring the limitless attack possibilities, PARANOID is focused on the final stage of the attack kill-chain—intended damage. This stage consists of finite malicious activity, such as file deletion, data exfiltration or malicious encryption.

Relying on the operating system’s call behavior, Nyotron’s patented Operating System Behavior Pattern Mapping (BPM) is a blueprint of all the normative ways that may lead to damage. This way, PARANOID deterministically knows actions that are “good” and blocks everything else. This implementation of the Positive Security Model is a completely new approach without the complexity, management overhead and poor user experience that are associated with techniques such as whitelisting.

PARANOID is immediately effective against upcoming unknown threats without the need to learn about their structure, their nature, their attack vectors, method or technique required by machine learning, artificial intelligence and other mathematical-based approaches.
PARANOID Technology

PARANOID Server – Back-end infrastructure component for management and reporting that can be deployed in either a physical, virtual or cloud environment.

PARANOID Agent – Lightweight agent protects Windows laptops, desktops and servers with less than 1% CPU overhead. PARANOID Agent can be deployed completely silently and does not require a reboot for deployment.

PARANOID Management Console – Web-based administrative console provides policy management and agent configuration and enables investigation of malicious activities.

Nyotron War Room – A 3-D representation of your environment offers full network and attack sequence visualization. The War Room can represent multiple networks or geo-location views, simplifying the way to analyze and respond to cyber attacks.

Supported Windows Platforms:
- Desktop: Windows 7 and Windows 10

Minimum System Requirements for the Agent are:

Hardware:
- Processor: Intel Core 2 duo, 2GHz or equivalent
- Memory: 2 GB

Software:
- Framework: .NET 2.0
- Free Space: 1 GB

PARANOID Platform Components and Deployment Options
Step-by-Step Forensics

Watching every operating system activity, PARANOID offers actionable incident intelligence with extensive forensic visualization. Security analysts can now easily understand what happened and when, as they follow the attacker’s steps and their impact.

Nyotron Managed Defense Services (MDS) for customers and MSSPs

Nyotron offers a flexible anti-APT solution based on an organization’s needs and nature. In addition to on-premise deployment, 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.

PARANOID’s Cutting Edge Story-Line Forensics
The PARANOID Advantage

PARANOID works seamlessly with currently installed anti-malware products to strengthen endpoint protection:

- No patient zero is required to detect a new threat
- No signatures or indicators of compromise are needed
- Persistent security never stops looking for new threats, even on already compromised endpoints
- Lightweight protection—no file scanning, antivirus definition updates or other resource-draining activities

Immediate Value

PARANOID is NOT a learning technology. As soon as it is silently deployed, it starts to protect—whether or not the asset is connected to the network.

SIEM, UEBA and SOC Integration

PARANOID enables full integration with SIEM, UEBA and other event management systems for deep endpoint security visibility. PARANOID dramatically narrows the "unknown threat gap", enabling cyber analysts to respond to developing threats immediately.

About Nyotron

Nyotron offers the last line of defense to help win the war on malware. Based on the industry’s first OS-Centric Positive Security model that only allows legitimate operating system behavior, Nyotron prevents data exfiltration, corruption and other damage. Nyotron seamlessly complements existing endpoint security products with a future-proof solution providing protection from any attack vector without foreknowledge of an exploit. The company’s headquarters is in Santa Clara, California, and R&D is in Israel. To learn more, visit www.nyotron.com.