KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

June 11, 2021

Nucleon Smart Endpoint

Nucleon Smart Endpoint is an Endpoint Protection Detection & Response (EPDR) solution for Windows and Linux. It takes a multi-layered Zero Trust approach to preventing malware execution and provides Machine Learning (ML) detection models to look for signs of compromise across managed endpoints. Nucleon Smart Endpoint offers built-in and customizable response and remediation playbooks.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Endpoint Detection & Response (EDR) solutions have become increasingly popular in just the last few years as a means to help security analysts determine if other security mechanisms such as Endpoint Protection (EPP) have failed, if their systems have been attacked and compromised, and if valuable data has been exfiltrated. Surveys show that 11% of cybersecurity breaches are targeted attacks, and 13% are acts of corporate espionage, designed to steal state or trade secrets. Malware and account takeovers are involved in 48% and 14% of attacks respectively. Almost every industry and every level of government agency are under attack. Organizations are justified in looking for additional security tools to discover and thwart such attempts. A main goal of EDR is often reducing the Mean Time to Detect (MTTD) and Mean Time To Respond (MTTR) to security incidents, given that many reports show that attackers can spend months inside organizations before being detected.

EPP began as antivirus and grew steadily in importance and effectiveness from the late 1980s through the early 2000s. Though the advent and usage of ML techniques may have led to some additional marketing buzz around EPP in the early 2010s, anti-malware technologies have never been over-hyped. Today EPP is widespread and mature, and that's a good thing, as attacks involving malware are frequent and still increasing. EPP products are designed to determine if code is malicious and, if so, prevent it from executing. EPP products have accumulated numerous other security functions, such as serving as endpoint firewalls, performing URL filtering, and controlling which applications are allowed to run on endpoints.

EDR solutions look for evidence and effects of malware or other malicious activities that may have slipped past EPP products and other security tools, such as email/web gateways. Security professionals refer to such data points as Indicators of Compromise (IoCs). Examples of IoC types include:

- MD5 file hashes
- Known bad IPs and URLs
- File/process name mismatches
- Unusual application and network port usage
- Unusual process injections
- Module load point modifications
- Registry changes

EDR solutions log activities centrally, allow administrators to examine endpoints remotely, and generate

reports often complete with attribution theories and confidence levels. EDR tools are host-based agents for detecting malware infection, command and control (C2) traffic, reconnaissance and lateral movement of bad actors, and signs of data exfiltration attempts. Additionally, as part of the detection process, EDR tools can also perform evaluation of threat intelligence information, event correlation, interactive querying, live memory analysis, and activity recording and playback. Using Machine Learning (ML) and Deep Learning (DL) algorithms can help produce normal activity baselines for comparisons, discover and classify anomalies, and reduce false positives.

EDR solutions have a management console for collecting and analyzing information from deployed agents, producing alerts, and facilitating incident response, threat hunting, and forensic investigations.

One of the advantages that EDR offers is the ability to automate investigations and responses. Playbooks often ship with EDR tools and can be configured on consoles and executed by agents. Responses can include actions such as case creation, forensic evidence collection, termination of processes, file removal, quarantine, memory analysis, and full endpoint restoration.

EDR systems typically output event information to Security Incident and Event Management (SIEM) platforms for centralized storage and analysis.

EDR solutions can provide additional insights into possible nefarious activities in your enterprise and can serve as a complement to other security tools. EDR is not a substitute for EPP, but rather a complement to EPP, email/web gateways, Network Detection & Response (NDR), and Distributed Deception Platforms (DDPs) as important components of modern security architectures.

EDR solutions require a special set of skills to not only implement and run but also from which to derive value. The inclusion of ML technology does not obviate the need for trained security analysts. Most organizations that successfully deploy EDR have a well-defined IT security organization and one or more SOCs (Security Operations Centers), staffed by knowledgeable security analysts. Such organizations would be categorized as at least Level 1 or 2 in the **Hunting Maturity Model.**

A few years ago, EDR was mostly used by these kinds of larger enterprises with dedicated security analysts. Today, however, EDR capabilities are sought after by a wider variety of organizations including smaller companies without EDR specialists. Managed Security Service Providers (MSSPs) and SOC-as-a-Service (SOCaaS) providers are offering expert managed detection and response services utilizing commercial EDR products.

Nucleon Security was launched in 2015 in France by a team of cybersecurity consultants who wanted to bring a Zero Trust approach to endpoint security. Nucleon Smart Endpoint was first made available in 2018. The company is a mid-stage startup that is actively growing and has customers in multiple countries across the EU, Africa, and the Middle East.

2 Product Description

Nucleon Smart Endpoint addresses both halves of EPDR with a four pillared approach: Prevention, Detection, Response, and Remediation. The product is instantiated as an agent with kernel and application-level components. Agents are available for Windows 7, 8, and 10; Windows Server 2008, 2012, 2016, and 2019; and CentOS, Debian, RedHat, and Ubuntu Linux. Linux agents have reduced capabilities, but full feature parity with Windows agents is planned for later in 2021.

Nucleon adheres to what they call the multi-layer Zero Trust architecture for preventing execution of malware. Zero Trust Architecture implies authentication and authorization for every action in a given system. Zero Trust at the network level means ensuring that users and programs are granted network access only if they are demonstrably identified and have permissions defined allowing that access. Zero Trust at the application and identity layers means the full context of each request (user, originating device, environmental attributes, and information about the target resource) is evaluated against pre-defined policies before allowing access to the requested resource. Nucleon implements Zero Trust at the process level on endpoints.

Nucleon Smart Endpoint takes two approaches to malware prevention. The first technique relies on static analysis of files using ML enhanced detection algorithms: files are examined for signs of potentially malicious behavior. Nucleon does not use traditional signature scanning or sandboxing, nor does it perform advanced runtime behavioral or memory analysis. In addition to its ML analysis, Nucleon Smart Endpoint agent shares suspicious code samples with VirusTotal for comparison. Nucleon Smart Endpoint also looks for known vulnerabilities (CVEs) on each protected system and presents scan results on the enterprise console.

The second EPP method involves the abstracted development and enforcement of rules, which are essentially customized allow/deny lists for process execution. By default, unapproved binaries are not allowed to execute. Nucleon Smart Endpoint "absorbs" normal user activities and workflows to develop a baseline of normal user-to-process interaction. This routinely collected information is used for ongoing tweaking of process rules per endpoint. In addition to process execution prevention, Nucleon Smart Endpoint's rules can also prevent local and remote file access and can prevent or terminate network connections. Moreover, the process rules can be extended to form a rudimentary type of Data Leakage Prevention (DLP) function, in that copying and moving data files to removable storage can be prohibited.

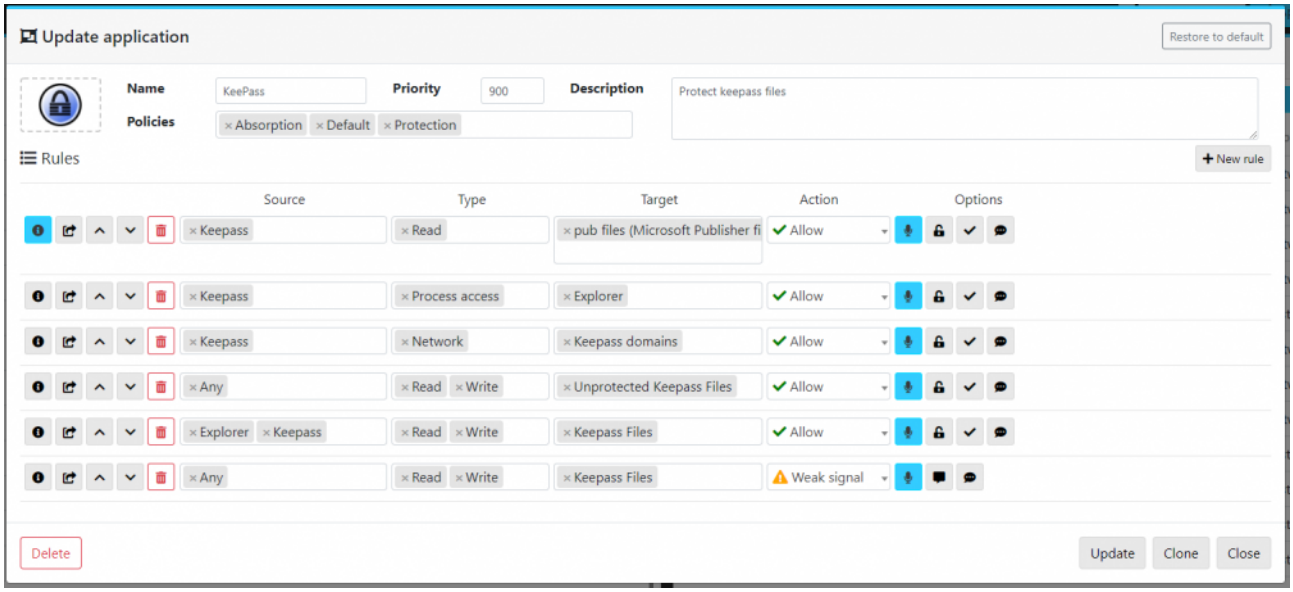

Figure 1: Nucleon Smart Endpoint process policy builder (Source: Nucleon)

System hardening can also help prevent endpoint compromises. Nucleon Smart Endpoint's process rules form the basis for customizable system hardening. Examples of hardening actions that can be taken automatically by Nucleon Smart Endpoint include imposing limitations on the use of PowerShell, disallowing the use of unusual TCP/UDP ports by applications (constraining web browsers to TCP 80/443), and preventing users from installing device drivers.

Nucleon Smart Endpoint's EDR functions also use ML detection algorithms to examine logs and registry and filesystem content changes to look for symptoms of compromise. Their ML detection models are based on in-house developed intellectual property, which are focused on unsupervised anomaly detection goals. The models are updated daily, and clients can benefit from updates to detection models without having to modify the rules or deploy updates manually. Nucleon Smart Endpoint examines up to 8,000 different file features. Nucleon Smart Endpoint concentrates on finding malicious activities used by malware in "living off the land", which are encountered in reconnaissance, lateral movement, privilege escalation, and exfiltration phases, as documented in LOLBAS.

Response features are an important consideration in EDR products. Responses begin with automation of investigation tasks. Smart Endpoint runs preliminary analytics on suspicious events, collecting information on the logged-in users, processes running, and files on the endpoint. If Indicators of Compromise (IoCs) are found, the latest threat intelligence can be pulled and assembled for analysts to consider.

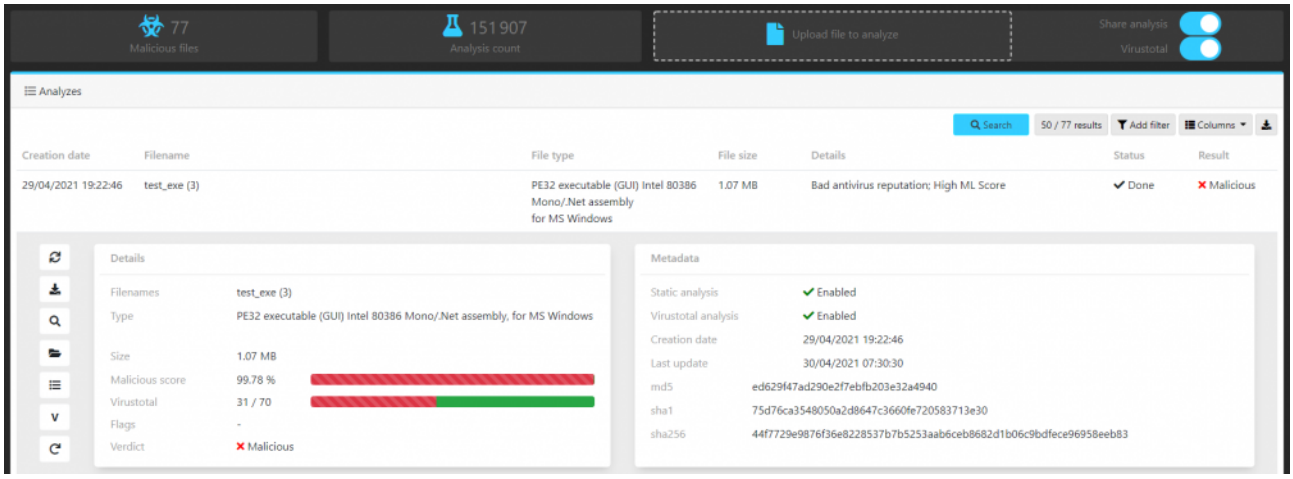

Figure 2: Nucleon Smart Endpoint analysis (Source: Nucleon)

Nucleon Smart Endpoint customer administrators can use the built-in playbooks and create new playbooks from templates for additional investigation actions.

For remediation, Nucleon Smart Endpoint enables a variety of actions. Remediation actions can be either manually initiated by customer admins and analysts, or fully automated actions at customer discretion. Examples of actions that are possible range from gathering and copying file information, quarantining files, deleting files, blocking network access, process termination, and full system restore to last known good point. To effect system rollbacks, Nucleon Smart Endpoint leverages the Windows Volume Shadow Copy.

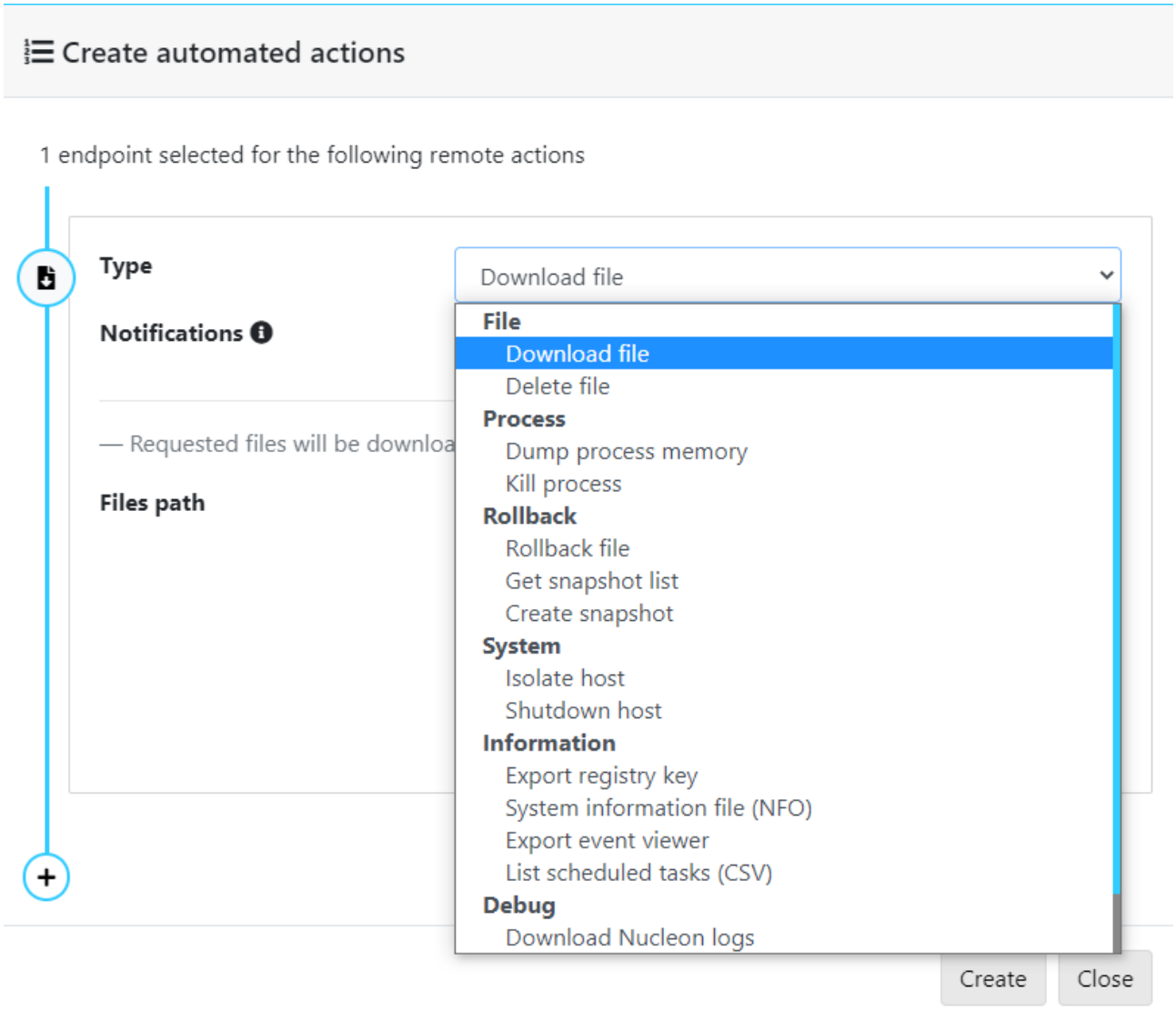

Figure 3: Nucleon Smart Endpoint remediation actions

Nucleon reports that most customers choose to allow less severe actions to be automated, such as evidence collection and restoration of single files, rather than more intrusive actions such as node isolation and full system rollbacks.

Nucleon can be deployed using available enterprise configuration management tools. For environments without desktop management tools, Nucleon can be installed by sending links to users. Automated discovery of endpoints and service level installation is not supported.

Nucleon provides a cloud-based console for customer administration. Access to the console requires either username/password or SMS OTP authentication. MSSP customers can set up delegated access to client instances.

The enterprise console features dashboards with standard reports and global activity maps. Analysts can drill down from the console into events for investigations. Analyst views include detailed timeline views,

process tree views, Nucleon risk scores for files, and VirusTotal scores for files. The Nucleon Smart Endpoint console can also display per-node and aggregated views of all nodes' CPU, memory, disk, and network utilization. This feature is useful for discovering low-level crypto-mining activities.

Nucleon Smart Endpoint can send event information over syslog to SIEMs, and event information can also be sent over APIs in JSON format. Connectors are available for Elastic Search and Splunk. At present, Nucleon does not offer integration with SOAR platforms.

3 Strengths and Challenges

Nucleon Smart Endpoint takes a different approach to EPP than most of its competitors. Rather than putting the emphasis on runtime behavioral and memory analysis, as most current generation EPP products do, Nucleon utilizes their multi-layer Zero-Trust architecture for authorizing process level execution on the endpoint. The use of ML is essential in the EPDR product space. Here too, Nucleon deploys its proprietary ML in a novel way. Nucleon employs ML to "absorb" normal user activities to develop a baseline of activities on which to base endpoint specific rules that prevent malware execution. Additionally, Nucleon offers LOLBAS-informed hardening and detection as well as vulnerability enumeration.

Nucleon's EDR covers the expected range of capabilities for aiding investigations, including IoC detection, CTI enrichment, and automated evidence collection. Nucleon offers a good range of remediation actions, from quarantining files to process termination to full system restore for affected machines.

As a newer entrant in the market, Nucleon has some areas for future enhancement. Adding methods for malware detection such as behavioral and memory analysis would be advantageous. Expanding security architecture integration would also be beneficial for enterprise customers. For example, support for SOAR will be necessary as more organizations adopt SOAR and will require EPDR vendors to provide connectors. Strong authentication to the cloud-based enterprise console should be mandatory, and additional forms of multi-factor authentication should be supported.

Strengths

- Single agent architecture includes EPP, EDR, and some limited DLP functionality
- System hardening and vulnerability assessment built-in
- Multi-layer Zero-Trust architecture at the process level
- Automated, ML-enhanced process rule baselining
- Good selection of remediation actions available, up to full system rollback
- Intuitive analyst interface with timeline and process tree views
- Enterprise visibility of nodes' CPU, memory, and network utilization

Challenges

- Additional runtime malware detection techniques needed
- API level integration with EPP products would be useful
- Asset discovery mechanism or integration with UEM solutions would be beneficial
- Support for SOAR platforms not present yet
- Needs strong authentication and MFA by default

4 Related Research

Market Compass on Endpoint Protection, Detection, and Response
Buyer's Compass on Endpoint Detection & Response
Leadership Brief: Defending Against Ransomware
Buyer's Compass on Endpoint Protection