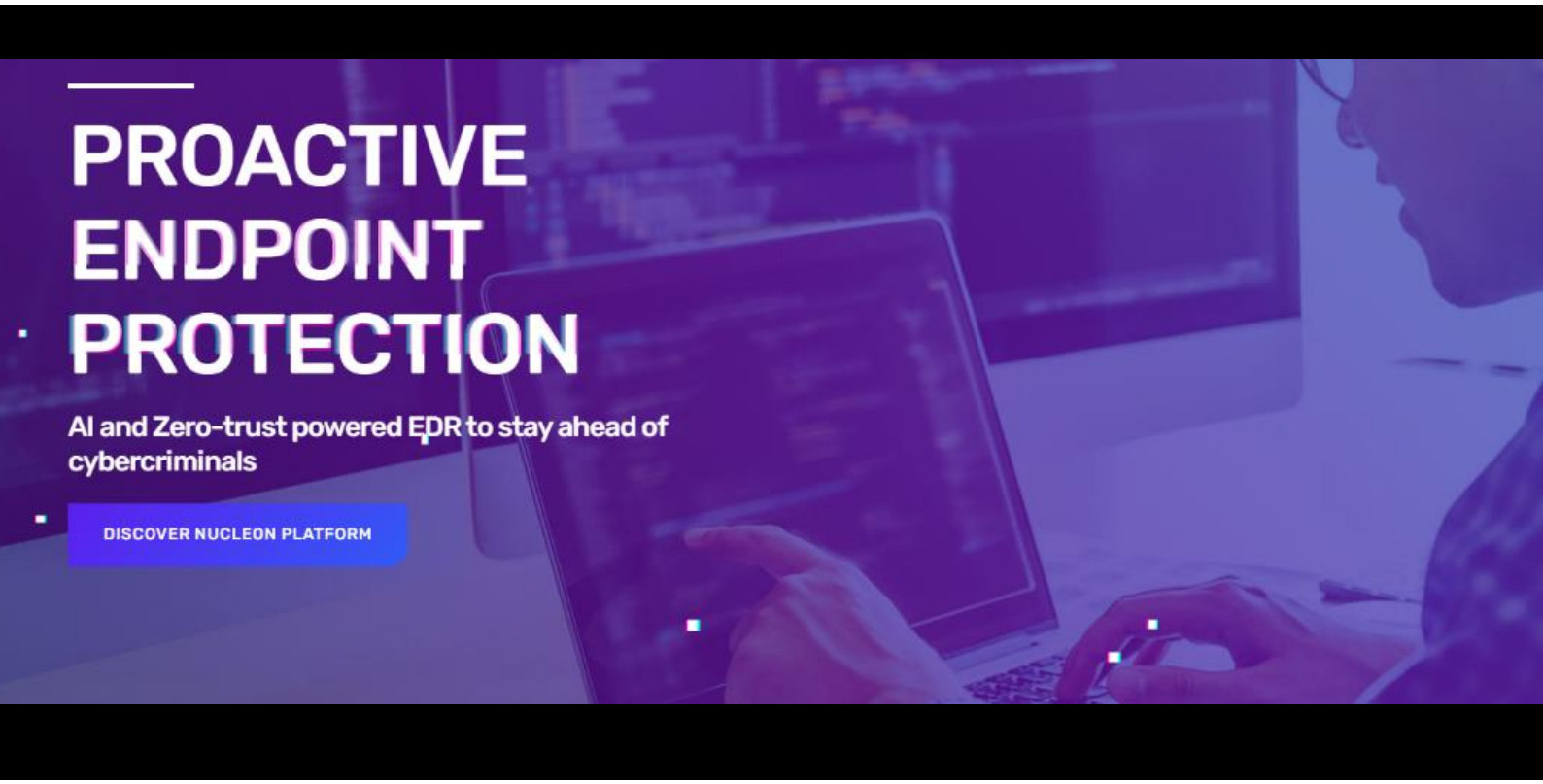
DIGITALSKILLS®
CYBERSECURITY SOLUTIONS
OFFICIAL DISTRIBUTOR IN PORTUGAL



BUSINESS CONTEXTUAL PROTECTION

Nucleon Smart Endpoint adapts its protection layers automatically depending on your critical data.

Nucleon
Protect data that matters

Nucleon Security – Product Overview with Case Studies

NUCLEON NEXTGEN ANTIVIRUS

Protection against **malware** and **ransomware** based on artificial intelligence. The best Cloud solution to protect your business without mobilizing your IT resources and impacting your budget.

Protection against cyber-attacks without compromise

With no administration effort and in complete autonomy, Nucleon NextGen Antivirus provides a very high level of protection based on technologies such as artificial intelligence. Dedicated to VSEs and SMEs, Nucleon NextGen Antivirus protects your business against cyber threats such as malware, ransomware and infected Word or Excel files.

Unlike traditional Antivirus, Nucleon NextGen Antivirus does not rely on the signature mechanism which is now obsolete. Indeed, Nucleon NextGen Antivirus continuously learns from new attacks around the world and creates a protection model. This model is sent every day to your workstations and servers to protect them from the latest attack typologies.

Reduce protection costs

No additional hardware or software is required to use Nucleon NextGen Antivirus .
In addition, Nucleon NextGen Antivirus is specially designed to limit administration actions, which saves you from mobilizing human resources.
Control your expenses related to the protection of your assets with monthly billing with or without commitment.

The Power of NextGen Antivirus in the Cloud

Centralized protection without additional IT resources Nucleon NextGen Antivirus democratizes the centralized management of desktop and server protection with the Cloud.

Instant protection

After acquiring licenses, deploy the agents on your desktops and servers and they will automatically connect to the Nucleon NextGen Antivirus management interface in the cloud.

Automatic updates

You don’t have to worry about updating or maintaining in operational condition, Nucleon Security engineers take care of it and it's transparent for you.

BENEFITS

- ✓ Comprehensive and simplified protection using Zero-Trust policies
- ✓ Real time visibility of system and network activities
- ✓ Refined and light agent the does not affect the production and users daily activities
- ✓ Centralized console
- ✓ Easy and quick deployment
- ✓ Cloud or On-premise deployment
- ✓ Personal data compliance

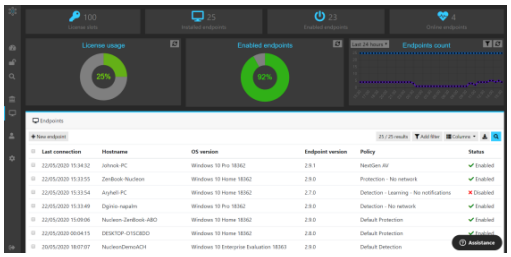
Comprehensive coverage against cyber threats

- ✓ Malware/Ransomware Protection
- ✓ Protection against compromised Word/Excel attacks
- ✓ Smart Scan
- ✓ Workstations and servers hardening
- ✓ Protection against network attacks
- ✓ Global monitoring of the health of the IT infrastructure (CPU and RAM)
- ✓ Cloud storage control (One drive, Box, Google Drive, etc.)

Enhanced visibility

DASHBOARD

INFRASTRUCTURE VISIBILITY



NETWORK VISIBILITY

SUPPORTED OPERATING SYSTEM

Windows CentOS Red Hat debian ubuntu

PERFORMANCES

- ✓ 1% < CPU
- ✓ 100m < RAM

GDPR COMPLIANCE

- ✓ Records of processing activities;
- ✓ Native pseudonymization and anonymization;
- ✓ Stores data encryption

NUCLEON ADVANCED BUSINESS PROTECTION

Cyber threat protection that adapts to your business and your most critical data. Explore the power of Artificial Intelligence and Zero-Trust and ensure your business continuity.

Comprehensive Approach to Cyber Threat Protection

Nucleon Advanced Business Protection protects desktops and servers by putting in place successive layers of protection to safeguard you during all phases of attacks. Nucleon Advanced Business Protection allows the identification of weak points in your infrastructure, blocks attacks and provides you with all the tools you need to investigate.

Protection tailored to your business and critical data

Nucleon Advanced Business Protection absorbs your internal uses, identifies your critical data, and then automatically creates specific protection rules. These rules protect your critical data from unauthorized access, leakage and blockage by ransomware.

Reduced cost of protection

No additional hardware or software is required to use Nucleon Advanced Business Protection.
In addition, Nucleon Advanced Business Protection is specially designed to limit administration actions, which saves you from mobilizing human resources.
Control your expenses related to the protection of your assets with monthly billing with or without commitment.

Endpoint Security with the benefits of the cloud

Centralized protection without additional IT resources
Nucleon Advanced Business Protection democratizes the centralized management of desktop and server protection with the Cloud.

Instant protection

After acquiring licenses, deploy the agents on your desktops and servers and they will automatically connect to the Nucleon Advanced Business Protection management interface in the cloud.

Automatic updates

You don’t have to worry about updating or maintaining in operational condition, Nucleon Security engineers take care of it and it's transparent for you.

Malicious behavior

Zero-Trust policies ensure that the attack techniques used by hackers are blocked. Sensitive scripting and administration tools are not allowed in order to block complex infection processes and fileless attacks.

Advanced file analysis

When a program that is not recognized by policies is executed, it is analyzed using a proprietary "machine learning" engine.
The agent's "SmartScan" functionality also allows files to be checked even if they are not running, thus keeping a healthy system at all times.

Easier investigation

The centralized administration console provides all the tools to identify the source of any suspicious behavior.
It is easy to understand the execution flow of a malware or even a business software.

Comprehensive coverage against cyber threats

- ✓ Vulnerability scan and management
- ✓ Absorption of usages and hardening of workstations and servers
- ✓ Malware/Ransomware Protection
- ✓ Incident investigation
- ✓ Removable devices control
- ✓ Protection against compromised Word/Excel attacks
- ✓ Smart Scan
- ✓ Protection against network attacks
- ✓ Global monitoring of the health of the IT infrastructure (CPU and RAM)
- ✓ Cloud storage control (One drive, Box, Google Drive, etc.)

BENEFITS

- ✓ Comprehensive and simplified protection using Zero-Trust policies
- ✓ Real time visibility of system and network activities
- ✓ Refined and light agent the does not affect the production and users daily activities
- ✓ Centralized console
- ✓ Easy and quick deployment
- ✓ Cloud or On-premise deployment
- ✓ Personal data compliance

SUPPORTED OPERATING SYSTEM

Windows CentOS Red Hat debian ubuntu

PERFORMANCES

- ✓ 1% < CPU
- ✓ 100m < RAM

GDPR COMPLIANCE

- ✓ Records of processing activities;
- ✓ Native pseudonymization and anonymization;
- ✓ Stores data encryption

NUCLEON DETECTION AND RESPONSE

Endpoint Detection, Response and Remediation Platform.

Comprehensive Cyber Threat Protection Approach

Nucleon Detection & Response platform ensures the protection of workstations and servers by implementing successive layers of protection to protect you during all phases of an attacks. Nucleon Detection & Response allows the identification of weak points on your infrastructures, blocks attacks and provides you with all the tools to investigate.

A real tailored protection of business data

Nucleon Detection & Response absorbs your organization's specific business uses, identifies your critical data, then automatically creates specific protection rules. These rules will protect your critical data against illegitimate access, leakage or blockage.

Identification and blockage of malicious behavior

Multi-Layer Zero-Trust policies block attacks techniques used by hackers on different levels:
At a system level, the protection rules will focus for example on the protection of sensitive administration scripts and tools in order to prevent complex infection like "fileless" attacks.
At a network level, the protection rules will restrict internet access to avoid data exfiltration. For example, the Microsoft Office suite only has access to the servers and domains it needs to function normally.
Many attack processes are based on malicious macros by abusing users, which is why Office Suite files are scanned before being opened.

The easiest way to investigate

All the tools needed to identify the root cause of an attack or to follow a suspicious behavior are made available at the centralized management console. It is simpler now to understand the execution flow of malware or your own software.

Remediation, isolation and Rollback

If the data is altered or compromised by malicious software, or simply by a user's inadvertence, it can be restored from the administration console. This functionality will always provide a solution in case of a cybersecurity incident and it is natively available with no need to install any additional components.
In case of suspicious behavior, the machine(s) can be remotely isolated from the network to prevent any additional damage. The remediation features allows a complete cleaning of the system that delete all the files created by the attack vector.

Remote actions

The administration console allows remote commands to be launched on one or more machines. These features facilitate investigation and incident response.

Global coverage against cyber threats

- ✓ Vulnerability management
- ✓ Workstations and servers hardening
- ✓ Protection against known and unknown Malware/Ransomware
- ✓ Investigation tools
- ✓ Removable devices control
- ✓ Protection against malicious Word / Excel
- ✓ Smart Scan
- ✓ Protection against network attacks
- ✓ Resources management
- ✓ Cloud Storage Control (One drive, Box, Google Drive, etc.)
- ✓ Remediation tools
- ✓ Rollback of altered or compromised files
- ✓ Remote actions (distant shell)

BENEFITS

- ✓ Complete and simplified protection using Zero-Trust policies
- ✓ Real-time visibility of system and network activities
- ✓ A purified and light agent which does not affect the production and the daily life of the users
- ✓ Centralized console
- ✓ Easy deployment
- ✓ Cloud or On-premise deployment
- ✓ Personal data compliance

SUPPORTED OPERATING SYSTEM

Windows CentOS Red Hat debian ubuntu

PERFORMANCES

- ✓ 1% < CPU
- ✓ 100m < RAM

GDPR COMPLIANCE

- ✓ Records of processing activities;
- ✓ Native pseudonymization and anonymization;
- ✓ Stores data encryption.

Endpoint Detection and Response Platform

NUCLEON EDR PARADIGM

Nucleon Smart Endpoint is based on 4 pillars:

BUSINESS CONTEXTUAL PROTECTION

Nucleon Smart Endpoint adapts its protection layers automatically depending on your critical data.

BUSINESS CONTEXT ABSORPTION
The smart agent learns continuously the internal data usage and the system interactions.

AUTOMATED RULES CREATION
Automated business-oriented security rules to provide a proactive protection of the business data.

MULTI-LAYER ZERO-TRUST
Set up successive protection layers on multiple levels in order to harden the work environment.

DETECT, RESPOND AND REMEDIATE

Nucleon Endpoint Detection and Response EDR is the most effective way to protect the value created by your organization against any threat.

Some benefits with Nucleon Smart Endpoint EDR platform

- ✓ check Effective business-oriented hardening
- ✓ check AI-powered detection to block unknown threats
- ✓ check Reduce security operational team fatigue
- ✓ check SOC Integration to detect new attack scenario

YOUR DEFENSE GEAR

All you need to defend and gain ground on cyber criminals.

LEARNING USAGES

Define the right hardening rules while maintaining business continuity. Users activities absorption allows identifying users' interactions with the information system and help create specific protection rules.

ZERO-TRUST

Establish the multilayer verification on process, network and data level. Every action on the system is checked in order to validate the authenticity of the source and its legitimacy to conduct the action.

MACHINE LEARNING

Detect unknown malware and ransomware using our continuous learning algorithm. Machine learning automated detection models by sector are used to protect against targeted attacks.

DEEP VISIBILITY

Identify blind spots and suspicious behaviors on your information system, and build enhanced correlation rules on your SIEM thanks to the increased visibility capabilities.

INVESTIGATION

Simplify investigation after an incident using increased visibility capabilities and graphical attack representation. Enrich your incident management tools with artifacts collected by the platform.

VULNERABILITY MANAGEMENT

Identify automatically the weaknesses of your information system. Be notified without delay when a CVE impacting your IT infrastructure is published, or when a vulnerable program is identified on your endpoints.

REMOTE ACTIONS

React effectively by performing remote actions on one or multiple endpoints in order to isolate them, get files or system information, stop a process, dump process memory and more. All necessary actions to respond if a suspicious behavior is identified.

REMEDIATION & ROLLBACK

Revive your business activity quickly by cleaning the system and getting back lost or corrupted data. The remediation and rollback features are the last resort after an attack, even at the initiative of a user.

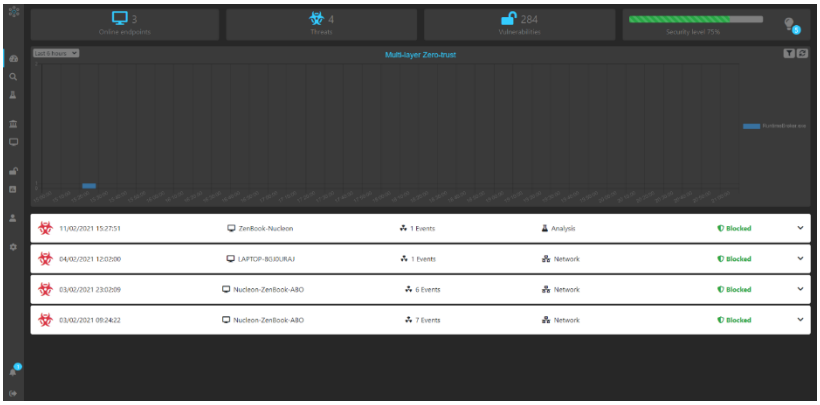
Maxime Vidal Madjar
CIO Group Gaumont

«We have chosen the EDR Nucleon Smart Endpoint to replace our traditional antivirus. We were convinced that this solution was in line with our plan to improve the security level of Gaumont's information system. We particularly appreciate the technical support of the security supervision team both for their skills and for their reactivity.»

ADMINISTRATION CONSOLE AND SITE SEGMENTATION

The administration console provides an overview of the events that have occurred on workstations and servers:

- ✓ Number of security notifications
- ✓ Number of workstations and servers started
- ✓ Number of events blocked per day
- ✓ The most vulnerable workstations and servers
- ✓ The most impacted / sensitive workstations in view of security events



Nucleon Smart Endpoint was designed to allow large organization to segment and delegate the management of geographic sites and subsidiaries.

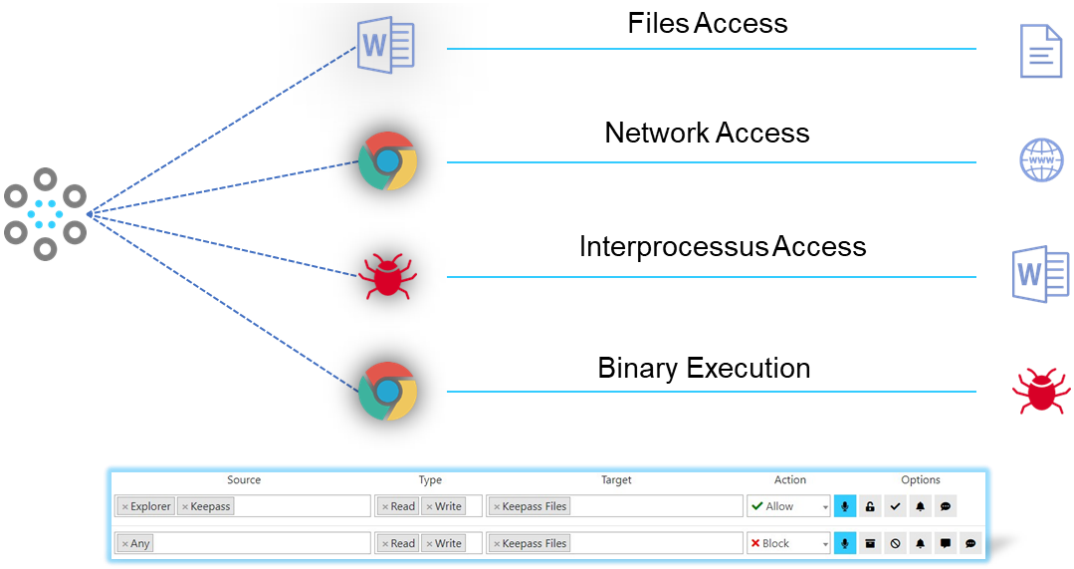
The organization CISO/CIO will have a global vision of all subsidiaries while assigning access to local relays.

PREVENTION USING ZERO-TRUST

The security policy based on the principle of Zero-Trust represents breakthrough innovation at the service of organization's cybersecurity.

Nucleon Smart Endpoint introduced Multi-layer Zero-Trust. This technology makes it possible to build several lines of defense in order to block threats on several levels:

- ✓ System and process
- ✓ Network
- ✓ Data
- ✓ Application

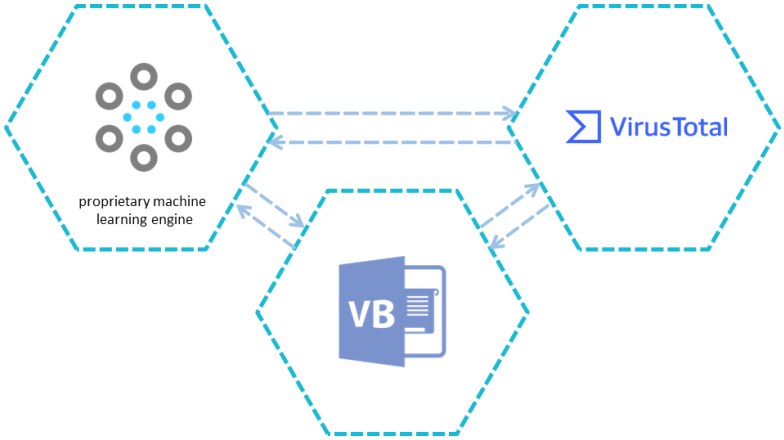


All applications are assigned network access, data and specific processes and cannot depart from these rules. By default, there are over 70 preconfigured applications preset.

DETECTION USING IA AND MORE

Nucleon Smart Endpoint has an Artificial Intelligence module to identify threats without having to study the signature or even the behavior of the software.
The heart of this module is built around a machine learning method called "Gradient Boosting".
This method solves regression and classification problems, it produces a prediction model in the form of a set of weak prediction models, generally decision trees. Then the model is generalized to provide a strong prediction.
In addition to our artificial intelligence results, Nucleon Smart Endpoint integrates the analysis results of over 70 Antivirus by connecting to Virus Total platform.

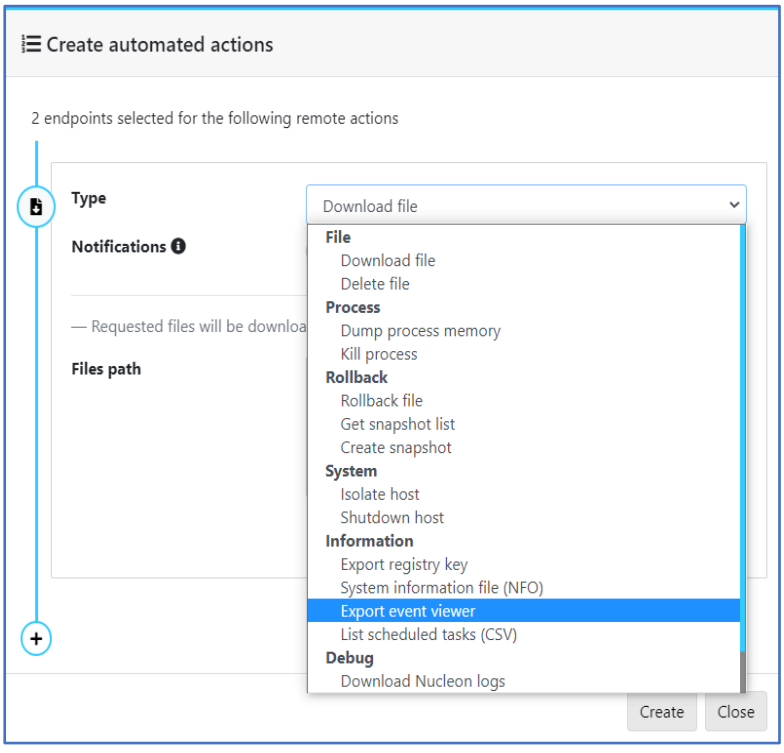
Finally, malicious macros remain the most widely used infection vector for deploying malware. It is for this reason that Nucleon Smart Endpoint embeds an analysis engine specific to this type of script.
Indeed, as soon as an attachment or a copy of a file containing a macro is received, the scanning engine takes over to identify any malicious attempt even before opening the file.



INCIDENT RESPONSE AND INVESTIGATION

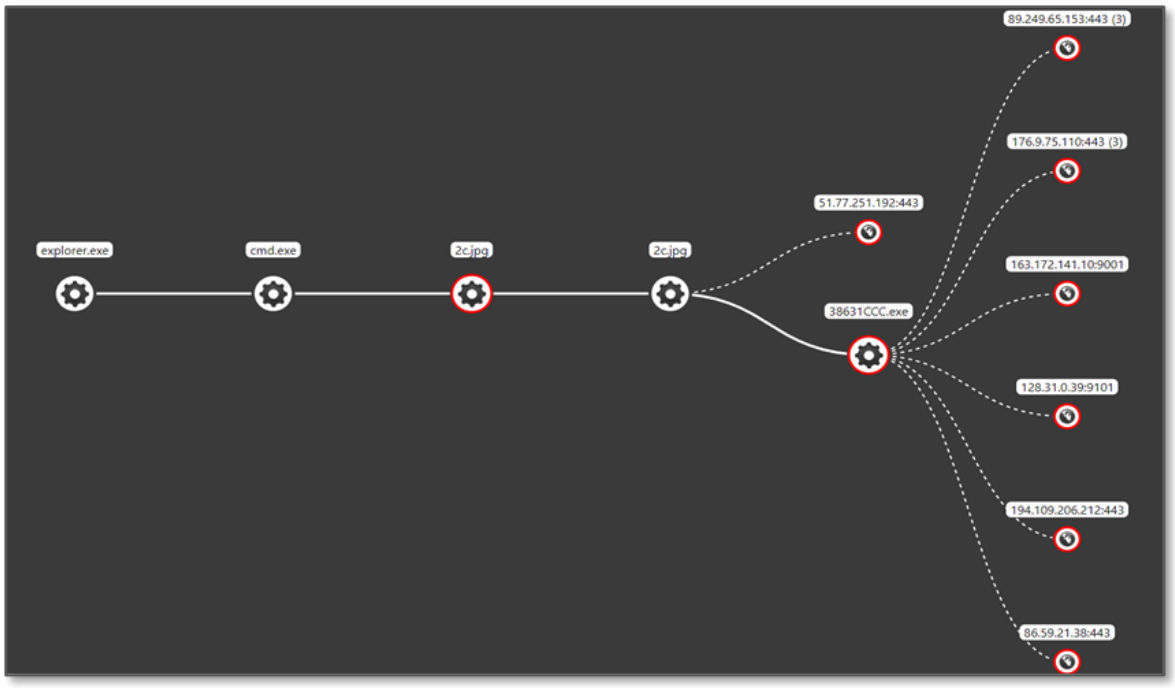
In the event of an attempted attack or suspected infection, Nucleon Smart Endpoint provides security teams with the necessary tools to respond quickly to the incident:

- ✓ Workstation isolation
- ✓ Disk memory recovery
- ✓ Recovering the memory of a specific process
- ✓ Retrieving the list of running processes
- ✓ Recovery of registry keys



By using the automated action view, a playbook of remote action can be created and executed on one or multiple endpoints.

Finally, in order to have a global view of an incident, Nucleon Smart Endpoint allows you to draw the execution diagram as in the example below:



VULNERABILITY MANAGEMENT

Nucleon Smart Endpoint offers a new way to manage vulnerabilities within the organization. This module needs no scan scheduling or to wait hours to have scan results, everything is automated and continuous.

The vulnerability scan is initiated when new software is installed, or a new vulnerability is released based on the "NIST" global vulnerability benchmark. The administrator is notified on the dashboard in near real time. The Nucleon Smart Endpoint administration interface provides a comprehensive view of the most impacted workstations and servers as well as the most critical vulnerabilities.

Nucleon
Protect data that matters

DIGITALSKILLS®
CYBERSECURITY SOLUTIONS
OFFICIAL DISTRIBUTOR IN PORTUGAL

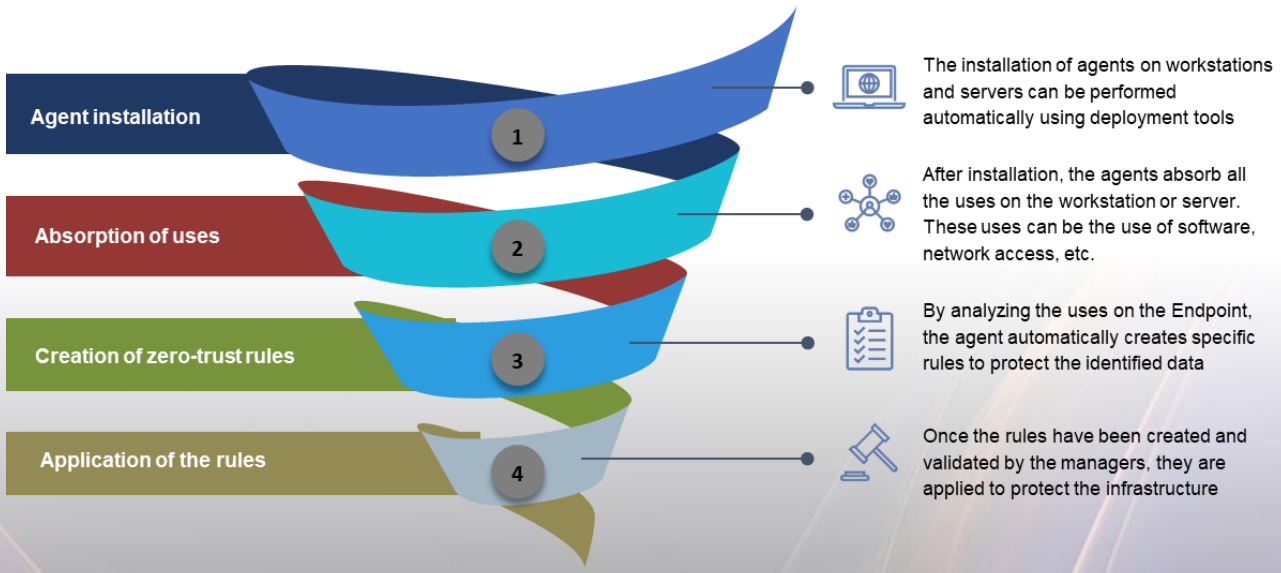
SUPPORTED OPERATING SYSTEMS

Nucleon Security supports a wide variety of Windows and Linux distributions as well as virtualization OSes.

Windows CentOS Red Hat debian ubuntu®

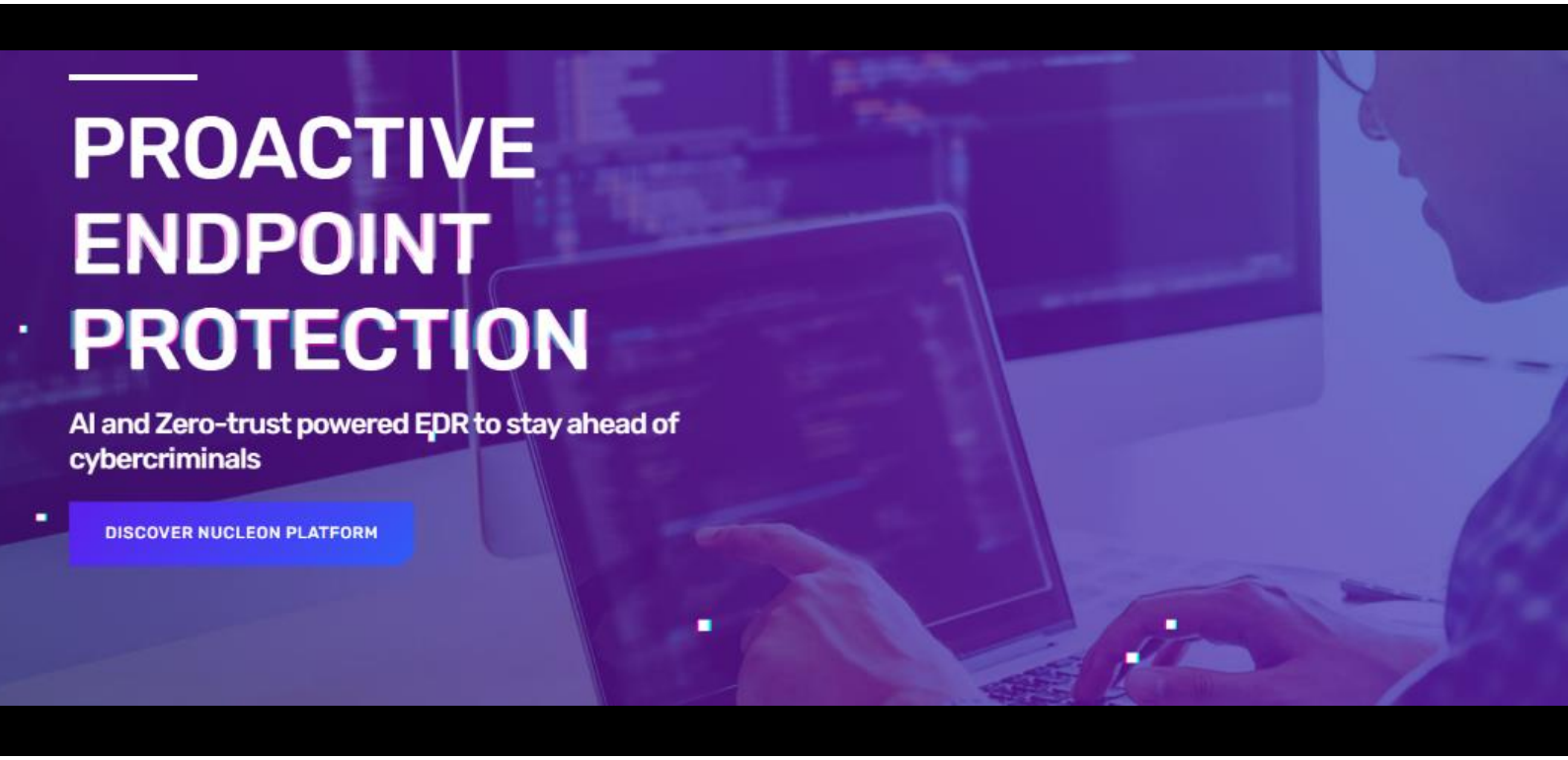
DEPLOYMENT

Nucleon Smart Endpoint can be used in cloud mode or on-premises mode. The agent can be deployed on endpoint using a wide range of deployment tools like GPOs or Puppet.



Capabilities	Description	NSE NextGen Antivirus	NSE Advanced Business Protection	NSE Detection and Response
Supervision Dashboard	Dashboard	✓	✓	✓
IT Infrastructure Global Health	Metrics, security level, CPU and RAM consumption	✓	✓	✓
Drive Smart Scanner	Passive scan of machine disks	✓	✓	✓
NextGen Office Macro inspector	Office macro analysis	✓	✓	✓
Lateral Movement Protection	Blocking the spread of malware	✓	✓	✓
Cloud Storage Control	On-demand blocking of DropBox, OneDrive, etc.	✓	✓	✓
Machine Learning Detection Engine	Analysis of executed files	✓	✓	✓
Multi-Layer Zero-Trust Basic Hardening	Basic system hardening	✓	✓	✓
Host based firewall	Network limitation rule		✓	✓
Multi-Layer Zero-Trust Business hardening	Business-Centric Advanced hardening		✓	✓
Deep Logging	Visualization of events and research		✓	✓
Deep investigation	Identifying the flow of actions		✓	✓
Vulnerability Management	Identification of vulnerabilities		✓	✓
External Peripheral Control	USB management application, external disks, etc.		✓	✓
Restauration (Rollback)	Restoring files following an internal attack or malware			✓
Remediation	Removing malicious elements after an attack			✓
Remote actions	Remote command execution on endpoints			✓

DIGITALSKILLS®
CYBERSECURITY SOLUTIONS
OFFICIAL DISTRIBUTOR IN PORTUGAL



BUSINESS CONTEXTUAL PROTECTION

Nucleon Smart Endpoint adapts its protection layers automatically depending on your critical data.

Nucleon
Protect data that matters

Case Studies

| Gaumont |

USE CASE: Gaumont

CONTEXT AND CHALLENGES

The business of the company is being reinvented with the arrival of new technologies This phenomenon increases the attack surface and induces new risks for the group.
Various issues have been identified by the CIO In particular, the previous Antivirus software was no longer providing the expected level of security, whether in terms of functionality, but also in terms of detection, given the new attack vectors that concern us today.
Furthermore, Gaumont uses encryption keys to secure its works. These encryption keys must be protected.

SOLUTION NUCLEON SMART ENDPOINT.

To address these issues, Gaumont has chosen Nucleon Security EDR Nucleon Smart Endpoint to ensure the security of workstations and servers The objective here is to ensure appropriate protection against ransomware but also data leaks thanks to its system of security policies.
The Nucleon Smart Endpoint solution is now deployed worldwide across all group subsidiaries, to ensure uniform and centralized security In addition, this approach makes it possible to provide global security indicators and identify weak points across the entire perimeter.

Appropriate protection thanks to the absorption of business uses and integrated security policies.

During deployment, the learning period allowed the solution to absorb user usage, and thus create different security policies specific to the customer's context Thanks to this important step, we were able to identify non legitimate applications.

Maxime Vidal Madjar
DSI Gaumont
«We chose the Nucleon Smart Endpoint EDR solution to replace our Antivirus. We were convinced that this solution was in line with our project to improve the level of security of Gaumont's information system.
We particularly appreciate the technical support of the security supervision team, both for their skills and their responsiveness.»

In addition, the Nucleon Smart Endpoint security policies provide protection by default to limit access to Office documents only to Office suite programs. But the objective of security policies is also to adapt to the context of the client as well as to its different populations of users. The learning phase made it possible to carry out this adaptation automatically, but we also brought additional rules to the context of the company.

This example of adaptation to the business illustrates very well the approach that we put forward to protect the assets of our clients, whatever the sector of activity.
Today, the entire Gaumont infrastructure is protected by Nucleon Smart Endpoint.
In addition to the solution implemented, Nucleon Security provides a 24 7 monitoring service to monitor security alerts and offer recommendations specific to the company's context. The common objective is always to continuously improve Gaumont's level of security.

COMPANY PRESENTATION

Combining production and distribution activities and with one of the most prestigious film catalogs in the world, Gaumont is today a major player in cinema. Its history merges with that of the 7th art and its 125 years of existence give it a unique status, made up of real experience and a constantly reinvented ability to innovate.

Gaumont is an international group headquartered in France, in Neuilly sur Seine. The group's activities are the production and distribution of cinematographic works, television films and TV series.

BENEFITS

- Protection of specific
- information assets
- Threat Sector Monitoring
- Global and unitary vision by subsidiary