Nucleon Detection & Response | Datasheet

Endpoint Detection, Response and Remediation Platform

Supported operating systems

Red Hat

debian ubuntu

Performances

- 1% < CPU
- 100Mo < RAM

GDPR Compliance

- Records of processing activities
- Native pseudonymization and anonymization
- Stored data Encryption

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.

Protection tailored to your business and critical data

Nucleon Detection & Response absorbs your internal uses, identifies your critical data, then automatically creates specific protection rules. These rules will protect your critical data against illegitimate access, leakage and blockage by ransomware.

Identification of malicious behavior

Zero-Trust policies block attack techniques used by hackers. Sensitive administration scripts and tools are not allowed to block complex infection processes and "fileless" attacks.

Network access is also restricted by policies to avoid abnormal access by software that is abused. For example, the Microsoft Office suite only has access to the servers and domains it needs to function by default.

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.

Nucleon Detection & Response | Datasheet

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

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)**