oplon®

SECURE ACCESS NIST

Oplon Secure Access supports the implementation of NIST guidelines in a variety of ways.
NIST issues a series of Standards and Best Practices to ultimately improve Cybersecurity and Risk Management, Oplon Secure Access' PAM can help you achieve these targets in an effective way.
This is how Oplon Secure Access can support NIST principles:

Access Control - AC

ACCESS CONTROL

Oplon Secure Access helps manage who can access critical systems or data, granting access to sensible resources only to whom has been authorized.

MINIMUM PRIVILEGED PRINCIPLE

It implements the Minimum Privileged Principle, assuring that users will have just the necessary permission to execute specific tasks, lowering the risk of unauthorized accesses.

Identification and authentication - IA

STRONG AUTHENTICATION

Supports the implementation of robust authentication implementations, such as Multi Factor Authentication (MFA), to grant access to privileged accounts just and only to legitimate users.

IDENTITY MANAGEMENT

Allows for centralized management of privileged users' identities, improving safety and trackability of activities.

Risk Assessment - RA

RISK EVALUATION

Oplon Secure Access provides visibility into the risks associated with privileged access, helping to identify and mitigate potential vulnerabilities.

ACTIVITIES MONITORING

Records and monitors all privileged users' activities, allowing to identify abnormal behavior and potential threats in real time.

Auditing e Accountability - AU

AUDIT TRAIL

Keeps a detailed register of all activities executed by privileged users, easing compliance to the NIST guidelines on trackability and accountability.

REPORTING AND REPORTAGE

Issues detailed reports of privileged users activities, useful for compliance verifications and safety audits.

System and information integrity - SI

CREDENTIALS PROTECTION

Securely manages all privileged accounts credentials, lowering the risk of credential compromission.

PASSWORD ROTATION

Automates privileged accounts' password rotation, increasing credential security.

Incident Response - IR

INCIDENT ISOLATION

Allows to rapidly isolate compromised accounts or suspect activities, limiting the impact of a security incident.

FORENSIC ANALYSIS

Delivers detailed data for post-incident analysis, easing causes identification and the implementation of corrective measures.

Security assessment and authorization - CA

SAFETY VERIFICATION

Supports continuous evaluation of safety practices related to privileged accesses, contributing to grant efficacy and updates to safety measures.

SAFETY POLICIES

Helps with implementing and keeping safety policies consistent with NIST guidelines, assuring the following of access management' best practices.

Implementing Oplon Secure Access does not only help with critical asset protection and privileged accesses management in a secure way, it also directly supports adherence to NIST guidelines and standards.
This contributes to create a more secure and compliant informatic environment, to best practices recognized on an international level.

Data and features may change at any time without prior notice.

oplon®

To find out more, visit our website
https://www.oplon.net
or write to **info@oplon.net**