AI–POWERED SECURE REMOTE ACCESS

FUDO

How Privileged Access Management Can HelpYour Company

Achieve NIS2 and GDPR Compliance?

Table of Contents

Getting to Know Privileged Access Management (PAM)

PAM is the term used to describe the policies and technologies used to protect, control, and audit access to privileged accounts, credentials, and resources in an organization's IT infrastructure. Privileged accounts such as system administrators, database administrators, and service accounts have their permissions raised to almost unlimited access to any part of an organization's IT environment. Therefore, compromised privileged access is one of the most dangerous security threats that can cause devastating breaches and data spills. PAM solutions are crucial for organizations to:

- Safely store and manage sensitive privileged credentials, such as passwords, keys, and certificates, in a secure vault.
- Enforce least privilege principles and zero standing privileges.
- Automate password rotation and just-in-time privileged access.
- Record and monitor all privileged user activities
- Protect access to critical infrastructure, applications, data, and system configurations
- Prevent malicious insider threats and external breaches from leveraging privileged access

PAM practices should be strong due to the large-scale risks related to compromised privileged credentials. PAM helps minimize attack surfaces, eliminate standing privileges, and secure access to an organization's most important digital assets.

Introduction to NIS2

The NIS2 Directive's main goal is to improve the resilience of critical infrastructure and digital service providers against cyber threats and ensure a coordinated response across European Union Member States.

The NIS2 Directive focuses on enhancing the cybersecurity posture of entities that are critical to the EU's digital economy. This includes essential and digital service providers. Mentioned entities must adopt appropriate and proportionate technical and organizational measures to manage cyber risks and safeguard network and information systems.

Entities are categorized within the directive as either "essential" or "important," based on their relevance to the Union's internal market and the potential societal and economic consequences of disruptions to their services. Essential and important entities typically operate within sectors and the types of entities highlighted below:

Energy	Transportation	Banking and Financial Infrastructures
Healthcare	Drinking Water and Wastewater	Digital Infrastructure and Cloud Services
Manufacturing and Production	Public Administration	Space

Some key objectives of NIS2 include:

- Expanding the scope to cover more business sectors vital to the EU.
- Mandating stricter cybersecurity requirements. Enhancing monitoring, detection, and incident reporting. Fostering greater cooperation between EU Member States. Assigning regulatory authority to competent authorities. Allowing penalties for non-compliance.

The NIS2 Directive became effective on January 16, 2023.

Member States are required to implement it into their national laws by October 17, 2024. Refer to the included timeline for the NIS2 implementation process, outlining critical dates and actions.

2/16/2023	NIS2 comes into effects
7/17/2024	First Cyber Crises Liaison Organisation Network (EU-CyCLONe) report
10/17/2024	Member States must adopt and publish measures to comply with the NIS2 Directive
1/17/2025	CSIRTs network shall assess progress made with regard to operational cooperation
4/17/2025	Member States shall establish a list of essential and important entities
10/17/2027	Revision of the directive

NIS2 Scope

The NIS2 Directive outlines essential cybersecurity and risk management measures for organizations across both the public and private sectors, detailing a comprehensive set of requirements that include:

- Implement comprehensive cyber risk management aligned with standards like ISO 27001, NIST CSF, CIS Controls.
- Perform regular risk assessments and implement appropriate safeguards.
- Maintain asset inventories of systems, hardware, software, services, and data flows.
- Conduct vulnerability assessments and remediation.
- Enforce identity and access management controls like role-based access and least privilege.
- Apply multi-factor authentication and stringent password policies.
- Segment networks, filter traffic, and monitor access.
- Deploy endpoint protection through antivirus and EDR solutions.
- Encrypt data in transit and at rest.

- Implement resilient data backup, restoration and disaster recovery capabilities.
- Collect activity logs with 90 days retention and integrate with SIEM solutions.
- Establish incident response procedures and notify authorities within 24 hours.
- Deliver security awareness training and education to end users.
- Ensure security of systems managed by third party vendors.
- Build redundancies and failovers to ensure business continuity.

In addition, covered entities are required to work with authorities for incident reporting, information sharing, and oversight.

How PAM Meets NIS2 Technical Controls

In addition, covered entities are required to work with authorities for incident reporting, information sharing, and oversight.

- Centralized vault for credentials enforces strict access governance over privileged identities and accounts.
- Just-in-time privilege elevation and automated rotation minimizes standing privileges.
- Granular access policies and network segmentation restrict access to only authorized resources.
- Multi-factor authentication adds layers of identity verification.
- Full session recordings provide detailed audit trails of privileged user activities.
- Real-time anomaly detection and alerting enables rapid incident response.
- Agentless architecture simplifies deployment across complex hybrid environments.
- Appliance hardening protects PAM infrastructure against attacks.
- High availability, redundancy, backups ensures resilience and disaster recovery.

To gain a deeper understanding of how PAM aids in meeting the NIS2 Directive's requirements, it's recommended to closely examine the specified articles below:

Article 21 Cybersecurity risk-management measures

This section mandates entities to take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems. PAM can help by ensuring that access to these systems is securely managed and monitored, reducing the risk of unauthorized access.

Article 23 Reporting obligations

This article outlines the obligation for entities to report significant service-impacting incidents promptly, ensuring affected parties are informed without increasing the reporting entity's liability. PAM solutions can aid in the detection, response, and recovery from cybersecurity incidents by controlling and monitoring privileged access, which is critical during incident investigation and mitigation efforts.

These articles highlight the importance of securing and managing privileged access as part of a comprehensive cybersecurity strategy to comply with the NIS2 Directive. Additionally, it's essential to consider specific paragraphs in the NIS2 Directive's preamble to ensure full compliance, highlighting its comprehensive approach to bolstering cybersecurity across the EU:

Paragraph 49 Strengthening Cyber Resilience with Comprehensive Cyber Hygiene Policies

PAM (Privileged Access Management) can significantly support cyber hygiene policies by managing and securing privileged access to network and information systems. It ensures that only authorized users have access to critical systems, enforces regular updates of privileged account credentials, and provides detailed audit trails of privileged activities.

Paragraph 51

Leveraging Innovative Technologies for Enhanced Cybersecurity

PAM can enhance cybersecurity by integrating innovative technologies, including AI, to streamline the detection and prevention of cyberattacks. It supports the automation of credential management and monitoring of user activities, aligning with data protection laws by ensuring data accuracy, minimization, and secure access.

Paragraph 57 Advancing Active Cyber Protection in National Strategies

PAM can significantly contribute to active cyber protection strategies by managing and monitoring privileged access, thus preventing unauthorized access and potential breaches. It enables real-time detection and mitigation of threats by controlling who can access vital systems and data, enhancing the overall security posture.

Paragraph 83 Ensuring the Security of Network and Information Systems

PAM can help to straighten the security of networks and information systems for both essential and important entities, whether managed internally or outsourced. By controlling and auditing access to these systems, PAM aligns with the NIS2 Directive's requirements for rigorous cybersecurity risk management and reporting, ensuring that entities can effectively protect their critical infrastructure from unauthorized access and potential security breaches.

Paragraph 89 Cyber Hygiene and Security Technology Integration

PAM supports the adoption of cyber hygiene practices by managing access based on zero-trust principles, facilitating regular software updates, and ensuring secure device configurations. It enhances identity and access management, crucial for network segmentation and user training on cyber threats. Additionally, PAM enables entities to integrate advanced cybersecurity technologies like AI or machine learning, boosting their defensive capabilities against evolving threats.

Paragraph 98

Encryption as a Standard for Communication Security

PAM enhances the security of electronic communications by enforcing access controls and automating policy decisions, complementing encryption and data-centric security practices. It supports the principles of privacy by design, ensuring that only authorized personnel access sensitive communication systems and data, thereby aligning with the directive's emphasis on strong encryption without compromising the integrity of end-to-end encryption methods.

Paragraph 102

Structured Approach to Incident Reporting and Management

PAM can aid in the swift detection and reporting of significant incidents by tracking and analyzing privileged user activities, potentially uncovering early indicators of a breach. It streamlines the reporting process by providing detailed audit trails and logs that can be crucial for early warnings, incident notifications, and final reports. PAM systems can also help prioritize incident response efforts without diverting resources from critical security tasks.

In summary, PAM provides valuable assistance for NIS2 compliance by mitigating third-party access risks, protecting systems with sensitive information, and preventing unauthorized access that could result in outages.

General Data Protection Regulation (GDPR) Overview

The EU GDPR provides detailed requirements in the sphere of collecting, processing, and protecting the personal data of EU residents. Key GDPR objectives include:

- Enhancing individual privacy rights. Mandating transparency into data practices. Tightening consent requirements for processing personal data. Broadening the definition of personal data.

- Establishing rights like access to and erasure of personal data.
- Requiring data protection assessments for risky processing activities.
- Imposing obligations for data controllers and processors.
- Requiring prompt data breach notifications.
- Allowing heavy penalties for non-compliance.

GDPR Requirements

At its core, GDPR aims to provide individuals with greater autonomy over their personal data and ensure that organizations are held responsible for security breaches or misuse. GDPR specifies several technical and organizational measures for securing personal data:

- Encryption of personal data in transit and at rest. Access management
- controls like role-based access, logging, and identity management.
- Network security through firewalls, intrusion detection, and segmentation.
- Data minimization by only collecting/storing required personal information.
- Resilient backup and recovery to ensure availability of personal data.
- Testing security controls through audits and vulnerability assessments.
- Incident response processes for detecting, investigating, and notifying personal data breaches.
- Due diligence to ensure processors adhere to GDPR obligations.
- Privacy by design principles embedded into engineering processes.
- Appointment of Data Protection Officers (DPOs).
- Maintaining records of data processing activities.
- Data protection impact assessments for risky processing activities.
- Adequate safeguards for transfers of personal data outside the EU.

How PAM Enables GDPR Compliance

PAM delivers important capabilities to enforce GDPR's technical controls around securing personal data:

- Access governance over identities that can access regulated personal data.
- Granular access policies aligned with least privilege principles.
- Automated rotation of privileged account credentials.
- Full recording and auditing of privileged user sessions.
- Alerting on anomalous activity to data containing personal information.
- Masking/redacting personal data where not required.
- Change management controls around access permissions.
- Swift deprovisioning of access when no longer needed.
- Securing databases and servers containing regulated personal data.
- Detailed audit trails showing access to personal information.

By controlling and governing access to regulated data, reducing exposure risks, and providing audit trails, PAM solutions enable organizations to more effectively meet GDPR compliance requirements.

Fudo Enterprise for NIS2 and GDPR Compliance

Fudo Enterprise's extensive privileged access management capabilities can be a valuable asset for NIS2 and GDPR compliance. Notable characteristics that make it easier to fulfill essential criteria are:

- Access architecture based on proxy allows for agentless implementation and eliminates standing privileges.
- Granular access policies enforce least privilege and zero standing access.
- AI-powered risk analysis detects anomalies and potential threats.
- Multi-factor authentication adds layered identity verification.

- Just-in-time provisioning grants temporary elevated access only when needed.
- Full session recording, monitoring, and text search provides detailed forensic audit trails.
- Real-time alerting quickly flags suspicious activities.
- Password management eliminates exposure by injecting credentials directly into target sessions.
- Integrating with SIEM, DLP and other security tools allow centralized visibility.

Moreover, Fudo Enterprise makes audit preparation easier by employing compliance dashboards, activity summaries and downloadable reports. With its common architecture, Fudo Enterprise is easy to implement, unlike others. Secondly, the advantage of the access model of proxy-based access is that it eliminates the standing privileges.

Fudo Enterprise: A Next-Generation Approach to PAM

There are different well-known PAM providers, but Fudo Enterprise offers more features such as:

Proxy architecture Fudo uses a proxy-based approach that removes standing privileges, unlike agents that persist access.

Just-in-time access Fudo provides time-bound just-in-time privilege elevation aligned with zero trust principles, which some vendors lack.

AI-powered analytics Fudo leverages AI to detect anomalies and analyze risk, a capability unavailable in many solutions.

Recording and indexing Fudo offers full text search and indexing of session recordings, more advanced than basic recording capabilities.

Password management Fudo automatically injects credentials into sessions, eliminating exposure, unlike incomplete credential protection in some tools.

Deployment Fudo uses an all-in-one architecture for rapid deployment unlike solutions requiring lengthy, complex deployments.

Licensing Fudo uses simple per-user pricing rather than metrics like servers, accounts, and sessions.

Ease of use Compared to relatively complex alternatives, Fudo provides greater usability through its web interface.

As compared to other competing solutions, Fudo Enterprise's proxy access, just-in-time privileges, artificial intelligence analytics, better auditing, and focus on usability stand out as the most effective PAM solution. Fudo Security's experience in PAM provides it with an advantage in adhering to standards such as GDPR and NIS2.

Conclusion

Under GDPR and NIS2, organizations face extensive cybersecurity and privacy mandates, making Privileged Access Management (PAM) a valuable tool for achieving compliance. Fudo Enterprise addresses these regulatory requirements with its integrated PAM solutions, featuring a proxy architecture, detailed access controls, multi-factor authentication, and monitoring capabilities. These features simplify enhancing cybersecurity from multiple aspects. Fudo Enterprise's user-friendly interface and robust security functionalities establish it as a top choice for organizations aiming to meet GDPR and NIS2 standards, providing a strong security foundation.