Future-Proof Your PSD2 and PSD3 Compliance with StrongDM

Ensure Secure, Auditable, and Policy-Driven Access Across Your Payment Infrastructure

Centralized Access Control	Comprehensive Audit Trails	Seamless User Experience
Manage and enforce access policies across all resources, ensuring compliance with PSD2 requirements from a single platform.	Automatically log every access request and session, providing the visibility needed for regulatory reporting and security investigations.	Enable secure, frictionless access for employees and third parties without compromising compliance or productivity.

How StrongDM Simplifies PSD2 and PSD3 Compliance for Financial Services

If you're in a financial services company in the EU, then you've heard of PSD2. With the lofty goal of creating a more integrated and efficient European payments market, PSD2 attempts to level the playing field for payment service providers. StrongDM's Zero Trust PAM platform enables financial services organizations to meet the rigorous requirements of the Revised Payment Services Directive (also known as PSD2 and forthcoming PSD3, to be implemented in 2026) while simplifying the complexity of secure access management. By centralizing control over access to critical payment systems, databases, and infrastructure, StrongDM ensures compliance with PSD2's focus on secure authentication, data protection, and transaction monitoring.

With StrongDM, organizations gain a unified platform to enforce role-based access, track user activity, and generate detailed audit logs. This reduces the administrative burden of managing compliance and provides the flexibility to adapt to evolving regulations and security needs.

Key Benefits of Using StrongDM for PSD2 and PSD3 Compliance

- **Granular Access Policies:** Restrict access to sensitive systems, meeting PSD2's SCA requirements.
- **Session Logging:** Log all user activity for simplified compliance audits.
- **Automated Reporting:** Create compliance-ready reports with minimal effort.
- **Third-Party Access:** Control and audit vendor access to protect payment data.
- **Multi-Factor Authentication:** Enforce MFA across all systems to meet PSD2 mandates.

strongdm

Meet the Updated PSD2 and PSD3 Requirements with StrongDM

StrongDM delivers a **Zero Trust PAM** platform that fulfills the critical requirements demanded of PSD2 and helps you prepare for upcoming PSD3 regulations, while also delivering the critical features required for PoLP, Just-in-Time access, and privileged access. Specifically:

Category	Requirements	How StrongDM Helps
Strong Customer Authentication (SCA)	Multi-factor authentication (MFA) to verify user identity for sensitive transactions.	Integrates MFA across all resources, including legacy systems, to enforce SCA seamlessly.
Access Control	Restrict access to systems and data based on user roles and business need.	Enables centralized, role-based access control for all IT resources.
Audit & Monitoring	Detailed logging of user activity and system access for compliance audits.	Automatically logs all user activity and provides easy-to-generate, compliance-ready audit reports.
Data Protection	Ensure the confidentiality and integrity of payment data.	Implements Zero Trust policies to protect sensitive data and control access at all levels. To secure sensitive customer information, businesses should anonymize and tokenize data, converting real data into a form that is useless to anyone who might intercept it.
Incident Response & Reporting	Prompt detection and reporting of security breaches or unauthorized access.	Provides real-time access visibility and detailed logs to support rapid incident response and compliance reporting.

StrongDM: Zero Trust Privileged Access

StrongDM's Zero Trust PAM provides precise control over privileged actions, enabling secure, on-demand access while minimizing attack surfaces by eliminating excess privileges. With continuous monitoring and instant mitigation, it ensures seamless compliance. It provides:

Automated Compliance Reporting

Generate on-demand reports with detailed logs of access activity, privileged session management, and security controls.

Centralized Access Management

Manage and control access to all critical resources—databases, servers, cloud environments, and more—through a single, unified platform.

Comprehensive Audit Trails

Record every user session, query, and action with full metadata, creating a detailed audit trail for forensic analysis and compliance reporting.

Granular Role-Based Access Control (RBAC)

Enforce least-privilege principles by assigning precise permissions based on user roles and responsibilities.

Real-Time Monitoring and Alerts

Monitor access activity in real-time and receive alerts for unusual or unauthorized behavior.

Risk-Based Access Policies

Configure access policies based on specific risk factors, such as user role, resource sensitivity.