Streamlining NIS2 Compliance with StrongDM

Simplify Compliance and Strengthen Network Security for Financial Services Enterprises with Zero Trust PAM

Frustration-Free Access	Stop Unsanctioned Actions	Continuous Compliance
Enable your team to securely access the resources they need to get the job done without frustration.	On-demand access reduces the attack surface and eliminates excess privileges. Continuous detection and mitigation instantly blocks harmful actions.	Policy-based action control ensures real-time, verifiable Zero Trust Compliance.

How StrongDM Simplifies NIS2 Compliance for Financial Services

The Network and Information Security Directive 2 (NIS2) demands greater compliance rigor from financial services organizations. With requirements for stricter access controls, real-time monitoring, and comprehensive reporting, financial organizations need solutions that enable compliance without overburdening their teams. StrongDM's Zero Trust Privileged Access Management (PAM) platform offers a powerful and straightforward approach to meeting these demands.

By centralizing and automating access controls, StrongDM ensures that financial institutions can maintain compliance with NIS2 mandates while improving security. The platform simplifies audit preparation with detailed logs and reports, enforces least-privilege access seamlessly, and integrates effortlessly with existing IT environments. StrongDM's dynamic approach helps organizations confidently meet NIS2 requirements without compromising operational efficiency.

How StrongDM Helps Financial Organizations Comply with NIS2:

- **Centralized Access:** Manage all access from a single platform for consistent controls.
- **Dynamic Policies:** Enforce least-privilege access aligned with NIS2.
- **Audit Trails:** Simplify reporting with detailed user activity logs.
- **Seamless Integration:** Secure modern and legacy systems effortlessly.
- **Real-Time Monitoring:** Detect and address access anomalies instantly.

strongdm

Meet the Updated NIS2 Requirements with StrongDM

StrongDM delivers a **Zero Trust PAM** platform that fulfills the critical requirements demanded of NIS2, while also delivering the critical features required for PoLP, Just-in-Time access, and privileged access. Specifically:

Category	Requirements	How StrongDM Helps
Access Control	Ensure access is restricted to authorized users only, based on least-privilege principles.	Centralizes access management and enforces dynamic, least-privilege access policies across all resources.
Incident Detection & Response	Implement systems to detect, report, and respond to security incidents in real-time.	Provides real-time monitoring, anomaly detection, and alerts to quickly identify and mitigate incidents.
Risk Management	Identify, evaluate, and mitigate cybersecurity risks continuously.	Enables proactive risk reduction through dynamic access controls and visibility into user activities.
Audit & Reporting	Maintain comprehensive records of activities and provide detailed reports for compliance.	Generates detailed logs and reports, simplifying compliance audits and meeting regulatory requirements.
Enterprise Integration	Ensure all critical systems and networks are securely integrated.	Seamlessly integrates with legacy and modern systems, securing all infrastructure without disruptions.

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:

Real-Time Monitoring and Alerts

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

Granular Role-Based Access Control (RBAC)

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

Comprehensive Audit Trails

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

Centralized Access Management

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

Automated Compliance Reporting

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

Risk-Based Access Policies

Configure access policies based on specific risk factors, such as user role, resource sensitivity, or time of access to support risk assessment requirements.