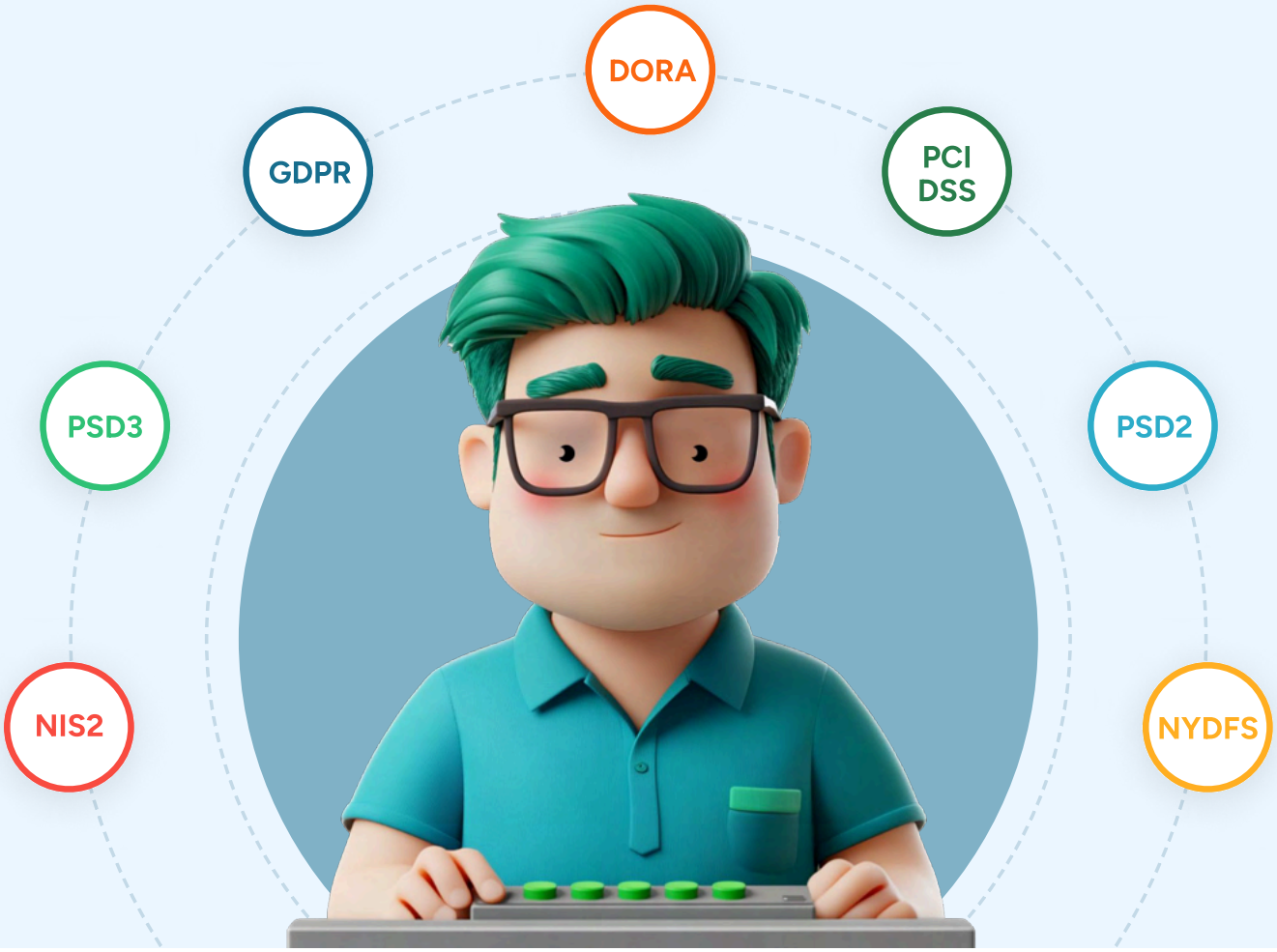
How Top Financial Services Companies Meet Critical Compliance Requirements with StrongDM

strongdm

Table of Contents



Keeping regulators happy might not sound like a thrill ride, but in financial services, it's non-negotiable. From safeguarding sensitive customer data to ensuring transaction integrity, financial services organizations are under constant pressure to juggle an ever-evolving web of regulatory standards. Whether it's PSD2, PSD3, NIS2, PCI DSS, or NYDFS, the rules are clear: protect data, respect privacy, and lock down access—or face the consequences.

But as any member of your security or compliance team will tell you, keeping up with these standards isn't getting any easier.

As financial institutions adopt new technologies, shift to hybrid environments, and expand globally, the regulatory landscape gets more complex. New rules pile on top of old ones, often with overlapping or conflicting requirements. Compliance isn't a project with a clear beginning and end—it's a labyrinth to navigate, and it requires rigorous access controls, detailed audit trails, and the ability to adapt to continuously changing mandates.

Security and compliance teams in financial services organizations are relying on Zero Trust access management solutions to cut through the complexity of compliance, streamlining processes and ensuring they stay ahead in an increasingly demanding regulatory environment.

Here's how they do it.

The Increasing Complexity of Financial Services Regulatory Requirements

As financial institutions adopt new technologies and expand their operations globally, compliance requirements have become increasingly complex. Regulations often vary by region, requiring institutions to meet overlapping or even conflicting standards. For example, while NIS2 enforces rigorous cybersecurity measures across the EU to protect critical infrastructure, PSD2 mandates robust protections for payment services and customer authentication to secure financial transactions within Europe. If that company has a branch in New York State, then they are also subject to NYDFS regulations as well. Many companies in financial services end up with a Venn diagram of overlapping compliance regulations, so verifying co-compliance becomes a regtech nightmare.

This complexity is compounded by rapid changes in the regulatory landscape. Emerging requirements often focus on mitigating modern threats, such as ransomware attacks and insider breaches, which goes beyond what typical regtech software can handle

Compliance frameworks certainly demand secure systems, but also:

- Detailed audit trails
- Proactive risk assessments
- Robust incident response capabilities

Financial institutions must also address these challenges while keeping up with customer expectations for seamless, efficient digital experiences.

Common Challenges in Achieving Compliance

Financial institutions face several persistent challenges in their compliance efforts:

1. **Access Sprawl:** As organizations grow, so does the number of systems, users, and access points, making it difficult to maintain consistent access controls.
2. **Shadow IT:** Unapproved tools and services can introduce vulnerabilities and compliance risks, as they often operate outside of established security policies.
3. **Audit Complexity:** Regulatory audits require institutions to provide clear, comprehensive documentation of access and activity. Manual processes and fragmented systems can lead to gaps or inconsistencies that jeopardize compliance.

StrongDM addresses these challenges with a unified platform that simplifies access management, enforces Zero Trust policies, and automates audit trails. By integrating seamlessly with existing infrastructure, StrongDM ensures that financial institutions can maintain compliance while reducing operational friction.

We'll explore how StrongDM helps financial services organizations achieve this, but first, let's examine what enterprises face as they seek continuous compliance.

Secure and Streamlined Access Management is Required

Central to compliance in financial services is the ability for users to manage access to critical systems and data effectively. This is, in large part, why these frameworks exist in the first place. Poor access controls can lead to unauthorized activity, data breaches, and regulatory penalties. It's these things that land companies in unwanted headlines and require them to pay big fines to regulators.

Yet, achieving secure and streamlined access management requires balancing the need for tight security with operational efficiency, ensuring that all legitimate stakeholdrs have the appropriate level of access without creating bottlenecks. Legacy systems, sprawling IT environments, and the adoption of hybrid or multi-cloud architectures only add to the complexity.

The Compliance Landscape in Financial Services

Key Regulations Shaping the Industry and Their Impact on IT/Security Teams

The financial services industry is governed by a web of regulations, each with specific requirements that directly influence the priorities of IT and security teams. Regulations such as SOX, GDPR, PCI DSS, GLBA, NYDFS, and others require enterprises to implement strict data protection policies, maintain detailed audit trails, and ensure proper access controls to prevent unauthorized use or breaches.

These regulations demand significant resources and expertise from IT and security teams, who must navigate technical and operational challenges to ensure compliance. For instance, PSD2 compliance requires strong authentication and secure handling of payment transactions, while PCI DSS emphasizes the protection of cardholder data through stringent security measures and controls. Financial institutions must also manage third-party risks and adapt to regional frameworks such as the EU's Digital Operational Resilience Act (DORA).

Meeting these diverse requirements often necessitates deploying a mix of tools, frameworks, and practices—a process that can strain internal resources. Check out some of the common compliance requirements and the corresponding actions organizations must take to meet them:

Compliance Requirement	How Enterprises Comply
Access Control	Implement role-based or attribute-based access controls, enforce least-privilege access, and regularly review permissions.
Data Protection	Encrypt sensitive data in transit and at rest, ensure secure storage, and implement strong data masking techniques.
Audit Trails	Maintain detailed, tamper-proof logs of all access and activities, and ensure logs are readily available for audits.
User Authentication	Enforce multi-factor authentication (MFA) for all users accessing critical systems and sensitive data.
Incident Response	Develop and document an incident response plan, conduct regular tests, and report breaches within mandated timeframes.
Network Security	Secure networks with firewalls, intrusion detection/prevention systems (IDS/IPS), and regular vulnerability scanning.
Risk Assessments	Conduct regular risk assessments to identify and mitigate vulnerabilities in systems and processes.
Third-Party Vendor Management / Risk Management	Evaluate vendor security practices, ensure contracts include compliance obligations, and monitor vendor access to systems.
Data Privacy	Ensure data processing aligns with user consent and privacy laws, and enable users to access, correct, or delete their data.
Continuous Compliance Reporting	Prepare and submit accurate, timely reports to regulators, detailing compliance measures and any incidents.
Change Management	Implement processes to track and approve changes to systems and software, ensuring they do not compromise security.
Security Awareness Training	Conduct regular training for employees to understand security risks, compliance obligations, and best practices.
Penetration Testing	Perform regular penetration tests to identify and address vulnerabilities before attackers can exploit them.
Data Retention Policies	Define and enforce policies on how long data is retained, securely deleting data once it is no longer needed.
Policy Documentation	Maintain clear, up-to-date documentation of security policies, procedures, and controls for both internal and external use.

Why Access Management Is Critical for Compliance

The Role of Access Control in Meeting Compliance Requirements

Access control, especially privileged access management, is foundational to achieving and maintaining compliance in the financial services industry. Regulatory frameworks mandate specific access management procedures and guidelines to ensure that only the right individuals can access sensitive systems and data. Properly implemented access controls support compliance by:

- **Limiting Unauthorized Access:** Ensuring that users have access only to the systems and data necessary for their roles minimizes exposure to sensitive information.
- **Supporting Audit Readiness:** Detailed access logs provide the necessary documentation for regulatory audits, demonstrating adherence to policies and controls.
- **Enabling Rapid Response to Incidents:** Robust access controls facilitate faster detection and containment of unauthorized activity, reducing the impact of potential breaches.

Risks of Inadequate Access Management

Failure to implement effective access management poses significant risks, including:

1. **Insider Threats & Third Party Risk:** Employees or contractors with privileged access can intentionally or unintentionally cause data breaches, financial losses, or compliance violations.
2. **Data Breaches:** Weak access controls create vulnerabilities that external attackers can exploit to access sensitive systems and information.
3. **Regulatory Penalties:** Non-compliance with access-related requirements can result in hefty fines, legal action, and reputational damage.

The Need for Centralized, Policy-Driven Access Solutions

The only way that financial services organizations can manage access across complex IT environments in a constantly changing environment is with a centralized, policy-driven approach. Fragmented access management increases the likelihood of errors, gaps, and inefficiencies, making it harder to ensure compliance. A centralized solution provides:

- **Consistency:** Uniform application of access policies across all systems and environments.
- **Visibility:** Comprehensive oversight of who has access to what, along with real-time monitoring and logging.
- **Scalability:** The ability to adapt policies as organizational needs and regulatory requirements evolve.

StrongDM's platform addresses these needs by unifying access management under a single, easy-to-use interface. With features like policy-based access control, real-time session monitoring, and automated logging, StrongDM enables financial institutions to manage access securely and efficiently, ensuring compliance with regulatory mandates while reducing operational overhead.

The **StrongDM Policy Engine** adapts effortlessly to complex multi-cloud setups, allowing organizations to apply and enforce consistent policies across providers. Whether integrating with AWS, Azure, or GCP, StrongDM ensures a unified and scalable approach to access control, enabling financial institutions to remain agile and compliant as their cloud strategies evolve.

The Rise of Zero Trust Principles in Compliance Frameworks

Zero Trust principles have emerged as a cornerstone for modern compliance frameworks. The Zero Trust model assumes that threats can originate from anywhere, both inside and outside an organization, and therefore enforces the principle of "never trust, always verify."

This paradigm shift is particularly critical in the financial services sector, where insider threats and sophisticated external attacks are constant concerns. By implementing Zero Trust architectures, institutions can ensure that every access request is authenticated, authorized, and continuously monitored, regardless of the user's location or device. These principles align closely with compliance objectives, such as enforcing least-privilege access and ensuring robust auditability.

The StrongDM Advantage for Financial Services

Overview of the StrongDM Zero Trust PAM Platform

StrongDM is a modern, Zero Trust Privileged Access Management (PAM) platform designed specifically to address the complex needs of financial institutions. By offering centralized, secure, and seamless access control across hybrid environments, StrongDM helps organizations enhance security, simplify operations, and ensure regulatory compliance.

How StrongDM Supports Compliance

Case Study - Axos and StrongDM Achieve Ongoing Compliance

The Compliance Challenge

Financial services organizations like **Axos Financial** must comply with strict regulatory frameworks such as NYDFS, PSD2, and NIS2, which demand rigorous access control, auditability, and risk mitigation for sensitive data. These regulations require organizations to demonstrate secure, controlled access to critical systems, maintain detailed audit trails, and regularly review permissions to ensure compliance. For a rapidly growing company like Axos, managing over 200,000 annual database permission reviews was an operationally taxing and error-prone process.

The StrongDM Advantage

StrongDM revolutionized how Axos manages database access, helping the organization meet compliance requirements efficiently and effectively:

1. **Streamlined Role-Based Access Control (RBAC):**
   StrongDM replaced Axos's manual, ticket-based access request system with a unified, role-based approach. Employees could now request access through a single, streamlined process, significantly reducing the complexity and administrative burden of managing permissions.
2. **Enhanced Security Through Zero Trust Principles:**
   By eliminating direct database access and routing all connections through StrongDM, Axos introduced an additional security layer. This approach aligns with the Zero Trust model required by modern regulations, ensuring access is only granted on a need-to-know basis and tightly monitored.
3. **Comprehensive Audit Trails:**
   StrongDM's centralized logging and audit capabilities provided Axos with detailed, real-time records of every access request, approval, and activity. These audit trails are critical for demonstrating compliance with regulatory standards like NIS2, which require organizations to maintain visibility into access and activity.
4. **Simplified Access Reviews:**
   The platform's intuitive interface and automation capabilities made it easier for Axos to conduct regular access reviews, ensuring that all permissions remain up-to-date and aligned with compliance mandates.
5. **Scalability and High Adoption Rates:**
   As Axos grew, StrongDM's user-friendly platform ensured smooth onboarding for new employees and allowed the organization to maintain secure access practices without disrupting operations.

Achieving Compliance Confidence

With StrongDM, Axos addresses the operational challenges of managing access across a complex IT environment while ensuring compliance with stringent financial services regulations. StrongDM's robust access controls, audit capabilities, and ease of use positioned Axos to not only meet but exceed compliance expectations, giving regulators and stakeholders confidence in their security posture.

FINANCIAL SERVICES COMPLIANCE USE CASE:

Automating Compliance Audits

The Challenge

Financial services organizations must meet stringent regulatory requirements, including generating detailed audit reports on access to sensitive systems and data. These reports often require pulling logs from multiple systems, reconciling inconsistencies, and proving compliance across a wide array of regulations. Manual audit processes are time-consuming, prone to human error, and often involve significant resource allocation from already overburdened IT and security teams.

The Solution

StrongDM's Zero Trust PAM platform centralizes logging and audit trail generation across all resources—databases, servers, cloud platforms, and network devices. By providing consistent, automated audit trails that are readily accessible in real time, StrongDM simplifies compliance reporting. Its granular logs capture who accessed what, when, and how, reducing the need for time-intensive data collection and manual log reconciliation.

The Outcome

Organizations save time and resources by automating previously manual audit processes. This not only reduces the risk of errors but also ensures compliance audits are thorough, accurate, and prepared for regulatory reviews. With StrongDM, financial services teams can shift their focus from reactive compliance tasks to proactive security management.

FINANCIAL SERVICES COMPLIANCE USE CASE:

Securing Access Across Multi-Cloud and Hybrid Environments

The Challenge

Financial services organizations are increasingly adopting multiple cloud providers alongside on-premises environments to enhance disaster recovery, resilience and avoid vendor lock-in. Managing secure access across these disparate systems is complex and resource-intensive. Traditional tools often require separate policies and configurations for each environment, creating silos that increase the risk of errors, security gaps, and non-compliance.

The Solution

StrongDM's Zero Trust PAM platform unifies access management across cloud and on-premises resources through a single, centralized policy enforcement framework. This allows security teams to define and apply consistent access policies, regardless of the underlying infrastructure. By providing a dynamic, identity-based approach to access control, StrongDM ensures secure connections to any resource without the need for multiple tools or fragmented processes.

StrongDM's policy-based platform allows institutions to define vendor-specific access policies, ensuring compliance with frameworks like DORA and GDPR. This centralized approach reduces risks from third-party access while maintaining seamless operations across hybrid and multi-cloud environments.

The Outcome

With StrongDM, financial services organizations can simplify operations, reduce the overhead of managing access policies, and eliminate the risk of policy inconsistencies. StrongDM ensures secure and seamless access across hybrid environments while maintaining compliance with industry regulations, giving teams confidence in their security posture as they scale.

FINANCIAL SERVICES COMPLIANCE USE CASE:

Preventing Unauthorized Access

The Challenge

Financial services organizations face constant threats from both insiders and external attackers attempting to gain unauthorized access to sensitive systems and data. Third-party users pose unique challenges to access management, as improper oversight can lead to insider threats and compliance violations. Managing these risks requires more than basic user authentication—it demands robust controls to ensure users have access only to what they need, when they need it, and nothing more. Without granular permissions and real-time oversight, organizations are vulnerable to data breaches, policy violations, and compliance failures.

The Solution

StrongDM's Zero Trust PAM platform provides granular permissions that enforce least privilege (ideally in the form of just-in-time access) across all resources. Every access request is authenticated and authorized based on dynamic policies, ensuring users only interact with the systems and data they are explicitly allowed to. Additionally, StrongDM includes session monitoring and logging, offering complete visibility into user actions and enabling rapid detection of suspicious behavior.

The Outcome

By leveraging StrongDM, financial services organizations enhance their security posture, mitigating risks from both internal and external threats. The platform's comprehensive audit trails and real-time monitoring also bolster compliance efforts, giving organizations confidence that they can demonstrate robust controls during audits and regulatory reviews.

How StrongDM Helps SoFi Achieve Compliance with Financial Services Standards

The Compliance Challenge

As a leading financial technology company, SoFi must adhere to strict regulatory standards like NYDFS, PSD2, and NIS2, which require rigorous access control, comprehensive audit trails, and robust security measures to protect sensitive customer data. Managing these requirements at scale presents significant challenges, particularly as SoFi continues to expand its technology stack and user base.

The StrongDM Advantage

StrongDM transformed SoFi's approach to access management, enabling the company to meet compliance requirements while maintaining operational efficiency and security:

1. **Unified Access Control Across Hybrid Environments:**
   SoFi operates a diverse IT environment with both cloud-based and on-premises resources. StrongDM's centralized access management allowed SoFi to enforce consistent policies across all systems, eliminating silos and ensuring a unified approach to security and compliance.
2. **Granular Permissions with Zero Trust Security:**
   StrongDM's Zero Trust PAM platform enabled SoFi to implement least-privilege access principles, granting users only the permissions necessary for their roles. This granular control aligns with compliance requirements for restricting unauthorized access and mitigating insider threats.
3. **Comprehensive Audit Trails:**
   StrongDM provided SoFi with real-time, centralized logging and audit trails, capturing every access request, session, and activity across the organization. These detailed records are essential for demonstrating compliance with regulatory standards that mandate full visibility into access and activity.
4. **Streamlined Access Reviews:**
   With StrongDM, SoFi automated and simplified the process of reviewing and managing user permissions. This ensured timely removal of unnecessary access and aligned with regulatory requirements for periodic access reviews.
5. **Scalability for Growth:**
   As SoFi continues to grow, StrongDM's scalable platform ensures that new employees and resources can be securely onboarded without disrupting existing workflows. The platform's ease of use also promotes high adoption rates, facilitating smooth transitions and ensuring compliance processes remain effective.

Achieving Compliance Confidence

With StrongDM, SoFi was able to address the complexities of managing secure access in a rapidly growing environment. The platform's robust access controls, audit capabilities, and scalability allowed SoFi to meet and exceed compliance requirements for standards like NYDFS, PSD2, and NIS2. By leveraging StrongDM, SoFi strengthened its security posture, reduced operational overhead, and gained confidence in its ability to satisfy regulatory demands while continuing to innovate and grow.

Measuring the ROI of Compliance with StrongDM

Reducing Costs Associated with Fines and Non-Compliance

Non-compliance with regulatory requirements can result in significant financial penalties, legal action, and reputational damage. By leveraging StrongDM's centralized and automated access management platform, financial institutions can reduce the risk of non-compliance and associated fines. StrongDM's policy-driven controls and real-time monitoring ensure organizations remain audit-ready, mitigating the costly consequences of compliance lapses.

Streamlining Audits and Operational Processes

StrongDM's centralized audit trails simplify compliance reporting across multi-cloud environments by unifying access logs from AWS, Azure, GCP and on-premises systems into a single, actionable view. This reduces manual reconciliation efforts and provides real-time insights for regulatory audits, saving time and resources.

Improving Team Productivity and Security Alignment

With StrongDM, financial institutions can enhance collaboration between security, IT, and compliance teams. The platform's intuitive interface and seamless integration with existing systems reduce the administrative burden of access management, freeing teams to focus on strategic initiatives. By aligning security and operational goals, StrongDM fosters a more productive and secure organizational environment, delivering measurable ROI in both cost savings and improved performance.

Getting Started with StrongDM

Steps to Integrate StrongDM into a Financial Services Environment

1. **Assess Current Access Management Practices:** Identify gaps in your existing processes, focusing on areas like access sprawl, manual auditing, and policy enforcement.
2. **Define Compliance and Security Goals:** Outline specific objectives that StrongDM will help achieve, such as reducing audit preparation time or improving least-privilege access.
3. **Deploy StrongDM Across Systems:** Install and configure the StrongDM platform to connect seamlessly with your existing IT infrastructure, including cloud and on-prem environments.
4. **Customize Access Policies:** Use StrongDM's intuitive interface to create and enforce granular, role-based access policies tailored to your organization's needs.
5. **Enable Real-Time Monitoring:** Activate session monitoring and logging to ensure continuous oversight and proactive threat detection.

Quick-Start and Best Practices for Compliance Teams

- **Leverage Pre-Built Templates:** Utilize StrongDM's policy templates to jumpstart compliance with regulatory frameworks like SOX, PCI DSS, and GDPR.
- **Train Your Team:** Provide training to IT, security, and compliance teams on using the StrongDM platform effectively.
- **Conduct Regular Reviews:** Periodically audit access policies and user permissions to align with evolving compliance requirements.
- **Monitor Activity Proactively:** Use real-time dashboards and alerts to identify and address potential issues before they escalate.

Leveraging StrongDM's Support and Resources

- **Dedicated Support Team:** Access 24/7 support from StrongDM experts to assist with deployment, troubleshooting, and optimization.
- **Comprehensive Documentation:** Explore a library of guides, FAQs, and how-to resources to maximize platform usage.
- **Ongoing Updates:** Stay compliant with the latest regulations through regular platform updates and feature enhancements.
- **Community Engagement:** Join webinars, forums, and events to learn from other StrongDM users and industry leaders.

By following these steps and leveraging StrongDM's robust support ecosystem, financial institutions can seamlessly integrate the platform, streamline compliance efforts, and strengthen their overall security posture.

strongdm

StrongDM is a Zero Trust access platform that centralizes and simplifies access management for all technical users across every resource in your infrastructure, whether on-premises or in the cloud. By embracing Zero Standing Privileges and implementing Just-in-Time (JIT) access across your full tech stack, StrongDM provides fine-grained, context-based policy enforcement in real time.

Security teams gain complete visibility and control over access and actions with advanced reporting and analytics, helping to identify unused access grants, inactive resources, and over-privileged roles to enhance security and compliance postures. End users enjoy fast, intuitive access to the resources they need when they need them, improving productivity and operational efficiency. Connect with us on **LinkedIn**, **YouTube** or head to **www.strongdm.com** to learn more.