Rocket® software

69% of IT Leaders Can't Rest Easy

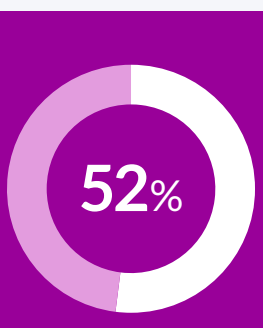
3 compliance blind spots are putting their business at risk.

In our 2026 IT Leaders Survey, one message came through clearly: **data security is the top reason IT leaders are lying awake at night**. As DORA and NYDFS requirements grow more complex and infrastructure stretches across on-prem, hybrid, and cloud, managing compliance is becoming increasingly difficult — especially when visibility is limited.

What's driving the late-night escalations?

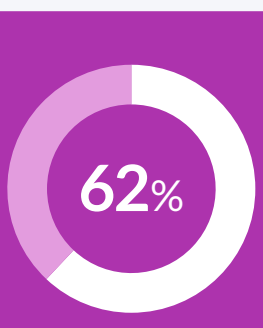
01

Fragmented access management



52% of IT leaders cite access control and identity management as a top challenge.

Separate credentials across enterprise systems and mainframes create more than friction; they introduce significant security risks.



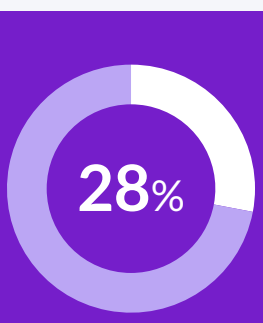
62% struggle with data quality in hybrid environments, compounding risks across regulatory compliance and secure data operations.

Siloed access systems make compliance audits more complex and time-consuming, leaving organizations vulnerable to internal and external threats.

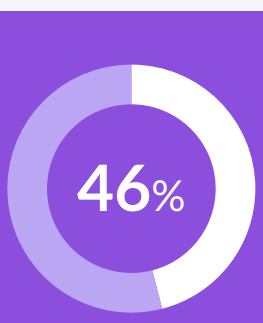
02

Compliance gaps in terminal emulators

Many terminal emulators lack native integration with enterprise Identity and Access Management (IAM), creating hidden vulnerabilities.



Only 28% of IT leaders feel their DevOps integration with mainframe and core systems is extremely effective.



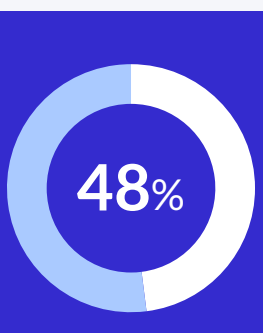
46% report data governance is a significant challenge.

As organizations modernize, incomplete access integrations quietly increase risk. Especially when governance standards demand end-to-end visibility.

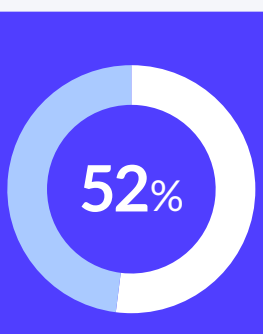
03

Operational inefficiencies

IT teams are stretched thin by password resets and access-related help desk tickets.



48% of organizations still rely on older IT systems for critical operations.



Meanwhile, 52% struggle to find staff with the right skills to support them.

The need to juggle multiple consoles for managing both desktop and web-based emulators further complicates administration, taxing IT resources and increasing the chance for human error.

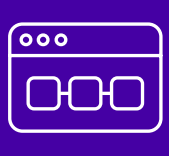
How to sleep soundly again

Unify access management

Extend enterprise IAM to terminal emulators to create a single, seamless approach to access management across the organization.

Close compliance gaps

Enable multi-factor authentication (MFA) across all host types, including IBM Z®, IBM® i, and Linux® VT, to strengthen security where it matters most.



Simplify operations

Consolidate desktop and web-based emulators administration into a single interface to reduce the burden on your IT teams.

Wake up to a better solution

Rocket® Secure Host Access extends enterprise IAM to terminal emulators, enabling MFA, simplifying compliance, and reducing operational inefficiencies.

Learn more about Rocket Secure Host Access

For a deeper understanding of the critical issues and emerging trends shaping IT leadership in 2026, explore the full findings in our latest IT Leaders Survey whitepaper.

Explore survey results

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-17449_Infographic_IT-Leaders-Survey-SHA_V3