Rocket® software

Confidence Doesn't Equal Compliance

New research shows the mainframe access blind spot putting financial services at risk, and how AI is exposing it.

Contents

Executive summary

Financial services leaders feel prepared. Recent Hanover Research findings, based on a June 2026 study of 250 director-level respondents across the US and EU, reveal that 94% of organizations are confident their mainframe access meets regulatory requirements. Nearly all – 99% – believe their approach aligns with security best practices.

Yet the same organizations tell a different story when you look at outcomes. Half have faced required audit remediations. More than two-thirds spent $500,000 or more fixing user access compliance issues in the past two years alone.

That gap between how secure organizations feel and how exposed they actually are is the most dangerous risk in your environment today. This paper examines where that blind spot lives, why traditional reviews keep missing it, how AI-powered auditing is now surfacing it, and what you can do to close it before an incident or regulator forces your hand.

Key takeaways:

Confidence in compliance is high, but audit findings and remediation costs remain widespread.

Green screen and legacy terminal access is the overlooked "last mile" of identity security.

Advanced controls like SSO (32%), passwordless authentication (36%), and session monitoring (44%) remain under-deployed.

AI is accelerating the discovery of these hidden gaps faster than manual reviews ever could.

Proactive modernization costs far less than reactive, incident-driven remediation.

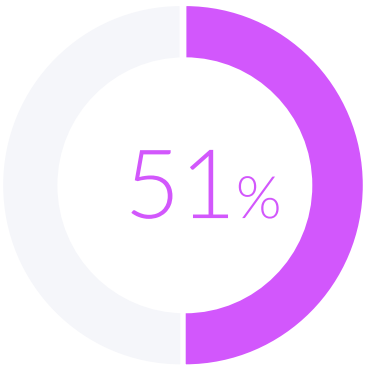
The paradox at the heart of financial services security

You review your access controls regularly. Half of organizations do so at least quarterly. You have clear ownership – cybersecurity teams lead accountability in 50% of organizations. You understand the regulations. Familiarity with PCI DSS (78%), DORA (74%), and NYDFS/23 NYCRR Part 500 (73%) is strong.

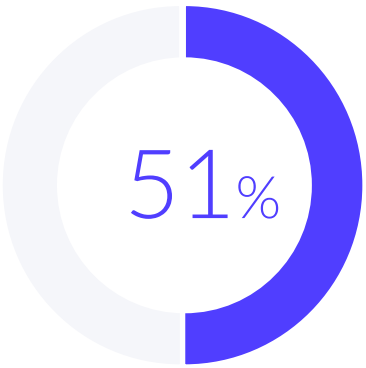
By every measure of process and governance, you're doing the right things. So why do the results keep telling a different story?

Consider the numbers side by side. While 94% of organizations express confidence in meeting compliance requirements, 51% have required remediation activities following an audit. Another 51% received audit findings related to insufficient access logging or monitoring. And 68% have spent at least $500,000 on user access remediation over the past two years, with 28% exceeding $1 million.

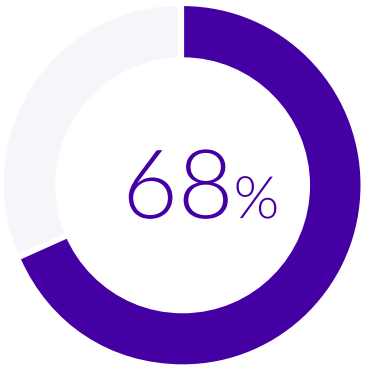
Confidence, it turns out, is not the same as compliance. Strong governance doesn't guarantee the adoption of modern security controls. You can review often, assign clear ownership, and still carry a gap you can't see.



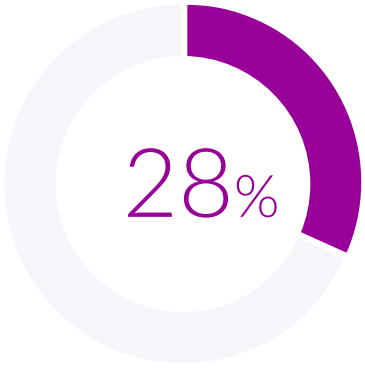
Have required remediation activities following an audit.



Received audit findings related to insufficient access logging or monitoring.



Have spent at least $500,000 on user access remediation over the past two years.



Have exceeding $1 million on user access remediation over the past two years.

Key takeaway:

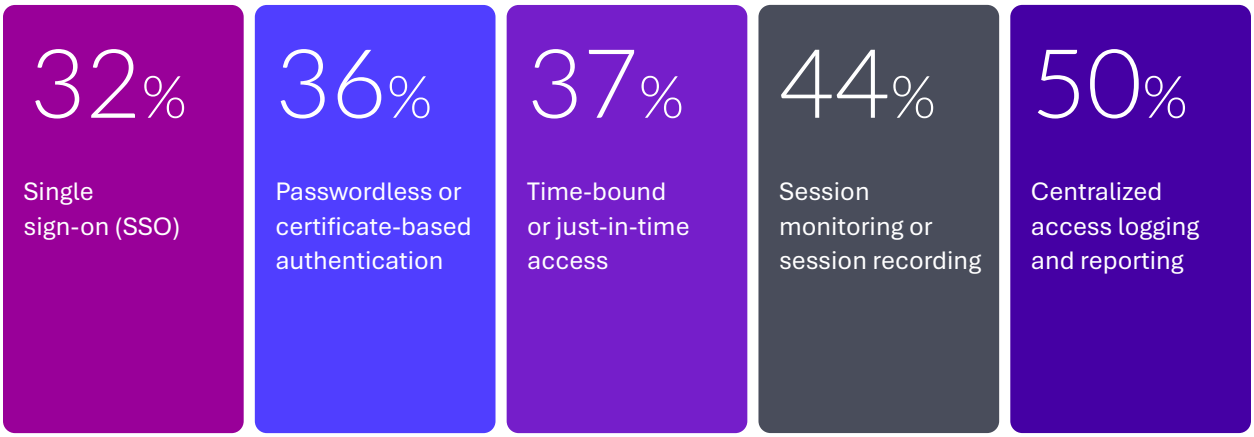
Disciplined process creates a feeling of readiness. But feeling ready and being audit-proof are two very different things.

Where the blind spot lives: the last mile of identity

The gap isn't in your firewalls or your cloud posture. It's in the place most compliance reviews barely touch: green screen and legacy terminal access to your mainframe and host systems.

This is the last mile of identity – the point where users actually log in to the systems holding your most sensitive data. And it's where modern controls are thinnest.

The research makes the pattern clear. Most organizations rely on foundational controls, with MFA and privileged access management each at 56%. But adoption drops sharply for the advanced capabilities that today's standards increasingly require:



These aren't minor omissions. They're the exact areas auditors scrutinize. When a third of organizations report that producing audit evidence for session controls (35%), privileged access (37%), MFA (36%), and access logging (32%) is very or extremely challenging, the reason becomes obvious. You can't easily prove what you haven't fully modernized.

Regulators are already pushing here. Under NYDFS, 48% of organizations report increased scrutiny of shared IDs and non-individual accounts – a hallmark weakness of traditional green screen access. DORA has driven 45% to accelerate plans to strengthen authentication. The pressure is mounting precisely where legacy access is weakest.

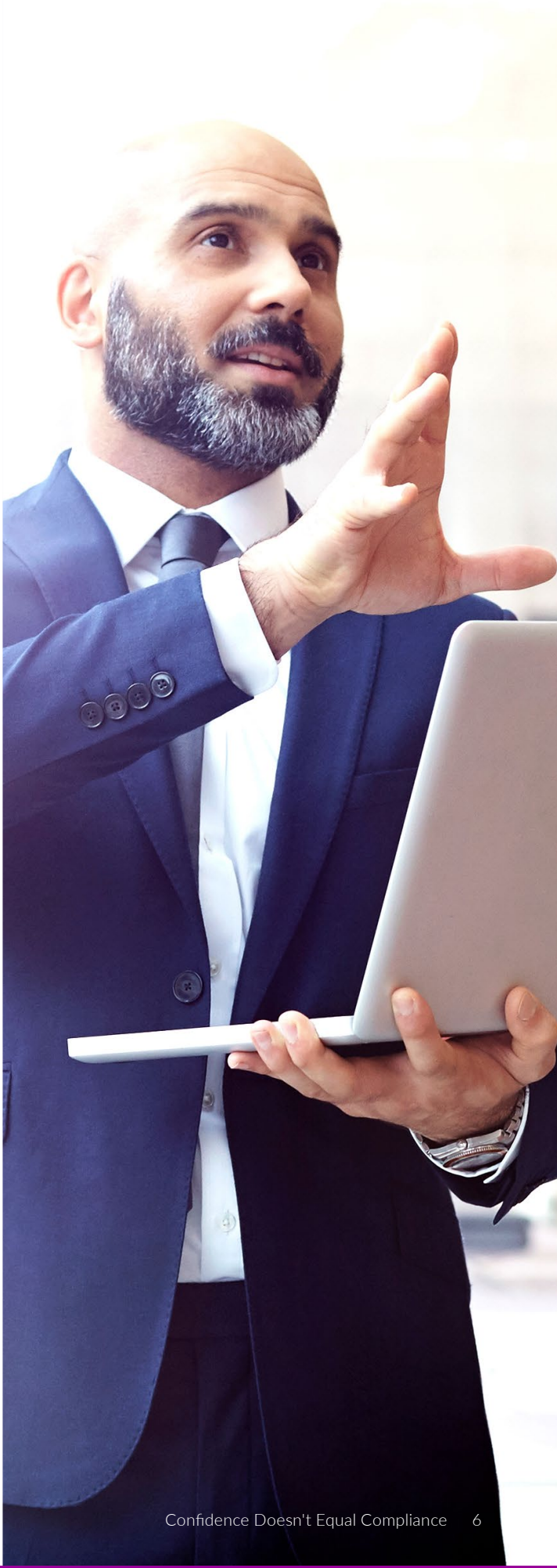
AI is turning on the lights

For years, mainframe access stayed in the shadows. Manual reviews looked where reviewers thought to look, and green screen access – familiar, stable, and quietly critical – rarely raised a flag. And “security by obscurity” was a reasonable strategy.

That era is ending. AI is now the force exposing these hidden gaps.

AI-powered audit tooling and analytics dashboards can correlate access logs, flag shared credentials, spot missing session controls, and surface authentication weaknesses across host systems at a scale and speed no manual team can match. In the Hanover study, the results delivered a blunt verdict: high confidence is masking ongoing mainframe access exposure, particularly among mid-market and European institutions, and organizations should re-baseline their risk using actual audit evidence rather than perception.

This cuts both ways. The same intelligence that helps you find and close gaps proactively is available to auditors, regulators, and attackers. AI doesn't create the vulnerability – it reveals it. The question is whether you find your blind spot first, or whether someone else finds it for you.



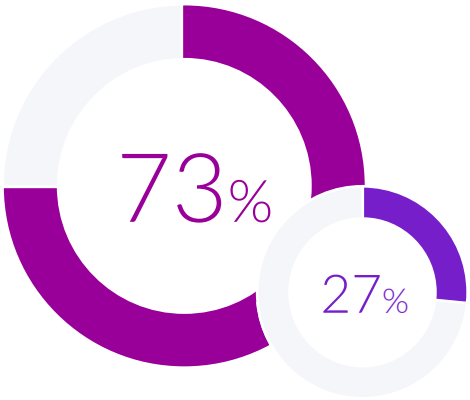
Key takeaway:

AI is compressing the timeline. Gaps that used to hide for years can now be surfaced in a single automated review.

The real cost of reacting instead of preparing

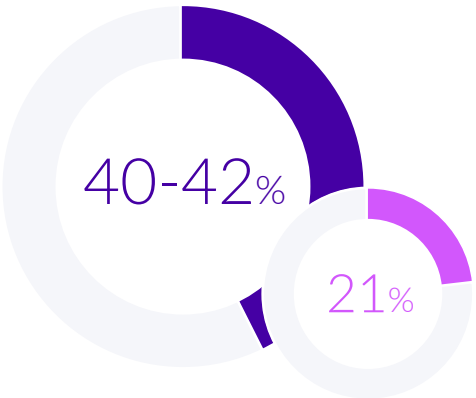
When a gap surfaces, the cost isn't just the fine. It's the drawn-out, resource-heavy scramble to fix it.

The data shows just how heavy that burden is:



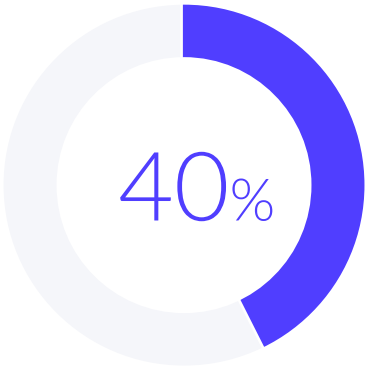
01

73% of organizations take four weeks or longer to formally close a finding,
with 27% need more than eight to 12 weeks.



02

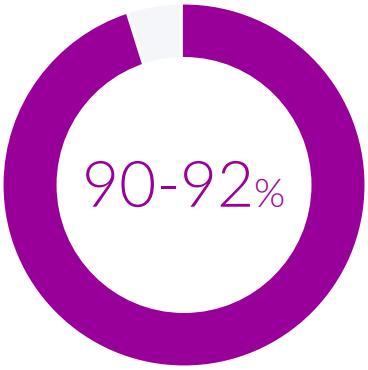
Remediation demands sizable teams
Depending on the control area, 40% to 42% of organizations pull in six to 10 employees, and up to 21% need more than 10.



03

The hours add up fast

Addressing a single issue in areas like MFA or privileged access requires 41 to 80 hours for more than 40% of organizations.



04

The stakes feel enormous

92% say potential financial penalties would be very or extremely impactful, and 90% cite increased risk exposure during the remediation period itself as a highly significant cost.

Despite understanding all of this, most organizations still wait. Change is triggered by a security incident for 28% of respondents and by increased regulatory scrutiny for another 28%. The awareness is there. The proactive action often isn't.

This is the trap of reactive compliance:

You know the risk, you know the cost, and you still find yourself fixing the problem under audit pressure rather than on your own terms.

Closing the gap: a proactive path forward

Here's the good news. The gap is well understood, clearly located, and entirely fixable. And you don't have to rip out your mainframe to close it.

Securing green screen and host access is one of the essential checkboxes for securing your mainframe as a whole. When you modernize that last mile of identity, you address the very controls that generate the most audit findings and the highest remediation costs.

This is where Rocket® Secure Host Access™ fits your journey. Built as a security-first terminal emulator, it integrates your green screen access directly with your existing identity and access management (IAM) solutions – so you achieve true defense in depth without disrupting the operations your business depends on.

Rocket Secure Host Access targets the exact gaps the research exposes:

MFA and SSO

extended to host systems through your existing IAM, eliminating the disjointed, shared-credential access auditors flag.

Passwordless and certificate-based authentication

to modernize the weakest link in legacy login.

Session monitoring and centralized logging

that make audit evidence straightforward to produce – turning weeks of scramble into actionable proof.

Centralized management

across desktop and web clients from a single console, so your team enforces consistent policy at scale.

The result is a defensible, audit-ready access posture that maps directly to the requirements driving your risk today – PCI DSS, DORA, and NYDFS/23 NYCRR Part 500 – all while keeping your critical systems running.

We understand these systems are mission-critical, and we'll meet you where you are. Modernization here doesn't mean disruption. It means closing a known gap before it becomes a known problem.

Conclusion: re-baseline before someone else does

Confidence is comfortable. But comfort is exactly what keeps the blind spot hidden. The organizations most exposed aren't the ones that know they have a problem – they're the ones certain they don't.

The path forward starts with honesty. Re-baseline your mainframe access risk using actual audit evidence, not perception. Look hard at the last mile of identity, where advanced controls remain thin and auditors are increasingly focused. Then close those gaps on your own timeline, before an incident or a regulator sets the timeline for you.

Your next step:

Request a mainframe access risk assessment with Rocket Software. In one focused conversation, we'll help you map your current host access controls against DORA, NYDFS, and PCI DSS requirements – and show you exactly where your blind spots are hiding.

Don't wait for the fine to find them first.

Speak to an expert today

Research findings referenced throughout are drawn from a Hanover Research thought leadership study prepared for Rocket Software, June 2026, based on 250 director-level respondents in compliance, cybersecurity, and IT operations at US and EU financial services and banking organizations with at least $500 million in annual revenue.

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-18796_WP_SHA_HanoverResearch_V3