Rocket® software

Protecting Policyholder Data at the Core

A modern access strategy for insurers

Contents

Executive summary

The global insurance industry, a sector built on risk assessment and management, is navigating a period of profound transformation. Shifting consumer expectations demand digital-first experiences, while intense market competition squeezes margins. Simultaneously, the cybersecurity threat landscape has never been more hostile, with insurers facing the dual challenge of underwriting their clients' cyber risk while protecting their own vast repositories of sensitive customer data.

This environment has given rise to complex data privacy regulations that mandate stringent protections for personally identifiable information (PII). For many insurers, the mission-critical mainframe systems that house this data present a unique challenge. These core systems are reliable and powerful, but the legacy green screen access methods often lack the sophisticated controls required by modern compliance frameworks.

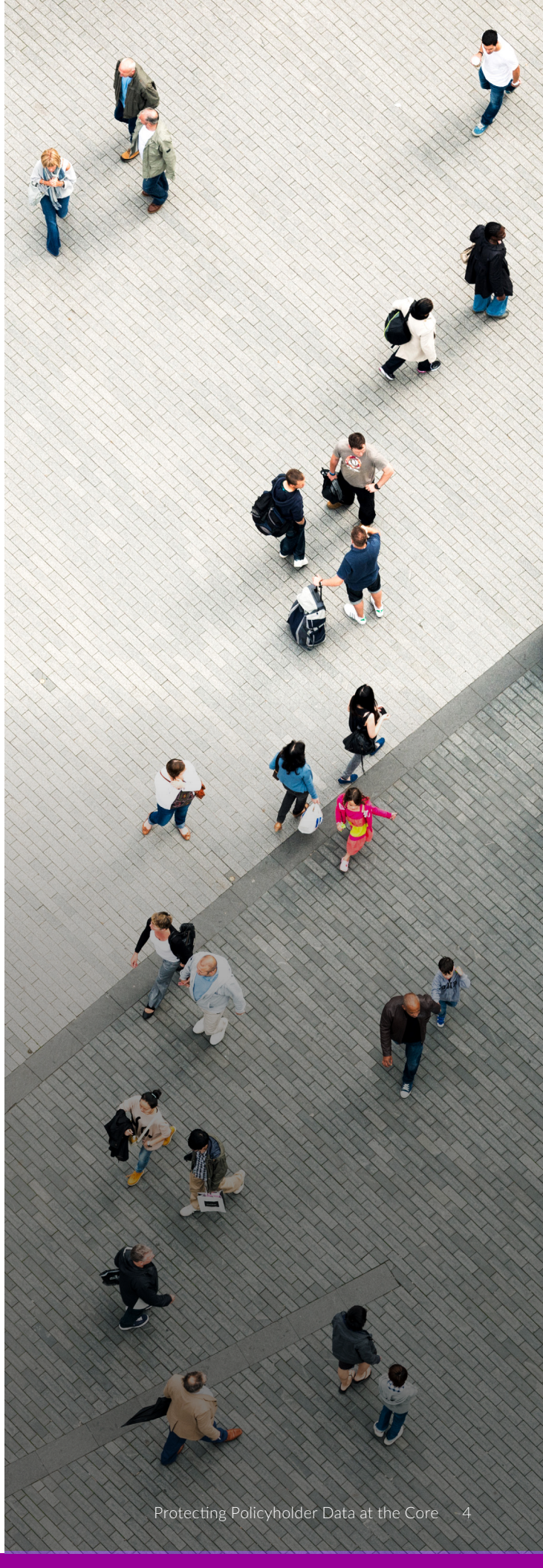
This whitepaper provides concrete, insurance-focused guidance for modernizing core system access to meet today's data privacy demands. It outlines strategies for implementing granular access controls, establishing detailed audit trails, and reducing administrative burden through integration and automation. By bridging the gap between legacy infrastructure and modern security, insurers can't only achieve compliance but also build a more resilient, efficient, and competitive enterprise.

The dual imperative: Digital innovation & data privacy

Insurers today find themselves at a crossroads. On one hand, the market demands rapid innovation. Customers expect seamless digital experiences, from instant quotes and personalized policies to automated claims processing. To deliver these services, insurers must leverage their data, integrating legacy backends with modern, cloud-enabled web and mobile applications.

On the other hand, this digital transformation expands the attack surface. Cybercriminals are actively targeting the insurance sector, recognizing the immense value of the customer data held within core systems. In response, regulators worldwide have enacted strict data privacy laws, such as GDPR in Europe and state-level legislation in the United States, imposing severe penalties for non-compliance.

This creates a dual imperative: innovate to stay competitive, but secure data to remain compliant and trusted. The key challenge lies in modernizing how data is accessed without disrupting the core systems that underpin the entire business.



Exposing the gaps: Legacy access in a modern threat landscape

For decades, terminal emulators – or green screens – have been the standard for accessing mainframe applications. While functional, these traditional access points weren't designed for today's interconnected, hybrid IT environments. They often operate as isolated silos, lacking the visibility and control required to defend against modern threats and satisfy auditor demands.

Key vulnerabilities of legacy access methods include:

Weak Authentication: Many legacy systems rely on simple username and password combinations, which are highly susceptible to phishing, credential stuffing, and other common attack vectors. This falls short of the multi-factor authentication (MFA) requirements stipulated by nearly all modern security frameworks.

Insufficient Audit Trails: When a security incident occurs, investigators and auditors need a clear, detailed record of who accessed what, when, and from where. Legacy access methods often produce logs that are difficult to parse or lack the necessary detail, making forensic analysis and compliance reporting a significant manual effort.

Lack of Granular Control: Traditional emulators typically provide broad access rights. It's difficult to enforce policies based on user role, location, or context. This "all-or-nothing" approach creates unnecessary risk, as a single compromised account could grant an attacker wide-ranging access to sensitive policyholder information.

Operational Inefficiency: Managing user access across fragmented, non-integrated systems is a heavy administrative burden. Manual provisioning and de-provisioning processes are slow, error-prone, and strain IT resources that could be focused on strategic modernization initiatives.

Strategies for modernizing core system access

To close these security and compliance gaps, insurers must adopt a modern approach to host access that integrates seamlessly with their broader IT and security ecosystem. This strategy isn't about replacing the mainframe but about securing the pathways to it. The following three pillars are essential for building a robust and compliant access control framework.

01

Implement granular access controls with IAM integration

The foundation of a modern access strategy is the ability to enforce strong and consistent identity controls. By integrating core system access with a centralized Identity and Access Management (IAM) solution, insurers can extend modern security protocols to their most critical applications.

This integration allows you to:

Enforce Multi-Factor Authentication (MFA): Move beyond outdated passwords and require a second form of verification for every user. This dramatically reduces the risk of unauthorized access from compromised credentials and is a core requirement for Zero Trust security models.

Enable Single Sign-On (SSO): Provide users with a frictionless and secure access experience. SSO simplifies password management, reduces help desk tickets related to lockouts, and ensures that access policies are managed centrally.

Implement Role-Based Access Control (RBAC): Define and enforce granular permissions that limit users to only the data and functions necessary for their jobs. This principle of least privilege is a cornerstone of effective data privacy and security.

A modern solution like Rocket® Secure Host Access™ acts as a security-first terminal emulator that bridges your mainframe environment and your enterprise IAM platform, allowing you to manage access with the same rigor you apply to your cloud and distributed systems.

02

Establish comprehensive and actionable audit trails

To satisfy regulators and accelerate incident response, insurers need complete visibility into all access activity. Modernizing access controls must include the deployment of systems that provide deep, centralized, and immutable logging.

An effective auditing solution should deliver:

Detailed Session Recording: Capture every keystroke and screen for high-privilege user sessions. This provides irrefutable evidence for forensic investigations and helps demonstrate compliance with strict monitoring requirements.

Centralized Logging: Consolidate access logs from all host systems into a single, unified view. This simplifies analysis and allows security teams to correlate events across the hybrid environment to detect sophisticated, multi-stage attacks.

Automated Reporting: Generate audit-ready reports automatically, saving hundreds of hours of manual effort. This allows your team to prove compliance with regulations like GDPR, CCPA, and others with push-button simplicity.

By providing a single pane of glass for all host access, you eliminate the "black box" of legacy systems and provide auditors with the clear, consistent evidence they require.

03

Minimize manual administration through automation

The skills shortage in the IT industry is particularly acute in the mainframe space. Insurers can't afford to have their most experienced IT professionals consumed by routine administrative tasks. Automation is critical for improving operational efficiency, reducing human error, and freeing up high-value talent to focus on innovation.

Integrating and automating access management delivers key benefits:

Automated User Provisioning: Automatically grant or revoke access rights based on an employee's role and status in your central HR or IAM system. This ensures that new employees get the access they need quickly and, more importantly, that access is immediately terminated upon departure, closing a common security gap.

Self-Service Capabilities: Empower users to manage their own credentials through the enterprise IAM platform, significantly reducing the volume of password-related help desk tickets.

Centralized Policy Management: Define access policies once in a central console and deploy them across the entire user base. This eliminates the need to configure individual desktops and ensures that security rules are applied consistently everywhere.

This approach not only strengthens security but also addresses the critical skills shortage by allowing smaller teams to manage large, complex environments with greater efficiency and control.

Turn compliance into a competitive advantage

For the insurance industry, data privacy is more than a regulatory checkbox—it's essential to earning and preserving customer trust. As insurers accelerate digital transformation, the security of core systems must be at the heart of every modernization decision. The risks are significant, and the stakes have never been higher.

Rocket® Secure Host Access™ is purpose-built to help insurers bridge the gap between legacy and modern infrastructure. By integrating advanced IAM capabilities, creating comprehensive audit trails, and automating access management, Rocket Secure Host Access empowers organizations to strengthen compliance, safeguard sensitive data, and unlock operational efficiency—all without disrupting business-critical systems.

Ready to move forward?

Learn more

Learn more about how Rocket® Secure Host Access™ can help your organization meet today's data privacy & modernization challenges.

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-17719_WP_SHAInsurance_V3