All or Nothing: Unified Identity Platform versus Point Solutions

With more threats, greater complexity, and growing costs, organizations need a unified identity platform to defend against identity-based attacks, drive efficiencies, and ensure business continuity.

Why Leaders Prioritize Identity

72% of IT executives say security is the primary factor when choosing an IAM provider. 82% of breaches involved the use of stolen credentials, phishing, and other human-related vulnerabilities. 100% of CISOs and tech leaders value cost-effectiveness over cost alone.

Benefits of a Unified Identity Platform

Organizations using a unified identity platform can realize significant benefits.

- Reduced risk of human error in managing entitlements
- Improved operational efficiencies for credential management
- Lower costs with automation

Organizations can extend those benefits by ensuring that their identity platform can support their environment today and scale over time to support future cloud investments.

RSA Unified Identity Platform

Automated Identity Intelligence

- Mobile threat detection
- Phish-resistant tokens
- AI-powered risk analysis

Authentication
- Advanced multi-factor authentication
- Software and hardware authentication
- Adaptive policies with context

Access
- Simplified access management
- Unified credential experience
- Federated identity

Governance & Lifecycle
- End-to-end viability
- Complete auditability
- Compliance readiness

Expect more from Identity. Contact RSA to learn how at: 1-800-995-5095

Without a unified identity solution, organizations pay more for weaker security.

©2023 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 03/23 Infographic

2 Ibid.

72% 82% 100% of IT executives say security is the primary factor when choosing an IAM provider. 82% of breaches involved the use of stolen credentials, phishing, and other human-related vulnerabilities. 100% of CISOs and tech leaders value cost-effectiveness over cost alone.