

Separately managing user identities and machine identities creates complexity in the enterprise. Bringing these technologies together in an integrated platform offers visibility and control, establishing a strong foundation for agility and improved ROI.

Modernizing the Digital Trust Ecosystem for Quantum Readiness

July 2025

Written by: Jennifer Glenn, Research Director, Security and Trust

Introduction

Digitizing business data was, and still is, a game changer

for building agile and productive business operations. It has made it much easier to use, share, and collaborate on data, which improves efficiency and offers better customization of customer-facing data.

Despite these benefits, digitization also opened the door for inappropriate data exposure and, in turn, violations of privacy and compliance rules. Due to these violations, businesses can incur direct costs, such as fines and legal expenses, and indirect costs, such as lost business.

Employees, customers, and partners — as well as the general public — need to have confidence that the businesses they work with, or for, can be trusted with their sensitive information. This means actively securing and maintaining the integrity and availability of that information. Data exposures and/or breaches erode trust in an organization and can have lasting consequences.

Organizations have traditionally relied on individual solutions to address this challenge. Identity management manages and controls access to digital resources based on the user. Data access governance uses the data as the control point for which information is available for use by people or machines. Encryption and key management should maintain the integrity of data as it moves through its life cycle. These are all very good technologies that work as intended and provide significant benefits in their respective areas. However, these individual technologies do not address the current problems.

Organizations will struggle to address digital trust — the confidence in an organization's ability to protect sensitive digital data — with multiple solutions. Creating a trusted foundation for digital data not only requires doing work to protect data at every stage of its life cycle — from development to delivery — but also requires the organization to prove that it can maintain this level of security.

AT A GLANCE

KEY TAKEAWAYS

- » The volume of human, nonhuman, and cryptographic identities is growing exponentially, making it difficult to accurately see and manage all of them.
- » Integrating management of all of these identity types into an integrated platform provides improved visibility, consistent policy enforcement, and simplified management.
- » These benefits are essential for addressing today's goals, like zero trust, and preparing for future market shifts, including post quantum.

It is possible to do this by combining and managing identity and access management (IAM), encryption, and cryptographic life-cycle management solutions to fulfill these two requirements:

- » **Creating digital trust internally:** From an internal perspective, digital trust initiatives are specific to that enterprise organization. This includes ensuring that the organization meets encryption standards, keeps secrets for development environments safe, and manages and rotates cryptographic keys for internal systems regularly. Digital identity access controls serve as a critical enforcement layer, ensuring that only authorized users and systems can access sensitive resources. This does not require any external vetting.
- » **Proving digital trust externally:** Looking at the requirements of digital trust externally requires evidence of the verification of digital identity and encryption by any other user, website, device, or nonhuman identity (NHI). This requires proof of identity and vetting to make sure the rest of the world has confidence in the data the organization is using. The use of digital certificates covers this requirement.

Tackling all of the pieces for digital trust — users, machines, and NHIs — while providing the correct attestation can be challenging. Policies may be inconsistent and expensive, and having the staff and skills to actively manage these technologies separately — while fulfilling both requirements — is nearly impossible. However, successfully combining the capabilities for protection and attestation into an integrated platform with a unified experience can offer a number of benefits to the organization.

Benefits of an Integrated Platform for Users, Cryptographic Assets, and Nonhuman Identities

Traditionally, two — perhaps even three — groups within an organization have handled the integration of information from identity and access management tools and cryptographic identity tools. This approach creates inconsistent policies, data appearing in multiple formats, and very siloed visibility into the risks for these areas. Combining information about user, nonhuman, and cryptographic identities within a shared architecture, aligned with individual enforcement technologies, such as IAM or PKI, can offer a number of advantages for organizations trying to achieve digital trust. In detail:

- » **Simplicity:** Combining all identity technologies into an integrated platform provides broad visibility of cryptographic and identity information. With an integrated picture of an organization's ecosystem, it's much easier to uncover and address risk.
- » **Efficacy:** With broad visibility, it is much easier to see how the risk and the fix will affect the availability of critical tools and information. This translates to prioritized protection with a focus on what matters most.
- » **Cost:** An integrated platform for managing all identity and cryptographic assets offers significant cost savings by leveraging economies of scale and reducing the complexity and operational overhead that an organization needs to manage and finance.
- » **Consistency:** Using the same information presented in the same way offers an organization a more consistent view of its critical cryptographic and identity information. This translates to better policy creation and enforcement.

Industry Trends Are Driving the Need for Integrated Identities Management

Cyberthreats continue to plague companies of all sizes in all industries. Data is the prize. Malicious actors are refining attacks to specifically target encryption and keys to compromise or exfiltrate data. Insiders are also posing a significant threat to data security and integrity. Whether accidental or intentional, exposure (or theft) of sensitive data is the primary concern. To meet organizational standards for trusted operations and to meet the necessary privacy or compliance regulations, companies need to rethink their approach.

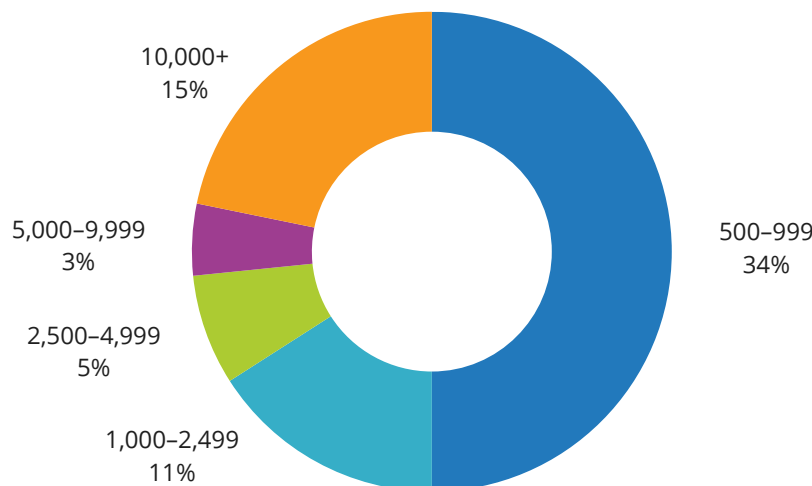
Organizations are now issuing and relying on far more digital certificates than in years past, often with shorter life spans and higher renewal frequencies. This increased scale and velocity make visibility and life-cycle management essential to prevent outages, compliance failures, and security risks.

Quantum computing raises significant questions about how to discover, prioritize, and modernize all of these certificates if traditional encryption is broken. The volume and complexity of transitioning these certificates is a massive undertaking. While companies of all sizes have some challenges modernizing their cryptographic post-quantum infrastructure, the smallest and largest organizations are struggling the most, but they face different impediments to implementation. In IDC's March 2025 *Data Security and Privacy Survey*, 34% of small organizations (500–999 FTEs) and 15% of very large organizations (10,000+ FTEs) indicated they had no plans to implement any quantum activities (see Figure 1).

FIGURE 1: **Organizations with No Plans to Implement Quantum-Resistant Encryption**

The smallest and largest organizations are the most likely to say they have no plans for quantum resistance.

Q When do you plan to implement quantum-resistant encryption into your organization?



n = 618

Note: This figure shows how respondents from different-sized organizations replied that they had no plans to implement quantum-resistant tools or initiatives into their organizations.

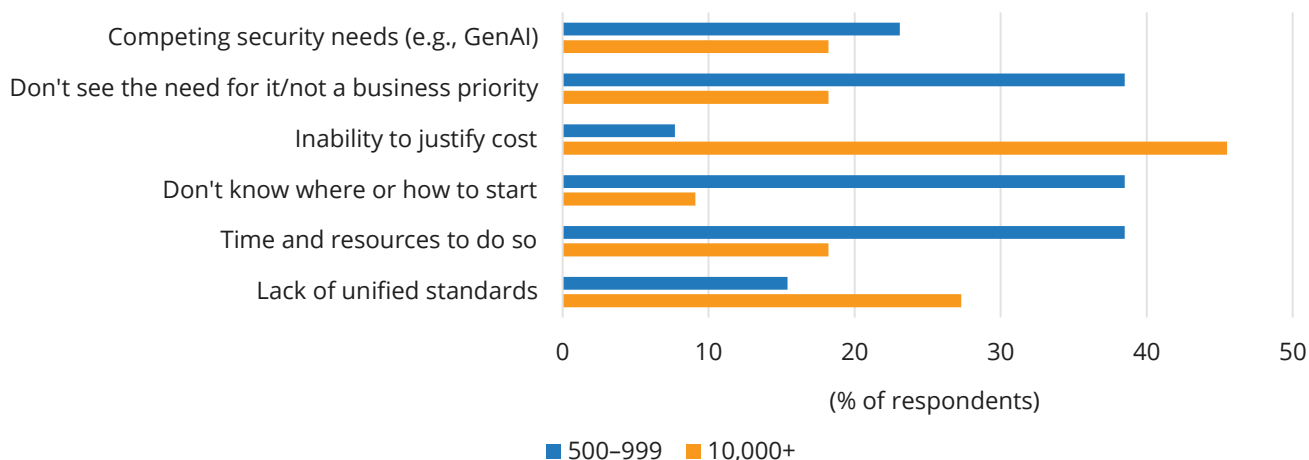
Source: IDC's Data Security and Privacy Survey, March 2025

The inability to justify cost hampered the largest organizations, and the smallest organizations struggled most with business priorities and the lack of time and resources (see Figure 2).

FIGURE 2: *Impediments to the Implementation of Quantum Resistance Are Different Between the Smallest and Largest Organizations*

Smaller organizations struggle with business priorities and resources; larger organizations have a hard time justifying the cost.

Q What is holding back your organization from implementing quantum-resistant encryption?



n = 38

Notes:

This figure only includes the respondents who indicated they had no plans for quantum-resistant encryption.

The numbers along the x-axis indicate the percentage of respondents' top answers.

The figure only shows the responses from the largest and smallest organizations.

Source: IDC's Data Security and Privacy Survey, March 2025

While transitioning to quantum-resistant algorithms is a struggle to justify for some organizations, modernization should not be as challenging. Modernizing user and cryptographic identities should not be as hard to justify. Full visibility across all identity and cryptographic identity assets not only supports operational resilience today but will also be critical for crypto-agility (i.e., the ability to swap crypto-algorithms quickly and easily for improved security). Crypto-agility offers an evergreen approach to managing all of these assets, creating a solid foundation for addressing current issues, such as shortened renewal cycles and transitioning to quantum-resistant cryptography.

Considering ISSQUARED for Integrated Identities Management

ISSQUARED Inc. is a cybersecurity solutions and services provider specializing in IAM, PKI, cybersecurity, IT infrastructure, and a broad range of professional and managed services. Founded in 2010, the company operates globally, serving clients across various industries, including healthcare and life sciences, finance, government, and technology. ISSQUARED has an established footprint with organizations seeking to protect their digital assets and ensure compliance with regulatory requirements. In addition to consulting and support, the company develops its own products to assist customers with addressing identity and infrastructure challenges.

The company offers two primary product lines within cybersecurity — PkeyFx and ORSUS — covering both cryptographic identity management and user identity management.

PkeyFx is a hybrid appliance-based solution designed for managing cryptographic identity assets, including digital certificates and keys. PkeyFx is a certificate life-cycle management solution that aims to streamline, simplify, and automate the management of digital certificates. Its intent is to enhance trust and security, simplify regulatory compliance, and improve operational efficiency for organizations of all sizes. PkeyFx is designed to manage and secure digital infrastructure that scales. It has the flexibility to incorporate multiple certification authorities (CAs) and support multiple environments for each customer on a single appliance. Capabilities of the PkeyFx product line include:

- » **PkeyFx Certificate Lifecycle Management (CLM)**, which is designed to manage digital certificates throughout their life cycle from issuance to renewal to destruction, across all cloud and on-premises environments
- » **PkeyFx Certificate Authority Manager (CAM)**, which is designed for enabling the creation, visibility, and management of an organization's private certificate authorities, including root and intermediate CAs (This capability includes the ability to manage private keys in a dedicated hardware security module [HSM].)

The ORSUS product line is designed for managing user identities and access privileges. Capabilities of this product line include:

- » **ORSUS Lifecycle Manager (OLM)** and **External Identity Access and Governance (EIAG)** to help manage user identities and access privileges for internal and external users to meet security and compliance requirements
- » **ORSUS Directory Services (ODS)** to unify an organization's individual identity directories under a single interface so that all systems and applications have a single place for consistent authorization and authentication policies

ISSQUARED is bringing these two products together to offer organizations an integrated approach for managing identity and cryptographic assets, with the flexibility to procure either product individually or as an integrated solution, based on the organization's specific needs. ISSQUARED's consulting and managed services offerings will support these products, including a range of readiness assessments to ensure organizations are well prepared for future needs. The benefits of this integration include:

- » Support for both cloud and on-premises environments, with cross-platform compatibility and feature parity across deployment models
- » Built-in connectors for external trusted authorities and discovery mechanisms to map and manage digital footprints
- » Standards-based support across product families — PkeyFx (e.g., ACME, SCEP, and REST APIs) and ORSUS (e.g., SCIM) — to ensure interoperability and extensibility
- » Quantum-ready architecture designed to integrate quantum-resistant encryption algorithms using certified quantum-ready hardware and software

The company will continue to expand the features and capabilities of both product lines, as well as for the integration between them.

Challenges

The markets for IAM solutions and cryptographic identity solutions (e.g., crypto keys, certificates, and HSMs) are mature, and the technologies are well entrenched within most organizations. Organizations that have invested heavily in IAM implementations, both in initial cost and customizations, may be reticent to move to a different solution. Similarly, a lot of

organizations have built their own solutions for managing cryptographic identity and transitioning to something new — even if it makes the job easier — can be a task they are not ready to tackle. The challenging nature of managing either one of these technologies, plus the existing financial and people investments to run them, may pose a hindrance for organizations to either transition to, or adopt, all the pieces of the platform.

Further, the markets for user identity management and cryptography solutions are quite large. Some vendors are offering both types of solutions, though they are likely to sell them individually. However, the market is starting to consolidate. The vendors in these markets see the parallels in their buyers and solutions, and a number of vendors are starting to merge to provide a single solution offering for all identities.

For ISSQUARED, bringing together two crowded software markets will be a challenge. The user identity management buyers may be reticent to give up on their existing time and financial investments. The cryptographic identity buyers are trying to navigate the shifting vendor landscape, as many of these companies are merging to offer consolidated platforms for keys, certificates, and secrets management.

To gain market recognition, ISSQUARED will need to differentiate with strong messaging and the value of integration. The company will also need to clearly articulate how the benefits of its platform outweigh the pain of removing established point solutions.

ISSQUARED has a strong vision for its platform with clear plans for advancing the capabilities of both product lines. Further, its history in services offers a good launchpad for understanding market challenges and provides a solid capability to distinguish itself in the space.

Conclusion

On the whole, security tools are very good at doing what they are designed for and are relatively successful at reducing risk. However, attacks are still getting through. User identities and cryptographic identities are typically the last points of defense against data exposure and theft. Integrating identities across the entire ecosystem is challenging but necessary for keeping these assets secure now and in the future. While this is important for cost, efficiency, and consistency, modern security initiatives, such as zero trust and cryptographic modernization, are increasingly driving this integration. Strong certificate and identity hygiene is also a critical prerequisite for future security challenges, such as the transition to post-quantum cryptography.

IDC believes the convergence of identity technologies will become a critical issue in the next several years. Finding and hiring skilled staff will continue to be a challenge. Economic uncertainty will force adjustments to IT and cybersecurity budgets. The increasing volume of all identities (cryptographic, user, and NHIs) will necessitate more consistent policies for data access. With an integrated approach for managing the identity ecosystem, ISSQUARED is in a position to successfully address these challenges.

Integrating cryptographic and user identities provides broad visibility and simplicity management for zero trust and post-quantum readiness initiatives.

About the Analyst



Jennifer Glenn, Research Director, Security and Trust

Jennifer Glenn is research director for the IDC's Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

ISSQUARED is a provider of Identity and Access Management (IAM), Cybersecurity, and Infrastructure solutions, trusted by both large and small enterprises to solve complex security challenges. With roots in hands-on practitioner experience, we take a practical, real-world approach to designing and delivering secure, scalable solutions.

Our PKI platform, PkeyFx, enables certificate lifecycle management at scale, supporting protocols like ACME, SCEP, EST, and REST APIs to help organizations maintain trust across hybrid environments. PkeyFx also integrates with our identity suite, ORSUS, for unified governance of identities and cryptographic assets.

With over 14 years of delivery experience and a leadership team grounded in decades of enterprise security work, ISSQUARED combines deep domain expertise with advisory, implementation, and managed services — across both our own and third-party platforms.

Learn more at www.issquaredinc.com and www.pkeyfx.com.



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)