

5 Ways Modern PKI Reduces Business Risk

See how modernization helps organizations gain visibility,
automate processes, and stay ahead of evolving risks.



ENTRUST



Introduction

Public key infrastructure (PKI) has long been the foundation of digital trust, securing identities, communications, applications, and data across the enterprise. But what was once a stable, behind-the-scenes system is now under increasing pressure. Certificate lifecycles are shrinking, machine identities are exploding, and post-quantum timelines are accelerating.

The **2026 Global State of Post-Quantum and Cryptographic Security Trends** report by Entrust and Ponemon Institute confirms it: systems and limited visibility are driving unmanageable complexity.

Modernizing PKI means maintaining control in an environment that's scaling beyond manual management. **The organizations best prepared for tomorrow's security challenges are getting ahead of it today.** Here are five ways modernizing PKI reduces risk.



1. Improve Visibility Into Cryptographic Risk

You can't secure what you can't see.

Most organizations don't have a complete inventory of their certificates, keys, and cryptographic assets. And that's a problem.

Without centralized visibility, expired certificates go unnoticed; shadow PKI environments emerge, and risk accumulates silently.

Ponemon Institute research shows a clear gap between awareness and action. Only about 43% of organizations report having full visibility into their certificates.

PKI MODERNIZATION ENABLES:

- ✓ Centralized discovery across environments
- ✓ Accurate inventory of all cryptographic assets
- ✓ A clear view of risk exposure

By establishing comprehensive visibility across certificates and cryptographic assets, organizations can move from reactive response to proactive security and governance.

2. Automate Operations to Effectively Scale

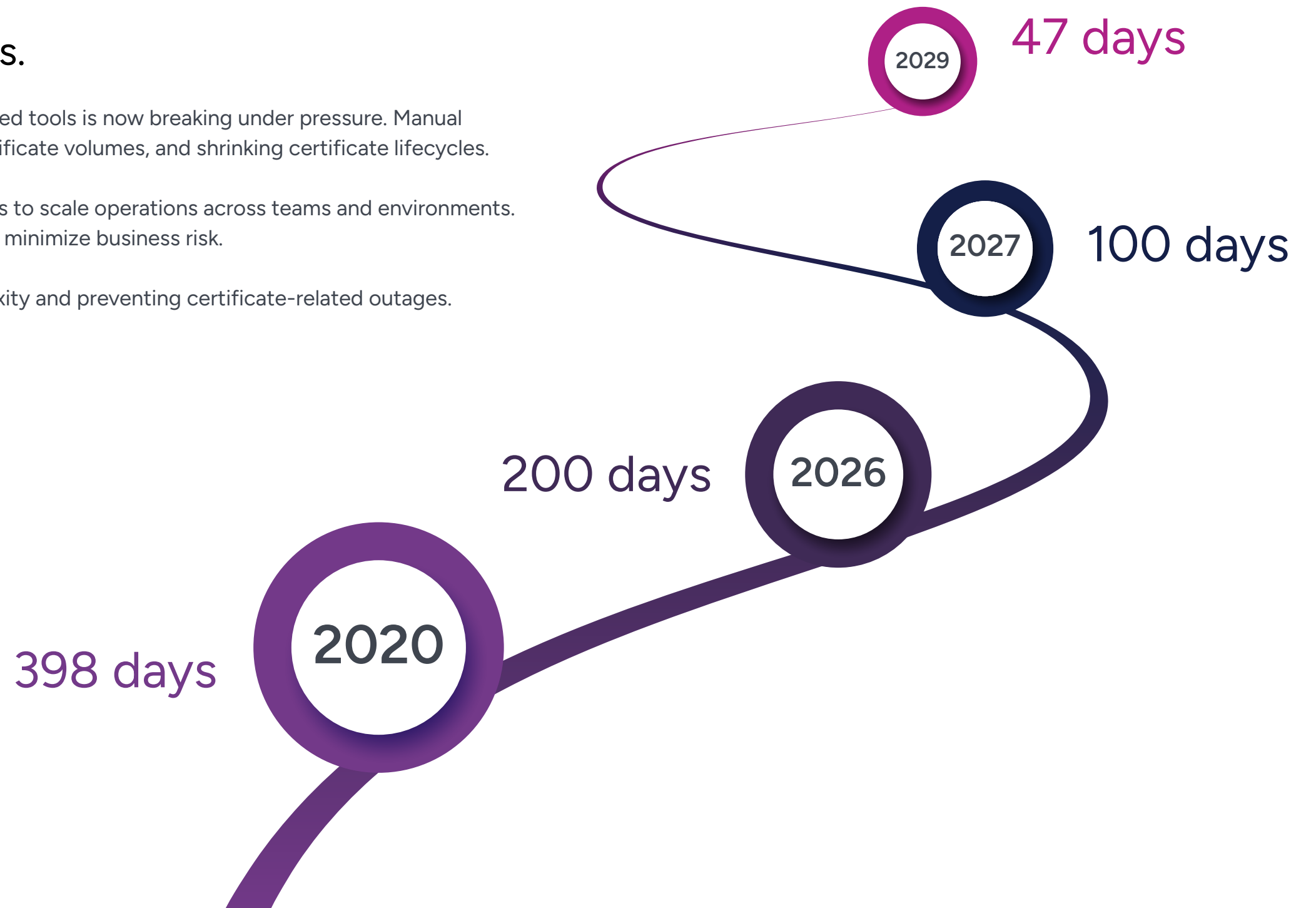
PKI wasn't built for today's demands.

What used to be manageable with spreadsheets, scripts, and siloed tools is now breaking under pressure. Manual systems can't handle multiplying machine identities, surging certificate volumes, and shrinking certificate lifecycles.

Automated certificate lifecycle management allows organizations to scale operations across teams and environments. This not only eliminates manual renewal processes but also helps minimize business risk.

This makes automation essential to reducing operational complexity and preventing certificate-related outages.

Certificate lifetimes are shrinking from 398 days to 47 – an 8x increase in renewal frequency.



3. Minimize the Risk of Certificate Outages

As certificate complexity grows, so does business risk.

PKI failures are both technical issues and critical business-impacting events.

EXPIRED OR MISCONFIGURED CERTIFICATES CAN CAUSE:

- ✓ Application downtime
- ✓ Customer-facing outages
- ✓ Revenue loss
- ✓ Reputational damage

Yet many organizations still lack the processes and visibility needed to prevent them. What used to be “infrastructure risk” is now a business continuity risk.

PKI modernization enables real-time visibility into certificate health and proactive lifecycle management, reducing the risk of outages and service disruption.



4. Meet Growing Compliance and Governance Pressures

Modern PKI turns governance into a competitive advantage.

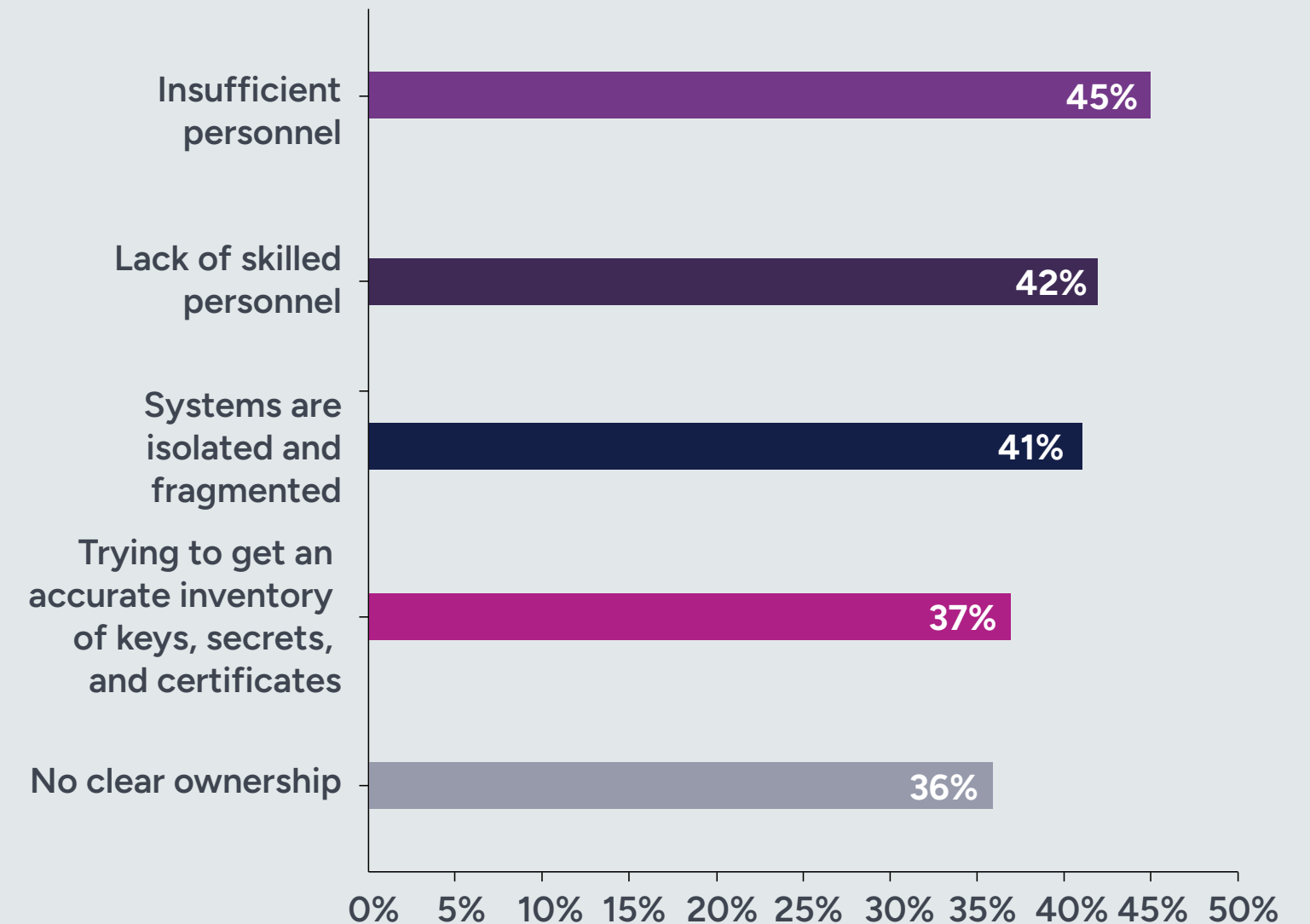
In addition to being a security tool, PKI has become a compliance control point. Organizations today face expanding regulatory requirements, audit expectations, and internal governance demands, yet many environments still suffer from inconsistent policies, lack of ownership, and fragmented control across teams.

Ponemon Institute data puts numbers behind it: 68% of respondents cite managing of cryptographic assets as either extremely or very difficult, citing insufficient staff (45%), lack of skilled personnel (42%), isolated and fragmented systems (41%), difficulty building an accurate inventory of keys, secrets, and certificates (37%), and no clear ownership (36%).

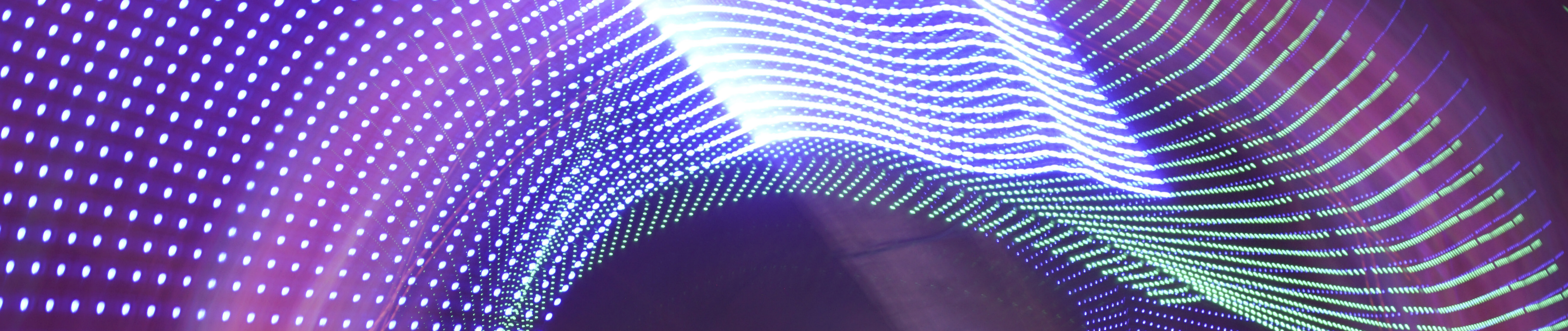
Without centralized governance, compliance becomes reactive and high-risk.

Modernizing PKI reduces exposure by enabling policy-driven governance and clear ownership of cryptographic assets, keeping organizations continuously audit-ready.

What makes the management of credentials difficult?*



*How respondents answered the question in the 2026 Global State of Post-Quantum and Cryptographic Security Trends report, Entrust and Ponemon Institute



5. Build a Strong Foundation for What's Next

The future of security requires crypto-agility.

Shorter certificate lifecycles, post-quantum cryptography, and the rapid growth of machine and AI-driven identities are reshaping the future of security. Over half of security leaders expect quantum threats within five years, yet only 38–40% are actively preparing – a widening gap between awareness and readiness, according to Ponemon Institute research.

Closing that gap means replacing legacy algorithms while meeting new cryptographic standards and maintaining uptime. This isn't a simple upgrade; it's a transformation, and one that requires organizations to be crypto-agile to adapt and scale.

Modernizing PKI provides a structured path for growth without re-architecting, while preparing for a post-quantum future.

Only 38%-40% of organizations are preparing for quantum threats, creating a gap between awareness and readiness, according to Ponemon Institute research.



From PKI Management to Cryptographic Control

PKI is a control point for digital trust that impacts uptime, compliance, and the ability to scale securely.

As certificate lifecycles shrink, machine identities grow, and post-quantum timelines accelerate, complexity is increasing faster than most organizations can manage. Most PKI environments weren't built for this.

THAT'S WHY MODERNIZATION IS AN IMPROVEMENT AND A SHIFT:

- ✓ From fragmented tools → centralized visibility
- ✓ From manual processes → automation at scale
- ✓ From reactive fixes → proactive control

Organizations that act now can move forward with confidence. Those waiting will be forced to respond under pressure.

At its core, PKI modernization is about maintaining control as complexity accelerates.

With Entrust, organizations can automate certificate management, centralize cryptographic visibility, and build the crypto-agile foundation needed for the future. Discover how Entrust PKI solutions can help you reduce risk, improve operational efficiency, and stay ahead of evolving security demands.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

©2026 Entrust Corporation. All rights reserved. Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners.
PK27Q2-ways-modern-pki-reduces-business-risk-eb



ENTRUST

SECURING A WORLD IN MOTION