

FEDRAMP HIGH

How Appian Turned Identity Proofing into a Competitive Advantage

NextgenID transforms a complex FedRAMP requirement into a strategic differentiator



CHALLENGE:

Bridging the Gap Between Enterprise Security and Federal Identity Standards

As a global leader in process automation with more than 40 security certifications, Appian understood what was at stake in falling short of compliance: lost federal opportunities, wasted engineering effort, and delayed market entry. Yet FedRAMP High exposed a new barrier: the requirement to meet Identity Assurance Level 3 (IAL3) under NIST SP 800-63-4. Unlike standard identity and access management (IAM) controls, IAL3 requires high-assurance identity proofing with in-person or supervised remote verification, biometric capture, and strict validation of government-issued identity evidence.

As Appian moved toward FedRAMP High, it quickly became clear that expectations between IAL2 and IAL3 identity proofing was the critical gap that could not be solved with existing tools, internal processes, or traditional vendors without introducing significant compliance, cost, and operational risk:

- **No scalable, audit-ready IAL3 identity proofing capability** capable of supporting a distributed global workforce
- **In-person verification requirements** made traditional approaches operationally impractical for remote and international employees
- **Building an internal solution** would have required new staffing, complex logistics infrastructure, and ongoing specialized identity expertise

KEY INSIGHTS:

Objective: Achieve FedRAMP High authorization by implementing a fully compliant IAL3 identity proofing capability, without building or operating a complex internal identity verification system.

Solution: Deploy a fully managed IAL3 identity proofing solution from NextgenID, enabling supervised remote verification, flexible enrollment options, and seamless integration with existing authentication systems.

BUSINESS OUTCOMES:

- Accelerated path to FedRAMP High authorization
- Eliminated need for dedicated identity proofing staff and infrastructure
- Reduced operational and logistical burden across teams
- Scalable solution that grows with workforce and demand

- **Existing vendor solutions failed** to fully meet supervised remote IAL3 requirements under NIST SP 800-63-4, creating a compliance gap that could block FedRAMP High authorization

“Every vendor we looked at fell kind of flat when it came to IAL3... no other solution met the expected requirements”

- Mark Lee, Director of Information Security, Appian

SOLUTION:

A Fully Managed, IAL3 Compliant Identity Ecosystem

The conclusion was clear: building in-house would create significant operational overhead without guaranteeing compliance. Appian selected NextgenID to deliver a comprehensive, fully managed identity proofing solution designed specifically to meet the highest federal assurance standards and to do so without requiring Appian to hire dedicated staff, manage hardware logistics, or maintain a complex internal identity infrastructure.



Onsite Attended Identity Proofing at Scale: At the core of the solution was NextgenID’s onsite attended identity proofing capability, enabling Appian employees to complete compliant IAL3 verification sessions without traveling to a central location and without Appian needing to staff or operate the process internally.

“It was clear and evident that NextgenID was purpose-built to meet IAL3 requirements”

- Mark Lee, Director of Information Security, Appian



Omnichannel Enrollment Infrastructure: To support Appian’s global workforce, NextgenID deployed multiple modalities to support secure, efficient enrollment:

- **On-site proofing stations** for high-volume enrollment at Appian offices
- **Distributed access points** across the U.S. for remote employees
- **Mobile identity kits** for international users, eliminating cross-border logistical barriers



Seamless Integration with Existing Security Stack: NextgenID integrated directly into Appian’s existing identity architecture:

- **High-assurance identity proofing and YubiKey binding** handled by NextgenID, linking verified identity results directly to hardware credentials
- **IAL3 credential requirements** managed and enforced
- **Hardware authentication**

The modular design allowed Appian to avoid replacing its IAM infrastructure while still achieving full compliance, reducing costs without adding cross-functional strain on HR, IT or Security teams.



Continuous Compliance and Standards Alignment: NextgenID’s dedication to fully compliant identity assurance ensures that the platform continuously evolves to meet changing regulatory requirements, which removed the compliance burden from Appian’s internal teams.

“We are built to operate inside complexity, not avoid it. We design to enhance infrastructure and take responsibility for making identity proofing work reliably in environments where the margin for error is zero.”

- Michael Harris, CTO and EVP, NextgenID

DEPLOYMENT:

Rapid Implementation with Global Reach

Appian brought identity proofing into its FedRAMP journey early, and NextgenID was up and running almost immediately in parallel with other compliance workstreams. Deployment was fast, lightweight, and required minimal internal effort, allowing Appian to stand up a fully compliant IAL3 identity proofing capability without slowing down its broader authorization timeline.

- **High-Volume Enrollment Execution:** During initial rollout, Appian processed nearly 300 employees through identity proofing in a compressed timeframe.
- **International Enablement Without Complexity:** For employees outside the United States, NextgenID's mobile kits eliminated the need for expensive travel or complicated shipping processes, enabling Appian to maintain consistent identity assurance standards across its global workforce.
- **Audit-Ready from Day One:** NextgenID provided the complete audit-ready IAL3 identity proofing capability out of the box, supporting Appian in demonstrating compliance to auditors without additional system development or workflow design.


"You shouldn't waste time where you can work with a partner that already has it figured out."


- Andrew Cunje, CISO, Appian


RESULTS:


Faster Compliance, Lower Costs, and Scalable Growth

By leveraging NextgenID's managed identity platform, Appian achieved its FedRAMP High objectives while avoiding the operational overhead associated with building and maintaining an internal solution.

 **Accelerated Time to Compliance:** With identity proofing handled by a trusted partner, Appian was able to focus on other critical aspects of its FedRAMP initiative, keeping timelines on track despite aggressive internal and external expectations.

 **Significant Operational Efficiency Gains:** NextgenID eliminated the need for dedicated identity proofing staff and reduced cross-functional strain on HR, IT, and security teams. The solution also removed the need to manage hardware, shipping logistics, and ongoing maintenance.

 **Improved Security and User Trust:** Employees were able to complete identity proofing quickly while maintaining confidence in how their sensitive data was handled.

 **Seamless Scalability:** As Appian continues to grow, NextgenID's platform scales effortlessly to accommodate new hires, new programs, and evolving requirements.

"Working with NextgenID ... is the number one thing that anyone could do to accelerate secure, validated identities in their business today."

- Andrew Cunje, CISO, Appian

WHAT THIS PROVES:

Identity Proofing is the Hidden Bottleneck in Federal Cloud Adoption

Appian's experience reflects a broader pattern across organizations pursuing FedRAMP High authorization: IAL3 identity proofing is often treated as a build-it-internally problem, when in practice it is a specialized capability that does not align well with ad hoc implementation. Most teams attempting this path absorb significant operational overhead to replicate controls that already exist in mature, purpose-built systems.

Appian's strategic partnership with NextgenID facilitated a production-ready identity proofing capability that could be deployed directly into Appian's existing architecture without requiring redesign or internal CSP development. The result is a platform that enters the federal market with stronger, more complete identity assurance capabilities already embedded rather than retrofitted. Appian's environment is now better positioned to support high-security federal use cases at scale, with identity proofing operating as a managed, compliant system enhancement.

"The organizations that get this right aren't building identity proofing from scratch. They're finding partners who've already done the hard work. We built NextgenID specifically because IAL3 kept showing up as the gap nobody had a real answer for. Appian recognized that early, and it made all the difference in their timeline."

– Mohab Murrar, CEO, NextgenID

Simplify Compliance. Start with NextgenID.

NextgenID delivers high-assurance identity proofing and enrollment through a nationwide network of secure identity stations and patented Onsite Attended technology. NextgenID's platform enables organizations to verify identities anytime, anywhere, combining remote supervision, biometric capture, and NIST-compliant processes to streamline credentialing while maintaining the highest levels of security and compliance. Designed for federal, enterprise, and mission-critical environments, NextgenID reduces operational burden while accelerating secure onboarding at scale.

Take your first step towards compliance with NextgenID by contacting the team at:

(888) 373-8648

info@nextgenid.com

www.nextgenid.com

10300 Eaton Place, Suite 105
Fairfax, VA 22030, USA

