IDC BLOG

SPONSORED BY:
Intellicheck

DATE:
May 2026

GUEST IDC BLOGGER:
Sam Abadir, Research Director
Risk, Financial Crime, and Compliance

Identity Is Infrastructure. Stop Building It Like It Is Not.

The case for treating identity verification as foundational infrastructure, not a feature

Identity is infrastructure: Why growing companies can't afford to build alone

I've watched a lot of promising companies hit the same wall.

The product is sharp. The growth is real. The team is executing. And then someone mentions regulatory requirements like identity verification almost as an aside.

That aside is where things start to go sideways.

Identity verification gets handed to an engineering team already stretched thin and scoped as a feature. And stretched thin is not an exaggeration. According to IDC's 2025 *Software Development Survey* (syndicated), nearly half of organizations say they need to hire additional developers just to meet current workload demands (see Figure 1). The engineering team builds exactly what they were asked to build. That is the problem. Nobody in the room knew how to scope it correctly. Nobody had the domain expertise, the document intelligence, or the regulatory and security depth the problem actually requires. What looks like a checked box turns out to be a liability.

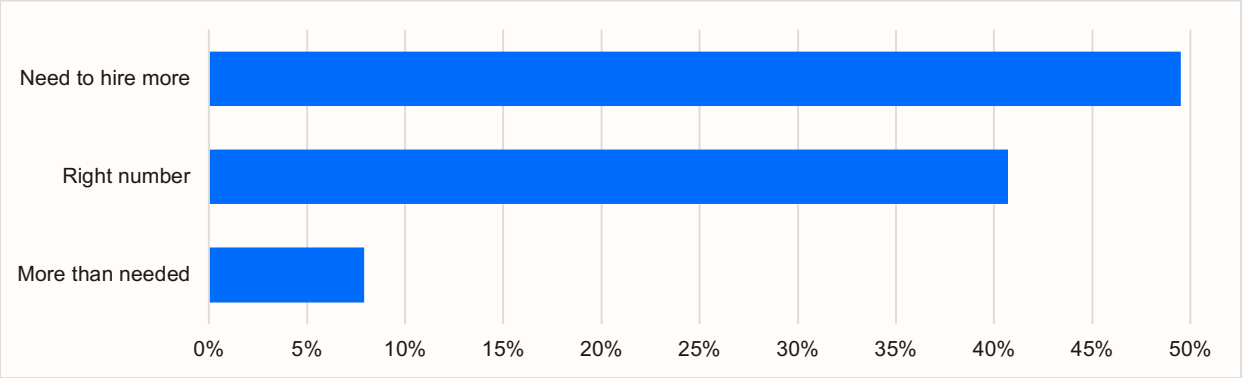
Identity verification is not a feature. It never was. Scoping it as one is the mistake.

Figure 1

One in two organizations need more developers to meet current demand

Most engineering teams are not resourced to build identity verification correctly

Q. How would you assess your company's current software developer staffing situation?



n = 524

Note: Data reflects North American organizations only.

Source: IDC's *Software Development Survey* (syndicated), 2025

The document problem is harder than it looks

Most organizations assume verifying an ID is a visual problem. Does it look real? Does the photo match?

That assumption is what fraudsters count on.

There are over 250 DMV-issued ID formats in circulation across U.S. states and territories, Canada, and Mexico. Each has its own barcode structure, security features, and format standards. Criminals use publicly available DMV templates to produce fakes that pass visual inspection easily. Reading the encoded barcode data correctly requires years of accumulated intelligence that no internal build acquires quickly. As AI-generated fakes improve, that gap only widens. AI-powered verification is what closes it, and it is what levels the playing field for organizations that could never build that capability on their own.

Building AI-powered verification is the beginning, not the end

Even if you scope it correctly and build it well, you have just signed up to own it forever.

DMV formats change. Fraud techniques evolve. Regulatory requirements shift. The build is not the cost. The maintenance is the cost. Identity verification never stabilizes. It is a permanent program with a permanent budget that has nothing to do with your core product. Most organizations do not budget for that when they make the build decision. They find out later.

The security depth problem

The same IDC survey found that security receives less developer time than any other activity tracked, averaging just 3.4 hours per week, less than meetings, emails, and debugging (see Figure 2).

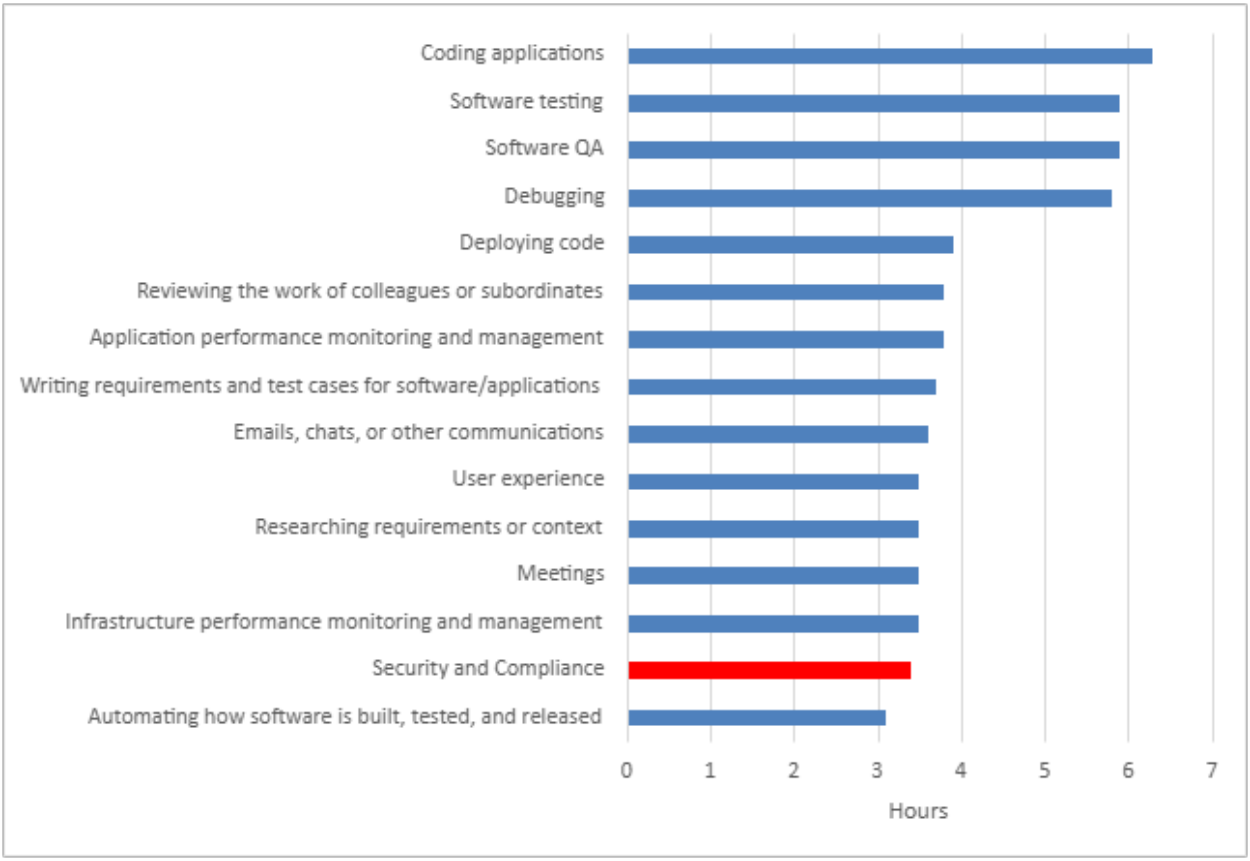
Identity verification is a compliance and security program. It requires depth, currency, and rigor that 3.4 hours a week does not produce. When it gets built by a team allocating that little time to compliance and security, the gaps are not edge cases. They are structural.

Figure 2

Compliance and security get the least attention of any developer activity

Identity verification demands security depth that most engineering teams are not resourced to deliver

Q. How many hours do you spend per week for each of the following activity or task?



n = 524

Note: Data reflects North American organizations only.

Source: IDC's *Software Development Survey* (syndicated), 2025

Every vertical has a regulatory driver

People assume identity verification is a financial services problem. It is not.

Financial services and fintechs have KYC and AML obligations. Hospitals have HIPAA and credentialing requirements. Retailers have state licensing obligations with real consequences when age verification fails. And the person you are hiring or giving system access to may not be who they say they are. A malicious insider who clears onboarding on a fabricated identity is a security problem, a negligent hiring liability and, in regulated industries, a compliance exposure that can take years to unwind.

The industry changes. The driver underneath it does not.

This is a strategy decision

Getting identity right gets you into partnerships, markets, and licensing conversations you could not access otherwise. It produces cleaner examination results and builds institutional credibility that takes years to repair once damaged.

The operational leader wants speed. The compliance leader wants defensibility. The right infrastructure partner resolves that tension. Technology has made that possible in a way it simply was not a decade ago, giving organizations of any size access to enterprise-grade fraud prevention and compliance capability through partnership rather than infrastructure spend.

Identity verification touches every customer you onboard, every employee you hire, and every regulatory relationship you manage. The decision is not a procurement call or an engineering call. It is a strategy call.

The organizations that treat it that way are building a foundation that scales. In an environment where fraud is accelerating and regulatory expectations are rising, that foundation is becoming the difference between companies that grow through complexity and companies that get stopped by it.

I've seen both outcomes. The difference usually traces back to one decision made early.

If this resonates, the conversation does not stop here. We are putting together a deeper look at how organizations are turning identity verification from a cost center into a competitive advantage. If you want to be the first to see it, visit **www.intellicheck.com**. We will make sure it finds you.