Deloitte.

An insurance policy of a different kind

Global insurer reduces complexity, costs, and risks with an IAM transformation

Digital Identity by Deloitte

Insurance	Identity access and management	Managed services | Operate	Corporate cloud
Industry	Core application	Key capabilities	Environment

Cyber Stories

The starting point

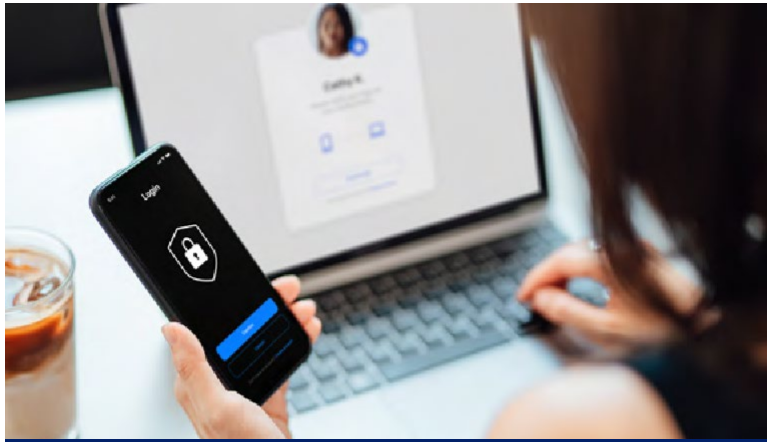
Even insurance companies need insurance—and not just the traditional kind. They need rock-solid safeguards for authenticating the systems, processes, and people at the heart of their business operations. The stakes are massive—and so are the opportunities for would-be attackers.

Not only are insurance companies prime targets for fraudsters and cyber criminals—for anyone looking to use even a small crack to gain entry to valuable data, funds, or other exploitable resources—they also are inherently complex businesses. Layers of sensitive customer data, payment and financial systems, core business apps, proprietary corporate information, and other digital assets—they all provide potential entries for evil-doers.

Airtight and effective identity and access management (IAM) has become essential for insurance leaders who want to ensure that their business systems and processes are also airtight.

Who can have access to which systems and which types of data? Who can access which digital apps and tools? Are the right permissions in place, and how can you constantly manage them? Questions like these can seem simple, but addressing them correctly and continuously requires a clear strategy.

That's why one insurance giant decided to take bold, focused action on a host of interconnected challenges—including costly in-house legacy systems and teams, a complex multivendor landscape, multiple in-flight modernization programs, and a lack of unified customer identities. The company's game plan: to consolidate IAM-related capabilities, transfer responsibilities from the IT organization to information security operations, and follow a new path that would reduce complexity, bolster compliance, and position the company for future needs.



Factors in focus

- ✓ Growing complexity and costs across business operations
- ✓ Multiple vendor relationships in the IAM realm
- ✓ Movement of IAM responsibilities from IT organization to information security operations
- ✓ Ongoing audit and compliance demands

The way forward

Working with Digital Identity by Deloitte, the insurance industry leader undertook a transformative digital identity program that tapped into the power of cloud technology to streamline IAM while also enhancing user experience, boosting compliance, and reducing costs.

The organization selected Digital Identity by Deloitte to design, implement, and operate its enterprise IAM environment, including privileged access management (PAM) and new customer IAM (CIAM) capabilities. The solution was managed and delivered as an innovation and outcomes-based 'Operate' service by Deloitte, moving the company from multiple vendors to a single vendor Deloitte for managing the entire access management landscape—including technology implementation, ticket servicing, and app onboarding.

Deloitte worked with the organization to host the new AM landscape in the client's own AWS cloud environment—with SailPoint for identity governance and administration (IGA), CyberArk for PAM, and Okta for single sign-on and customer IAM. Building a single, integrated program for IAM and related needs required a broad range of capabilities and professionals across the "advise, implement, operate" spectrum—including analysts, engineers, developers, and IT architects, as well as specialists in cloud security operations and network security operations. Functioning as an extension of the client's team, these specialists brought a holistic, problem-solving approach focused on industry-specific needs, strategic objectives, integrated operations, and quality outcomes—rather than just transactions. Deloitte also brought proven processes and methodologies to the project—especially around change management, through a corps of Deloitte organizational change specialists equipped with industry leading practices and standards.

During the transformation journey, the insurer's move to an Operate service was quickly put to the test—with news of a concerning industry breach. Cyberattackers were attempting to learn which businesses had purchased cyber insurance. If they

Insights to inspire

Tackle complexity by thinking beyond your data, processes, and technologies. Zoom out to assess the complexity and the value of your vendor relationships, too.

Look at Operate services as an opportunity to embed continuous advantage—by addressing strategic and unforeseen needs, not just routine transactions.

Don't be reluctant to rethink responsibilities within the enterprise. Just because a project or a need is heavily dependent on IT doesn't mean your IT organization has to "own" it.

could identify cyber-insured companies, the attackers might realize an easier payday—expecting those companies to meet ransomware demands more readily, for example, knowing they were covered by insurance. The insurance company turned to solutions and services provider Deloitte to take action quickly—securing all the external-facing customer apps that touched on its cyber-insurance offerings and enabling multifactor authentication for all of them.

In addition to giving the insurer a more cost-effective managed services relationship that was strategic and proactive rather than merely transactional, the transformation project also brought big benefits in other areas—helping to embed continuous advantage across the company. As part of its move to a central cloud environment and a single vendor through a managed Operate service, the company was able to improve its toolset for supporting audit and compliance needs, provide its customers with a more meaningful and secure sign-on experience, and create a roadmap to guide future ambitions for cloud and access management.

Seamless consolidation of multiple vendors into one client-owned cloud environment, with one managed services provider.

A modern security infrastructure and **reduced cyber risk** profile.

Centralized IAM onboarding of nearly 900 apps from across different platforms.

Cost savings through Deloitte's Operate services and new efficiencies.

An enhanced customer experience with customer IAM.

Effective/efficient controls to guide audit and compliance needs.

A roadmap to guide future cybersecurity and cloud capabilities.

In addition to giving the insurer a more cost-effective managed services relationship that was strategic and proactive rather than merely transactional, the transformation project also brought big benefits in other areas—helping to embed continuous advantage across the company.

Let’s talk cyber

How is your organization insuring itself for today’s and tomorrow’s cyber needs? Discover how Deloitte’s worldwide team of industry-focused specialists can support you every step of the way and help you respond with confidence no matter what the future brings. Contact us to get the conversation started.

www.deloitte.com/digitalidentity
www.deloitte.com/cyber

Contacts

Sunny Aziz
Principal
Deloitte and Touche LLP
saziz@deloitte.com

Anthony Berg
Principal
Deloitte and Touche LLP
antberg@deloitte.com

Naresh Persaud
Managing Director
Deloitte and Touche LLP
napersaud@deloitte.com

Kavitha Beenukumar
Senior Manager
Deloitte and Touche LLP
kbeenukumarrenuka@deloitte.com

Jan Vanhaecht
Global Digital Identity Leader
Partner, Deloitte Belgium
jvanhaecht@deloitte.com

Tim Corder
Digital Identity by Deloitte Product Leader
Managing Director, Deloitte Global
tcorder@deloitte.com

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.