Deloitte.

Insuring the future with a Zero Trust approach

Global leader drives new business value with a modern security architecture

Financial Services
Industry

Zero Trust security architecture
Solution

Cyber Stories

The starting point

For a large global insurance company headquartered in Europe, complexity has been an ongoing reality—one that can have serious implications for security, the costs to support it, and the company's ability to enable new business models. Operating through dozens of entities across the world, the insurance company must not only manage a complex IT landscape and third-party ecosystem but also adhere to an ever-changing framework of regulatory requirements.

Staying compliant, avoiding fines, protecting brand reputation, supporting the business, and efficiently managing systems have become persistent challenges—and corporate imperatives. At the same time, the company has moved rapidly to adopt cloud solutions, provide a modern workforce experience, and embrace globally shared services to control costs.

Amid these complexities and ambitions, the company realized that the traditional perimeters of the enterprise were morphing—driven by cloud adoption, remote work, and reliance on third parties.

Company leaders also realized that their existing security architecture was too complicated and diverse to support the future of the organization. It was costly to support, susceptible to increased cyber and regulatory risks, and delivered an inferior experience for the workforce—requiring multiple employee IDs and no single sign-on (SSO) capabilities in many cases. It was time to rethink the organization's approach to security, and a Zero Trust posture would be critical.

Factors in focus

- Growing business complexity, including global footprint and extensive third-party ecosystem
- Diverse regulatory compliance needs, spanning multiple countries and regions
- Need to control costs and support shared services
- Focus on enabling a modern workforce experience
- Cloud-first business strategy to drive the future of the business

The way forward

With Zero Trust, organizations can adopt the principles of least-privileged access and context-aware authentication—through a "never trust, always verify" approach to providing and continuously validating access to systems and data. It allows users and devices to securely connect to enterprise applications and data over any network, at any time.

But adopting Zero Trust requires comprehensive strategic planning and capabilities, to help create and maintain a risk-based security architecture while also creating a new culture and mindset around Zero Trust.

To begin the Zero Trust journey, the insurer turned to Deloitte, with whom it had already been working on several cyber projects. Deloitte helped the company explore the possibilities for Zero Trust and establish its vision through an interactive lab—allowing organization leaders to understand Zero Trust implementation needs, identify specific challenges, target opportunities for new value, and build consensus on their approach.

After laying a strong foundation through the lab, the insurer collaborated with Deloitte to develop a tailored Zero Trust strategy, including assessing the current landscape, defining initiatives, and establishing a value-based roadmap. As the project moved forward, the two organizations worked together to set up a centralized program with a dedicated team to govern the project, develop a communications strategy, and engage various key stakeholders.

Insights to inspire

Build a vision. Establish consensus for what your Zero Trust journey will look like—including where it will begin, how it will proceed, and how it will unlock bottom-line benefits for your business.

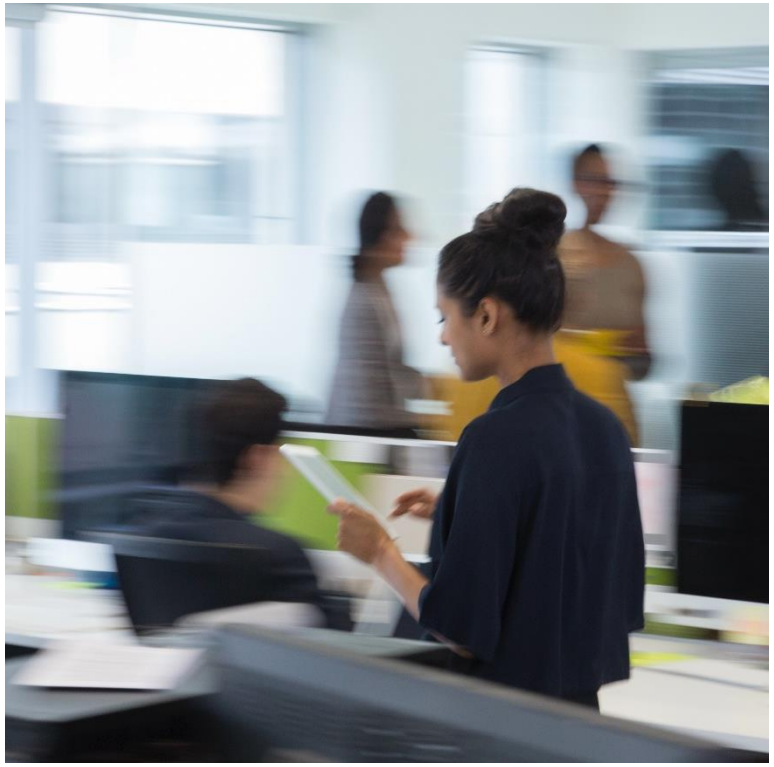
Build a team. Form a central group of specialists who can manage your Zero Trust efforts as a unified program—overseeing everything from compliance to communications strategies.

Build a culture. Shape a new Zero Trust mindset across the enterprise by providing training tools, communicating proactively, and enlisting champions for Zero Trust.

Building a new Zero Trust target architecture, as a "landing zone" for new and existing applications, was central to the work going forward. Deloitte and the insurance company collaborated to design and develop an architecture that encompassed scores of scenarios and use cases, and dozens of technical domains across the company. They also designed the architecture so that it could be scaled across thousands of business applications that the company uses worldwide. The work involved a wide range of professionals, with Deloitte bringing an interdisciplinary Zero Trust team that included specialists in systems architecture, identity, cybersecurity, network and device management, and cloud solutions.

To help shape a new culture and Zero Trust mindset, Deloitte built and launched Zero Trust training materials and communication campaigns for the company, helping promote awareness and enlist Zero Trust champions for the program. The company continues to work with Deloitte as it takes an incremental approach to onboarding employees and rolling out Zero Trust across its technical domains and the regions where it operates.

As it moves forward, the company is already seeing the benefits of its modern security architecture. The transformation has simplified the IT landscape and system access across the enterprise, helped curtail costs, elevated security for critical business processes, sped up implementation of business requirements, and reduced the potential for regulatory risk—while providing a modern experience for the workforce and supporting the company's cloud-first strategy.



The achievements

Reduced complexity and increased standardization across the IT and business process landscape

Greater visibility into the organization's security and regulatory compliance posture—helping reduce risk

A modern security architecture to support a more cyber-resilient organization and future business ambitions

Reduced security maintenance costs, enabling greater investments in innovation for maintaining

An improved employee experience that supports the expectations of the modern workforce

Let’s talk Zero Trust

How will your organization create a modern security architecture that allows you to unlock bottom-line benefits for the business? Discover how Deloitte’s worldwide team of industry-focused cyber specialists can help you identify new opportunities for value with a Zero Trust approach. Contact us to get the conversation started.

deloitte.com/cyber

Contacts

Marius von Spreti
Partner
Cyber Risk Advisory, EMEA
mvonspreti@deloitte.de

Deloitte.

Cyber Stories