Allianz

Edge computing and cyber security

© AdobeStock

ALLIANZ COMMERCIAL

Introduction

Edge computing is transforming the way organizations process and manage data by moving computing from centralized data centers to locations closer to the data source. This shift addresses the limitations of traditional cloud computing, such as high latency, excessive bandwidth consumption, and concerns about data sovereignty (whereby data is subject to the laws and regulations of the country or region where it is collected). Edge computing enables faster decision-making, increased network efficiency and improved security. In industries where real-time data processing is critical — such as healthcare, autonomous vehicles, smart cities, and industrial automation – edge computing enables systems to respond instantly, making it a transformative technology.

The impact of edge computing is evident in market trends, with global investment expected to reach $228bn for 2024, which represents a 14% increase over 2023, and rising to $378bn by 2028.[1] However, while edge computing offers significant benefits, it also presents challenges, particularly in the areas of cyber security and operational management. For sectors such as insurance, where secure, reliable data processing is vital to critical decision-making, harnessing the benefits of edge computing while managing its inherent risks will be essential.

[1] International Data Corporation, Worldwide Spending on Edge Computing Forecast to Reach $378 Billion in 2028, Driven by Demand on Real-time Analytics, Automation, and Enhanced Customer Experiences, September 10, 2024

© AdobeStock

© AdobeStock

The evolution from cloud to edge

As cloud computing struggles with the sheer amount of data produced by businesses, computing ‘at the edge’ can provide solutions to problems such as latency, bandwidth limitations, and data privacy concerns.

Cloud computing has long been the foundation of modern IT infrastructures, offering businesses flexible, scalable solutions for data storage and processing. Over the past decade, the cloud has enabled organizations to outsource the maintenance and management of IT resources, allowing them to focus on innovation and business growth. But the cloud has certain limitations. As businesses generate ever-increasing volumes of data, largely driven by the growth of the Internet of Things (IoT), cloud infrastructures are struggling to keep pace.

One of the key challenges associated with cloud computing is latency. When data must be transmitted across significant distances to centralized data centers for processing, there are unavoidable delays. For applications requiring real-time or near-real-time responses, such as telemedicine, autonomous vehicles, or industrial robotics, this latency is not an option. In addition, the bandwidth required to send substantial data volumes to the cloud can be excessive, which places considerable strain on network infrastructure and leads to increased operational costs.

There is also a growing awareness of the need to address data privacy and security concerns. The transmission of sensitive data to the cloud increases the risk of breaches, while compliance with strict data protection regulations can be complex.

Meeting the demands of the digital world

Edge computing was developed as a solution to these challenges. By processing data at or near the source, it reduces latency, alleviates bandwidth constraints, and enhances data security. Edge computing is not a replacement for cloud computing; rather, it is a complementary solution that decentralizes some computing tasks. In this hybrid model, edge devices are responsible for preliminary data processing and analysis, while the cloud remains the primary location for long-term storage, advanced analytics, and larger-scale data aggregation.

This transition from cloud to edge computing represents a fundamental shift in IT architecture. Organizations adopting edge computing are moving towards a more decentralized approach that allows for faster, more responsive, and more secure data processing. For industries that depend on real-time insights and actions, such as healthcare, manufacturing, and insurance, the evolution from cloud to edge is essential for keeping pace with the growing demands of the digital world.

What does edge computing mean for business?

Edge computing has rapidly become a vital tool for businesses in sectors that rely on real-time data to inform decision-making and drive operational efficiency.

Edge computing is set to be a game-changer in the world of data processing, offering significant benefits in terms of performance, efficiency, and real-time capabilities. The adoption of edge computing presents new opportunities for industries to enhance customer experiences, improve risk management, and offer more personalized products. However, the transition towards decentralized data processing also presents a range of new challenges, particularly in the context of cyber security.

For businesses in sectors such as manufacturing, healthcare, retail, and finance, the ability to process data locally provides a competitive advantage. A recent survey of C-level executives in 18 industries across 16 countries found 83% believe edge computing will be essential to remaining competitive in the future. Meanwhile, 81% think failure to act quickly could lock them out from the full benefits of the technology.[2]

Rapid response potential

In the manufacturing sector, edge computing facilitates real-time monitoring of production lines, enabling operators to respond rapidly to potential issues. This results in reduced downtime, increased efficiency and, ultimately, cost savings. The capacity to act on real-time data is of particular importance in industries where even a few seconds of delay can result in significant losses.

The rapid expansion of IoT devices highlights the need for localized data processing, as these devices generate vast quantities of information that must be processed promptly to provide actionable insights. A 2023 survey into the commercial adoption of IoT and edge computing found 64% of respondents were deploying IoT solutions, and 33% of respondents were already using edge computing solutions, with an additional 30% indicating plans to deploy within the next 24 months.[3]

In the healthcare sector, edge computing is transforming the way patients are monitored in real-time and how diagnostics are conducted. The generation of data from wearable devices and smart medical equipment can be processed ‘at the edge’, providing healthcare providers with instant feedback and improving patient outcomes. With telemedicine, real-time processing of health metrics enables doctors to make prompt decisions, which is crucial in emergency situations.

The personal touch

Edge computing is also proving beneficial for retailers and financial institutions. In the retail sector, edge computing is facilitating the delivery of personalized customer experiences through the processing of data at the point of sale, enabling the provision of real-time product recommendations and dynamic pricing adjustments. In financial services, edge computing improves fraud detection and speeds up transaction processing, enhancing both security and customer satisfaction.

By maintaining sensitive data at the local level, businesses can also comply more readily with rigorous data privacy regulations, reducing the risk of exposure and breaches.

Edge computing is transforming how businesses operate by providing faster, more efficient, and more secure methods of data processing. As industries continue to generate vast amounts of data from IoT devices and other sources, edge computing will play an increasingly vital role in ensuring that data is processed and acted upon in real-time.

[2] Accenture, Leading with Edge Computing: How to reinvent with data and AI, 2023
[3] Eclipse IoT, 2023 IoT & Edge Commercial Adoption Survey Report

Cyber security challenges

A vast array of devices and an expanded attack surface present challenges to maintaining security and integrity with edge computing. A robust and tailored response is essential.

While edge computing offers numerous benefits, it also presents a range of cyber security challenges. One of the most significant risks is the expansion of the attack surface due to the distributed nature of edge devices. In contrast to traditional cloud environments, where data processing takes place in centralized, secure data centers, edge computing involves multiple endpoints that are frequently deployed in remote or uncontrolled locations. The decentralization of edge computing creates a greater number of potential entry points for cyber-attacks.

The heterogeneity of devices used in edge computing systems exacerbates security vulnerabilities. Edge environments often include a diverse array of devices from various manufacturers, each with its own operating system, firmware, and communication protocols. This lack of standardization increases the complexity of securing the system as a whole, creating inconsistencies that attackers can exploit. Devices that lack regular updates, use outdated protocols, or have weak default configurations can serve as weak links, compromising the entire network.

Implement specific security measures

Ensuring the integrity and privacy of data is another critical issue. The processing of data across multiple devices and locations presents significant challenges in maintaining security and integrity. Limited processing power and storage capacity in many edge devices make it difficult to implement traditional security measures such as strong encryption or intrusion detection systems. These devices can also be vulnerable to physical tampering, particularly when used in public or less secure settings.

To address these challenges, organizations must implement robust endpoint security solutions tailored to the specific requirements of edge devices. This includes lightweight encryption protocols, secure boot processes, and continuous monitoring to detect and respond to potential threats in real-time. It is equally important to ensure secure communication between edge devices and central networks, using advanced encryption techniques and secure communication protocols such as TLS/SSL (Transport Layer Security/Secure Sockets Layer).

Addressing the lack of standardization requires industry-wide efforts to establish and enforce uniform security standards for edge devices. Manufacturers and organizations should collaborate to develop and adopt frameworks that ensure interoperability and consistent security practices. This could include common certification standards for device security, regular patching mechanisms, and unified protocols for secure communication.

Multiple jurisdictions means multiple regulations

Edge computing frequently involves processing data across multiple geographic regions, each with its own set of regulatory requirements. Meeting these diverse regulations, such as GDPR (General Data Protection Regulation) in Europe or HIPAA (Health Insurance Portability and Accountability Act) in the US, can be complex. Organizations must develop comprehensive data governance strategies to guarantee that data processed at the edge is protected in accordance with local laws.

By addressing these challenges – including the heterogeneity of devices and lack of standardization – organizations can unlock the full potential of edge computing while minimizing the cyber-security risks it presents. Comprehensive security frameworks, continuous monitoring, and industry collaboration are essential to safeguarding edge environments in an increasingly connected world.

© AdobeStock

How does edge computing impact the insurance industry?

Insurers and their customers can benefit from the efficiencies enabled by edge computing, including faster claims processing, personalized innovations, and the integration of real-time data.

Edge computing can transform the insurance industry by enabling real-time data processing at its source. Unlike traditional cloud systems, edge computing reduces latency, accelerates decision-making, and enables localized analysis. This shift addresses challenges in claims processing, pricing models, and fraud detection while introducing considerations for cyber security and liability management.

Streamlining claims processing

Claims processing has historically been labor-intensive, involving data collection, manual reviews, and delays. These inefficiencies increase costs and reduce customer satisfaction. Edge computing automates workflows and enables real-time data analysis to mitigate these issues.

IoT devices such as industrial sensors, building management systems, and fleet telematics are central to this transformation. Smart sensors in commercial buildings and industrial plants monitor equipment performance, environmental conditions, and security, allowing insurers to assess risks and streamline claims related to mechanical failures, fires, or structural damage. For example, sensors detecting overheating machinery or gas leaks can trigger early intervention, preventing extensive damage and expediting insurance responses. In fleet management, telematics devices track vehicle usage, driver behavior, and accident conditions, providing immediate data on factors like speed, impact severity, and location. This allows insurers to validate claims efficiently and assess liability more accurately.

Edge computing also strengthens fraud detection by instantly analyzing event data. Inconsistencies between reported claims and actual conditions can be flagged in real-time, protecting insurers from financial losses and fostering customer trust.

Driving personalized insurance models

Edge computing fuels personalized insurance innovations like telematics and usage-based insurance (UBI). Telematics devices monitor driving behaviors, enabling dynamic premium calculations based on real-time risk factors. Safe drivers benefit from lower premiums, while risky behavior results in higher rates.

This personalization extends to health and property insurance. Wearable devices monitor metrics like activity levels and heart rates, allowing insurers to offer tailored plans or adjust premiums dynamically. Smart home sensors detecting risks such as fires or burglaries enable insurers to adjust policies proactively.

Predictive analytics, enhanced by edge computing, amplifies these benefits by integrating real-time data with factors like weather and traffic. In automotive insurance, edge-based analytics forecast accident risks and alert drivers. In commercial settings, predictive maintenance powered by edge computing prevents costly equipment failures, benefitting insurers and clients alike.

Navigating cyber security risks and liability challenges
Despite its advantages, edge computing introduces significant cyber security risks. Its decentralized nature increases the attack surface, making devices more vulnerable to breaches, data theft, and disruptions. Insurers must adjust risk models and develop specialized products to address incidents involving edge devices, including coverage for breaches, business interruptions, and recovery costs.

Liability determination in edge environments is particularly complex. Responsibility for breaches often spans device manufacturers, software providers, and users. Insurers must define liability terms clearly in policies, ensuring comprehensive protection for all stakeholders.

Balancing innovation with risk management
To fully realize edge computing's potential, insurers must invest in research and development and form strategic partnerships with technology providers. Staying ahead of advancements enables the design of products that meet evolving needs while addressing emerging risks. Tailored incident response services for distributed edge environments are also vital for operational resilience.

Edge computing offers the insurance industry faster claims processing, more accurate pricing, and enhanced customer engagement. However, it requires robust approaches to cyber security and liability management. Insurers that balance innovation with effective risk mitigation will unlock significant value, redefine customer experiences, and strengthen their position in a data-driven world.

© AdobeStock

Allianz Commercial:

Medhi Meyer
Cyber Risk Consultant
medhi.meyer@allianz.com

Rishi Baviskar
Global Head of Cyber Risk Consulting
rishi.baviskar@allianz.com

For more information contact
az.commercial.communications@allianz.com

Follow Allianz Commercial on LinkedIn

www.commercial.allianz.com

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions. All descriptions of insurance coverage are subject to the terms, conditions and exclusions contained in the individual policy. Any queries relating to insurance cover should be made with your local contact in underwriting and/or broker. Any references to third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz of the content of such third-party websites. Neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group is responsible for the content of such third-party websites and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group does make any representations regarding the content or accuracy of materials on such third-party websites.

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.
Commercial Register: Munich, HRB 208312

March 2025