Edge Computing & Cybersecurity:

A New Frontier in Securing Critical Infrastructure

Akkodis Group Nordics

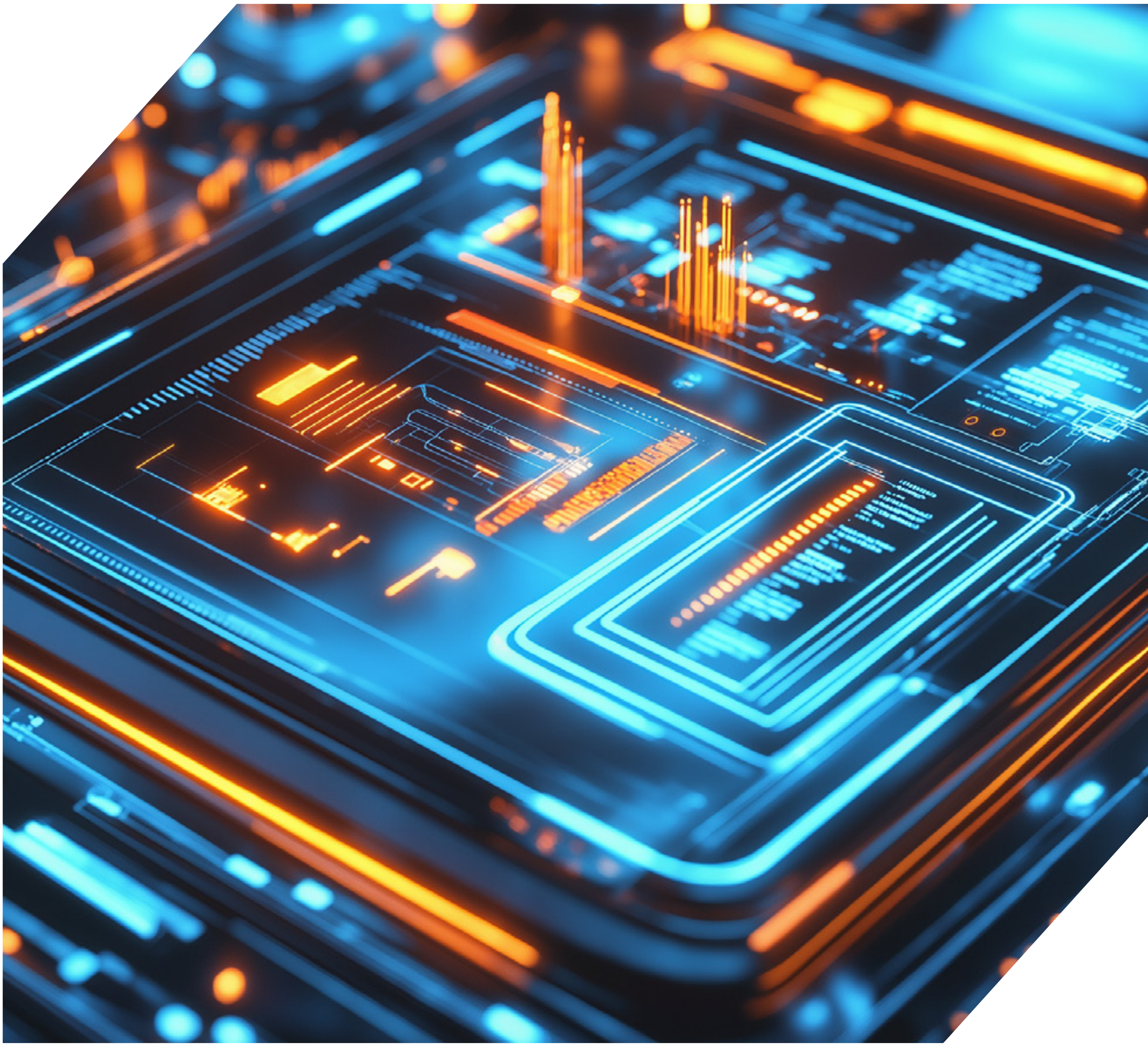


Table of Contents

A New Era of Localized Security

As industries like defense, energy, maritime, and transportation become more connected, the demand for secure, real-time data processing is rising. Edge computing is meeting this demand by moving data processing closer to its source. This approach not only enhances efficiency but also strengthens cybersecurity, offering critical protection for sensitive data and essential operations.

How Edge Computing Enhances Data Security

Edge computing enhances data security by processing data locally and reducing reliance on central servers. With fewer data transfers, the risk of interception by cybercriminals is lowered. The decentralized structure of edge computing minimizes single points of failure, making it harder for attackers to compromise the entire network. Real-time monitoring on edge devices enables instant threat detection and response.

Additionally, on-site devices benefit from physical security measures that restrict unauthorized access, providing an extra layer of protection.

Less Data in Transit, Less Risk

Processing data locally means fewer data transfers over potentially vulnerable networks. This limits the risk of data interception, making it harder for cybercriminals to exploit in-transit information.

Decentralization for Greater Security

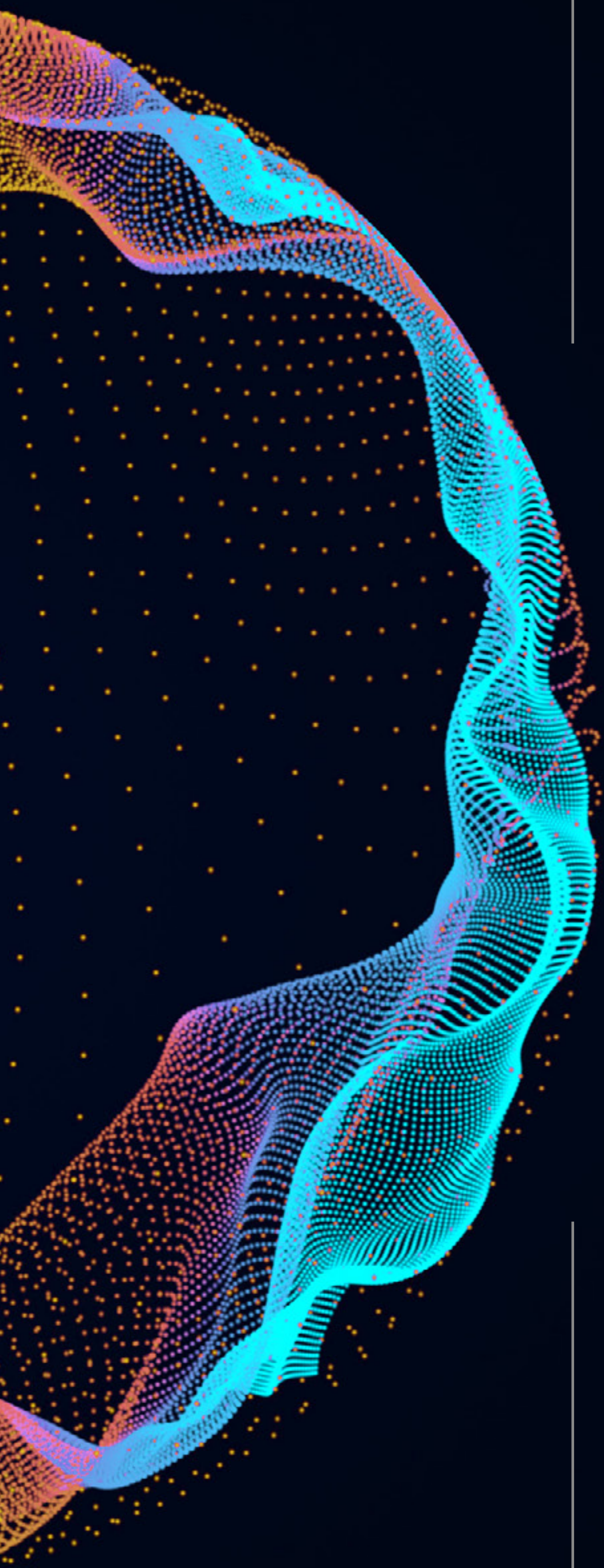
Edge computing distributes data across local devices rather than a central server. This decentralization reduces the system's single points of failure, making it much harder for attackers to access an entire network.

On-the-Spot Anomaly Detection

Edge devices can monitor activity in real-time and quickly react to security threats. By detecting suspicious behavior on-site, they can immediately block or isolate attacks without waiting for central server instructions.

Stronger Physical Security

Edge devices can monitor activity in real-time and quickly react to security threats. By detecting suspicious behavior on-site, they can immediately block or isolate attacks without waiting for central server instructions.



Edge Computing vs. Cloud: Security at the Edge

Faster Response

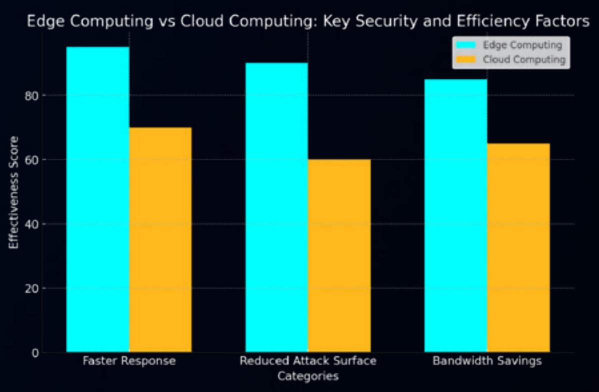
Edge systems process data on-site, allowing them to act on threats instantly. In contrast, cloud solutions require data to travel back and forth, creating potential delays in detecting and responding to issues

Reduced Attack Surface

With the cloud, vast amounts of data are centralized and thus more appealing to cyber attackers. Edge spreads data across multiple points, which reduces the appeal and accessibility of a single-target attack

Bandwidth Savings

Edge devices process and store data locally, reducing dependency on the cloud and lowering both the volume of data sent and associated security risks



How Edge Reduces Operational Costs

Lower Data Transfer Costs

By processing data on-site, edge computing reduces the amount of data sent to central or cloud servers, lowering bandwidth expenses

Reduced Cloud Storage Needs

Edge devices reduce the reliance on costly cloud storage by handling real-time processing locally and ensuring only the most critical, actionable insights—smart data—are sent to the cloud. This optimized approach delivers the best of both worlds: local agility with global intelligence.

Minimized Latency-Related Costs

Localized decision-making prevents costly delays and downtime, enhancing operational efficiency.

Efficient Resource Allocation

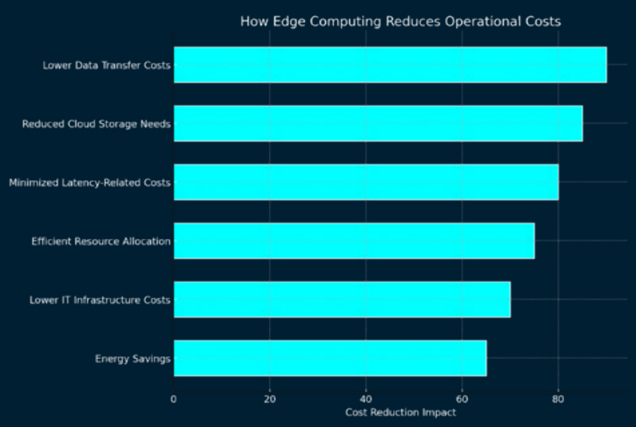
Localized data handling frees up cloud resources for high-priority tasks only, avoiding overuse charges.

Lower IT Infrastructure Costs

Edge reduces the need for extensive central infrastructure, minimizing setup and maintenance costs.

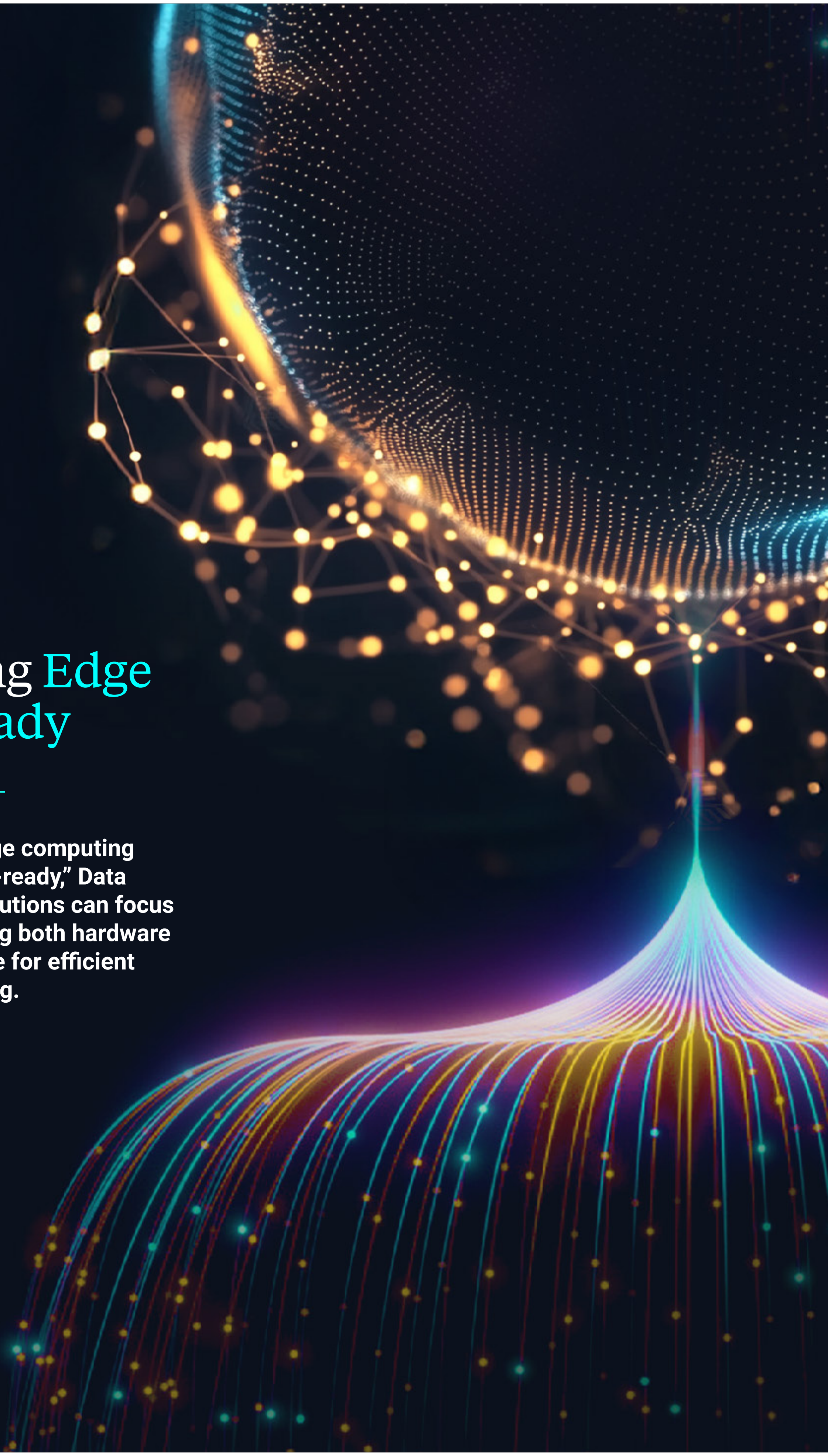
Energy Savings

Edge devices use less energy by reducing data transmission and allowing for more energy-efficient operations, especially in remote locations.



Making Edge AI-Ready

To make edge computing systems "AI-ready," Data Respons Solutions can focus on optimizing both hardware and software for efficient AI processing.



1 Hardware Optimization for AI Workloads

Service: Select or customize hardware (e.g., GPUs, FPGAs, or specialized edge processors) that can efficiently handle AI algorithms directly on the edge device.

Focus: Ensuring that edge devices have the necessary computational power to perform real-time AI tasks, like image recognition, anomaly detection, or predictive maintenance.

2 Lightweight AI Model Development

Service: Develop or optimize AI models specifically for edge environments, focusing on smaller, domain-specific models with minimal latency and high accuracy.

Focus: Streamlining models to ensure they work within the limited processing capabilities of edge devices without compromising performance.

3 Edge AI Software Integration and Deployment

Service: Integrate edge AI frameworks (like TensorFlow Lite or PyTorch Mobile) and optimize AI software to run efficiently on edge hardware.

Focus: Enabling edge devices to process AI tasks independently, reducing latency and reliance on cloud-based AI processing.

4 Data Management for Edge AI

Service: Design data pipelines to manage data flows that AI models rely on, storing data locally as needed while synchronizing with central systems.

Focus: Providing efficient data handling to support continuous learning and updating of AI models on edge devices.

5 Edge AI Monitoring and Optimization

Service: Monitor AI model performance on edge devices, providing periodic updates, optimizations, or retraining as necessary to ensure model accuracy.

Focus: Maintaining AI readiness over time, allowing for seamless updates and adapting AI to new data patterns or environmental changes.

Key Risks of Using Edge Computing

Increased Attack Surface

Each edge device adds a new point of entry, making it challenging to secure all devices effectively.

Physical Security Risks

Edge devices in remote or unsecured locations can be vulnerable to tampering or theft.

Data Consistency Challenges:

Managing data across multiple edge devices can create issues with data consistency and accuracy.

Limited Processing Power

Edge devices have limited capacity, which can lead to performance issues for complex tasks.

Maintenance and Reliability

Distributed devices can be harder and more costly to maintain, with individual failures potentially disrupting operations.

Data Privacy and Compliance

Ensuring each edge device meets compliance standards is complex and requires robust security configurations.

Network Dependencies

Edge devices may still rely on networks for data sharing, which can be problematic in areas with unreliable connectivity.

Scaling Complexity

Expanding edge infrastructure across multiple locations can become complex without robust management tools.

NIS 2 Compliance: Essential for Critical Sectors

NIS 2, a directive from the EU, mandates that operators in essential sectors implement stringent cybersecurity protocols. Here's what it entails:

Risk Management

Regular assessments of cybersecurity risks with tailored security measures.

Incident Reporting

Organizations must report cybersecurity incidents swiftly, ensuring rapid response and transparency.

Access Control

Strict controls to prevent unauthorized access to sensitive data and systems.

Supply Chain Security

Security checks are required for all suppliers, ensuring that risks are managed across the full network.

NIS 2 compliance builds trust and enhances resilience, especially in critical sectors like defense, energy, maritime, and transportation.

Edge Computing’s Cybersecurity Benefits in Key Sectors

Edge powers autonomous and connected transport with low-latency, high-security solutions, protecting passengers and infrastructure.

Edge enables fast, local responses to grid issues, helping maintain service reliability while meeting strict cybersecurity standards.

By processing data on-site, edge computing supports remote, secure operations even in environments with limited connectivity.

Real-time, localized data processing enhances operational security and resilience against attacks on sensitive data.

Conclusion:
Edge Computing as a Cybersecurity and Cost-Saving Asset

Edge computing isn’t just a technology upgrade; it’s a powerful security and costsaving enhancement. By keeping data close to its source, minimizing transmission, and using a decentralized architecture, edge computing builds resilience against cyber threats. Combined with NIS 2 compliance, it offers critical sectors like defense, energy, maritime, and transportation a secure, efficient, and future-ready infrastructure.

How we can help:

Services to Support Edge Computing and NIS 2 Compliance

Edge Infrastructure Design and Deployment

Design edge computing architectures optimized for each client's specific industry needs. Customizing robust, localized solutions that can handle real-time processing, environmental constraints, and ensure data consistency

NIS 2 Compliance Assessment and Consulting

Conduct compliance assessments, providing gap analysis and tailored recommendations to meet NIS 2 requirements.

Implementing risk management protocols, data access controls, incident response plans, and supply chain security measures aligned with NIS 2.

Edge Device Management and Monitoring

Deploy and manage edge devices with monitoring systems that provide real-time data and security alerts, ensuring resilience and continuity.

Maintaining device health, managing data storage needs, and enabling remote updates to keep edge infrastructure secure and efficient.

Data Consistency and Synchronization Solutions

Implement data management frameworks to ensure data consistency across distributed edge devices, reducing risks of data errors or inconsistencies.

Developing solutions that synchronize data when connectivity permits, ensuring accuracy and compliance across all edge devices.

Regulatory Documentation and Training

Prepare NIS 2 compliance documentation and train client teams on cybersecurity best practices, regulatory requirements, and edge-specific protocols.

Ensuring that clients are fully equipped to maintain compliance independently and securely manage edge infrastructure.

Engineering a Smarter Future Together.

Contact

Birger A. Sundet
Sales Director

sales@datarespons.com