SECURING THE EDGE

Best Practices for Edge Computing Security

Connection®
we solve IT®

TABLE OF CONTENTS

03 INTRODUCTION

04 OVERVIEW OF CHALLENGES IN SECURING THE EDGE

05 BEST PRACTICES FOR EDGE COMPUTING SECURITY

08 STRATEGIES FOR INTEGRATING EDGE AND CLOUD SECURITY

09 EMERGING TRENDS AND FUTURE CONSIDERATIONS IN EDGE COMPUTING SECURITY

10 CONTACT CONNECTION

INTRODUCTION

As edge computing continues to be adopted across industries, especially for applications that require real-time data processing, there has also been an increased focus on edge security. The decentralized nature of edge computing creates a number of vulnerabilities, making robust security measures imperative.

This guide explores the security challenges of edge computing and what the best practices are to increase edge computing security.

OVERVIEW OF CHALLENGES IN SECURING THE EDGE

Securing the edge presents unique challenges, with network complexity standing out as a significant hurdle. The distributed nature of edge computing involves a multitude of interconnected devices, each requiring secure communication and protection. Implementing robust network segmentation and access controls becomes complex when dealing with a vast array of edge devices. Addressing this challenge requires a holistic approach that combines advanced networking solutions such as Software-Defined Networking (SDN), with adaptive security policies.

Another significant challenge for edge security is managing data in distributed environments. The decentralized nature of edge computing means that sensitive data is generated and processed across a diverse set of locations. Ensuring data integrity, confidentiality, and compliance with privacy regulations becomes a complex endeavor. Organizations need to implement robust data governance strategies that encompass encryption, access controls, and secure data transmission protocols. Addressing this challenge involves adopting edge-native security solutions that empower organizations to exert control over data across its entire lifecycle, from creation to storage and transmission.

BEST PRACTICES FOR EDGE COMPUTING SECURITY

Securing the edge in a distributed computing environment requires a holistic approach encompassing both hardware and software elements. Here are best practices recommended to enhance the security of edge computing:

Implement Robust Access Controls

In an edge computing environment, where distributed devices may be geographically dispersed, robust access controls become instrumental in restricting interactions with edge systems to only authorized personnel or devices to prevent unauthorized access. This involves defining clear rules and permissions. The implementation of strong authentication mechanisms, such as multi-factor authentication (MFA), adds an extra layer of identity verification.

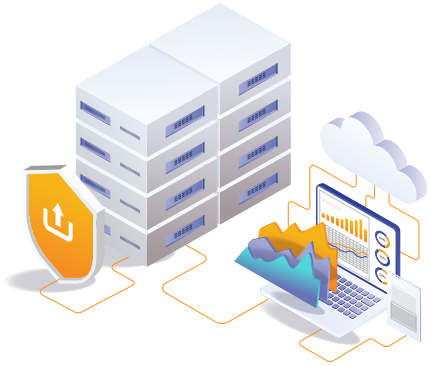
Encrypt Data in Transit and at Rest

Employing end-to-end encryption for data transmitted between edge devices and central systems adds a layer of protection, preventing unauthorized interception and ensuring the confidentiality of information during transit. Additionally, encrypting stored data on edge devices is crucial to securing sensitive information, especially in scenarios where physical access might be compromised. This ensures that even if a device falls into the wrong hands, the encrypted data remains unintelligible, maintaining the integrity and confidentiality of critical assets within the edge computing infrastructure.

Continuous Monitoring and Intrusion Detection

Implementing real-time monitoring solutions enables the prompt detection of unusual activities or potential security breaches within the edge environment. By deploying intrusion detection systems (IDS), organizations can proactively identify and respond to malicious activities, enhancing the overall security posture of the edge computing infrastructure. This vigilant monitoring ensures that any anomalies or unauthorized access attempts are swiftly identified and addressed, minimizing the risk of security incidents and fortifying the resilience of edge systems against potential threats.

BEST PRACTICES FOR EDGE COMPUTING SECURITY
(CONTINUED)



Update and Patch Management

A proactive approach to update and patch management, with regular updating and patching of both operating systems and software applications on edge devices, is crucial to addressing known vulnerabilities and maintaining a resilient security posture. Because edge devices are dispersed across various locations, it can be challenging to implement updates uniformly. The limited bandwidth and connectivity issues associated with some edge environments also pose constraints, requiring organizations to optimize the update process to minimize disruptions. Additionally, the diverse range of edge devices, each with its own specifications and requirements, adds complexity to the update management strategy. Therefore, a systematic and tailored approach is necessary to navigate these challenges, ensuring that updates are applied efficiently without compromising the availability and performance of edge systems.

Incident Response Planning

The development of an incident response plan and regular testing that is tailored to edge computing environments is crucial. Any incident response plan should outline clear procedures for detecting, responding to, and recovering from security incidents. Proactive measures, such as threat intelligence sharing and scenario-based simulations, enhance the readiness of incident response teams. It is also important that personnel are well-trained to follow established protocols in the event of a security breach.

Edge Device Authentication

To fortify security at the device level, edge device authentication mechanisms must be strengthened. To prevent unauthorized access across a diverse range of devices in edge deployments, use secure boot processes and hardware-based authentication, where applicable.

Data Integrity Verification

It's important to implement mechanisms to protect against tampering during transmission or storage and to verify the integrity of data at both the source and destination by using checksums, digital signatures, or blockchain technology.

BEST PRACTICES FOR EDGE COMPUTING SECURITY
(CONTINUED)

Collaboration with Security Partners

Selecting secure edge computing partners requires a thorough evaluation of their security posture. This involves assessing their commitment to security, the robustness of their security measures, and their track record in delivering secure solutions. Collaborating with partners who prioritize security in their products and services contributes to building a resilient edge infrastructure. Establishing clear expectations regarding security standards and compliance, along with regular audits and assessments, ensures ongoing adherence to security best practices throughout the partner-client relationship.

Employee Training Awareness

Providing thorough training to personnel involved in managing and maintaining edge environments is an essential security best practice. Fostering a culture of cybersecurity awareness helps mitigate risks associated with social engineering and insider threats.

STRATEGIES FOR INTEGRATING EDGE AND CLOUD SECURITY

Integrating edge and cloud security seamlessly is critical for creating a cohesive and resilient cybersecurity infrastructure. However, integration of edge and cloud security involves a multifaceted approach. Organizations need to adopt a unified security framework that encompasses both edge and cloud components. This includes leveraging cloud-native security services that extend to the edge and integrating edge-specific security solutions.

Implementing identity and access management (IAM) solutions consistently across the edge and cloud is crucial. Additionally, adopting a Zero Trust security model, which assumes that no entity inside or outside the organization's network should be trusted by default, is an effective strategy for reinforcing security at the convergence of edge and cloud.

EMERGING TRENDS AND FUTURE CONSIDERATIONS IN EDGE COMPUTING SECURITY

The future of edge security will be shaped by adaptability and scalability. Edge computing is expected to witness increased integration with 5G networks, presenting both opportunities and challenges for security. As edge devices become more diverse, future security measures must be agile enough to accommodate various use cases and device types. Standardization efforts will play a crucial role in streamlining security practices across different edge implementations.

Additionally, the ongoing evolution of regulatory frameworks will impact edge security considerations, requiring organizations to stay proactive in aligning their security postures with emerging standards and compliance requirements.

At the same time, advancements in technologies that enhance protection and resilience, including lightweight security protocols and encryption mechanisms optimized for resource-constrained devices, are gaining prominence. Machine learning and AI-driven threat detection capabilities are being integrated into edge security systems, enabling real-time identification of anomalies and potential security breaches. As edge architectures evolve, security technologies are adapting to provide granular control, visibility, and threat intelligence across diverse edge environments.

Fostering a proactive approach to edge security is paramount in addressing the challenges and embracing the evolving trends in this dynamic landscape. By prioritizing robust network strategies, data governance, and staying abreast of emerging technologies, organizations can fortify their edge environments, ensuring a secure and resilient foundation for the future of computing.

COTACT CONNECTION

If you need help getting started with an edge computing strategy or implementation, reach out to your Account Manager or contact us for more information.

Connection®
we solve IT®

1.800.800.0014
www.connection.com/EdgeComputing

Connection®

we solve IT®

1.800.800.0014 ■ www.connection.com