

## EDGE COMPUTING: THE 4<sup>th</sup> INDUSTRIAL REVOLUTION

#### Introduction

We're on the cusp of the next major advance in infrastructure modernization. The traditional data center is nearly dead. The future is in Industry 4.0. Within this marriage of cyber and physical systems, trends in automation, connectivity, processes, and data exchange are shifting. Enterprises have found that advanced sensors that communicate with edge devices, edge networks, and edge data centers can offer higher levels of responsiveness, output, and efficiency than previous generations of infrastructure.

Although edge infrastructure adoption remains in its infancy, by 2025, the market is expected to reach a valuation of \$250 billion.<sup>1</sup> New edge infrastructure is designed to reduce latency, enhance system reliability, optimize for 5G and yield security advantages. Nonetheless, edge infrastructure also requires security. We're not in Kansas anymore and your data is no longer in a centralized data center or a cloud environment.

#### The edge evolves

A growing number of modern enterprises rely on data for real-time decision making. Sensors that can process data quickly can increase productivity and results. In a classic example, a self-driving car that must transmit data to a far-off processing center can present a more agile and efficient response to traffic pattern shift when processing data at the edge.

Business leaders everywhere are looking to reduce latency in order to increase operational efficiency. Lower latency not only solves older business problems; it can offer new opportunities for innovation too.



In the case of a self-driving car, an information processing delay could result in a dangerous situation.

## System reliability

The edge also eliminates a central point of failure. Previously, a single data center that experienced a disruption could have significant downstream effects across organizations and verticals. The decentralized nature of the edge disposes of this difficulty. Rather, edge enables organizations to isolate disrupted or attacked systems quickly and easily.

## Edge computing and 5G

At the end of the day, edge computing is designed to allow for hyper-communication and seamless interactions between disparate industrial machinery, computers, robots, and independent systems. While that's not the only rationale for the continued evolution of edge, it's a strong case. In order to enable smooth inter-device functionality, edge is often deployed in tandem with 5G rollouts. As a result, business leaders can transform business connectivity and capabilities. For many organizations, edge and 5G together can unlock unprecedented value add.

In addition, as organizations load hundreds or thousands of new devices onto networks and data from each device hits servers and storage systems, bandwidth can quickly become overwhelmed. The introduction of both edge and 5G together can conquer this challenge. Many continued technology developments and new business ventures will only be possible through the unified use of edge and 5G.



By 2022, over 55 billion edge devices will be on the market.

By 2025, estimates expect that number to hit 150 billion.<sup>2</sup>

2 https://www.ibm.com/blogs/industries/rob-high-edge-computing/



#### Edge has long existed in certain industries.

Retail chains, hospitality franchises and other groups have proven ROI in relation to edge computing. Yet, many of these edge solutions were custom-tailored to individual organizations. The new ubiquity of edge and mass-production of edge infrastructure means that other industries are beginning to buy-in. Purchasing edge as a pre-fab package also means that organizations can deploy it more quickly than otherwise and that there are fewer technical risks.

#### Is your industry next?

Industries that are quickly capitalizing on edge operations include telecommunications, manufacturing, military service providers, and healthcare. In more ways than one, edge computing can offer organizations of all kinds an edge over the competition.

#### Security advantages

Organizations that handle sensitive client data often opt for edge due to increased capacity for security monitoring and control. More centralized monitoring and control can mean fewer issues. From educational institutions to medical facilities, this aspect of the edge is appealing. The potential for cyber theft, physical theft and data leakage diminishes. For example, when storing biometric data in an owned edge server, fewer opportunities exist for third-party breaches.

Further, use of edge requires less physical space than traditional data centers and can be less clunky than cloud storage centers. As a result, organizations that rely on edge may have less real-estate to secure. This translates to fewer potential endpoints for hackers to exploit.

#### Other benefits

Edge computing offers a variety of benefits for businesses. Often overlooked advantages include:

- Fewer demands on cloud bandwidth, which can mean faster data processing all-around.
- Decreased server resource requirements.
- A "green" appeal, as smaller distributed environments can prove more ecologically friendly due to their smaller energy consumption demands.
- More cost-effective cooling systems; as it can be cheaper to cool down a series of smaller spaces than larger ones.
- If we move away from cloud storage, could we finally say goodbye to misconfigurations as a top cause of cloud-based breaches?

# What is the difference between edge computing and fog?

The edge and fog are similar, as they both push data processing and analysis to locations that are close to the data's origin. Edge computing typically either occurs on the device's sensors, or in a gateway that is on the device. Fog computing involves processing information on LAN hardware, making processing and analysis ever so slightly more distant from the device itself.

#### Securing your edge

As with IoT, the design of edge computing took place first, and security surfaced as an afterthought. The evolution of security mechanisms for edge computing has not kept pace with the evolution of the edge itself. When deploying edge-based infrastructure, as a surface-level safeguard, be sure to apply two factor authentication, and to manage your passwords.

On a more technical level, ensure that your organization deploys data-at-rest encryption, boot time integrity checks, hardware, and software attestation regarding identity. The latter can provide opportunities for increases in manageability and security via network-and-SaaS-based platforms. In addition, for your cloud-to-edge security set up, ensure that you rely on zero trust network access (ZTNA) to verify and monitor edge to cloud connections.

For edge devices and software in the cloud, enterprises can attach nano agents. This provides effective security for fully distributed environments. Nano agents can monitor IoT, OT and edge devices to identify potential cyber attacks. They search for both known attacks and anomalies that reflect attempts to exploit zero-day vulnerabilities. If a threat appears imminent, nano agent technology can block attack or alert security teams.

Enterprise-grade security implementation, combined with orchestration, oversight, and device management can feel like an intimidating mission. For organizations invested in cloud security solutions, obtaining adequate edge security could be as simple as reaching out to your security provider. For example, Check Point Software now offers edge security through Equinix Network Edge. Network Edge is a virtual networking service that allows customers to extend into more locations by establishing a virtual point of presence within Equinix data centers. This joint solution gives customers the ability to deploy edge security on top of cloud security infrastructure within minutes; anywhere in the world.<sup>3</sup>

3 Network Edge-Modernize Your Network, Virtually, Equinix <u>https://www.equinix.com/resources/data-sheets/modernize-your-network</u>



#### Conclusion

At present, organizations are reevaluating architecture needs and all the more so in light of the ongoing coronavirus pandemic and remote work. The advantages of edge computing offer wide appeal. The evolution of edge computing remains ongoing, however edge and ultra-connectivity are about to revolutionize business and tech. Will your enterprise be ready? Ensure that you have the right planning and resources to secure your edge infrastructure.

#### Case study

When Starkey Hearing Technologies needed to secure edge-compatible technologies, they turned to a trusted vendor. "Modern malware changes every day," said Starkey's IT Manager of Network Services, Joe Honnold. "We needed more advanced capabilities to protect our laptops and other edge devices. We called Check Point and asked how we could better leverage our Check Point gateway infrastructure to increase our protection."<sup>4</sup>

For more information about how you can secure your edge, reach out to your Check Point sales representative. For additional cyber security thought leadership insights, visit <u>Cyber Talk</u>.

4 Check Point Software Technologies LTD, Starkey, <u>https://www.checkpoint.com/customer-stories/starkey-hearing-technologies/</u>

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

#### www.checkpoint.com

© 2021 Check Point Software Technologies Ltd. All rights reserved.