LTIMindtree

WHITE PAPER

Secure Edge Computing

On-the-edge data protection with always-on security approach

Vishwas Samant, Principal Enterprise Architect – CIS LTIMindtree
Punit Joshi, Senior Specialist - Network– CIS LTIMindtree

Table of Contents

Abstract

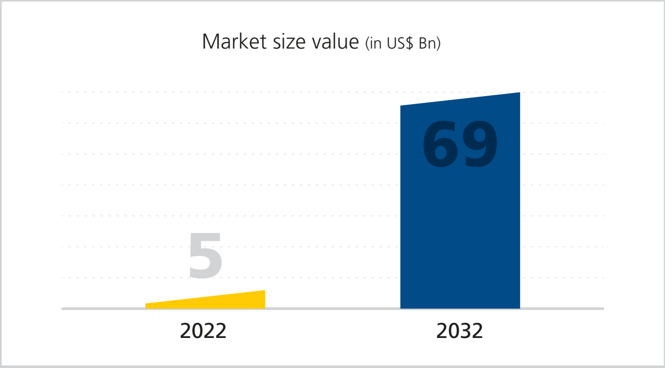
Today’s enterprises know that it is critical to ensure the security of their IT (Information Technology) environments, and the security present in traditional on-premise networks and the cloud is extended to the edge. This whitepaper provides enterprises with the foundations for implementing an in-depth security strategy at the edge by addressing four areas of security at the edge:

- Platform security at edge locations
- Data security in transit and at rest
- How those services and others can be used to implement the security best practices outlined in the design principles of the edge
- The security aspects of additional edge services, which enterprises can use to help secure their edge environments or expand operations into new environments

The above four elements offer core principles for designing a security strategy at the edge, and demonstrate how services can provide a secure environment extending from on-premises to edge devices encompassing the cloud.

Introduction to edge computing

Edge computing is a capability that moves computing to the edge of the network, where it is closest to users or the source of the data. By placing computing services close to these locations, the user benefits from faster, more reliable services. Edge solutions can reduce and consolidate the number of independent endpoints interfacing with core computing resources, limiting the amount of data traversing the network and more secure data management. Primary drivers include the need to accelerate data processing or otherwise overcome latency and network capacity and availability issues, with potential cost-savings, better security, and improved compliance as additional benefits. A key growth driver is the increasing quantity of data being created and consumed at the edge.



Source: Fact.MR

CAGR
30.01%
(2022-2032)

In the following scenarios, it is beneficial to have data processing near to use or source of data:

There is no internet, or the signal is limited

The data cannot be transferred off-site because of security concerns or privacy regulations

When a device needs to analyze data and make split-second decisions

Every enterprise is unique, and "edge" can mean something different to different enterprises. Edge use cases and technology can range from autonomous vehicles, medical devices, oil rig sensors, industrial robots, nautical GPS (Global Positioning System), and meteorological devices. Even Mobile phones and robot vacuums are also examples of edge devices.

Security at the edge

Edge solutions raise cybersecurity and privacy concerns because mission-critical data may be generated and analyzed outside the traditional IT perimeter. The majority of enterprises believe that by bringing data storage and processing closer to the end-user, edge solutions will increase security vulnerabilities for their businesses.

This paper discusses edge services that are available to provide a secure environment, from the on-premises, cloud to the edge devices.

A botnet is a collection of online devices that have been infected by malware, allowing malicious actors to control them. Cybercriminals utilize botnets to instigate attacks, which include malicious activities like credentials theft, unauthorized access, data theft, and DDoS (Distributed Denial of Service) attacks. Botnet attacks are especially prevalent in the Edge because of its decentralized nature, so securing Edge is the key to a successful migration. Ransomware is another type of malware that could have an easier time infiltrating the multiple endpoints created within IT infrastructure, although it may have a harder time making it all the way to DC (Data Center) or centralized environment from an Edge server. While this may sound comforting, do not be quick to feel relieved, because Edge data can often be the data that keeps operational.

In the current threat landscape, security strategies of an enterprise are focusing on on-premise and cloud infrastructure, and unfortunately, IIoT/OT security takes a backseat or fails due to cost or complexity, leaving organizations at risk.

In a recent study, it was discovered that 90% of respondents had suffered an assault of some kind on their operational technology (OT) or industrial IoT (IIoT) systems in the previous year.

Unsecured data exfiltration IoT devices are susceptible to data theft. This occurs when a third party uses a company's IoT ecosystem or devices without authorization to copy, transfer, or retrieve data. It may have three major impacts as mentioned on the next page:

Impact information

Devices and IoT ecosystems are vulnerable to intrusions by outside parties who want to tamper with the data. For instance, IoT devices could be persuaded to rig television station ratings.

Theft of intellectual property

IoT devices can have their intellectual property regarding how they are made or how they connect to the internet stolen because they are deployed in the field and lack a physical or network border.

Device control lost

An IP-based security camera being hijacked and integrated into huge botnets is an example. To prevent various risks, it is essential that security be included in IoT devices and ecosystems. Therefore, barriers known as depth perspective and defense must be put in place. Devices need to be resistant to such attacks and maintain flawless operation both during and after an attack. Ignoring these dangers entails profound consequences, including business disruptions, compromised confidential information, and harm to an enterprise's reputation and brand.

Therefore, security must be fully assumed by every enterprise that participates in an IoT ecosystem. Edge security involves several aspects, including:

Secure perimeter: Securing access to edge computing resources using encrypted tunnels, firewalls, and access control.

Securing applications: Edge computing devices run apps that need to be secured beyond the network.

Proactive threat detection: Implement proactive threat detection technologies that will identify a potential breach as early as possible.

Patch & vulnerability management: Automated patching to keep devices updated and reduce potential surface attacks; continued maintenance and discovery of known and unknown vulnerabilities.

Secure by design itself

While many enterprises have relied historically on perimeter-based security, they are increasingly shifting towards a zero-trust architecture. With more computing taking place outside of the traditional secured environment, innovative approaches are needed to safeguard both the deployed edge solution and core enterprise systems and data.

Zero-trust

Given that edge solutions often run autonomously, they should be developed using zero-trust principles. Zero-trust assumes that no component is to be implicitly trusted and that we need to authenticate, authorize, and protect all data and communications. Enterprises must ensure that edge solutions are secure by design itself. Every building block—from hardening the operating systems for IoT devices, and securing connectivity through safeguarding the edge compute and distributed data and protecting backend cloud systems—should be addressed from the start. Edge computing must also be tightly integrated into the enterprise's cybersecurity fabric. Grounded in a zero-trust mindset, this perspective reflects the need to recognize the convergence of traditional IT-focused cybersecurity with Operational Technologies to ensure the security of endpoints. Edge Security to find all devices, assess all known risks, watch how they behave, and secure every digital interaction.

Secure access service edge

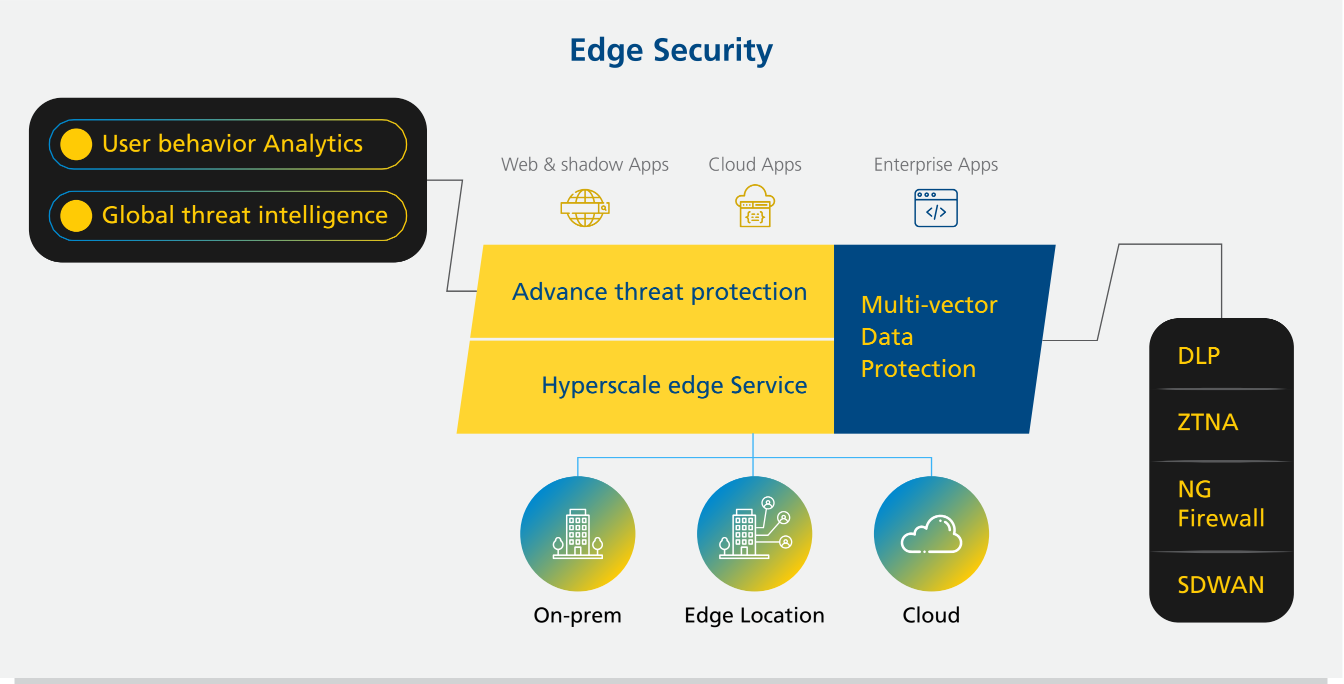
Secure Access Service Edge (SASE) delivers converged network and security services from a single, globally distributed, and cloud-native platform. Scale, acceleration, and edge compute capabilities to delight customers are integrated with Zero Trust Network Access (ZTNA), web application and API (application programming interfaces) protection-as-a-service (WAAPaaS), and cloud secure web gateway (SWG) services to protect users. Enterprises can secure and enable corporate resources while securing and delivering their sites, applications, and APIs.

Vulnerability control

Protection from device vulnerabilities that VM (Virtual Machine) cannot detect and from devices that you cannot see. **Edge security is needed in order to obtain a true device risk score, which includes information about each device vulnerability that has been passively and actively found.**

Network segmentation

Confidently segment all edge devices and apply zero-trust policies to prevent attacks and lateral movement of threats by eliminating NAC (Network Access Control) blind spots. Get meaningful device segmentation through deep profiling, assessment, and policy enforcement of each device.



Below mentioned three edge protections can help secure the connection points between the on-premise, Cloud, and edge devices or applications:

- Secure content delivery
- Network and application layer protection
- Distributed Denial of Service (DDoS) mitigation

Secure content delivery

Secure content, delivery provides content including data, videos, applications, and APIs, very quickly and securely to users. These should be delivered over secure transport, using the recommended version of Transport Layer Security (TLS) to encrypt communications between endpoints. If necessary, there are several methods that you can use to help secure that same content through restricted access, including signed URLs (Uniform Resource Locator), signed cookies, and token authentication.

Network and application layer protection

Edge networks are architected outside of the security perimeters of on-premise and cloud. Extending security to edge-end devices requires network and application security and continuous monitoring, as well as encryption of data in transit and at rest.

DDoS mitigation

DDoS mitigation as a defense layer is important for enterprises operating at the edge with mission-critical operations that cannot afford outages. DDoS attacks are deliberate attempts to exhaust resources, so they are unavailable to users. Common types of DDoS attacks are SYN floods that exploit the TCP protocol; reflection or amplification attacks that use the User Datagram Protocol (UDP); and HTTP (Hyper Text Transfer Protocol) floods that target web servers' capacity.

How to secure edge environment?

Enterprises need to implement security measures at all layers to secure edge devices and applications.

01

Role-based access control

Implement the least privilege policy and enforce role-based access control with the appropriate authorization for each layer in the edge environment.

02

Traceability

Monitor, identify, alert, and audit actions and configuration changes to an environment in real-time. Integrate log and metric collection with AIOPS or AI (Artificial Intelligence) based systems to automatically investigate and act.

03

Security at all layers

Use a multi-layer security control approach. Apply to all layers (for example, edge gateway, network, platform, operating system, application, and code).

04

Protect data in transit and at-rest

Use encryption, tokenization, and access control to protect data in transit and at rest.

05

Prepare for security breach

Prepare for a security incident by having incident management and investigation policy, and processes that align with enterprise requirements.

Conclusion

Although enterprises continue adopting the edge to gain the benefits of low latency, security remains a top concern. With increasing interest in new use cases and services like smart manufacturing, augmented and virtual reality, and the high interest in online gaming, there is a clear need for edge computing. However, the edge is not a standalone product or an offering but an enabler for use cases requiring security, resilience, and low latency in combination with other technical solutions like private networks. Enterprises need to secure edge devices and applications, and create an integrated, layered security perimeter at edge locations to secure content delivery, protect the application layer, and mitigate DDoS attacks.

Enterprises need to adopt the common security design across on-premises, cloud, and edge to provide a seamless experience and access to endpoints to connect through several sources like Wired, Wireless, Cloud, etc. There is always a need to provide tight control and the best authentication, authorization, data control, logging, compliance, and governance. As the number of IoT/ Wired and Wireless endpoints is increasing there is a requirement to transfer their data in real-time to different destinations, which could be analytics software hosted on on-premises, cloud, or edge locations.

The Edge security should be designed and implemented robustly so that overall security and connectivity requirements are fulfilled, including endpoint security, not allowing unwanted devices, mitigating threats in real-time from devices, and isolating those devices.

Reference

https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-cloud-and-edge-infrastructure

https://www.factmr.com/report/4761/edge-computing-market

https://assets.barracuda.com/assets/docs/dms/NetSec_Report_The_State_of_IIoT_final.pdf

Authors

Vishwas Samant

Principal Enterprise Architect
CIS LTIMindtree

With over two decades of experience in IT, Vishwas Samant is a thought leader and expert in strategy and transformation. He has worked extensively with large-scale clients across many sectors, including banking, telecom, and manufacturing. Furthermore, his expertise includes developing IT operating models, enterprise infrastructure and application technology roadmaps to help companies achieve their vision. Using digitization and innovation, he has pioneered transformation in a highly diverse environment and executed multimillion-dollar global programs. His focus remains on infrastructure designing and adoption, as well as transformation consulting.

Punit Joshi

Senior Specialist - Network
CIS LTIMindtree

Punit has 11+ years of varied IT experience as an Enterprise Network Transformation expert, and Network & Security Architect. He also specializes in developing enterprise network solutions to help clients to optimize network performance and security. His focus remains on network transformation consulting, and next-generation technology adoption.

About LTIMindtree