WHITE PAPER

Edge Security

Intel® Smart Edge Security Features

Introduction

The emergence of cloud computing technologies, 5G capabilities and the growth in real-time data flows and content have created a need for low latency cloud computing at the network edge. This has given rise to the need for multi-access edge computing (MEC). MEC servers are placed at the edge of the network and can be used for a wide variety of decentralized cloud computing applications.

Since these servers are not located in the protective boundaries of large data centers, they must be designed to manage additional threat vectors that could arise at the edge of the network. Accordingly, mitigating these increased threat vectors requires MEC servers to be designed with a security-first foundation to minimize the attack surface area. In parallel, the introduction of new capabilities in these new network locations brings an opportunity to advance an enterprise's security toolset. Intel Smart Edge has designed its MEC solution with built-in advanced security. These disciplines help ensure multi system operators (MSO), mobile network operators (MNOs) and enterprises can deploy these solutions with confidence.

Intel Smart Edge is a MEC platform that overcomes traditional burdens of systems hardening, which previously required a significant systems integration effort leveraging multiple technologies and products. Implementation of traditional systems was cumbersome, operationally complex, and difficult to ensure the MEC system adjusted to the ever-changing world of cyber security in hostile and unprotected locations.

The platform natively helps secure and separates data and governance, securing between groups or disparate organizations without an assumption of trust. This paper discusses many of the security features of Intel Smart Edge offering and how these security features can help protect and enhance the user experience for both the customer and the service provider.

Intel Smart Edge: MEC Platform with Integrated Security Features

Intel Smart Edge launched its MEC controller and MEC edge node as a software solution that helps secure the edge demarcation, bringing an abstracted, simple API and user interface for both the enterprise and mobile network operator. This open platform allows for the introduction of new edge applications while supporting the integration of existing cloud native applications into the MEC environment.

The MEC controller and MEC edge node are optimized to take advantage of Intel processors, accelerators and platform security technologies. Intel Smart Edge supports traditional Wi-Fi, LTE and 5G capable radios. The MEC application environment leverages user adjacency, enabling an "as-a-service" ecosystem in which virtual applications are deployed, managed and run at the cloud edge, promising low latency and high bandwidth for over-the-air data transmission.

Edge computing and large cloud data centers present a larger target for malicious actors, due to the converged nature of much of the data. To help enable better security models that are required to address this, Intel works closely with the ecosystem to develop a "hard in the middle" approach to its security features.

Table of Contents

Introduction 1

Intel Smart Edge: MEC Platform with Integrated Security Features 1

Intel® Smart Edge: Created with Security in Mind 2

Going a Step Further at the Secure Edge. 3

Risk and Mitigations 4

Future Uses for Intel Smart Edge 4

Conclusion. 5

Traditional security models typically focus on blocking unauthorized access at the outer boundary, after which there is an implicit or explicit assumption of trust within the boundary resulting in targets that are not further secured. Intel Smart Edge security capabilities use a zero-trust model for all connections, users, and applications — even its own internal microservices — therefore reducing attack opportunities. If traditional security is analogous to the locks of the exterior door of a house, the Intel Smart Edge platform extends the traditional boundary threat protection with locks and surveillance on every door, hallway and room. This provides a new, powerful control point to help manage malicious adversaries, allowing interception, blocking, and control before traffic is allowed beyond the first network hop.

As shown in Figure 1, the MEC edge node is an edge network and virtualization platform, fulfilling the role as a delegated demarcation point between operators and enterprises. The centralized cloud native and horizontally scaling MEC controller software is designed to run in a client datacenter or service provider's cloud. All management of the edge node is done through the MEC controller and intentionally, direct management of any MEC edge node is not allowed. Thus, management and control of multiple MEC edge nodes is handled by this cloud native MEC controller.

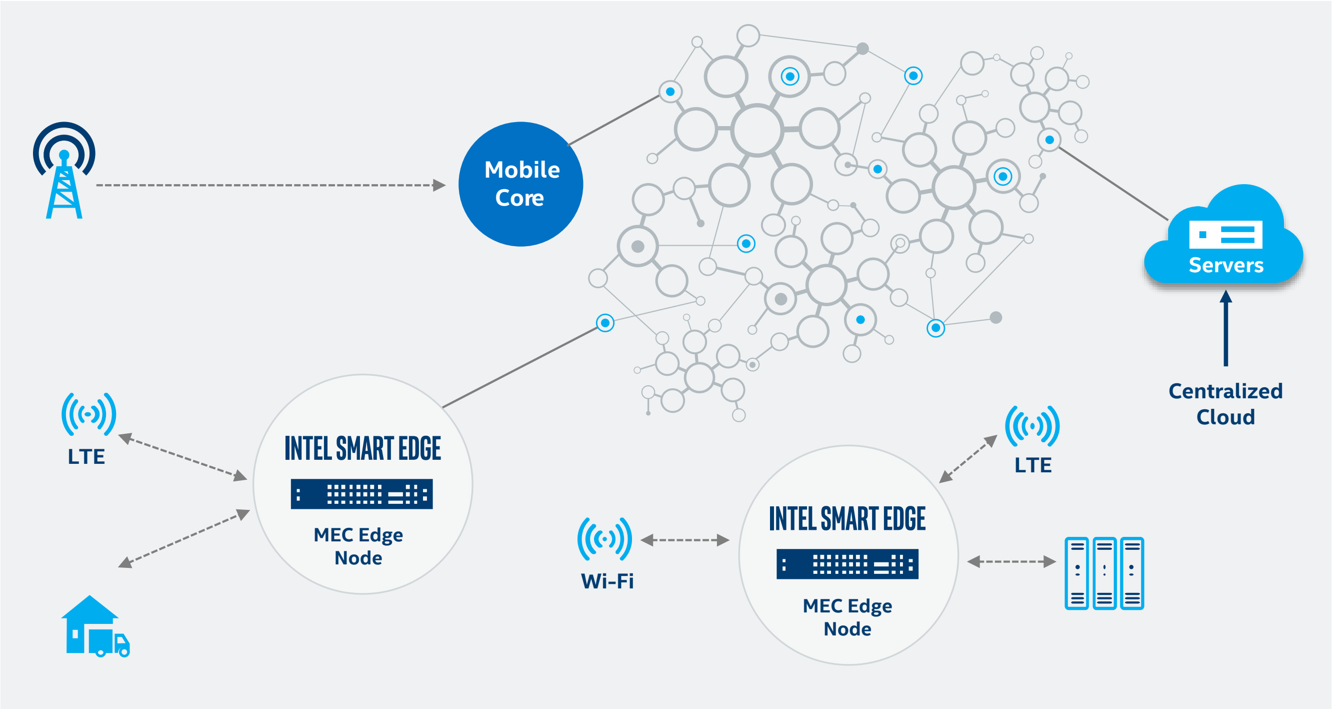

Figure 1. Network Architecture for Intel Smart Edge

Intel® Smart Edge: Created with Security in Mind

Simplification and effortlessness are essential attributes in any system that aims to truly enhance security. The platform has a deliberate focus on the reduction of operational burdens, including domain knowledge, to help administrators deal with existing difficult and complex hardening tools and practices. Security becomes more accessible when transparently integrated.

Following the confidentiality, integrity and availability security model, the design focuses the system's security features through an extensive use of cryptography for all aspects of platform communication and control:

Confidentiality: Symmetric or asymmetric encryption of traffic

Authenticity: Asymmetric signing and attested authorization

Integrity: Asymmetric signing of payloads

Non-Repudiation: Protection and non-transport of private keys

With security in the forefront of all development activities, the Intel Smart Edge platform architecture has some similarities to more traditional cloud infrastructure, with additional key enhancements to address the unique needs of an edge premises platform.

In the edge node, the transport layer enforces policies to explicitly shape and transform the network data to ensure only authorized communication flows are enabled. Beyond the context of traditional firewalls, these policies are tied to hardware-authenticated users leveraging mobile device agnostic features at the underlying mobility network layer.

Along with security features within Intel Smart Edge, the use of Intel architecture capabilities further enhances the hardware and software security. Intel Smart Edge is implemented on Intel architecture-based platforms to support a wide range of use cases without rewriting any software. This includes support for four-core Intel Atom®

processors for light workload MEC servers installed on a pole or within a base station, as well as support for Intel® Xeon® Scalable processors for higher-throughput points-of-presence or large enterprise applications.

Security and accelerating security processing technologies available in many Intel-based servers offer further security enhancements. Intel® Software Guard Extensions (Intel® SGX) are used in the MEC platform to provide hardware-based memory encryption capabilities that enable isolation of specific application code and data in memory. For encryption / decryption, Intel® QuickAssist Technology (Intel® QAT) is available to accelerate many performance-sapping data encryption and decryption algorithms and operations. Another important platform technology is the trusted platform module (TPM 2.0), a microcontroller that stores keys, passwords, digital certificates and other secrets that can be used to authenticate and verify platform integrity.

Going a Step Further at the Secure Edge

The design includes application-level and user-level policy controls that limit who has access to defined networks. The controller manages multiple tenants, which allows for an operator to delegate to many organizations in the same platform with audit-able secure boundaries between each organization. This feature can also be leveraged to ensure that different, high-functioning software platforms can work alongside each other in a highly secure, isolated fashion.

Along with these specific policy controls, which limit access, the trust circle briefly discussed above is an important security differentiator within the Intel Smart Edge MEC infrastructure compared to traditional cloud architecture. Both enterprises and operators need control of the demarcation point in a manner that establishes auditable, independent control that does not exceed the control boundary.

Intel Smart Edge also takes complicated public key infrastructure (PKI) issues and makes them simpler for users as shown in Figure 2. Chain of custody and non-repudiation of all platform entities mean that there is a hardware-backed audit trail from the point of edge node software activation, the point the edge node is accepted into a controller domain, and the entire lifecycle of both edge node and controller services. The process and audit trail begins with the signing of the Intel Smart Edge MEC software and the certificate issued to the edge node. During activation, additional trust chains are initialized under the particular MEC controller platform. Fully automating this process significantly eases adoption for the operators and enterprises that use the MEC platform. This takes a commonly avoided and often improperly implemented problem, public key infrastructure, and makes it simpler to the point where in many cases it is completely transparent.

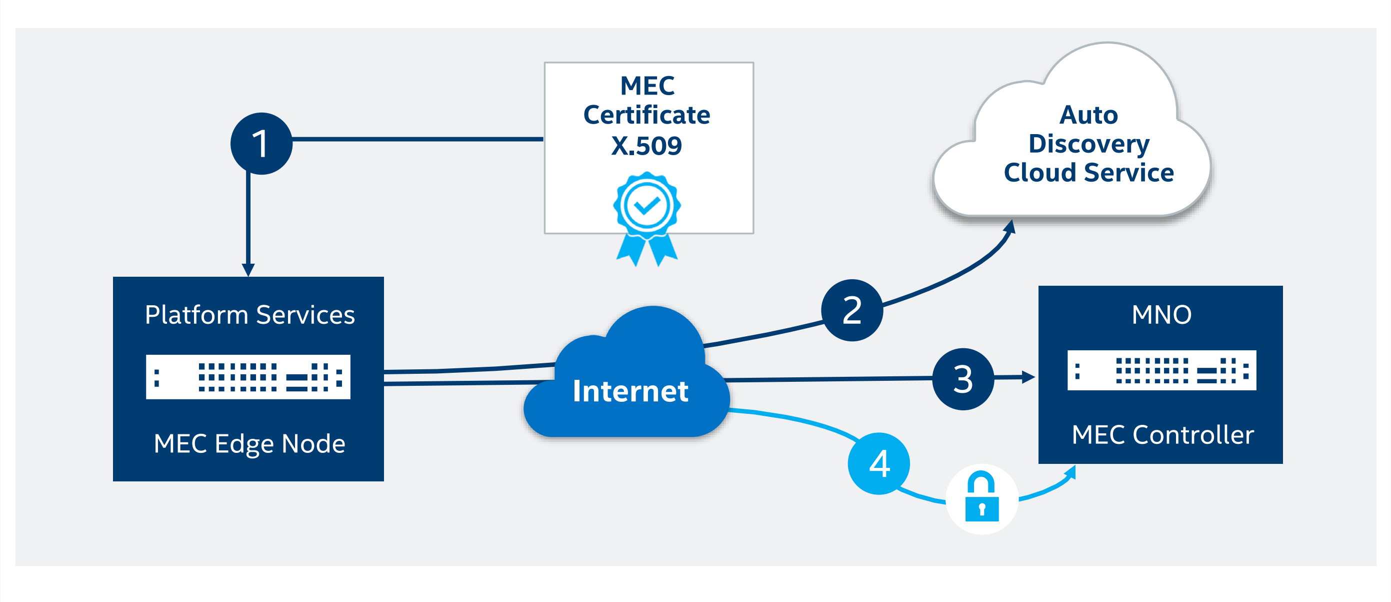

Figure 2. The MEC provisioning and activation cycle.

Cryptographic key management while operating in an assumed hostile environment is another critical aspect of the MEC application security in Intel Smart Edge. When a new Intel Smart Edge offering is implemented, the new entity must prove its identity using cryptographic keys. These keys start with the Intel Smart Edge controller and are delegated to specific operators. In the on-boarding process, the software being run is matched and then it exchanges Intel Smart Edge certificates for controller deployment specific certificates. As a precautionary measure the controller certificates have a much shorter validity period and must constantly be renewed. This additionally reduces risks by allowing for key and certificate rotation. These keys are used both to authenticate a user to the platform and for all forms of platform communication. All platform communication uses mutual authentication, authorization, encryption, and maintains non-repudiation because private keys are never shared or transported. All key management is done agnostic to an administrative user. Each MEC service can store and manage its own keys and, as a result, does not require an online central authority service for authenticating peer communication.

All network traffic flowing through the MEC platform must pass a variety of security checkpoints and firewall filters. Put simply, traffic that is not explicitly allowed is immediately dropped. The platform also enforces network traffic from any MEC platform service to require transport security at a minimum. The MEC platform does not expose nor allow any interactive remote access methods into a MEC service environment by design. All configuration and management must be done from the MEC controller through secure channels such as the REST API or web user interface.

The MEC edge node supports end-to-end encryption of all user plane traffic, and while mobile device traffic may go to an unencrypted web server, it is encrypted by the MEC platform, thus maintaining confidentiality throughout the underlying transport process. In addition, strict traffic control rules exist within the MEC edge node to enforce user and control plane isolation. The control plane does not have direct access to the user plane data and vice-versa.

After MEC edge node enrollment, each edge node maintains a cryptographically unique IPsec tunnel for direct secure communications with a MEC controller. On the outermost security layer, all traffic flowing from the MEC edge node to the MEC controller must flow through this secure IPsec tunnel. Within the IPsec tunnel, peer service communication must undergo an additional security layer conducted with TLS mutual authentication using unique cryptographic keys stored in each service. Because services need to approve communication with one another each time a request is made, a malicious service cannot simply impersonate another service or replay previously made requests without undergoing cryptographic verification.

Risk and Mitigations

As with any system, the MEC platform has security risk in configuration and implementation. Intel extensively tests the MEC edge node and MEC controller prior to deployment. Key security features play a critical role in testing, including constant monitoring for unusual activity, to help identify a breach quickly after it occurs. This testing and monitoring are intended to help lower the technical security risk of implementing the MEC controller and MEC edge node.

It is not possible to account for every possible threat that a customer may encounter, including very dedicated, well-resourced threats, so it is important for platform security to be as robust as possible. This due diligence may deter many malicious actors. Further, constantly operating in an assumed hostile environment and helping ensure a strong baseline security posture provides the customer and the operator piece of mind that their edge applications are protected following a defense-in-depth methodology.

Future Uses for Intel Smart Edge

Internet of Things: Intel Smart Edge can be used to enable services for the Internet of Things (IoT). While there may not be one single application or feature that can easily address all IoT security concerns or use models, Intel Smart Edge is able to provide many needed features to serve these applications and devices. Some of these services include: IoT network security, IoT authentication, IoT certificate management, IoT security analytics, and IoT application security. Intel Smart Edge also works with many of the unique protocols and standards, essentially sandboxing these systems from the rest of the network.

Retail Wireless Network Security: Leveraging 4G/5G networks and the MEC edge node, on-site user experiences can be improved in physical retail stores for both store employees and customers. Such applications may require a secure, seamless, and high throughput and low latency experience. Beyond just the user experience, security is the foundation upon which premise solutions must be built. Intel Smart Edge operates in a zero-trust model such that only explicitly authorized traffic is allowed. As long as the retail chain IT staff is able to validate users, devices, and access levels, MEC will keep those access levels separate by allowing for differing networks and supporting security tools to be aligned and/or housed on the MEC.

Retail Analytics: By enabling low latency and high bandwidth, Intel Smart Edge also supports new, engaging experiences, such as virtual reality (VR) and augmented reality (AR) products and ultra-high definition (4K) product video content. The analytics offered through the platform facilitate precise in-store operations and logistics and speed transactions with its point-of-sale addition. By combining many of the features of Intel Smart Edge such as location-based customer personalization, Intel is able to offer advanced metrics and deliver new perspectives about the store and its information/experiences to the retailer.

Conclusion

There are many benefits to delivering security focused, low latency applications at the edge of the network. Intel Smart Edge offers a MEC platform that is usable and accessible to all operators and customers while enhancing on security, allowing enterprises to deploy existing and new applications to locations that previously did not exist, thus enabling new user experiences and accelerating new revenue. Intel Smart Edge software platform helps further improve the user experience and enables enterprises to take advantage of 5G. The security features and use cases in this paper are just some of the ways that Intel Smart Edge helps improve security at the network edge in the ever-changing technology landscape. To learn more, please visit www.intel.com/smartedge or contact your local Intel representative.

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.