ZEDEDA SECURITY ARCHITECTURE

Security for the Distributed Edge

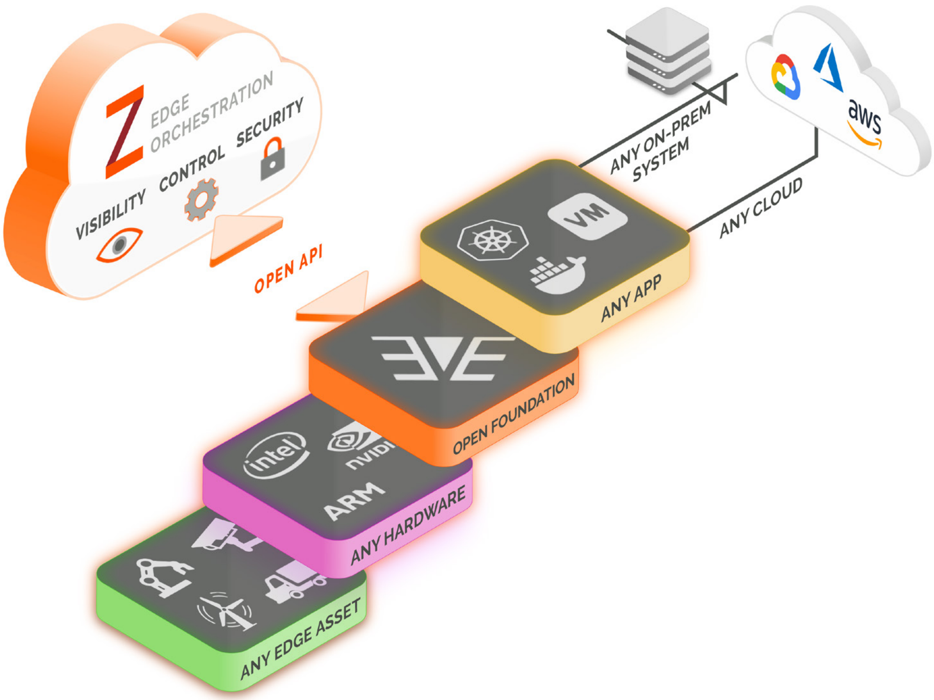
Introduction

ZEDEDA is a simple and scalable cloud-based orchestration solution that delivers visibility, control and security for the distributed edge, giving customers the freedom to deploy and manage any app on any hardware at hyperscale while connecting to any cloud or on-premises systems. With ZEDEDA, customers can now seamlessly deploy and manage any edge compute node to instantly unlock the value of edge data and make real-time decisions.

ZEDEDA has architected its cloud-based orchestration solution to meet the security, safety, uptime and usability needs of both OT and IT organizations, enabling them to focus on driving business outcomes. It is optimized to address the unique requirements for deploying computing at the distributed edge – outside of secure data centers, both on-premises and in the field. The solution leverages the open source EVE-OS from the Linux Foundation's LF Edge to provide a solid security foundation while abstracting the complexity of the diverse hardware, connectivity and software at the distributed edge, and eliminating any vendor lock-in.

This paper outlines the key features of both EVE-OS and ZEDCloud, each of which has been architected with a security-first approach.

Contents



ZEDEDA Distributed Edge Orchestration Solution

Balancing OT and IT Needs

When designing and deploying distributed edge solutions it is critical to balance the needs of both Operations Technology (OT) and IT. Top business priorities for OT include safety, efficiency, throughput, quality, and uptime, as they oversee operations in environments such as the factory floor, oil refineries and warehouses. Security is a means to this end. Meanwhile, security priorities for IT revolve around data protection, compliance, governance, and privacy.

Key to striking a balance is recognizing that the implications of security breaches are uniquely different between IT and OT operations. In the IT world, a security breach, such as one that leads to stolen credit card data, typically plays out over long periods of time and at great scale. In contrast, a breach of an industrial process is likely to have an immediate impact on production and safety. Given these implications, OT has historically kept their systems disconnected from the network.

The promise of Industrial IoT is connecting traditionally isolated OT machines and processes to broader networks to drive new business outcomes through visibility and analytics. Connected edge solutions must be built with a security-first focus that protects legacy assets and provides a consistent foundation for security and manageability regardless of use case.

Given the diverse mix of technologies and skill sets at the edge, implementing security also requires a focus on usability. Many of the breaches we have seen in the IoT space over the past several years have been a result of security measures being an afterthought, too complex and difficult to implement, or bypassed altogether.

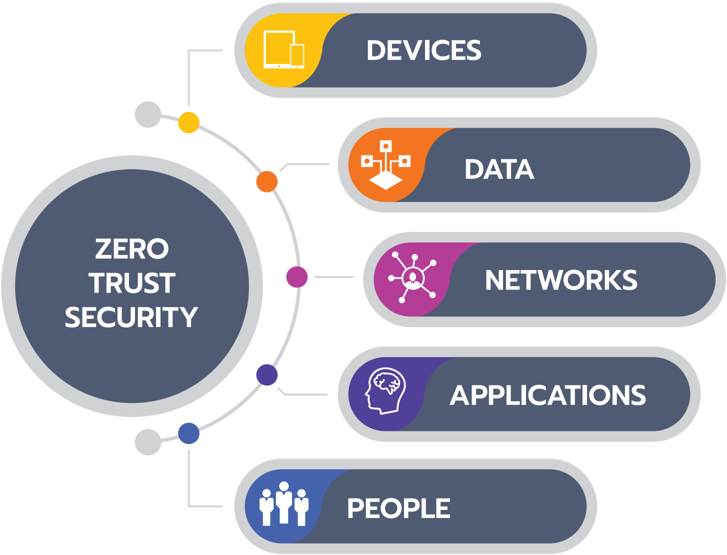
ZEDEDA Security Architecture Philosophy: A Zero Trust Model

Distributed edge computing requires addressing typical IT security concerns when it comes to network and application security, including configuring credentials and keys. But it also requires addressing unique threats that are introduced when deploying diverse physical infrastructure in the field. Examples of this include threats due to physical access, such as stealing devices, cloning disks and loading malware, or replacing firmware through local USB ports. Additional threats are introduced due to the common lack of a network perimeter in the form of firewalls and intrusion detection systems. Exacerbating all of the above is a mix of skill sets in the field, with more limited availability of IT security support compared in the cloud.

Our goal is to eliminate such security concerns for the deployment of hardware and applications at the distributed edge by providing a holistic approach built from the ground up.

The ZEDEDA solution addresses security starting at the hardware and firmware level. We do this by leveraging silicon-based root of trust such as standard Trusted Platform Modules (TPM) to prevent cloning of edge devices or their disks, using cryptographic identities for the edge devices and the application instances, plus standard Transport Layer Security (TLS) on the network, and disk encryption tied to the TPM. This is combined with state-of-the-art security approaches in ZEDCloud.

However, security is not accomplished solely by a collection of state-of-the-art **technologies**. Security processes and human factors are equally important. Supporting security **processes**, such as the ability to observe applications and the underlying EVE-OS to look for anomalies, and enabling secure and robust patching of both applications and EVE-OS, are vital. Furthermore, one must consider the role of **people,** as exemplified by simplifying secure on-boarding of edge nodes without requiring IT expertise by the installer, and leveraging crypto-based ID to eliminate username and associated password management for EVE-OS.



ZEDEDA Zero Trust Security Architecture Philosophy

The fundamental security principle of need-to-know is critically important at the distributed edge because many security issues are present on devices without strong physical access control. This implies that the various infrastructure components should be strongly isolated from one another, and that applications and their data need to be isolated from the infrastructure components. This isolation is pervasive in the ZEDEDA solution because the end user's applications and data are completely separate from the ZEDEDA edge components, and furthermore never transit to ZEDCloud.

The deployment lifetimes at the distributed edge are significantly longer than in centralized data centers. This increases the likelihood that security-relevant bugs will need to be patched during the lifetime of the edge nodes and applications. But such patching must not become an attack vector for an intruder. As we will show below, ZEDEDA's comprehensive solution ensures protection against this with signed configuration and images, hardware root of trust, measured boot, and remote attestation.

However, before a new security issue can be identified, fixed, and patched, there can be attempts to exploit it in the field. ZEDEDA makes it possible to mitigate security issues before serious harm through isolation between components, defense in depth, and visibility. An example of this is how EVE-OS can only be controlled via an API that exposes the minimal necessary functionality to ZEDCloud, and users cannot log directly into EVE-OS. Rather, all admin interactions are performed through ZEDCloud on the other side of the API with Role-Based Access Control (RBAC).

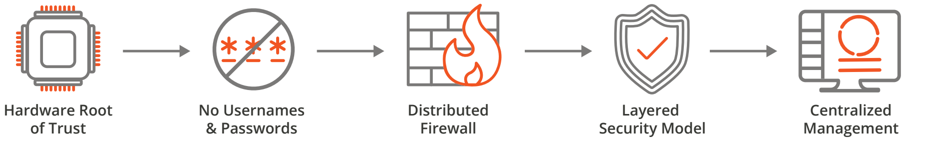
Security, as we have discussed above, is largely an IT concern. However, secure infrastructure is paramount for hosting OT applications in order to maximize uptime and safety and ensure data provenance from critical processes. While not covered in this white paper, the ZEDEDA solution is architected to maximize uptime through mechanisms for automatic failback and recovery after failures or configuration mistakes, combined with state-of-the-art availability approaches in ZEDCloud.

EVE-OS Security Architecture

ZEDEDA is one of the founding members of LF Edge in the Linux Foundation and has contributed EVE-OS to Project EVE to deliver an open source, vendor-agnostic and standardized architecture for hosting distributed edge computing workloads. EVE-OS is a lightweight, secure, open, universal and Linux-based distributed edge operating system with open APIs for remote lifecycle management. The solution can run on any hardware with current support for both Intel and ARM processor architectures and co-processors (e.g., GPU, FPGA). It leverages different hypervisors and container runtimes to ensure isolation between the EVE-OS foundation and the applications above.

For large-scale application deployments it is best to use immutable workload standards such as OCI-compliant containers that make it clear which versions of an application are deployed across distributed edge computing nodes. However, the ability to host VM images on EVE-OS enables support for applications that leverage their own software update mechanisms.

The security capabilities in EVE-OS outlined in the following sections are complemented by capabilities in ZEDCloud.

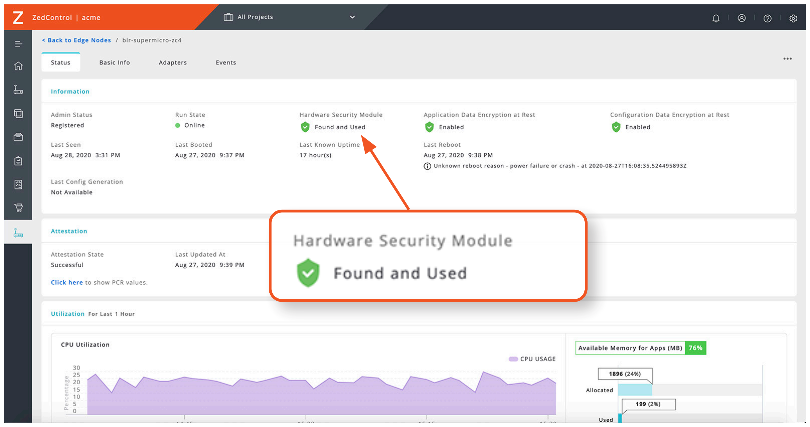


EVE-OS Zero Trust Components

Edge Identity Management

Unlike consumer devices, such as laptops and smartphones, which have some user interface and physical control to enter credentials (e.g., fingerprint, username/password), distributed edge computing nodes installed in remote locations do not typically have a local display and user interface. Therefore, it is important that a robust identification and authentication mechanism is put in place to protect against an attacker attempting to spoof the identity of an edge node. And because the edge nodes take all of their instructions from ZEDCloud, they need to authenticate that they are communicating with the correct ZEDCloud instance.

Instead of username/passwords, EVE-OS and ZEDCloud use strong cryptographic identities to prevent cloning and spoofing of edge nodes. EVE-OS leverages the cryptographic identity created in the factory or supply chain in the form of a private key generated in a TPM chip. This identity never leaves that chip and the TPM is also used to store additional keys (e.g., for an application stack such as Azure IoT Edge). The corresponding public key in the form of an X.509 certificate is registered in ZEDCloud as part of onboarding an edge node. ZEDEDA provides several approaches for this secure onboarding process, each of which depends on constraints due to device manufacturer and/or supply chain.



Information

Admin Status
Registered

Run State
Online

Hardware Security Module
Found and Used

Application Data Encryption at Rest
Enabled

Configuration Data Encryption at Rest
Enabled

Last Seen
Aug 28, 2020 3:31 PM

Last Booted
Aug 27, 2020 9:37 PM

Last Known Uptime
17 hour(s)

Last Reboot
Aug 27, 2020 9:38 PM
Unknown reboot reason - power failure or crash - at 2020-08-27T16:08:35.524495893Z

Last Config Generation
Not Available

Attestation

Attestation State
Successful

Last Updated At
Aug 27, 2020 9:39 PM

Click here to show PCR values.

Hardware Security Module
Found and Used

This local certificate is used with standard TLS (known as mutual TLS) in all communication with ZEDCloud, ensuring that ZEDCloud can always correctly identify the edge node.

EVE-OS trusting ZEDCloud

Each edge node is configured at the manufacturer or in the supply chain to trust "its" ZEDCloud instance. This imprinting is done by specifying one root certificate which EVE-OS will trust as belonging to "its" ZEDCloud; this certificate will be sealed by the TPM to prevent unauthorized modification to the root of trust. The particular ZEDCloud instance will have X.509 server certificates issued under that root certificate following standard operational procedures for certificate management.

Supporting content-inspecting TLS proxies

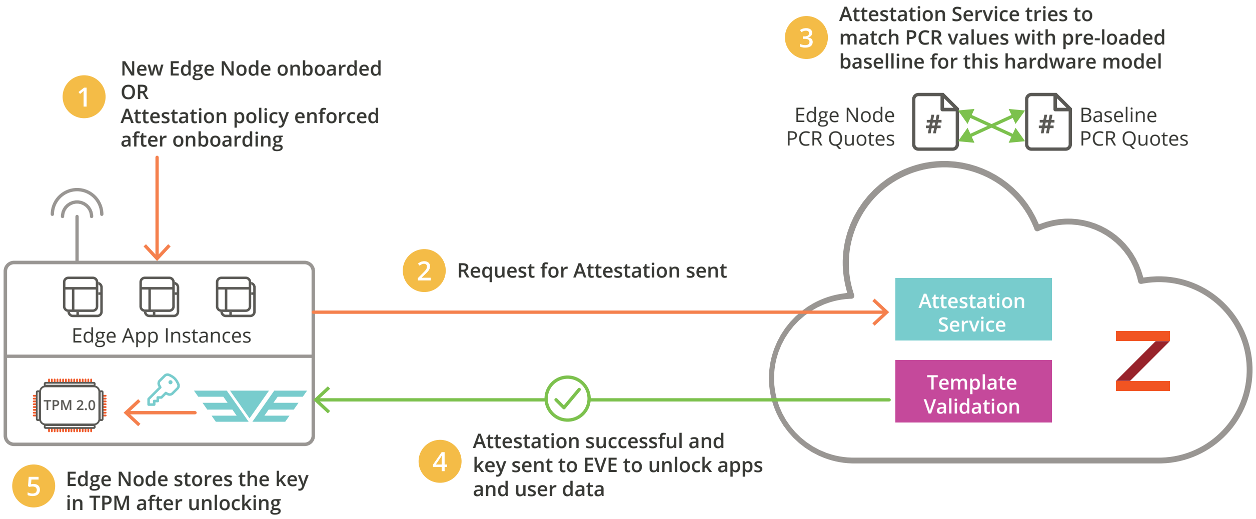
In some cases, the edge nodes are deployed in networks where security administrators use content-inspecting (also known as man-in-the-middle) proxies to detect the leakage of critical data, such as intellectual property.

The ZEDEDA solution can operate in such an environment without loss of security and the associated risk to operational safety. This is performed automatically by layering what is known as object security with its own cryptographic signatures on top of the transport security provided by TLS. Security admins can inspect the content, but any modification to the content by the proxy will be detected and rejected by EVE-OS and ZEDCloud.

Firmware and Software Integrity

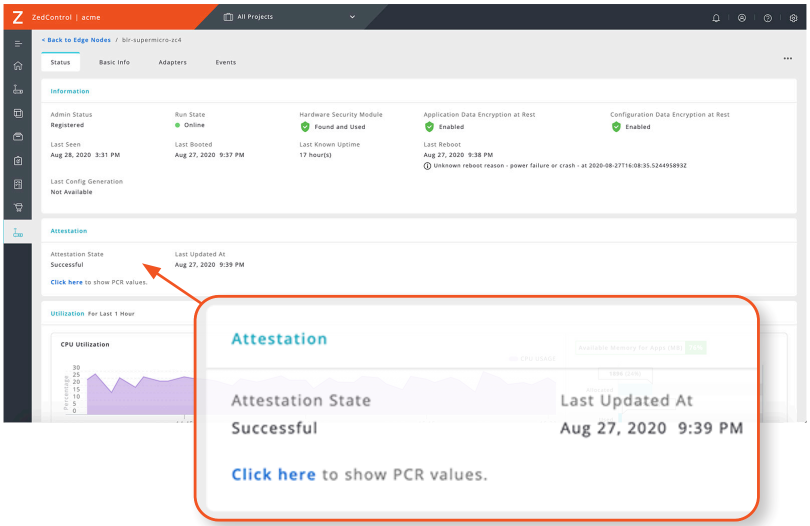
Compared to infrastructure in secure data centers, distributed edge nodes are often physically accessible, enabling attackers to potentially replace some of the firmware or software on the node and potentially compromising applications and related data.

The ZEDEDA solution prevents this by using standard measured boot in combination with remote attestation to ZEDCloud before any update to firmware or EVE-OS will be accepted. These mechanisms use the TPM as part of booting the firmware and software so that any changes to firmware or EVE-OS will be detected by the TPM, producing a different set of hash measurement values sent to ZEDCloud. Security relies on a secret key, which never leaves the TPM chip; the firmware and software on the edge node cannot spoofed.


1
New Edge Node onboarded
OR
Attestation policy enforced after onboarding
Edge App Instances
TPM 2.0
5
Edge Node stores the key in TPM after unlocking
2
Request for Attestation sent
4
Attestation successful and key sent to EVE to unlock apps and user data
3
Attestation Service tries to match PCR values with pre-loaded baselline for this hardware model
Edge Node PCR Quotes
#
#
Baseline PCR Quotes
Attestation Service
Template Validation

Every boot of EVE-OS is measured and verified by ZEDCloud before ZEDCloud grants access to restricted resources stored on EVE-OS, such as the application data volumes. The details of this approach ensures that if no firmware or software was updated, the boot of EVE-OS will complete and the applications will get access to data volumes without requiring any connectivity to ZEDCloud. A restart after power failure proceeds in disconnected mode. But when there is a firmware or software update, ZEDCloud will check the measurements against known and approved values for different versions of the BIOS firmware and EVE-OS software.

If the measurements are not approved, the edge node will revert back to the previous version of EVE-OS but it will continue reporting to ZEDCloud so that the operational team can observe if there is a potential security issue (or a misapplied firmware or software update).



Information

Admin Status
Registered

Run State
Online

Hardware Security Module
Found and Used

Application Data Encryption at Rest
Enabled

Configuration Data Encryption at Rest
Enabled

Last Seen
Aug 28, 2020 3:31 PM

Last Booted
Aug 27, 2020 9:37 PM

Last Known Uptime
17 hour(s)

Last Reboot
Aug 27, 2020 9:38 PM
Unknown reboot reason - power failure or crash - at 2020-08-27T16:08:35.524495893Z

Last Config Generation
Not Available

Attestation

Attestation State
Successful

Last Updated At
Aug 27, 2020 9:39 PM

Click here to show PCR values.

Utilization For Last 1 Hour

Attestation

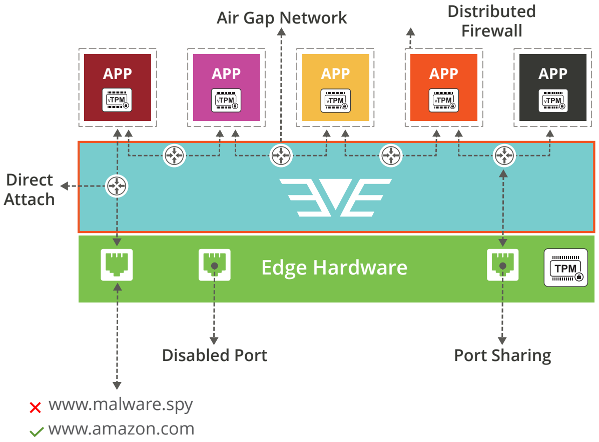
Attestation State
Successful

Last Updated At
Aug 27, 2020 9:39 PM

Click here to show PCR values.

Networking and I/O Connectivity

The networking needs at the distributed edge are much richer than in the cloud, both in terms of downstream and upstream connectivity. Downstream of a distributed edge node there is often one or more local networks connected to sensors, actuators, and systems. Connectivity can be in the form of Ethernet, but also common are wireless radio technologies and non-IP wired transports such as serial (e.g., RS485 for Modbus RTU) in legacy environments. Upstream connectivity is typically in the form of Ethernet via some enterprise network to reach the Internet, but cellular radio is also common and satellite communications may be leveraged for highly remote locations.



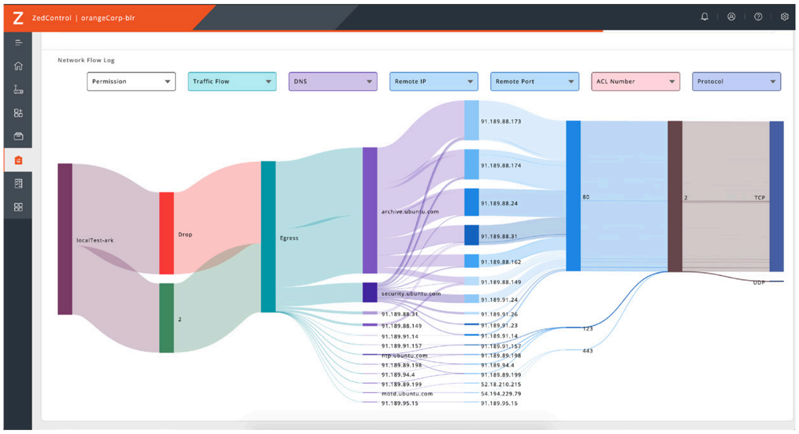
Secure Application Connectivity

Further complicating upstream connectivity, an OT organization or third-party service provider deploying an edge computing solution may not have full insight or control of the enterprise network being used. We often see complications due to various proxy and firewall configurations in the IT network, which have an impact on both the configuration and security of the OT solution.

The ZEDEDA solution addresses security for application networking and other connectivity by associating deployed applications with the set of network and I/O ports they are allowed to use, and leaving all other ports disabled. If a specific application requires special device drivers which might not be fully trusted, the I/O device can be directly attached to the application, thereby removing the need to install unknown device drivers in EVE-OS.

Furthermore, each application has a set of firewalls rules port network configuration with a 'default deny' stance, and associated visibility into rule violations. Applications can be connected to one or more 'network instances' which allows for applications which are only connected to, for example, a shop-floor network and an 'air gap network' to provide additional layers of security. One can also specify a network instance, which becomes part of a Virtual Private Cloud (VPC) by using the IPsec configuration from the public cloud provider. The VPC implementation is external to the deployed application itself and cannot escape from the VPC, nor can outside attackers penetrate the VPC.

This not only protects the applications from network-based attacks and protects the EVE-OS infrastructure from potentially compromised applications, but it also protects the network and other edge nodes should an application on a node become compromised.

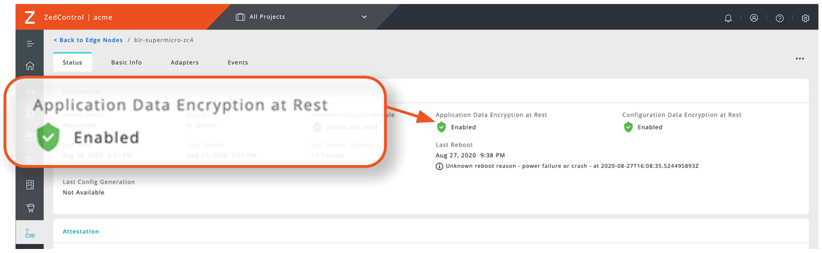


Example of Application Data Flows, Including Flows that are Rejected by Firewall Rules

Encrypted Data Store

The applications deployed on EVE-OS,and more importantly their data, is likely to contain business-sensitive information. EVE-OS stores this data in encrypted form to ensure that even a physical attack resulting in theft or duplication of the disk cannot access the data. ZEDEDA also provides the option to store data in clear text for applications that prioritize storage performance over security.

This encryption builds on top of the measured boot and remote attestation capabilities to prevent an unauthorized BIOS firmware or EVE-OS update (which might contain back doors) from gaining access to the data. If the measured boot check determines that there has been no firmware or software change, then the encrypted file system with the application data can be accessed immediately upon boot of the device. Otherwise, the remote attestation to ZEDCloud is required before ZEDCloud can provide the secret needed by the device to decrypt the file system. This leverages a standard mechanism to seal a key in the TPM under the measured boot results.



Application Data Encryption at Rest
Enabled

Admin Status
Registered

Run State
Online

Hardware Security Module
Found and Used

Last Seen
Aug 28, 2020 3:31 PM

Last Booted
Aug 27, 2020 9:37 PM

Last Known Uptime
17 hour(s)

Application Data Encryption at Rest
Enabled

Configuration Data Encryption at Rest
Enabled

Last Reboot
Aug 27, 2020 9:38 PM
ⓘ Unknown reboot reason - power failure or crash - at 2020-08-27T16:08:35.524495893Z

Last Config Generation
Not Available

Managing sensitive data like datastore credentials

Edge nodes often need credentials to access private datastores to download edge applications and to connect to WiFi networks. These credentials are handled more carefully than the rest of the configuration processed by the edge node. They are encrypted using object encryption from a vault in ZEDCloud to a target microservice in EVE-OS, and that microservice only keeps the decrypted information in memory. This object encryption means that content inspecting TLS proxies cannot read those credentials.

Application Support

Edge applications may desire to leverage hardware-based root of trust for their own identity, onboarding and authentication with centralized services. EVE-OS enables this as a service to guest applications through a certain set of virtual TPM (vTPM 2.0) functions. Using the vTPM library from LF Edge EVE Tools, edge applications can access the hardware-based TPM 2.0 to use a predefined set of TPM based keys for TLS handshake and cryptographic signing. With this open source application toolkit, EVE-OS enables guest applications to interact with TPM 2.0 hardware and implement crypto-based authentication and provisioning with root of trust placed in hardware.

An example of extending the hardware root of trust to the guest applications is when this capability is used to deploy an application stack, such as Azure IoT Edge on EVE-OS. By integrating the vTPM library into the Azure IoT Edge runtime, it is enrolled into Azure DPS using Endorsement Key from the TPM 2.0 hardware. This means that the identity of the deployed Azure IoT Edge instance is now locked into its host hardware, even though Azure IoT Edge is running as a virtualized guest application.

ZEDCloud Controller

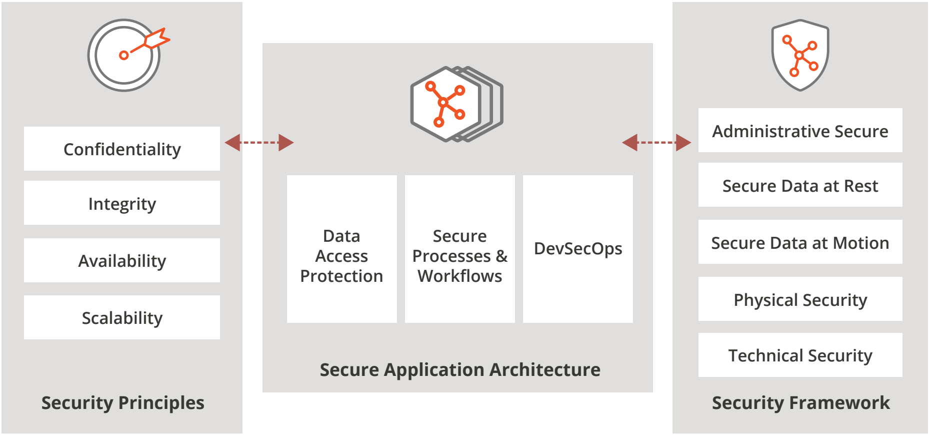
Overview

The ZEDCloud architecture is multi-tenant, scalable and highly secure. Security is one of the key considerations across all layers of the architecture. It encompasses areas that include the security of customer data, infrastructure, network and applications. In keeping with the principle of least required access, the architecture ensures that all workflows and processes are secure at every level while adhering to security best practices.

Security is also enhanced through integrations with select ecosystem partners. An example is ZEDEDA's seamless integration with Azure IoT that enables users to connect edge devices with the Azure IoT Edge runtime to Azure IoT using a policy-based approach. In other examples, ZEDEDA simplifies deployment of complementary OT security applications like Nozomi Guardian and Microsoft CyberX and virtual firewalls such as vSRX from Juniper Networks.

Key Capabilities

- **Hyper-scale:** A multi-tenant architecture fully geared towards orchestrating edge applications and several customer tenants within the cloud offering. The architecture is capable of supporting easy onboarding of distributed edge nodes at scale.
- **Support for heterogeneous hardware vendors:** ZEDCloud provides the freedom to Bring Your Own Application, orchestrate and manage its life cycle on the hardware vendor of your choice.
- **Project and policy-based:** Categorization with project and policies constructs enables a frictionless onboarding of devices and application in an OT friendly way.
- **Extensible ecosystem via REST APIs:** REST APIs offered by ZEDCloud allow for custom integrations.
- **Data security:** ZEDCloud services use secure communications across various channels within the deployment. All data in motion is secured using industry standard protocols such as HTTPS, TLS (Transport Layer Security). Additionally, all customer metadata stored at rest is encrypted.



ZEDCloud Security Pillars

Security Principles

Confidentiality

ZEDEDA's security architecture ensures that enterprise data assets corresponding to their edge infrastructure are not accessed by unauthorized users. This is achieved by specific audit logging, the applications identity management (IDM), and Role Based Access Control (RBAC).

Integrity

Data integrity refers to protecting enterprise assets from unauthorized modification or deletion of data, and ZEDEDA's security framework addresses this at multiple levels. At the outermost level, it uses typical user access authentication, authorization and securely stored credentials for logging into the system. The principles of 'least access' are followed to limit permissions to the bare minimum.

Availability

High availability of data, irrespective of application state, is a key ZEDEDA security design principle. At no point is the data owned by the enterprise inaccessible due to malfunctioning applications and the underlying IaaS. This is achieved by using clustered configurations, replicated databases that store data in multiple places.

Scalability

Centralizing security in a monolithic manner may be effective but it may impact performance and scalability of an application. ZEDEDA addresses this by delegating various security checks to the right system components using a distributed multi-node vault as a cornerstone.

ZEDCloud Security

ZEDCloud is architected using a micro-service approach with supporting services implemented in a redundant multi-node manner as needed. This micro-service design improves redundancy as well as the secure isolation of data. Multiple instances of ZEDCloud, a.k.a. as clusters, are logically separated. ZEDCloud ensures that both internal and external interactions are highly secure.

Data access and protection

Transport Layer Security (TLS) is leveraged for secure communication both between internal services and with surrounding infrastructure. This provides authorized users with secure connectivity to all external components.

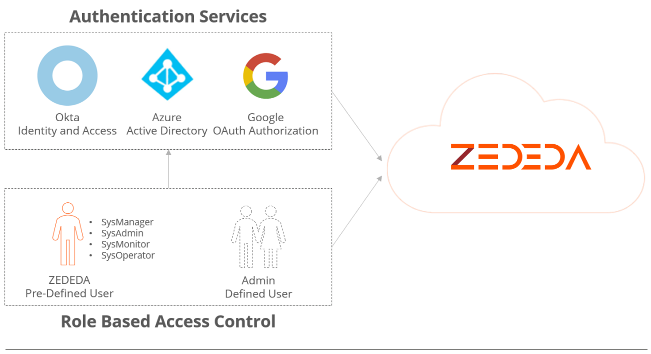
Secure processes and workflows

Sensitive data at rest is encrypted using symmetric-key encryption (e.g., AES-256) with these keys stored in the secure vault. Secure communication channels are used for all data in motion. The API gateway ensures that only authorized users gain access and this access can be revoked as, and when, required. Proper data handling is ensured by the presence of a consistent middleware, as part of all the services running for an application.

DevSecOps

Necessary security tools incorporated in the Continuous Integration/Continuous Delivery (CI/CD) pipeline ensure that a secure foundation is built and delivered to the SaaS environment, and are a part of the process followed with ZEDCloud. These include, among others, static and dynamic analyses of source.

Application Security



Application Security

User authentication

ZEDCloud handles user authentication by offering a secure identity solution through either local authentication or through a Single Sign-On (SSO) provider using OAUTH. Multi-Factor Authentication (MFA) can be implemented to further increase security when a SSO provider is used.

Role-based access control

In the spirit of principle of least privilege, ZEDCloud implements fine-grained Role-Based Access Control (RBAC) that provides the ability to limit how different personas interact with the system. Access and capabilities are governed by the role and related permissions assigned to each user.

Application security audit events

Major events related to access to the system, as well as data, are logged. This helps maintain an audit trail for privacy and compliance purposes. These events subsequently can be sent to 3rd party SIEM vendors, for instance Splunk.

Passwords and sensitive data

A central multi-node redundant vault has been implemented to protect secrets and sensitive data (e.g., authentication credentials, SSL certificates) used throughout the system. The vault stores and creates the secrets and sensitive data, to which access is controlled on a need-to-know basis. Any sensitive data in the persistent stores is encrypted with a key stored in the vault.

Infrastructure Security

Virtual Private Cloud

At the lowest level, ZEDCloud runs on top of a Virtual Private Cloud (VPC) configured to separate the critical components from the outside world. Strict network access control policies restrict traffic to only what is needed to provide connectivity to the ZEDCloud Controller and deployed edge nodes through the EVE-OS API. Management access to ZEDCloud is only permitted through a VPN connected to the VPC. This significantly reduces the attack surface of the cloud infrastructure.

System baseline

Inside the VPC, ZEDCloud consists of multiple Virtual Machines (VM). These VMs are bootstrapped from a secure image, and an automated process keeps the base software up to date and continuously monitors for identified vulnerabilities (e.g., through tracking CVEs) triggering additional software updates as required.

System access

In addition to limiting access to the system through the VPC, a Web Application Firewall is used to protect against common attacks. All API requests are checked for validity in the Service Router to further protect the system.

Vulnerability scanning

Frequent vulnerability scanning and penetration tests help ensure that both internal and external threats are mitigated. The following actions are taken as part of the best practices adopted for ZEDCloud:

- Automated static and dynamic analyses of source code changes as part of the continuous integration
- Regular penetration testing of software by an independent 3rd party to exceed OWASP-10 standards
- Scanning and updating the 3rd party libraries used to build the software for reported vulnerabilities
- Continuous scanning of the base software for reported CVEs

Summary

The edge is a continuum and not all edge computing environments are created equally. ZEDEDA has architected its orchestration solution from the ground up to meet the unique requirements of distributed edge computing deployments, which traditional data center tools do not address. ZEDEDA supports a highly diverse mix of hardware and applications, accommodates legacy infrastructure, protects edge nodes that have no physical or network security perimeter, and balances needs for a mix of OT and IT users.

Together, the ZEDCloud subscription service and open source EVE-OS foundation establish a zero trust security model and defense in depth to ensure that there are no compromises to critical operations. The result is a simple-to-use solution that enables organizations to securely orchestrate distributed edge computing deployments at scale with preferred hardware, applications and clouds. Visit www.zededa.com for more information.

About ZEDEDA

ZEDEDA, the leader in orchestration for the distributed edge, delivers visibility, control and security for edge computing deployments. ZEDEDA enables customers the freedom of deploying and managing any app on any hardware at scale and connecting to any cloud or on-premises systems. Distributed edge solutions require a diverse mix of technologies and domain expertise, and ZEDEDA provides customers with an open, vendor-agnostic orchestration framework that breaks down silos and provides the needed agility and future-proofing as they evolve their connected operations.

Customers can now seamlessly orchestrate intelligent applications at the distributed edge to gain access to critical insights, make real-time decisions and maximize operational efficiency. ZEDEDA is a venture-backed Silicon Valley company, headquartered in San Jose, CA, with offices in Bangalore and Pune, India. For more information, contact info@zededa.com.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current ZEDEDA product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from ZEDEDA and its affiliates, suppliers or licensors. ZEDEDA products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of ZEDEDA to its customers are controlled by ZEDEDA agreements, and this document is not part of, nor does it modify, any agreement between ZEDEDA and its customers.