Onclave TrustedPlatform®

June 2024

Contents

Onclave TrustedPlatform®

The Onclave TrustedPlatform® is a comprehensive solution designed to ensure secure communications and safeguard against sophisticated cyber threats, including those sponsored by state actors. This platform represents a unified approach to integrating identity security, access management, and network segmentation, offering a cohesive framework that supports the implementation of Zero Trust Network Access (ZTNA), Secure Access Service Edge (SASE), Executive Order (EO) 14028, and future requirements. The Onclave TrustedPlatform® facilitates the straightforward implementation of a Zero Trust Architecture (ZTA) network across both existing (brownfield) and new (greenfield) infrastructures. Its modular design allows for deployment in virtualized environments or as physical appliances, providing flexibility for organizations to transition towards ZTA compliance seamlessly over any IP-based network architecture. Onclave Networks commits to delivering robust security measures to protect critical infrastructure and ensure the integrity of communication networks.

Onclave's TrustedPlatform Compared to Other ZTA Solutions

Our TrustedPlatform is a groundbreaking secure communications ZTA network solution, proudly being the first to earn an Authorization to Operate (ATO eMASS 3551) on the prestigious DHA and White House Communications Agency networks, sanctioned by the Defense Health Agency (DHA). Harnessing Onclave's innovative First Principle approach, this state-of-the-art solution uniquely delivers Dynamic Refactoring Network™ capabilities with unparalleled ZTA controls, setting a new standard in network security.

The structure consists of two primary network components shown in Figure 1:

1. **TrustedEdges**: Positioned ahead of assets intended for protection, these create a secure network segment. While assets maintain their addressing through the TrustedEdge, they transition to the Zero Trust network.
2. **TrustedBrokers**: Acting as bridges, these combine the endpoints of TrustedEdges and the devices operating behind them to forge an enclave or network.

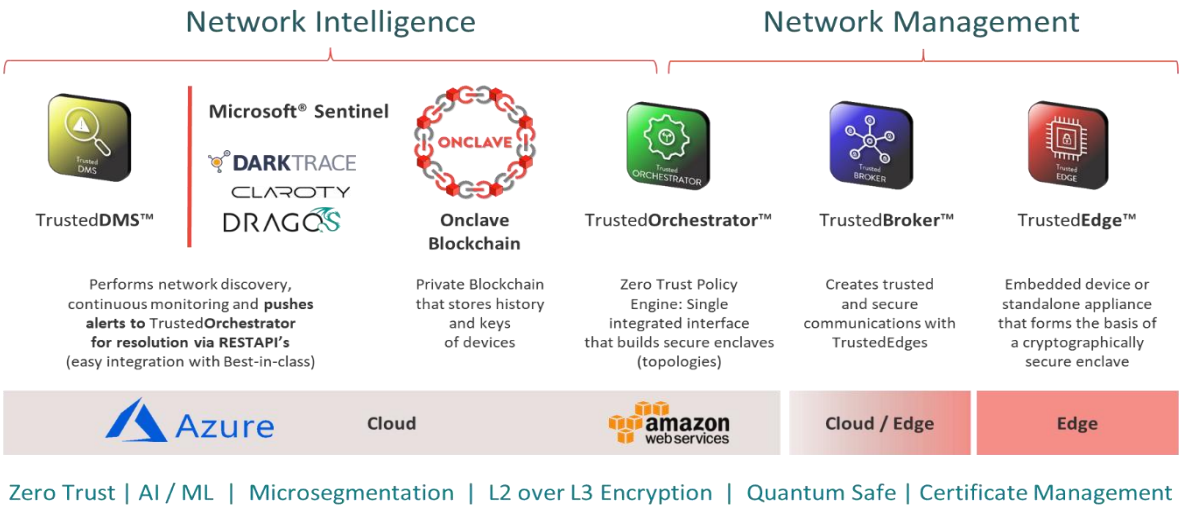


Figure 1 - Onclave TrustedPlatform Components

Both TrustedEdge and TrustedBroker stand out with their ability to integrate into several enclaves. This versatility allows diverse devices and users to connect seamlessly with multiple services. After establishing trust within their designated enclaves, transitioning between them is effortless, whether initiated by users or

managed by the Orchestrator operator. Figure 2 illustrates the flexibility of Onclave's **Dynamic Network Refactoring**.

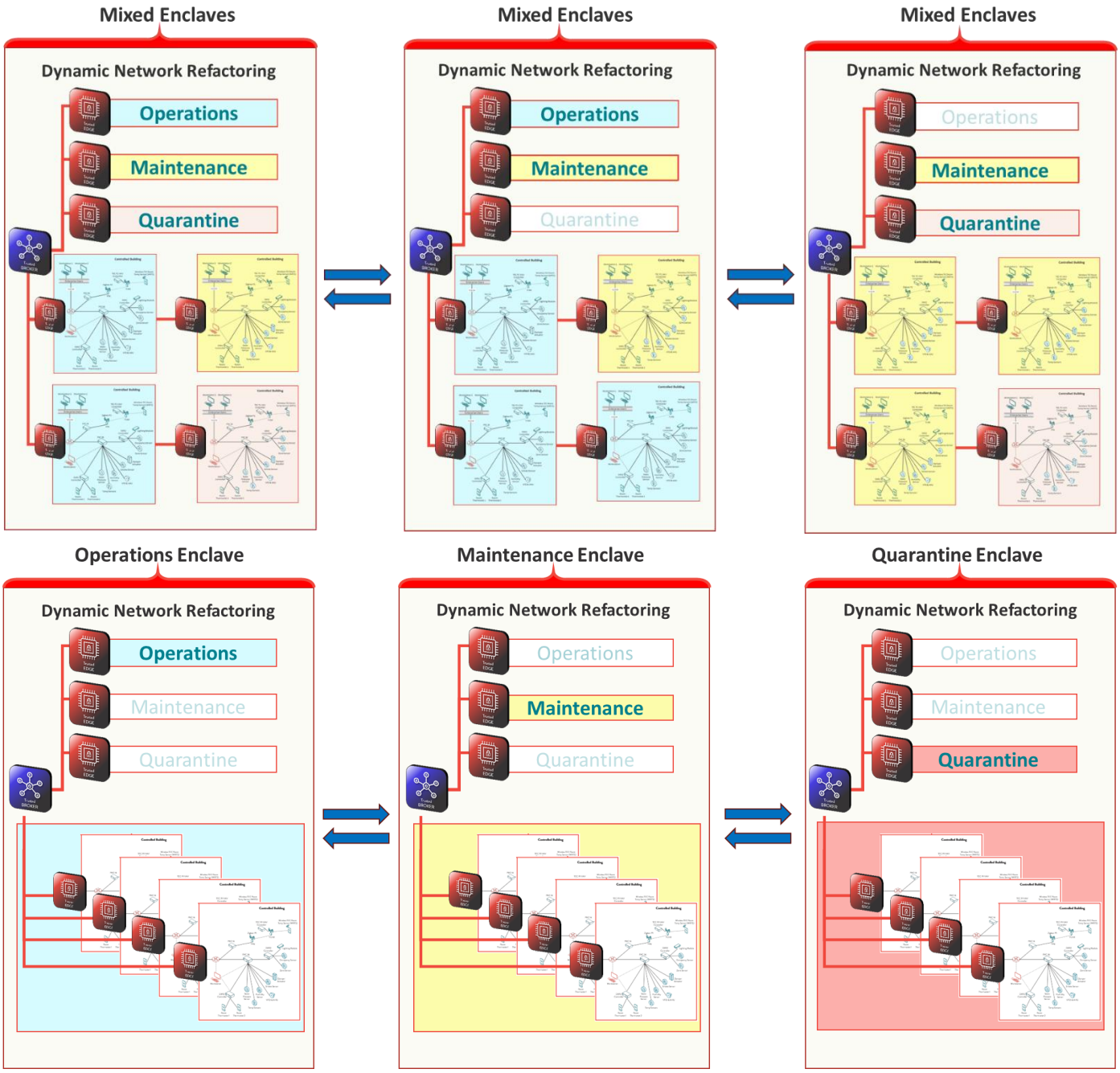


Figure 2 – Onclave's Dynamic Network Refactoring - TrustedEdges and TrustedBrokers in multiple enclaves

Easy to Deploy and Manage

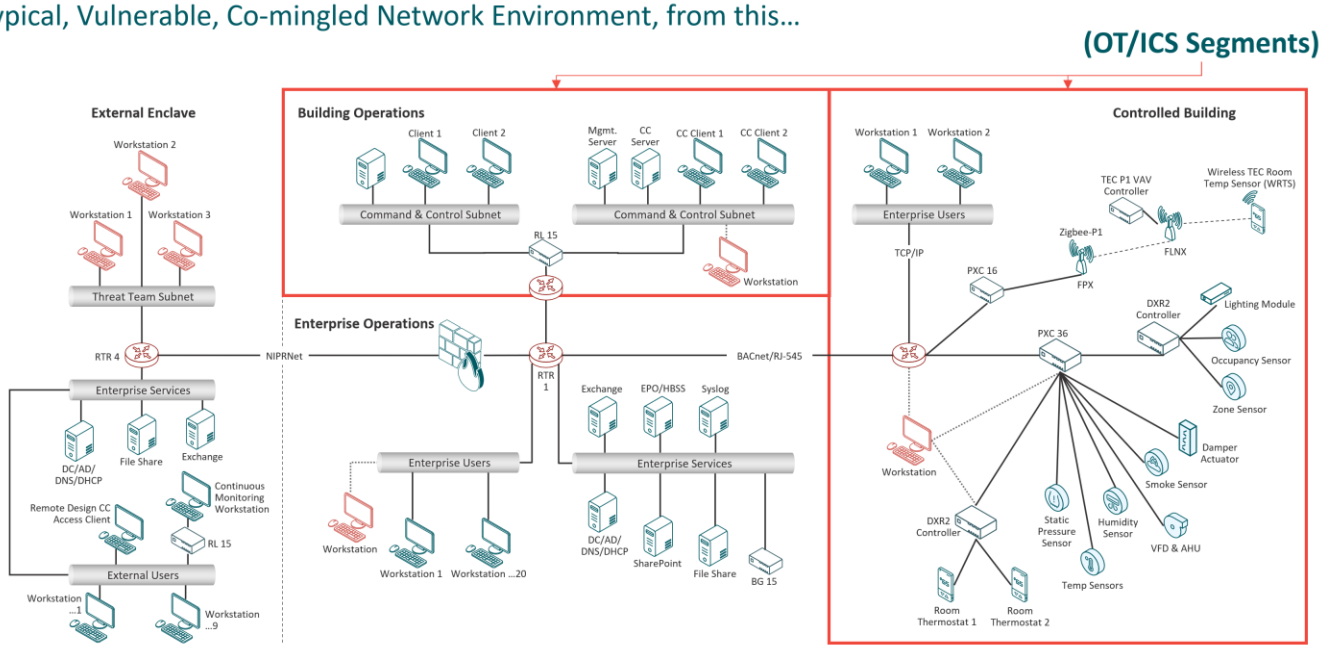
Onclave's policies are easily modifiable, as complex certificate and key rotation operations are fully automated requiring no user intervention. Monitoring for new and compromised systems is also kept simple, with a focus on third-party integration for those who want more advanced compromise analytics to drive Onclave quarantine operations. Quarantine, which is often an operational headache with other frameworks, is comparatively painless with Onclave, enabling remote remediation without disrupting mission-critical operations. Onclave's approach extends to the manageability of operations as a whole, as remote systems can

be patched within the assigned enclaves for patch maintenance without exposing the operations enclaves to remote hostile activity as shown below. Cybersecurity is completely compatible with automation and operational productivity with the Onclave TrustedPlatform®.

First Principles Benefits

- Unencumbered by the constraints of adapting existing network solutions to ZTA requirements.
- Dynamic Network Refactoring.
- Automated certificate and session management eliminates administrative overhead, configuration errors, or the circulation of revoked certificates.
- Transparency to the user and to applications eliminates misconfiguration and user friction.
- Easily integrates with existing enablement services like Active Directory, PKI/KMS, and Endpoint Security.
- No IP changes are required on servers with existing routes between subnets.

Typical, Vulnerable, Co-mingled Network Environment, from this…



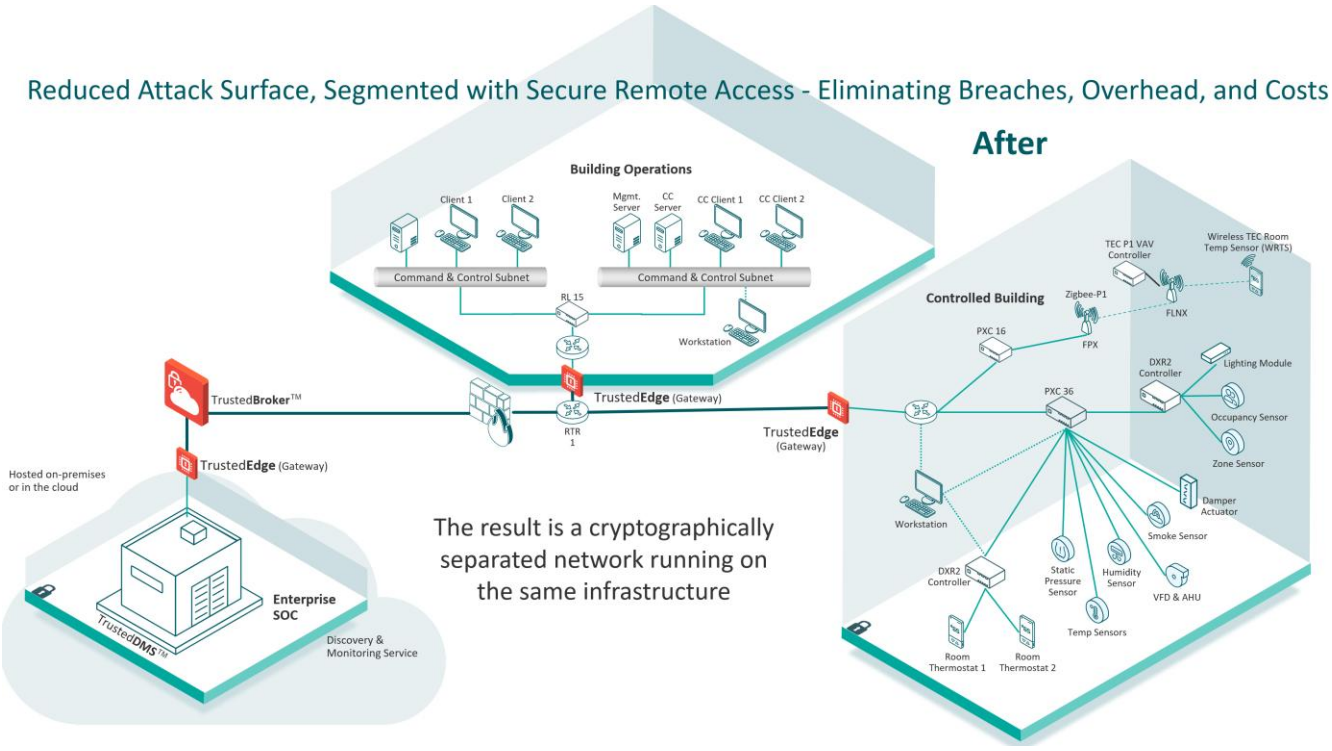


Figure 3 - Deploying into a Brownfield environment

Onclave's Trusted Communications Framework

The Onclave TrustedPlatform® is anchored in the innovative Trusted Communications Framework, a foundational concept that not only predated the National Institute of Standards and Technology's (NIST) Special Publication 800-207 on Zero Trust Architecture (ZTA) but also aligns seamlessly with it while providing expanded control mechanisms. This strategic alignment underscores the platform's development from first principles, unencumbered by the constraints of adapting existing network solutions to ZTA requirements. As a result, the Onclave TrustedPlatform® offers distinctive features and capabilities not found in other ZTA solutions, highlighting its unique value proposition in the cybersecurity landscape.

Onclave's TrustedPlatform enforces the ZTA controls and maps to the NIST 800-207 publication and the ZTA 7 Pillars

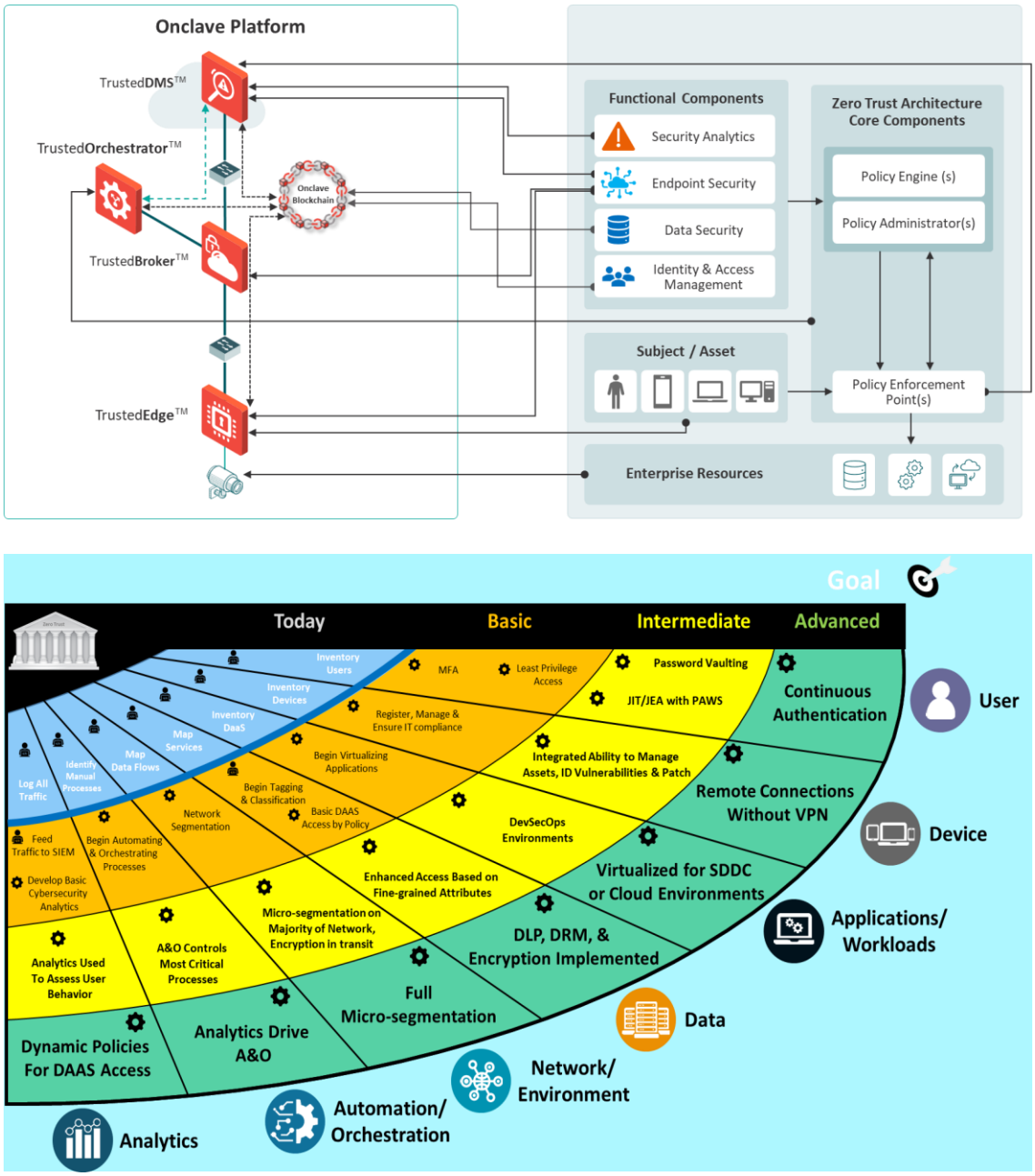


Figure 4 - NIST 800-207 and 7 Pillars

Quantum Ready

Onclave Networks TrustedPlatform is a secure communication platform that integrates NIST post-quantum cryptography (PQC) algorithms to protect against potential threats from quantum computing. The platform includes key encapsulation and digital signature algorithms, as well as an alternative symmetric encryption algorithm, the Qwyit cipher. The platform has been tested and validated through functional tests, security evaluations and penetration testing. Onclave's TrustedPlatform is built to easily integrate with other platforms and can benefit a variety of industries that prioritize secure communication, such as finance, healthcare, and government. Future developments for the platform include adding support for additional quantum-resistant algorithms, optimizing the performance of existing algorithms, and providing dynamic control of algorithm key size and security level per enclave based on security requirements.

Telehealth Solutions

Onclave's TrustedPlatform has been recognized for its potential to enhance security in the healthcare industry. Specifically, Onclave has been referenced in NIST SPECIAL PUBLICATION 1800-30C for securing Telehealth Remote Patient Monitoring Ecosystems. This recognition highlights the platform's ability to provide secure and reliable communication in the transmission of sensitive patient information and data between healthcare providers, patients, and medical devices.

Furthermore, Onclave's TrustedPlatform has also been included in the NATO "Zero-Trust Architectural Framework Enterprise" (ZAFE) pronounced SAFE, hospital in a box. This designation highlights the platform's ability to support secure communication and data management in austere and high-threat environments, making it ideal for deployment in disaster response and military medical operations.

In summary, Onclave's TrustedPlatform provides a secure and reliable solution for the healthcare industry, ensuring the protection of sensitive patient information and data. Its recognition by NIST and NATO showcases its ability to enhance security in telehealth and medical operations, making it a valuable asset for healthcare organizations looking to improve their cybersecurity posture.

ZAFE

Onclave's TrustedPlatform can be used to secure healthcare in several ways:

1. Confidentiality of patient data: With the integration of NIST post-quantum cryptography algorithms, the TrustedPlatform provides strong encryption and secure communication of sensitive patient data, ensuring its confidentiality.
2. Secure data exchange between healthcare providers: The TrustedPlatform can be used to establish secure network overlays between healthcare providers, enabling them to exchange patient data securely and comply with regulations such as HIPAA.
3. Remote patient monitoring: The TrustedPlatform can be used to secure the transmission of patient data collected from remote monitoring devices, ensuring the privacy and security of this information.
4. Clinical trial management: The TrustedPlatform can be used to secure the exchange of trial data between research institutions, ensuring the confidentiality of sensitive information and enabling compliance with regulatory requirements.
5. EHR systems: Onclave's TrustedPlatform can be integrated into electronic health record (EHR) systems, providing a secure and robust infrastructure for storing and exchanging patient data.
6. Telemedicine: The TrustedPlatform can be used to secure the communication between patients and healthcare providers during telemedicine consultations, ensuring the confidentiality of sensitive information.

Overall, Onclave's TrustedPlatform can play a crucial role in securing healthcare by providing robust encryption and secure communication, enabling healthcare organizations to comply with regulations and protect patient privacy.

TrustedPlatform Dataflow and Enforcement Controls

All TrustedEdges and TrustedBrokers are assigned to each other using the TrustedOrchestrator. First, an enclave is defined using the TrustedOrchestrator. Once the enclave is defined, TrustedEdges are assigned to TrustedBroker pools to form the segments of the enclave. There are an elaborate set of out of band communication messages exchanged between the Orchestrator, the Blockchain Interface, and the Edges and Brokers that enables each Edge and Broker pair to be notified via the Blockchain Interface (BCI) at the time

that the Orchestrator operator defines the topology of an enclave. Based on the instructions expressed by the Orchestrator, the Edges and Brokers will negotiate with each other to establish a bilateral trust agreement using an out of band TLS transport. The data exchanged to establish trust are encrypted tokens sent by both the TrustedEdge and TrustedBroker devices. The receiving device uses the public key stored in the Onclave Blockchain of the sending device to decrypt the token and determine if trust can be established. Based on the security level established at the time of defining the enclave, appropriate asymmetric key encryption algorithms will be imposed. This communication methodology is enforced for all messages, which include state messages from the Orchestrator using the BCI to the devices being managed. The key pairs created are elliptical curve and NIST post-quantum asymmetrical keys that are created when either a TrustedEdge or TrustedBroker is registered with the Onclave Secure Blockchain. Registration of these devices require that they present a unique software identity created when the TrustedEdge or TrustedBroker devices are provisioned. These unique identities are formed using a hash identity of the Onclave Secure Blockchain the devices are registering with.

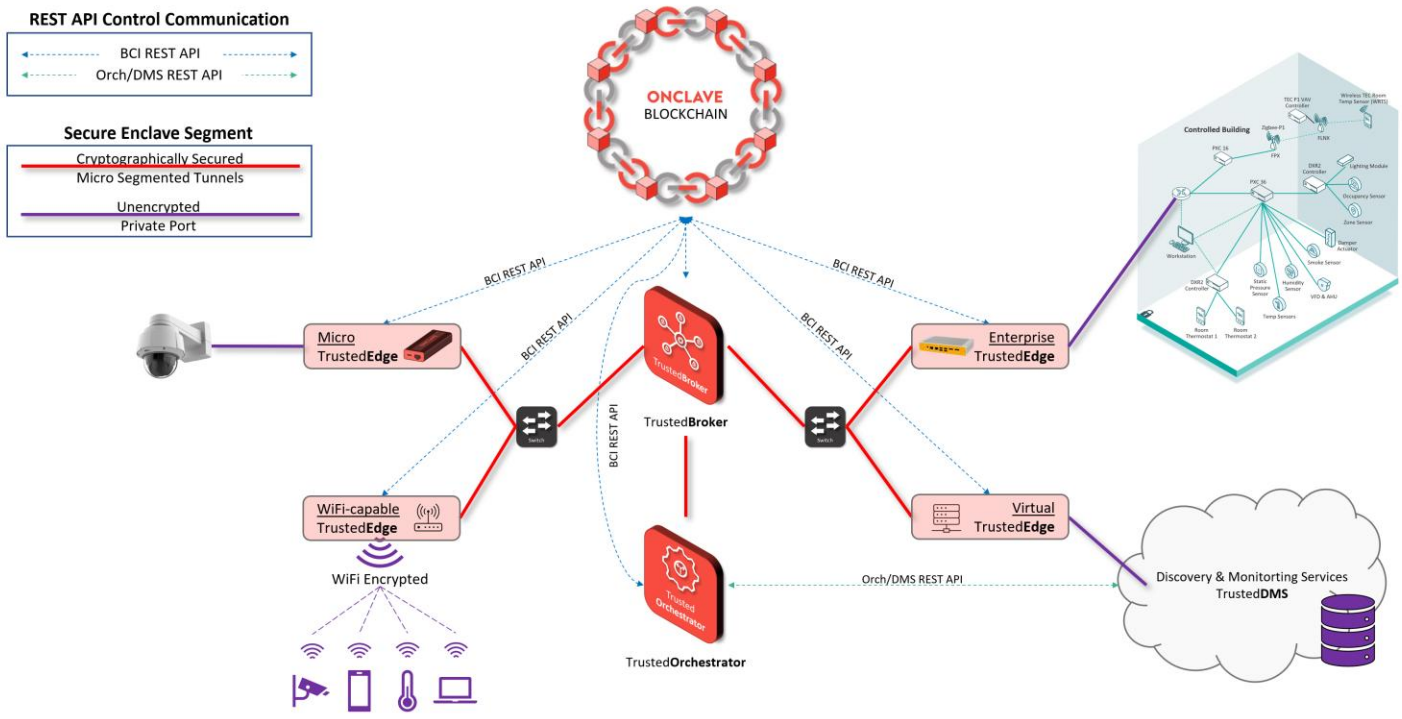


Figure 5 - Bimodal Communication Design Provides Concurrent Data Collection from Multiple Sources

The data communications channel is handled using the AES256 GCM symmetric algorithm to create the micro segmented session tunnels that form the secure enclaves. Before any micro segmented session tunnel can be created, the participating TrustedEdges and TrustedBrokers have to establish a bilateral trust relationship as described above. The security constructs just defined form the basis of the Onclave TrustedPlatform Zero Trust Architecture. With this foundation Zero Trust controls can be enforced with separate data and management communication channels which aligns with the NIST 800-207 Zero Trust Architecture publication and ensures total adherence to the separation of data and management control planes between inter and intra operating environments.

Onclave's dual layer security solution using an encrypted layer 2 inside an unencrypted layer 3 port tunnel is a transport agnostic overlay that conforms to existing installed networks, deployed to create security segments

that stretch from edge to core or edge to cloud. Common degraded path scenarios occur in the backhaul resiliency frameworks for remote edge and near edge environments. To manage route control, customer's often rely on SD-WAN or transport bonding solutions to manage their backhaul resiliency policy across their diverse carriers. As an overlay, our software assumes the presence of route resiliency platforms like an SD-WAN between us and the backhaul links, such that our connectivity has the same network resiliency as the existing deployed environment, but now with our added ability to microsegment within that location specific security enclaves as well as their secured endpoints in corresponding data center, co-lo, or cloud destinations.

The data of the traffic we secure can be utilized by SD-WAN providers as a routing policy, as well. If the customer, for instance, has used our platform to isolate their most critical data segments, then the SD-WAN would be configured to give traffic associated with our enclaves priority within their backhaul and route policies. If, on the other hand, they wanted to isolate lower priority systems that happen to possess significant security vulnerabilities (such as found on building sensors, HVAC units, or building environmental systems), they might instead choose to map our platform to a lower priority SD-WAN path because it is a segment that they are willing to cannibalize during a period of network congestion or other degradation.

For those customers concerned about complete loss of connectivity to their remote sites, we typically utilize a deployment topology where our edges and a broker (or brokers) are deployed at the site, so that loss of backhaul cannot result in a loss of connectivity between the security segment enclaves. This prevents the backhaul links from either becoming a congestion/degradation point or potential failure point in the traffic between segments.

Figure 6 - One of Onclave's Monitoring Dashboards

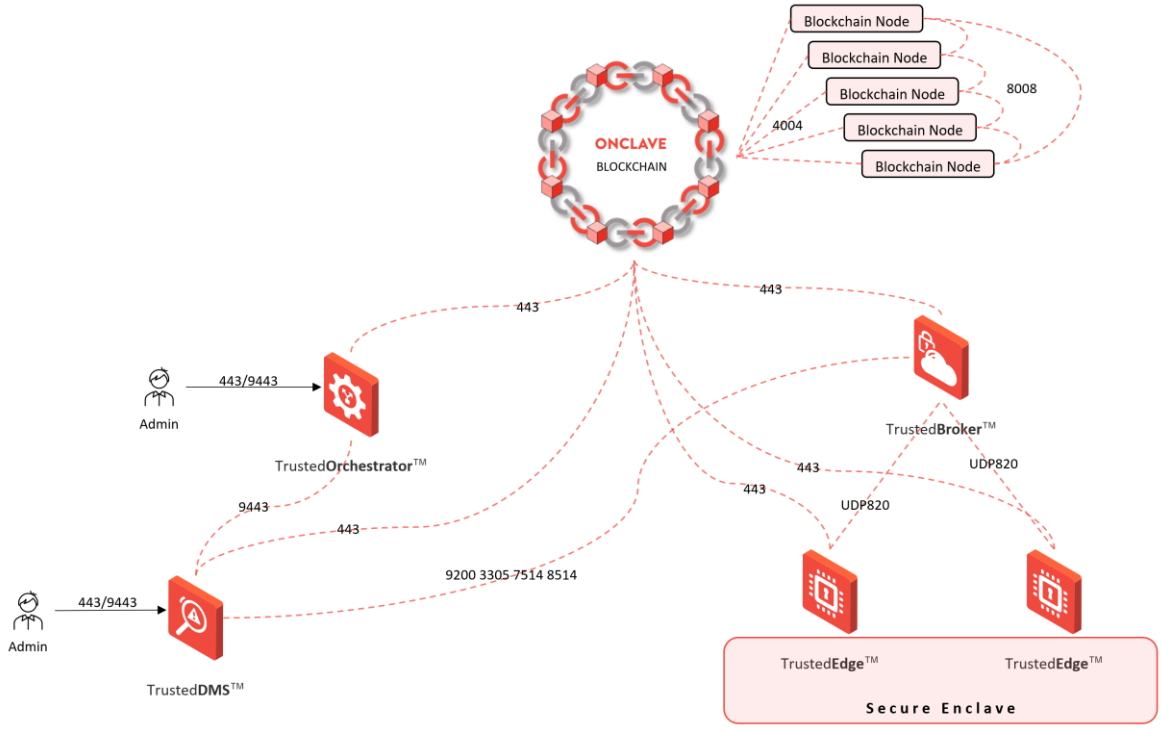


Figure 7 – Dataflows

Business Benefits

- Drives growth, margins, and client loyalty by eliminating barriers to digital transformation.
- Enhances Internet of Things (IoT) solutions by embedding Onclave, which uniquely preserves the integrity and confidentiality of digital communications.
- Reduces the risk, cost, and complexity of digital transformation at scale and speed.
- Increases profit margins and cost savings through the ease of deployment, simplified certificate management, and lower network overhead.
- Increases new and existing revenue by extending the value of existing offerings and introducing enhanced security offerings.
- Accelerates portfolio and platform transformation.
- Delivers differentiated client value.
- Increases client loyalty by reducing losses due to unsecure data movement

Enterprise Risk Reduction

- Session-unique ephemeral certificates protect previous, current, and future sessions against replay attacks.
- Requires endpoint authentication (certificate) and validation (KeyID), so unknown requests are ignored and unacknowledged.
- Point-to-point encrypted tunnels protect all IP traffic with one of the most trusted protocols.
- Is a proven technology with active deployment by the U.S. government.
- Improves network encryption of data in transit.
- Leverages today's cloud environments to enable key distribution at scale.
- Creates point-to-point private networks on the fly, terminating at a virtual TrustedEdge.
- Derives new ephemeral encryption keys for each connection, which greatly reduces the risk of "break once, run everywhere" and replay attacks.
- Authenticates endpoints prior to establishing any connections or exposing any resources.
- Moves traffic entirely within enclaves without the additional creation of externally accessible endpoints.
- Changes the economics and utility of point-to-point encryption and authentication.
- Transforms encryption from an edge-to-device solution to a device-to-device solution.
- Enables encrypted, secure data communications in scenarios where it is currently impossible, difficult, or too expensive to scale.

Cost Savings

- Software-based capability eliminates the need for additional expensive network appliances such as routers and VPN concentrators, and associated operational costs.
- Simplified key and certificate management reduces administrative costs.
- Comprehensive set of APIs leverages existing services and platforms.
- Pluggable encryption facilitates transformation and consolidation of services and platforms.
- Onclave's Dynamic Network Refactoring™.

Summary

The Onclave TrustedPlatform is a comprehensive solution that provides secure communication and network segmentation for Zero Trust Architecture (ZTA) compliance. It consists of two main components: TrustedEdges and TrustedBrokers, which create and connect secure enclaves across any IP-based network. The platform is based on the innovative Trusted Communications Framework, which aligns with the NIST 800-207 publication on ZTA and provides expanded control mechanisms. It also integrates NIST post-quantum cryptography algorithms to protect against potential threats from quantum computing. The Onclave TrustedPlatform offers several benefits, such as easy deployment and management, dynamic network refactoring, automated certificate and session management, transparency to users and applications, integration with existing services, and no IP changes required on servers. It uses a bimodal communication design that separates the data and management communication channels, and an encrypted layer 2 inside an unencrypted layer 3 port tunnel, which is transport agnostic and conforms to existing installed networks. It also uses session-unique ephemeral certificates, point-to-point encrypted tunnels, and endpoint authentication and validation to enforce ZTA controls. The Onclave TrustedPlatform has been recognized by NIST and NATO for its potential to enhance security in the healthcare industry, especially in telehealth and remote patient monitoring ecosystems. It can provide secure and reliable transmission of sensitive patient data and information between healthcare providers, patients, and medical devices. It can also support secure communication and data management in austere and high-threat environments, making it ideal for deployment in disaster response and military medical operations. The Onclave TrustedPlatform can help drive growth, margins, and client loyalty by eliminating barriers to digital transformation, enhancing IoT solutions, reducing the risk, cost, and complexity of ZTA implementation, increasing profit margins and cost savings, and delivering differentiated client value. It can also reduce losses due to unsecure data movement, improve network encryption of data in transit, and enable encrypted, secure data communications in scenarios where it is currently impossible, difficult, or too expensive to scale.