ENCLAVE™

Microsegmentation for Enterprise & SMB

USE CASES

• Single platform for both IT and Cyber teams to manage access controls.

• Blocks lateral and ransomware movement inside corporate environments & across remote networks.

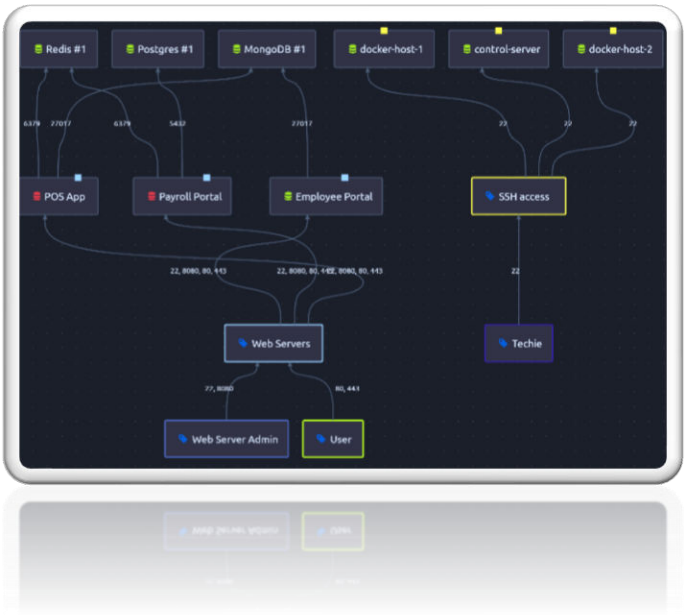
• Deployable to environments via installable agent. There is no need to rip and replace anything.

• Provides automated microsegmentation with low administrative overhead.

• Provides high-level and detailed information about network traffic on all devices.

• Provides an automated ACL-like workflow writing and maintaining rules.

• Blocks access and only allows what's granted to each device.



Key Benefits

- Enclave seamlessly combines access control, microsegmentation, encryption and other secure networking concepts to create a comprehensive solution.
- A network infrastructure management platform made to ease managing on-premise and hybrid network infrastructure.
- Detect hidden assets, visualize your network and control communication flow so you can microsegment on demand.
- Enclave allows IT & Cyber teams to easily segment networks, place the right staff in those segments and manage traffic.

The Challanges

Your organization's environments are a target for cyber attackers. The data, business processes, access control devices, system acounts and intellectual property all have tremendous value to attackers. In many cases these are not one-off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and business leaders to be vigilant and recognize when something is not right.

The ultimate goal of cybersecurity is to ensure the available, reliable and secure operation of business or IT environments from procurement to retirement.

Current best practices and models expect network segmentation within IT environments. This limits the potential for cyberattacks and reduces the impact of any single security incident. In a modern cybersecurity context, ensuring that there are strict controls and firewalls between each level, as well as robust authentication and authorization measures, is vital.

IT and cybersecurity teams have limited collaborative tools and resources to effectively implement modern measures. Segmentation is difficult to effectively implement and more challenging to manage ongoing. Ransomware's impact, as a modern threat, is more destructive due to lack of barriers and segmentation in corporate IT environments.

SideChannel | ENCLAVE

ENCLAVE™

SYSTEM REQUIREMENTS

Microsoft Windows

Linux (x86 / ARM)

MacOS

Docker Images

Virtual Machines

Rugged small-form factor HW

INTEGRATIONS

AWS IAM Identity Center

Google Workspace

Microsoft O365

Microsoft Active Directory

Okta

Duo

OpenID Connect (OIDC)

SAML 2.0

RESTful API

ADDITIONAL INFO

On-Premise / Cloud Deployment

Supports AES-256 bit encryption

FIPS 140-2 Certified

Available via GSA

The Solution

Enclave is a modern network segmentation platform that combines – access control, asset inventory, encryption and zero trust network access – to create a breakthrough microsegmentation solution that prioritizes both IT and cybersecurity's highest level needs. Enclave is purpose-built to simultaneously secure and segment your networks. Limit the damage a bad actor can do by decreasing the digital square footage they can explore. Easily implement access controls for employees, support staff, and third party vendors while never distrupting current operations.

Platform Components

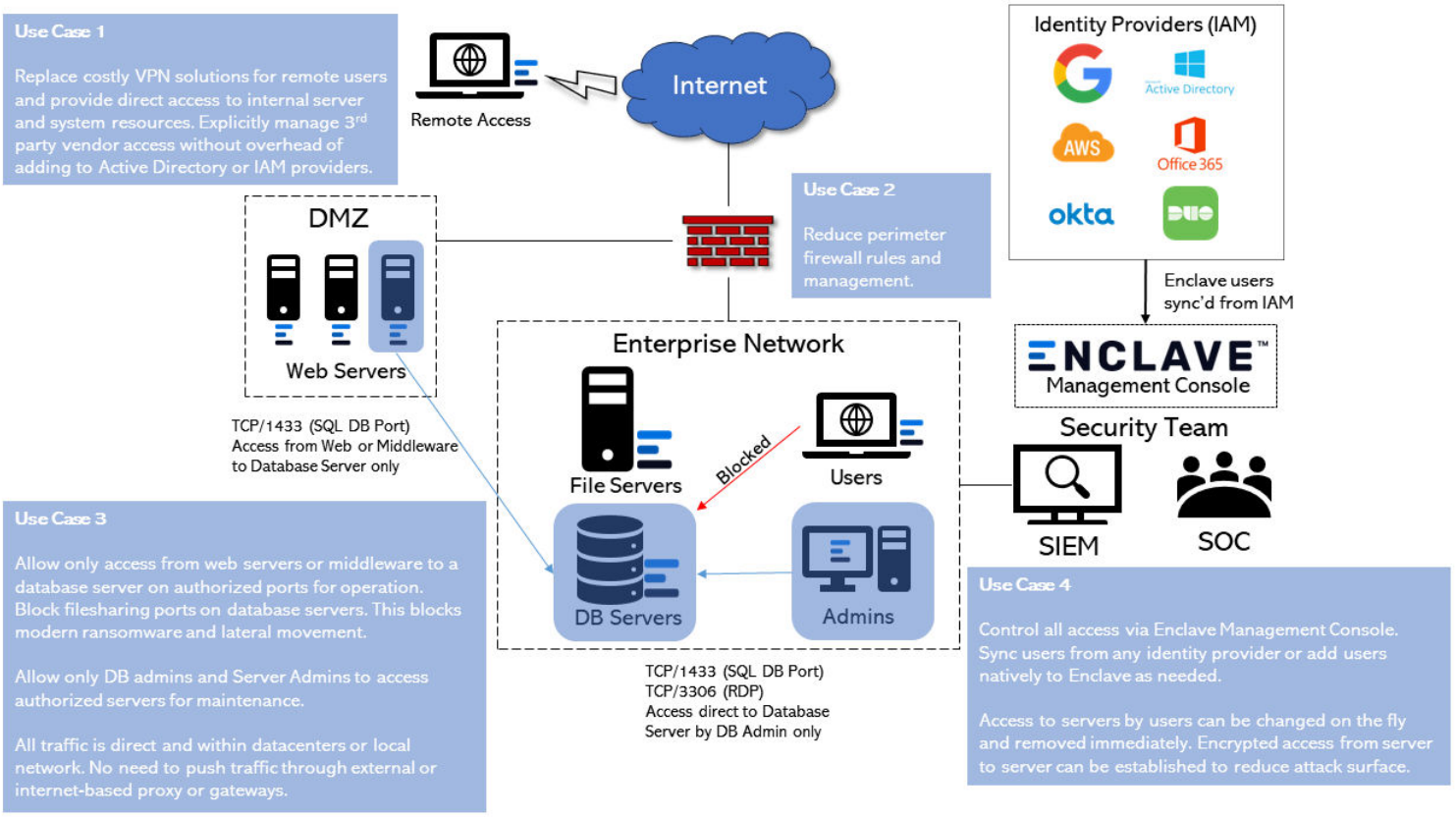
1. Enclave management console (EMC) is the central control for the platform. In the EMC, you configure your enclaves (microsegments), manage how machines (or users) will authenticate, and alter any configuration.
2. Agents are the end users of an enclave. An agent is the installed bundle that you place on all IT nodes to be managed in the EMC. Agents are also deployable via rugged small form factor (RSFF) tactical systems inline with OT/ICS/SCADA or legacy OS based systems.
3. Beacons provide resolution between nodes. Enclave works by creating an overlay network (a network that is not routable from the internet). Beacons exist to translate the overlay IP space to the physical IP space. Beacons do their best to support direct connections between nodes, but if a direct connection is not possible, the beacon can also act as a relay, passing traffic between nodes.

Key Features

Segmentation: Utilizing overlay networks, firewalls, and a Zero Trust network permissions model to create spaces where access is only granted to specified machines and users.
Asset Discovery: Detect unknown assets sitting on the network.
Enhanced Visibility: Gain insights into unused or underused assets, helping in optimization and finding potential cost savings.
Track and Manage Assets: Monitor all the devices and applications within the network, categorizing and sorting them according to your policies and privilege levels.
Real-Time Vulnerability Scanning: Continuous network scanning identifies and tags potential vulnerabilities and points to their exact location.
Prioritization and Management: Categorize vulnerabilities based on CVSS severity scores and potential impact, allowing for targeted remediation.
Integration with Tools: Seamlessly integrate with existing security solutions to create a multi-layered defense system.
Done for you: Enclave is fully managed. Implementation is as simple as installing an agent.
Align with policy changes on the fly: Making changes is as easy as dragging and dropping.
Visual Mapping: Generate real-time visual maps of how information is flowing within the network, identifying bottlenecks or insecure paths.
Collaboration and Planning: Easily share accurate diagrams with different teams, aiding in coordinated planning and response.
Compliance and Reporting: Maintain compliance by having a detailed inventory that can be leveraged for audits and reporting. Meets controls in NIST SP 800-53, NIST CSF, DoD Zero Trust Model, CISA Zero Trust Model, CMMC, and ISO 27001:2022.

ENCLAVE™

Enclave Deployment Diagram & Use Cases



ABOUT SIDECHANNEL

SideChannel helps emerging and mid-market companies protect their assets. Founded in 2019, the company delivers comprehensive cybersecurity plans through a series of actions branded, SideChannel Complete.

SideChannel deploys a combination of skilled and experienced talent, and technological tools to offer layered defense strategies supported by battle-tested processes. SideChannel offers Enclave; a network infrastructure platform that eases the journey from zero to zero-trust. Learn more at sidechannel.com.