BLOCK ARMOUR

Securing a US-based Public Healthcare Organization with

Block Armour's Secure Shield Zero Trust Platform

INTRODUCTION

In the face of increasing cyber threats and the need to safeguard sensitive healthcare data, a US-based public healthcare organization in California, the United States of America, turned to Block Armour's cutting-edge cybersecurity solutions to fortify its critical infrastructure and protect sensitive information. This case study explores how Block Armour's technology helped the healthcare organization achieve its security goals while maintaining strict regulatory compliance with regards to storing and accessing sensitive EHMR data.

BACKGROUND

The healthcare organization is a government-operated entity responsible for providing healthcare services and medicine to citizens. It manages a vast amount of sensitive data, including patient records, medical data, personally identifiable information (PII), protected health information (PHI), and electronic medical records (EMRs).

CHALLENGE

The organization faced several challenges:

Remote Work Transition

The COVID-19 pandemic forced the organization to implement remote and hybrid working arrangements for its employees, increasing the need to secure remote access to sensitive data.

Unauthorized Access Prevention

It was crucial to ensure that only authenticated and authorized devices could access sensitive data, including company-provided laptops and devices.

Data Leak Prevention

The organization needed robust measures to safeguard against data leaks and malware infections. They needed a solution that could reduce the attack surface significantly, preventing any possible instance of access to sensitive data. The requirement was for an effective solution that contained or restricted access to data and minimizing the potential damage.

Regulations and Compliance

Being a public healthcare organization, they need to comply with federal regulations and industry standards such as HIPAA compliance.

BLOCK ARMOUR'S PROPOSED SOLUTION

Block Armour's Unified Secure Access, powered by Blockchain and SDP architecture, secures on-prem systems, providing compliant access for office and remote users. It simplifies Zero Trust implementation, replacing traditional products with next-gen Server Protection and Network Access.

To address these challenges, the healthcare organization adopted Block Armour's Zero Trust Network Access Control Solution, which offered the following functionalities and features:

Inherent Zero Trust Network Access:

Ensured that all network access followed a Zero Trust model.

NIST Compliance:

Aligned with the National Institute of Standards and Technology (NIST) Zero Trust framework.

Regulatory Compliance:

Ensured regulatory compliance with the latest standards set by the US government, such as HIPAA.

Data Integrity:

Separated control and data planes for enhanced data integrity.

Flexible Deployment:

Block Armour Secure Shield can be deployed both on the cloud and on-premises. Being a highly regulated entity, the customer wanted a solution that could be deployed on-prem. This key differentiator gave Block Armour an edge over the competition, offering a comprehensive Zero Trust framework deployment within the organization's data center/servers.

Encrypted Access:

Provided zero-trust and encrypted access for both cloud-based and on-premises applications.

Trusted Device Identity:

Utilized secure mechanisms to establish trusted device identities.

Device Posture Checks:

Performed checks to ensure device security before granting network access.

Server Protection:

Protected servers with a zero-trust architecture.

Single Pane of Glass:

Offered a unified visibility dashboard.

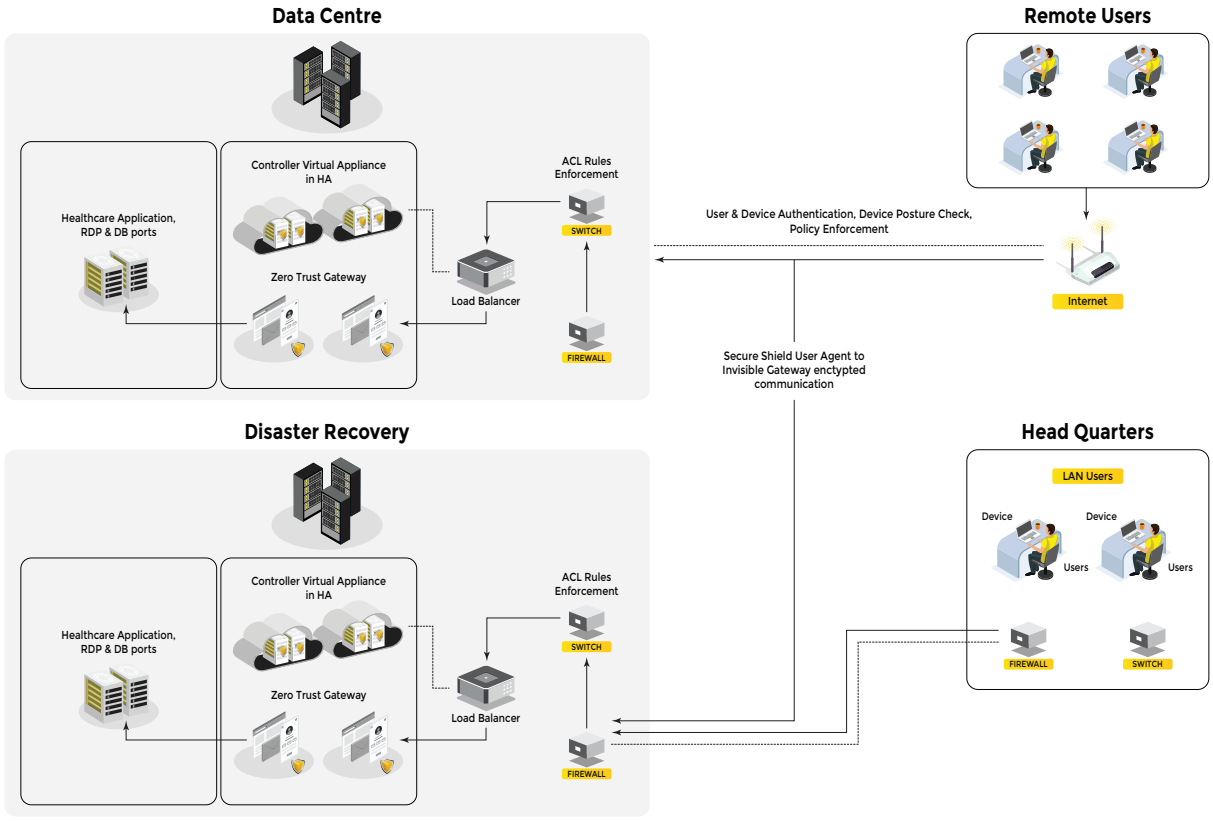
Simplified Licensing:

Streamlined licensing model for ease of use.

SOLUTION ARCHITECTURE

Block Armour's Secure Shield Architecture (SSA) formed the foundation of this solution. SSA, built on Zero Trust principles, secured the organization's enterprise systems with a single platform. Key components of SSA included:

- Secure Shield Controller: Centralized Management server that performs user-device authentication, policy management and tamperproof logging.
- Private Permissioned Blockchain: Automated tamper-proof device digital identities.
- Zero Trust Gateway: Deployed in an on-prem Data Centre environment, making servers/ applications invisible and allowing access only to authorized users and devices.



In this deployment:

- Secure Shield Controller instances are deployed in the Data Centre, Disaster Recovery.
- Zero Trust Access Gateways are deployed in the Application Server Segment.
- User Agents are installed on employees' endpoints.

WORKFLOW

User Authentication:

Legitimate users input their credentials in their authorized devices, triggering the SSO. The agent automatically logs into the the system with the user credentials.

MFA is Triggered (Optional):

After the authentication process is completed, multi-factor authentication gets triggered.

Device Posture Check (Optional):

The device's security posture is evaluated to ensure compliance.

NAC Created Tamperproof Digital Identity:

The combination of the username and password entered via the authorized device creates a unique tamperproof digital identity validating the user-device combination. This digital identity is created and stored on the blockchain, making it impossible to spoof.

Secure Access Connection:

Post validation and authorization, a secure access tunnel is established between the device and private servers where applications and data are stored within the organization. Authorized resources and Zero Trust Access Gateway details are sent to the user device.

Encrypted Access:

A secure, encrypted connection is established between the user device and the resource server/ application. This secure access tunnel offers encrypted, micro-segmented access between endpoints and applications and private servers within the enterprise.

Continuous Protection:

The Gateway remains invisible to other network systems, ensuring continuous protection.

Immutable Logging:

All access logs and activities performed are stored on the blockchain for tamper-proof visibility.

RESULTS/BENEFITS

Block Armour's Zero Trust controller was deployed on-prem in the organization's data center. The SDP architecture of the solution ensured only legitimate users and devices go through the workflow to access applications and sensitive data stored in the organization's servers. access it offered also

The use of the Zero Trust gateway greatly helped in reducing the attack surface. The Gateway rendered the organization's private servers invisible to external attackers and thus protected the organization's sensitive data and applications from compromise.

This implementation fortified the organization's cybersecurity posture, ensuring the safeguarding of sensitive data and critical infrastructure and adherence to compliance. Block Armour's solution effectively mitigated the risk of data breaches, malware attacks, and unauthorized access, providing a robust defense for this US-based public healthcare organization.

BLOCK ARMOUR

info@blockarmour.com
linkedin.com/company/BlockArmour
spacearmour.io
twitter.com/BlockArmour