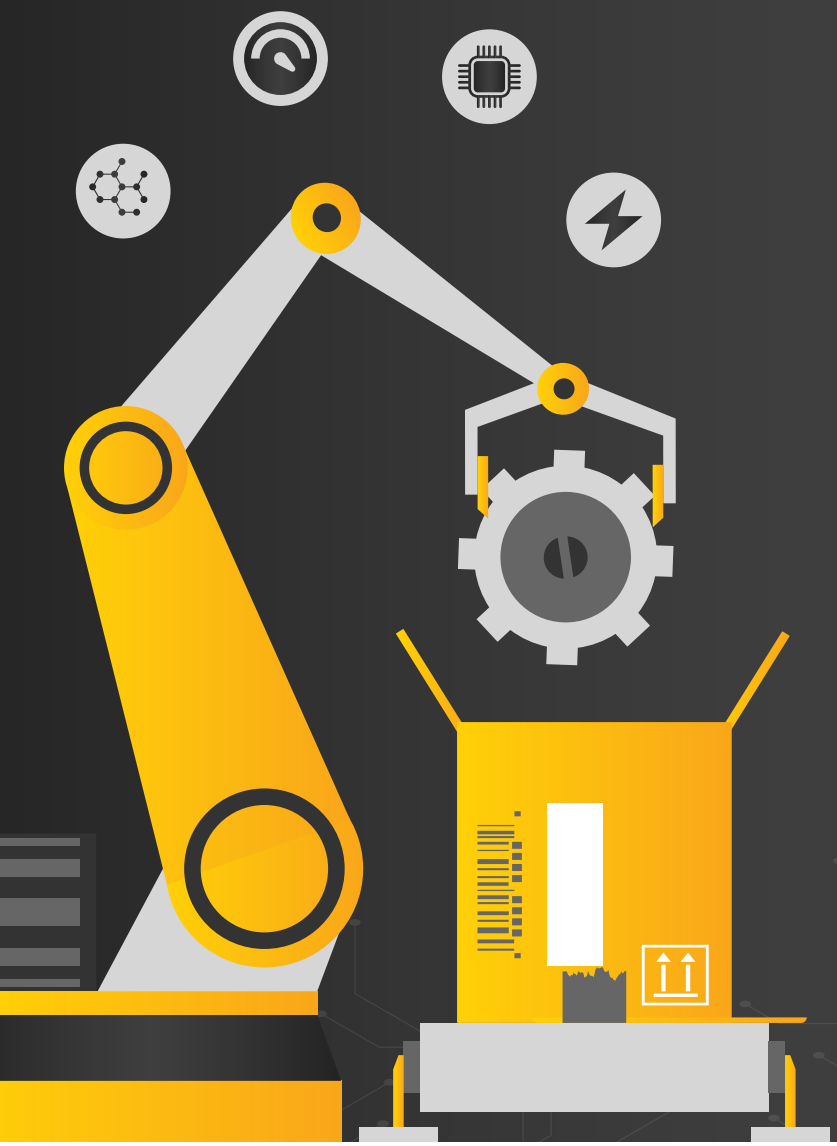
BLOCK ARMOUR

CASE STUDY

A leading manufacturer uses Block Armour to secure its SCADA systems and Cloud-based data analytics platforms while enabling tamper-proof communication across the critical OT-IT interface

Situation

The client, a subsidiary of a leading Japanese manufacturer of consumer electronics and associated services is rolling out digital transformation programs that will see it shifting to an Industry 4.0 model and adopting cloud technologies across its operations including Data Analytics



Challenge

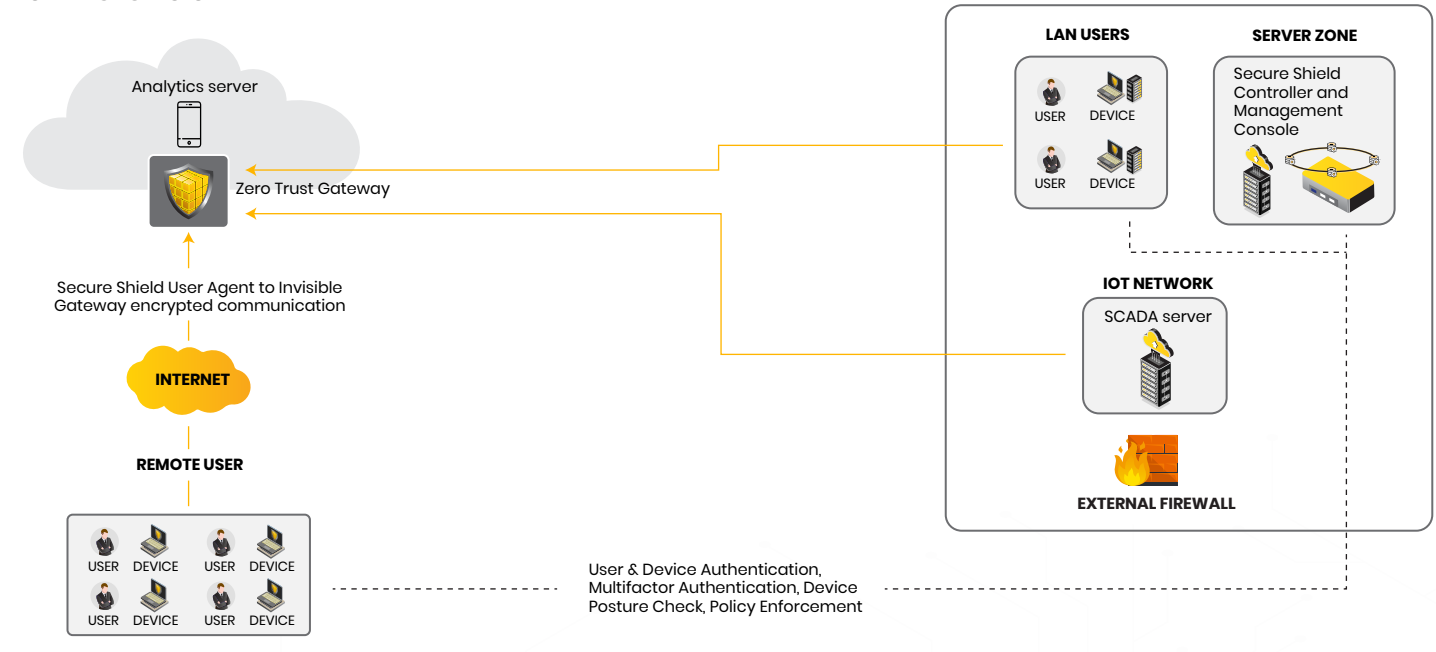
- As the organization continues to adopt Industry 4.0, its legacy security systems were no longer adequate to protect the evolving IT and OT environments, leaving them vulnerable to attacks.
- Key requirements included protecting the OT environment from IT-based cyber attacks by creating a virtual air-gap, securing the new Cloud-based Data Analytics platform from attacks especially those originating on the Internet, preventing Man-In-The-Middle (MITM) attacks and compromise of data while in transit between the SCADA systems and Cloud data lakes; all while allowing only authorized users and devices to communicate securely with Data Analytics applications

Solution

- Block Armour deployed its award-winning Secure Shield platform within the customer's IT environment with the on-premise controller ensuring policy based secure and compliant access by authorized users and devices only after strong authentication and posture validation.
- A Zero Trust gateway was deployed in the Cloud to secure the Data Analytics server and make it undiscoverable on the network. Software-based agents were installed on the SCADA system and the user end-points to ensure pre-access authentication, authorization, and micro-segmented encrypted communication.

Result

- The customer was successfully able to secure its on-prem SCADA systems and Cloud-based data lake / analytics applications and ensure secure tamper-proof communication between the two.
- The Data Analytics applications were rendered invisible on the Cloud network to ensure that only authorized users from authorized devices could access this application based on a defined policy.
- A micro-segmented secure access reduced the attack surface area against malware and ransomware threats.



Block Armour Secure Shield platform secured the client's SCADA systems as well as its Cloud-based data lake and analytics platforms while ensuring a secure micro-segmented and encrypted communication across the critical OT-IT interface based on Zero Trust principles