

How Block Armour enabled secure remote access to on-premise as well as SaaS applications for a Fortune 500 Oil and Gas firm subsidiary?



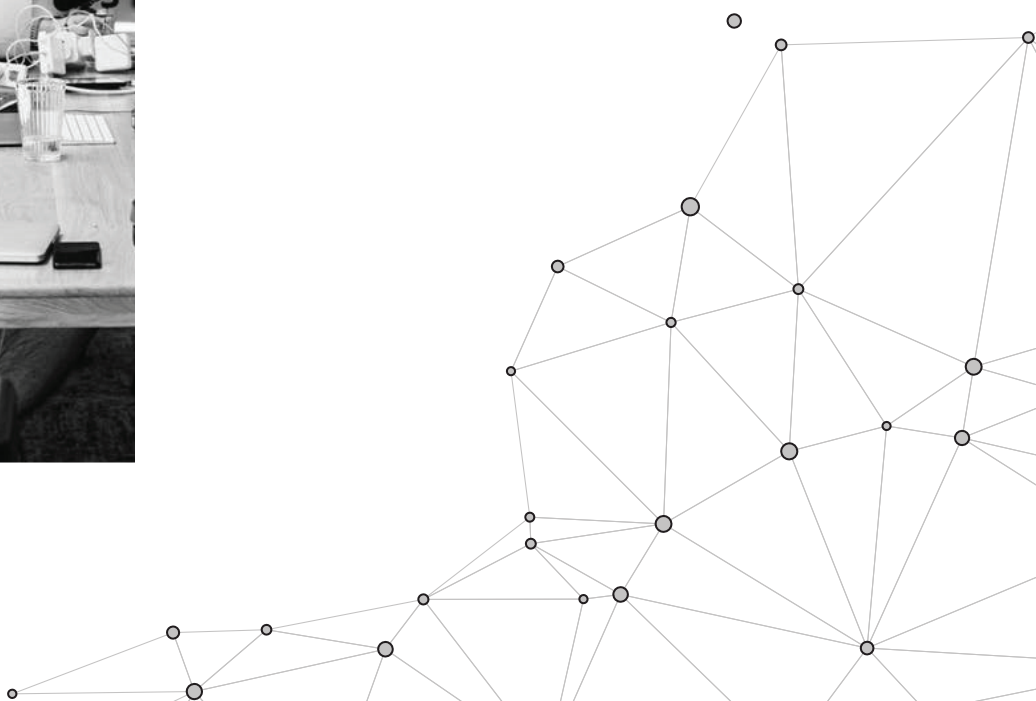
The Challenge



For one of our prestigious clients, a leading player in the Oil and Gas distribution sector, working from office was the norm. All employees carried out their daily activities from their desks at the company offices. Remote working was very minimal and used only by the executive management when they were traveling.

As the COVID-19 pandemic became a global problem, governments across the world called for lockdowns and workplaces had to be closed. Organizations were faced with an unprecedented, novel challenge of ensuring business continuity without endangering employee health and safety. Organizations had to implement a complete paradigm shift in the way they worked without much notice. Remote access was to be provided to all employees so that work could continue as before.

Our client had a combination of on-premise and SaaS solutions that their employees needed to access. The immediate need was to leverage existing resources but enable connectivity for all users.



Major Concerns

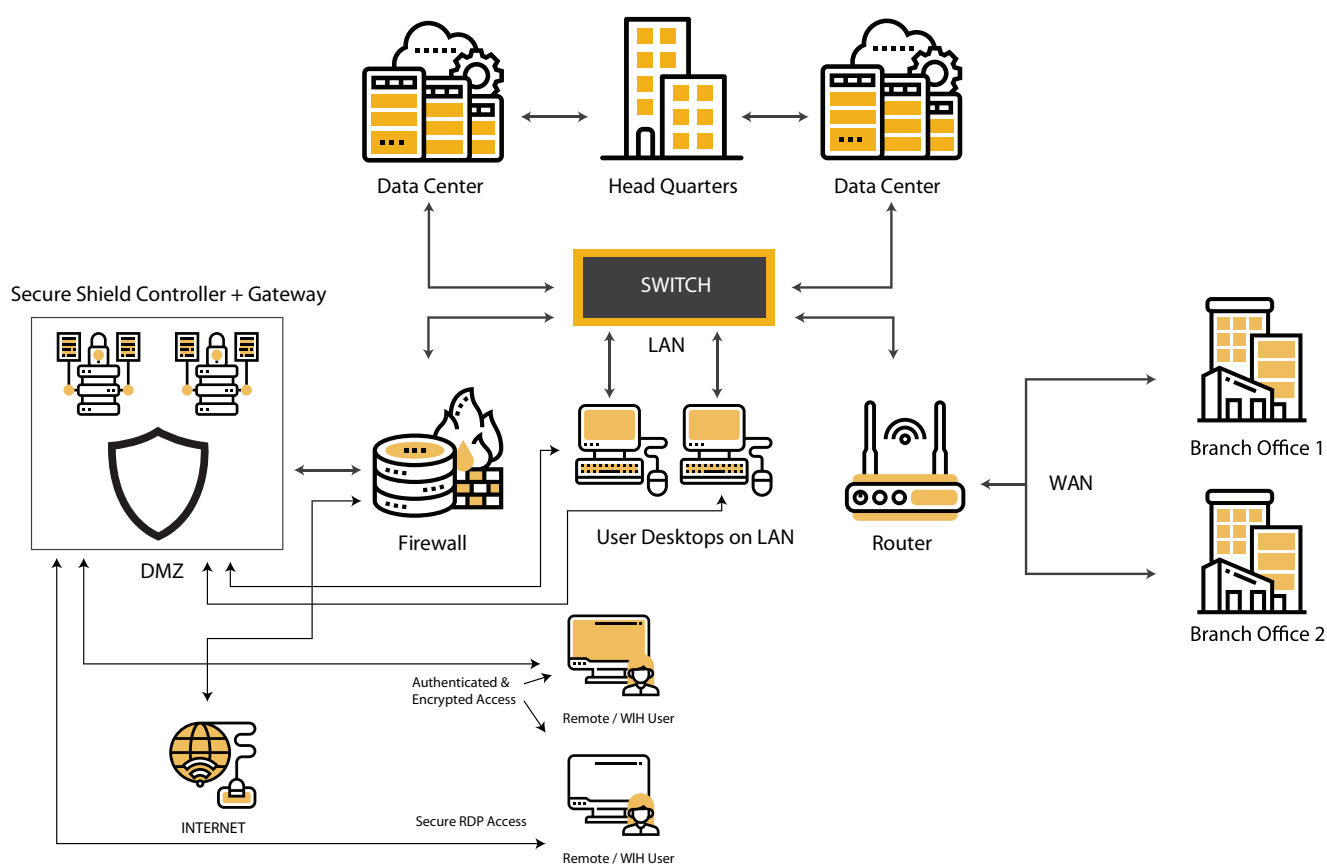
The issues faced by our client were:

- 🛡 Inability to issue company-issued laptops and mobile devices that had proper security measures in place, to all users due to the pandemic
- 🛡 Inability to scale up the VPN for all employees due to dependence on hardware upgrade, which was a challenge during Covid-19
- 🛡 Lack of proper security measures on personal devices
- 🛡 Inability to control access from unauthorized devices
- 🛡 Inability to maintain necessary antivirus or protection on personal devices of employees
- 🛡 High risk of malware attacks, and therefore high risk of viruses and trojans spreading across VPN
- 🛡 Legacy ERP system that was difficult to access on traditional TLS-based connections



The Solution

Block Armour implemented the Secure Shield product providing secure Remote Access to the organization's employees enabling access to organization applications. The solution is robustly designed using Zero Trust, Software Defined Perimeter (SDP) architecture, and Blockchain technology. The Remote Access solution provides maximum security for enterprise systems and cloud servers by making them invisible to prevent malicious attacks at the same time facilitating secured communication channel to access the applications. Our solution also ensured holistic security by providing user and device authentication and encrypting user-server communication.



Unlike the traditional VPN, which was both complex and cumbersome to deploy, Secure Shield was easy to implement and manage. Also, minimal changes were needed in the organization's IT environment, thereby, bringing down costs and reducing the implementation time.



Secure Shield enabled precision remote access to the customer's legacy ERP system from authenticated and authorized users and devices and ensured rogue systems will never connect to corporate network. For certain users, RDP access was enabled to user desktops within the corporate LAN without exposing the internal network over the Internet. By enforcing RDP policies, we additionally ensured the integrity of sensitive data and prevented data leakage.



Our solution ensured that both the user and device were authenticated before allowing access to applications. By making use of the solution's micro-segmentation capability, access was allowed only to explicitly authorized user and device pair to use specific required applications. In this manner, our solution prevents lateral movement which cybercriminals use to gain access and exfiltrate sensitive data.

Since Secure Shield provides access to only business traffic, all the non-productive traffic originating from personal devices never reaches the corporate network, thus, eliminating corporate network traffic congestion and providing better performance for accessing business applications remotely. Application-level access was provided to the employees who needed it, thereby ensuring lesser surface area for any attacks. The organization also had the visibility into the level of access its employees had and were able to make necessary adjustments as per the requirements.

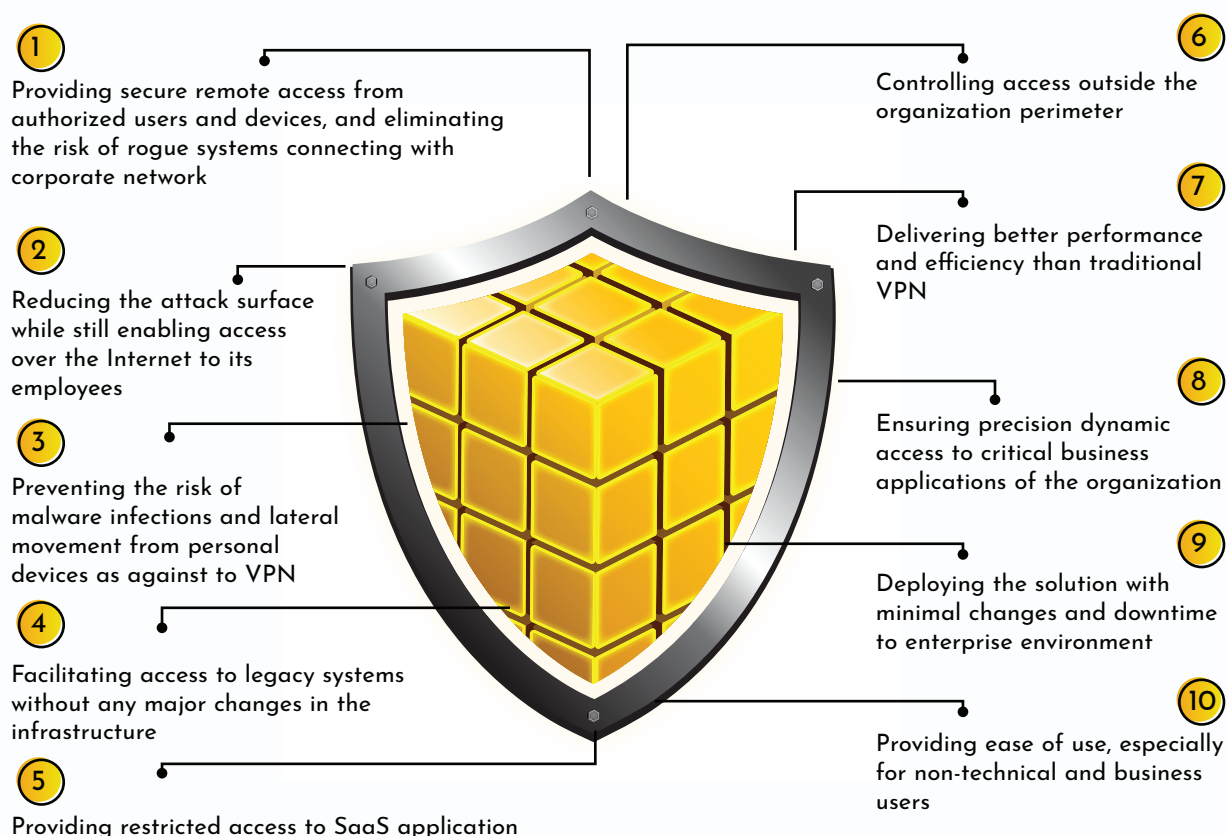


Secure Shield provides dynamic access to applications based on device ID instead of IP address. This feature was utilized to provide access to customer's SaaS application. The SaaS application URL was earlier exposed over the internet and anyone with valid user credentials could access the application. This posed a security risk where an attacker can phish the user credentials and get access to the application. Using Secure Shield, the customer was able to restrict access to SaaS application only from authorized devices, reducing the overall attack surface and controlling the access outside of organization's perimeter.



With these security measures in place, our Remote Access solution helped the organization to quickly enable secure access with enhanced security, thereby empowering teams of remote workers without sacrificing security or productivity. Our solution helped the organization in providing employees with granular, micro-segmented network access to business applications.

Customer successfully addressed their challenges using Secure Shield and the following benefits were delivered:



Results

Block Armour rapidly deployed its Remote Access solution to allow the employees to securely and efficiently access the company's on-prem and cloud-based systems from home. Maximum security was enforced although users were accessing corporate applications through their home computer. For an organization who had always used in-office access to business applications for their workforce, Block Armour helped in a smooth transition to secure, application-based access for employees using their corporate as well as personal devices when working from home.

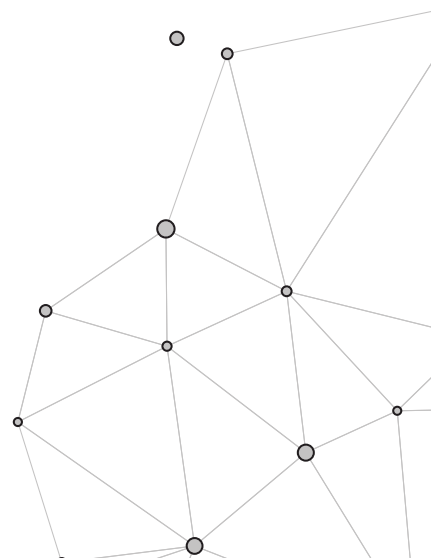


We deployed Block Armour's Zero Trust solution to enable secure remote access to our on-premise as well as SAAS applications. The solution facilitated seamless access for our business teams, and helped us immensely; allowing us to run normal business operations during the Covid-19 crisis



Sidharth Shandilya

Head IT, Indian Oil Tanking Limited



Email: info@blockarmour.com

Website: www.blockarmour.com

Linkedin: <https://www.linkedin.com/company/block-armour/>

Twitter: <https://twitter.com/BlockArmour>