BLOCK ARMOUR

UNIFIED SECURE ACCESS

Are you worried about cyber-attacks in the new normal post Covid-19?

The sudden onslaught of the COVID-19 pandemic has driven uncertainties across several industries. Organizations have turned to technologies like Cloud to facilitate rapid digital transformation and maintain essential business continuity in this 'new normal' wreaked by the pandemic. Separately, IT management teams have extended legacy tools like VPN to sustain operations and enable remote access to IT-systems for employees working from home.

But the vanishing enterprise perimeter now presents a whole new reality for network security.

Cyberattacks are on the rise and legacy tools like VPNs are unable to deliver secure and compliant access for today's modern enterprise-IT environments. Estimates suggest that the rate of cyberattacks could double since 2019 and rise by four times compared to five years ago this year.

Why have cyber-attacks become more successful?

This rapid adoption of Cloud technology and employees working from home due to Covid-19 has resulted in highly distributed and hybrid IT environments. Organizations extended existing VPN infrastructure to enable remote access to employees. Additionally, several organizations used Windows Terminal server/Remote Desktop (RDP) based access for the same. The legacy architecture of VPN creates a conduit for cyberattacks and RDP has several weaknesses, which can be easily exploited by malicious actors. These factors have resulted in providing attackers with the right environment to exploit these vulnerabilities and to launch targeted attacks. Most ransomware attacks in the last few months have been specifically designed to take advantage of this combination.

To add to this, current cybersecurity solutions (mostly point products) only address a specific problem and it is left to the organization to implement a suite of products, increasing cost, complexity and the need for skilled resources to manage them.

The Solution – Block Armour Unified Secure Access (USA)

Block Armour offers a **Unified Secure Access** solution to provide secure and compliant access to enterprise-IT systems for users working within the office or remotely. The integrated solution - based on Zero Trust principles - delivers secured access to on-prem and Cloud / multi-Cloud based systems. The solution replaces four traditional point products (NAC, VPN, multi-Factor Authentication and Cloud Firewalls) while additionally delivering next-gen **Zero Trust Network Access** and **Server Protection**. It provides protection against **malware / ransomware** spreading to the corporate network while the inbuilt device posture check ensures access only from trusted and compliant devices. It also provides a single pane of visibility for all network access, and can be deployed **on-premise** or in the **Cloud**.

Block Armour Unified Secure Access (USA)

Based on our award-winning Secure Shield architecture, the solution is helping organizations consolidate their Cybersecurity investments while enabling them to enforce Zero Trust principles and defend against next-gen cyberattacks. It has provided **cost savings of more than 40%** vis-à-vis existing solutions for customers.

Key Benefits

- Protects against ransomware/malware spreading into the corporate network
- Secures critical application server resources by rendering them invisible to unauthorized user
- Blockchain based Digital Identity and Access Management for all users and devices
- Pre-access device posture ensures compliance to corporate standards and better protection against attacks
- Single pane of visibility and access management for all network access
- Provides better Return on Investment (ROI)
- Easy to deploy and manage
- Supports on-premises, multi-cloud, and hybrid environments

info@blockarmour.com
www blockarmour.com
http://www.linkedin.com/company/block-armour
http://www.twitter.com/Blockarmour