BLOCK ARMOUR

Secure Shield

Zero Trust Simplified

Enable your users connected to the corporate network or on the go, to safely access your applications hosted in your Data Center or in the Cloud.

Secure Shield is a holistic next-gen cyber security solution designed on the principle of Zero Trust - “Never Trust, Always Verify”. It protects systems and applications from a wide range of threats (DDOS/Malware/Ransomware) and mitigates the Risk of Vulnerability Exploitation by cloaking vulnerabilities. It renders systems and applications invisible to attackers and a robust mechanism using blockchain securely identifies and authenticates users and devices before granting them access to these invisible systems. Secure Shield can provide secure access to and protect systems deployed on-premise, on public/private cloud or hybrid environments using a single console.

KEY USE CASES

- Enable organisations to securely transition to cloud
- Provide secure access to users from only compliant and patched end-points/devices
- Network Admission Control (NAC) of End Points for Cloud & On-prem access
- Allow partners/employees to securely connect via internet/MPLS/4G
- Provide secure access from devices which are not part of domain

KEY VALUE PROPOSITION

- Single network access control fabric for remote as well as internal users
- Protect unpatched/non-hardened systems/applications
- Can be deployed fully on-premise with no dependency on cloud/internet
- Complete visibility and control of “who has what access”, whether on-premise or in the cloud

BLOCK ARMOUR

Invisible Systems

- Removes Applications & Services from direct visibility of attackers
- Protects unpatched servers and applications
- Protection from known and unknown threats

Precision Access

- Provides just in time and just enough access to specific applications
- Prevents lateral threat movement
- Reduces surface area of attack
- Grants access only to specific application, not underlying network

Tamper proof Logs

- Increased visibility due to immutable logs stored on Blockchain
- Integration with third party log monitoring solutions

Micro - Segmentation

- Enforces tightly coupled access to services & applications
- Isolates systems in the same Vlan

Anytime Anywhere Access

- Single platform & console to enforce unified security policy across cloud & on-prem
- Provides application specific access to remote or mobile employees/contractors
- Eliminates the distinction between being on & off the corporate network
- Provides remote access to applications & services without requiring VPN or DMZ
- Supports BYOD access

Phishing Resistant Authentication

- Tamper proof digital id's used for authenticating device & user
- Access provided based on combination of user and device
- Mutual authentication performed between client & server
- Integrated 2-factor authentication
- Superior to IP address or geo location-based authentication

Auto Malware Containment

- Access allowed only to whitelisted programs
- Feature supported on BYOD devices
- Malware/Ransomware cannot propagate to Enterprise network

Device Posture Check

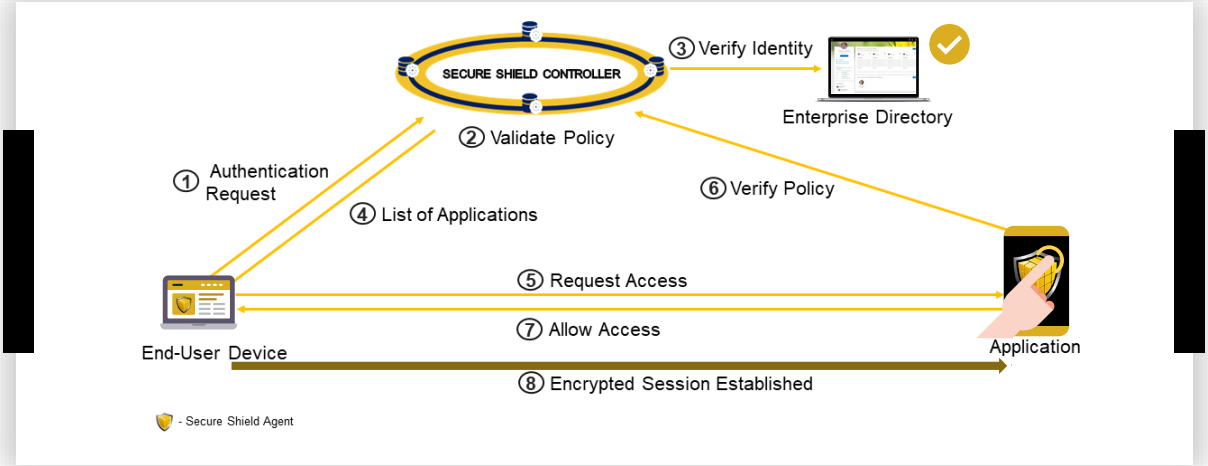
- Access permitted only from compliant devices
- Posture check policies support following checks on the end-point
  - Patches deployed
  - Anti-Virus
  - Corporate Domain
  - Registry key check
  - Disk Encryption
  - Malicious files

Components & Architecture

Secure Shield consists of Controller, Zero Trust Gateway, Management Console and Agents. Controller and gateway can be deployed on-premise or in the cloud. Agents are deployed on end-points. The controller stores identities, policies, logs and integrates with AD/LDAP, third party systems. Gateway and agents download and enforce policies from controller delivering secured and encrypted network access between end-points and servers.

Deployment Architecture

Single pane of control and visibility



Secure Shield offers end to end security by protecting the server/application, user authentication and communication, ensuring that access to the network and systems is granted only to authorized users and compliant devices.

It is very easy to deploy, and organizations can implement zero-trust security for on-prem and/or cloud systems in a few days. One of the key features is to gradually onboard users and systems without disrupting access to non-protected applications/servers.

Secure Shield offers a single console for enforcing anytime anywhere access and provides real time visibility of “who is accessing what”, irrespective of whether the system is on cloud or on the corporate network.

Specifications

SUPPORTED OS	Microsoft Windows 10, 8.1, 8, 7 Microsoft Windows 2016, 2012 R2, 2012, 2008 Ubuntu, CentOS, Red Hat
SUPPORTED CLOUD PLATFORMS	Azure, AWS, Google Cloud, Linode, Digital Ocean and equivalent
SUPPORTED PLATFORMS	Virtual Machines, Bare Metal
ENCRYPTION	TLS 1.2, RSA 4096, AES 256
INTEGRATION	AD, LDAP, Syslog, SSO, REST API for integration with third party solutions
DEPLOYMENT ARCHITECTURE	On-premise & Cloud Deployment
BCP/DR SUPPORT	The platform architecture supports real-time replication between Primary site and DR site. A separate BCP/DR license must be purchased

About Block Armour

Block Armour has operations in India and Singapore. Our vision is to build cutting edge next-gen cyber security products using emerging technologies like Blockchain to transform enterprise cybersecurity and offer future-ready protection to secure critical data and infrastructure. Block Armour has solutions which provide holistic security for IT infrastructure, Data Protection & IIOT.

Block Armour has been rated amongst **Top 20 Global Cyber Security Start-ups for 2017, 2018 and 2019.** We are an **Airbus accelerated company** and featured by Accenture among the **Top 25 Cyber Security Innovators Globally**

For more information about us, please visit

www.blockarmour.com

BLOCK ARMOUR