

BLOCK  ARMOUR



BLOCKCHAIN

Defined Perimeter

Experience the power of Software Defined Perimeter (SDP) with Blockchain Technology

What is Software Defined Perimeter?

Software Defined Perimeter (SDP) is a cutting-edge security framework that revolutionizes network security. It moves beyond traditional perimeter-based security models and embraces a dynamic, granular approach to secure network connections. SDP originated from the Defense Information Systems Agency (DISA) in response to evolving cybersecurity threats. Its aim was to develop a more robust and adaptive security framework that could safeguard critical networks against advanced attacks. Today, SDP has gained significant recognition and adoption across industries.



Why SDP?

With the rise of cloud computing and remote work, traditional perimeters are becoming blurred. Legacy security models struggle to combat advanced cyber threats and comprehensively secure today's hybrid and distributed enterprise-IT environments. SDP addresses these challenges by providing a proactive and adaptive security approach that aligns with the evolving threat landscape. It empowers secure access to resources, regardless of their location, be it in the cloud or on-premises.

Block Armour's Blockchain Defined Perimeter (BDP)

By combining SDP with the power of blockchain technology, Block Armour's Blockchain Defined Perimeter (BDP) solution delivers an unparalleled level of security and trust for any organization. BDP enables fine-grained access policies based on user + device digital identity, device posture, and other contextual factors. It enables the enforcement of least privilege access, granting users access only to the resources they need, enhancing security and minimizing risks.

1. Digital Identity:

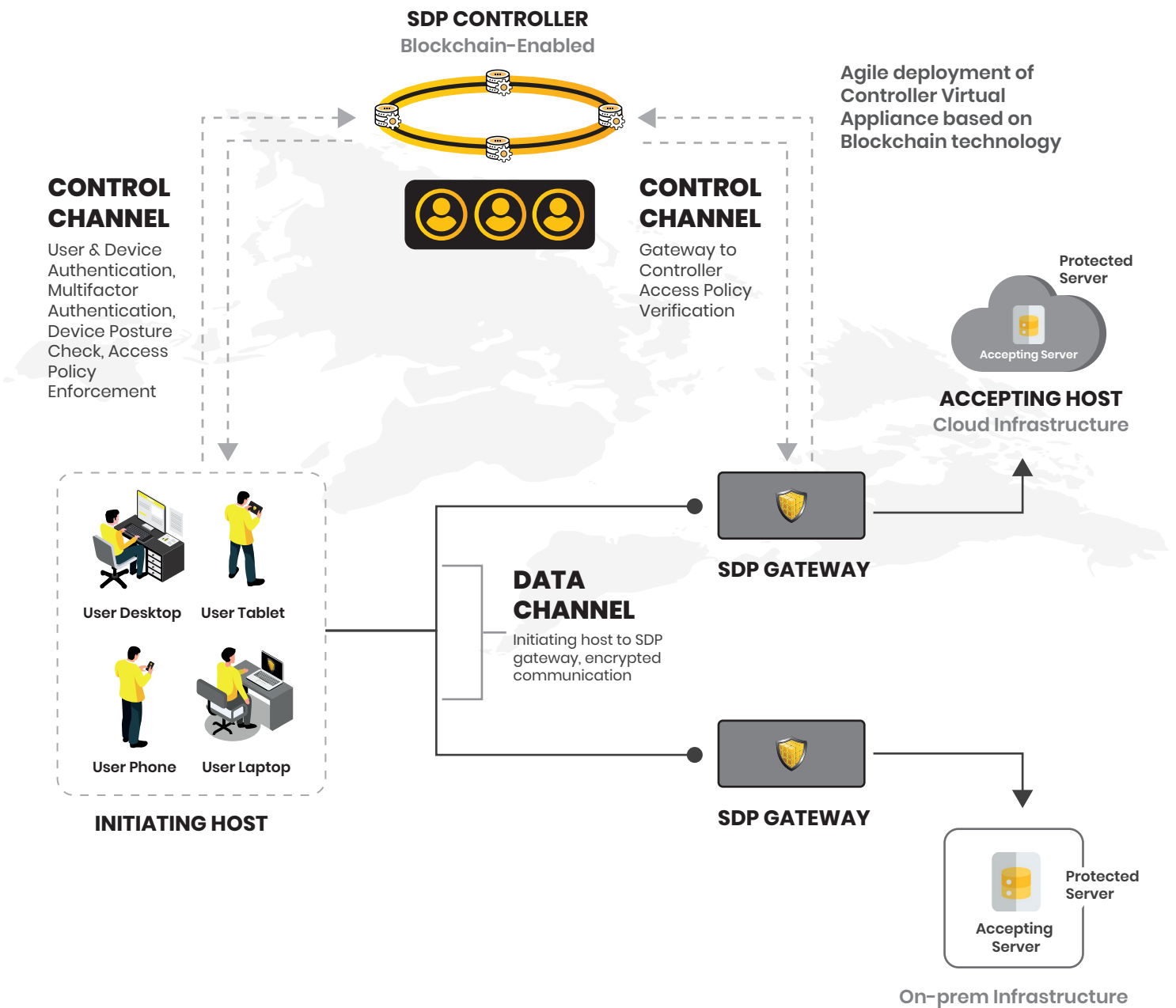
BDP provides a decentralized and immutable identity management system. Each user and device have a unique digital identity stored on the blockchain, and their access rights and attributes can be recorded and verified through smart contracts. This ensures that only authenticated and authorized entities can establish connections within the SDP.

2. Distributed Trust and Consensus:

Multiple nodes in the network participate in the validation and verification of access requests, ensuring that decisions are not centralized, reducing the risk of single points of failure or malicious manipulation.

3. Immutable Audit Trail:

The Blockchain's inherent immutability enables the recording and storing of audit trail of admin and network activities. This deters insiders threats, enhances accountability, and aids in forensic investigations in case of security incidents.



Key Benefits of BDP

- Granular Access Control:** BDP enables fine-grained access policies based on user + device digital identity, device posture, and other contextual factors. Organizations can enforce least privilege access, granting users access only to the resources they need, enhancing security and minimizing risks.
- Improved User Experience:** With BDP, users can securely access resources from anywhere, using any device. Say goodbye to cumbersome VPNs, as BDP offers seamless connectivity and a frictionless user experience.
- Scalability and Agility:** BDP allows organizations to dynamically provision and deprovision network connections, adapting to changing business requirements. It provides the flexibility to scale your network security infrastructure and accommodate evolving needs.

Get the Block Armour BDP advantage for:

1. Secure Remote Access:

Enable remote employees, partners, and contractors to securely access corporate resources without traditional VPNs. Only authorized and authenticated users can establish connections, reducing the risk of unauthorized access.

2. Privileged Access Management:

Allow strict access controls for privileged accounts and ensure that only authorized users with the necessary privileges can access critical systems and data, mitigating insider threats.

3. Micro-segmentation:





Granular segmentation within network segments for precise access based on user roles, workloads, or applications and minimize lateral movement, thereby containing potential threats and enhancing overall security.

4. Multi-Cloud Security:

Provide secure access to hybrid and multi-cloud based resources. Extend security policies and controls to the cloud and ensure consistent security across hybrid environments.



UNLOCK THE POWER OF BLOCKCHAIN DEFINED PERIMETER TODAY!

 www.blockarmour.com
 info@blockarmour.com
 [linkedin.com/company/BlockArmour](https://www.linkedin.com/company/BlockArmour)
 twitter.com/BlockArmour

BLOCK  ARMOUR
Singapore | UK | USA | UAE | India