BlastWave

Enabling Zero-Trust Network Access with BlastShield

Enabling Zero-Trust Network Access

As organizations have moved to connect their operational technology (OT), IT and IoT platforms while supporting an increasingly remote workforce, network complexity and attack surface have soared . Stolen credentials and phishing were involved in almost 70% of data breaches in 2022.[1] It is more important than ever for businesses to adopt zero-trust network access (ZTNA) strategies to protect their applications and data from bad actors and insider threats.

What Is Zero-Trust Network Access?

Enterprise network complexity has outstripped legacy methods of perimeter-based network security because there is no single, easily identified enterprise perimeter. ZTNA has emerged as an approach to network security that assumes there is an attacker in the network. Zero trust principles suppose[2] that an enterprise-owned network is no more secure than a public network. According to Gartner, "ZTNA is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications." The applications are hidden from discovery, and access is restricted via a trusted broker to a set of named entities. The broker verifies the identity of a user before allowing access and prohibits lateral movement elsewhere in the network.

---

[1] 2022 Data Breach Investigations Report (DBIR). Verizon. 2022.

[2] "NIST SP 800-207: Zero Trust Architecture." U.S. NIST. August 2020.

Mitigating Security Risks

Virtual private networks (VPNs) and remote access approaches, such as SSH or remote desktop protocol (RDP) have long been used to access enterprise and cloud applications. These solutions lack strong authentication and expose destination IP addresses to the public Internet, making it easier for attackers to target. These approaches are also vulnerable to lateral and man-in-the middle (MITM) attacks.

Hybrid Workforce Productivity

Over the past three years, we have gone from spending 5% of our time working from home to 60%, a 12x increase.[3] Ensuring the productivity of a hybrid workforce requires protecting employees and corporate networks. Employees require direct and fast access to applications and data repositories. Networks using VPN remote access, antiquated hub-and-spoke topologies and legacy hardware are prone to network reliability and bandwidth challenges. Both security and performance should be considered in migrating to a ZTNA.

Simplifying Network Security Management

Managing legacy VPNs and remote access networks can be tremendously complex. VPNs lack microsegmentation controls. Network administrators must manage firewalls, ACLs, identity management platforms, and multi-factor authentication (MFA). For many organizations, managing this sprawl of network security solutions, client credentials and X.509 digital certificates is complex, overwhelming and prone to human error.

BlastWave BlastShield™

BlastShield is a zero-trust network access (ZTNA) solution that provides secure, high-performance access to applications, machines, and containers in a peer-to-peer mesh using encrypted tunnels. The solution creates a software-defined perimeter (SDP) around IT and OT assets, making them invisible to non-authenticated users, regardless of physical location. BlastShield is easy to use and replaces multiple network security solutions such as VPN, MFA, deception, CASB, data loss prevention (DLP), SASE, PAM and microsegmentation. BlastShield redefines the security stack.

---

[3] "The Rise of Working from Home." Economist. April 8, 2021

BlastShield Zero-Trust Network Access Solution

BlastShield Overview

BlastShield brings three breakthrough products, any of which separately is best-in-class, into a consolidated, simplified platform:

1. Phishing-resistant passwordless MFA
2. High performance, peer-to-peer ZTNA, and
3. Simple to deploy and manage microsegmentation.

Functionally, BlastShield is an in-line IP subnetwork that creates a zero trust protective shield around critical IT/OT assets and data by making them undetectable by modern network scanning and traffic analysis tools. BlastShield creates a Software-Defined Perimeter (SDP) network using a peer-to-peer architecture that can be deployed on any packet-based network.

The BlastShield ZTNA solution comprises:

- **BlastShield Agent** – software image hosted by a Linux/Windows server
- **BlastShield Gateway Agent** – software image running on an x86 hardware or virtual machine
- **BlastShield Client** – software image that can be deployed on a user device for single-use access to the BlastShield network
- **BlastShield Authenticator** –software image for iOS and Android mobile devices for user passwordless MFA. Available via the Apple App Store or Google Play Store.
- **BlastShield Orchestrator Server** – server that can be deployed in the cloud or as a VM

About BlastWave

BlastWave's zero trust networking solutions reduce cybersecurity management complexity without sacrificing performance. The BlastShield™ software-defined perimeter (SDP) proves you can't hack what you can't see. Try BlastShield at blastwave.com/getstarted