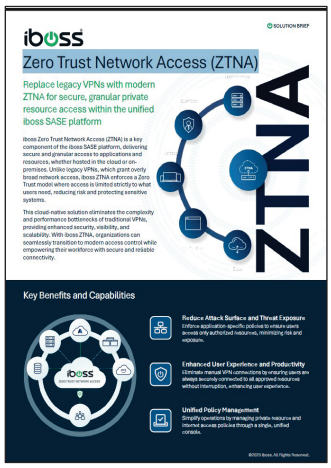


Zero Trust Network Access (ZTNA)

Thank you for downloading this iboss solutions brief. Carahsoft serves as iboss' Master Government Aggregator® making the company's cyber solutions and services available to the Public Sector through Carahsoft's network of reseller partners, Solutions for Enterprise-Wide Procurement (SEWP) V, Information Technology Enterprise Solutions – Software 2 (ITES-SW2), NASPO ValuePoint Cooperative Purchasing Contract, and other contract vehicles.

To learn how to take the next step toward acquiring iboss' solutions, please check out the following resources and information:

For additional resources:
carah.io/ibossResources

For upcoming events:
carah.io/ibossEvents

For additional iboss solutions:
carah.io/ibossSolutions

For additional iboss NetBackup solutions:
carah.io/ibossNetBackup

To set up a meeting:
iboss@Carahsoft.com
(703)-889-9710

To purchase, check out the contract vehicles available for procurement:
carah.io/ibossContracts

For more information, contact Carahsoft or our reseller partners:
iboss@carahsoft.com | (703)-889-9710

Zero Trust Network Access (ZTNA)

Replace legacy VPNs with modern ZTNA for secure, granular private resource access within the unified iboss SASE platform

iboss Zero Trust Network Access (ZTNA) is a key component of the iboss SASE platform, delivering secure and granular access to applications and resources, whether hosted in the cloud or on-premises. Unlike legacy VPNs, which grant overly broad network access, iboss ZTNA enforces a Zero Trust model where access is limited strictly to what users need, reducing risk and protecting sensitive systems.

This cloud-native solution eliminates the complexity and performance bottlenecks of traditional VPNs, providing enhanced security, visibility, and scalability. With iboss ZTNA, organizations can seamlessly transition to modern access control while empowering their workforce with secure and reliable connectivity.

Key Benefits and Capabilities

Reduce Attack Surface and Threat Exposure

Enforce application-specific policies to ensure users access only authorized resources, minimizing risk and exposure.

Enhanced User Experience and Productivity

Eliminate manual VPN connections by ensuring users are always securely connected to all approved resources without interruption, enhancing user experience.

Unified Policy Management

Simplify operations by managing private resource and internet access policies through a single, unified console.

©2025 iboss. All Rights Reserved.

Overcoming VPN Limitations with Zero Trust

Challenge

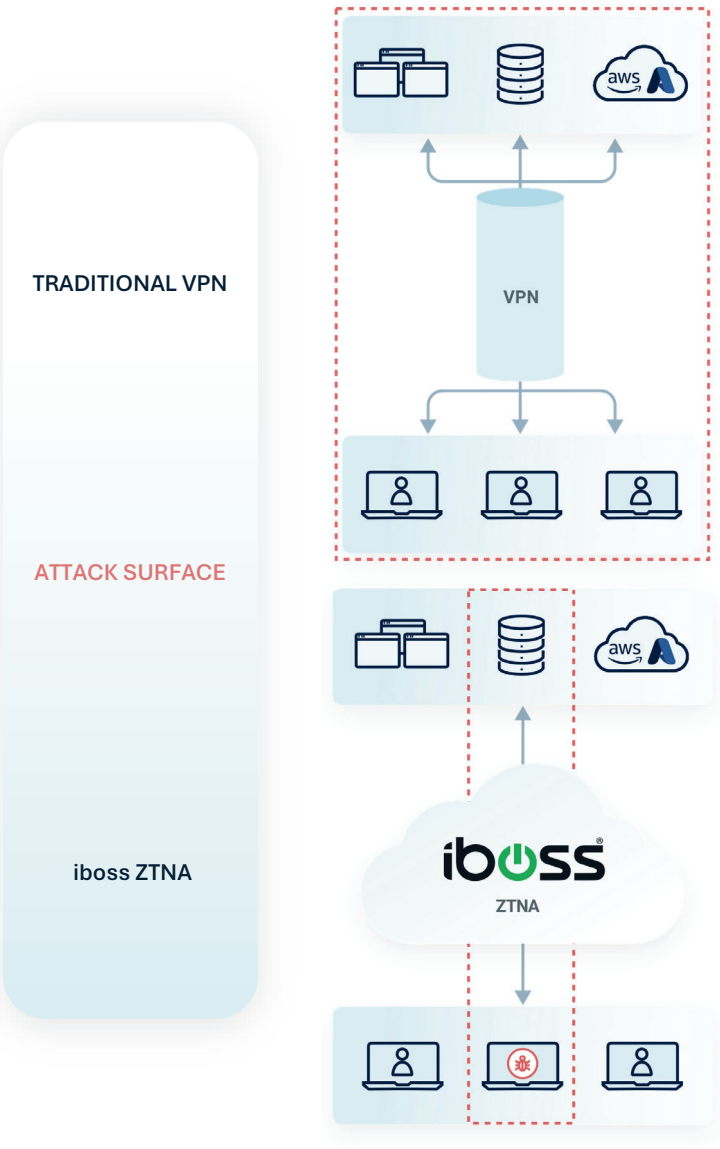
Traditional VPNs provide broad access to network resources, creating vulnerabilities and increasing the risk of lateral movement in case of a breach. They also suffer from performance bottlenecks and require expensive on-premises hardware, which limits scalability.

Solution

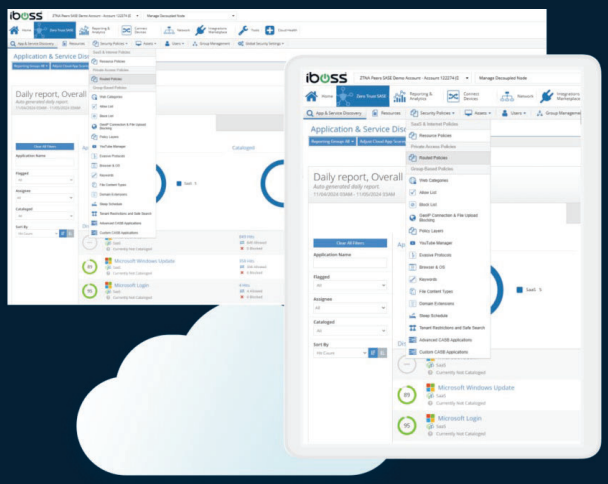
iboss ZTNA replaces legacy VPNs with a modern, cloud-native platform that provides seamless, always-on access to approved applications and resources. By enforcing Zero Trust principles, access is restricted to only what users need, with connections dynamically authenticated and monitored. The iboss platform scales effortlessly to support hybrid and remote workforces, ensuring performance and security for all users, regardless of location.

Benefit

By replacing VPNs with iboss ZTNA, organizations benefit from application-specific access policies, reduced attack surfaces, and enhanced performance through cloud-native delivery.



Why Choose iboss for Zero Trust Network Access?



Unlike traditional solutions or fragmented Zero Trust offerings, iboss integrates ZTNA into a unified Secure Access Service Edge (SASE) platform. This holistic approach enables organizations to enforce consistent security policies across both internet and private resource access while simplifying management through a single, intuitive interface. By consolidating tools and operations, iboss eliminates complexity, streamlines policy enforcement, and provides comprehensive visibility across all access points, reducing administrative overhead and enhancing both security and operational efficiency.

With always-on connectivity and robust cloud-native performance, iboss ZTNA also ensures seamless user experiences while removing the need for costly on-premises hardware. This makes it a scalable, cost-effective, and future-ready solution for securing dynamic environments such as hybrid and remote workforces.

©2025 iboss. All Rights Reserved.

Key Use Cases

Secure Remote Workforces

Enable always-on, secure access to applications for hybrid and remote employees. iboss ZTNA eliminates manual VPN connections and enforces application-specific access, reducing the attack surface and improving user experience. By dynamically verifying user and device trust, iboss ensures seamless connectivity to authorized resources, boosting productivity while protecting sensitive data from unauthorized access.

BYOD and Third-Party Access

Provide vendors and contractors with secure, limited access to specific applications. iboss ZTNA replaces broad VPN permissions with granular policies, restricting third-party access to only what is needed. Continuous verification and session monitoring further reduce risks associated with insider threats and compromised credentials, ensuring sensitive resources remain protected.

Enhance Hybrid Cloud Security

iboss ZTNA eliminates the need for backhauling traffic through VPNs, providing direct, secure connections to applications. This reduces latency, improves performance, and enables organizations to manage access through a single platform, ensuring consistent security across hybrid infrastructures.

Prevent Malware Propagation and Data Loss

Contain threats by isolating compromised devices. iboss automatically revokes access for infected devices, stopping ransomware and malware from spreading. By limiting access to only approved applications, the solution minimizes the impact of attacks, protecting critical systems and data from disruption.

Simplify Compliance Audits

Maintain detailed logs and enforce granular access policies for regulatory compliance. iboss ZTNA provides visibility into user activity, ensuring access aligns with frameworks like GDPR, HIPAA, and NIST Zero Trust. The platform's logging and reporting capabilities streamline audits, demonstrating compliance and enabling quick response to potential access violations.

Reduce IT Complexity

Consolidate access and security management into one unified platform. iboss ZTNA eliminates the need for multiple point solutions by combining Secure Internet Access and private resource access management. This simplifies operations, reduces administrative overhead, and ensures consistent policy enforcement across all access points, enhancing security and efficiency.

How it Works

1. User Authentication via iboss Cloud Connector

Users connect through the iboss Cloud Connector, which establishes a secure tunnel to the iboss platform. iboss integrates with Identity Providers (IdPs) to authenticate users, ensuring only authorized individuals gain access.

2. Device Posture Assessment

iboss evaluates device compliance, checking for factors like anti-malware status, firewall activation, and disk encryption to confirm that devices meet security standards before granting access.

3. Contextual Access Evaluation

iboss assesses contextual factors, such as geolocation and IP address, to determine the legitimacy of each access request.

4. Granular Policy Enforcement

Based on user identity, device posture, and contextual information, iboss enforces resource-specific access policies, ensuring users can only access authorized resources, thereby minimizing the attack surface.

5. Continuous Monitoring & Threat Containment

iboss continuously monitors user traffic for anomalies and threats, allowing for real-time responses to potential security incidents. If a device is detected as compromised, iboss automatically revokes its access to prevent the spread of malware or ransomware.

6. Comprehensive Logging and Reporting

iboss logs every access request, session, and resource interaction, providing detailed visibility into user activity.

©2025 iboss. All Rights Reserved.

Features

Application-Specific Access
Granular access control ensures users can only access authorized resources.

Automatic Threat Containment
Instantly revoke access for compromised devices to prevent malware or ransomware from spreading across the network.

Comprehensive Logging and Monitoring
Gain detailed insights into user activity and resource access to identify risks and enhance security.

Automatic Resource Discovery
Identify and catalog network resources by logging user connections, simplifying audits and improving compliance.

Unified Security Platform
Manage secure Internet access and ZTNA within one platform for consistent policies and reduced complexity.

Consistent Security Enforcement
Apply uniform malware defense and data loss prevention policies for internet and private application access.

Cost-Effective Protection
Combine security and access control, saving up to 50% compared to multiple standalone solutions.

Advanced Threat Detection
AI/ML-powered analysis and deep content inspection to identify sophisticated threats beyond legacy methods.

Reduced Attack Surface
Proactively prevent unauthorized access and limit insider threats by allowing access only to required resources.

Data Loss Prevention
Protect sensitive data by restricting access to approved resources and preventing unauthorized exfiltration.

Simplified Policy Management
Intuitive cloud-based interface simplifies policy enforcement, access control, and security configuration management.

Enhanced User Experience
Provide seamless, always-on access to resources, improving productivity without compromising security.

Identity Integration and Adaptive Access
Seamlessly integrate with Identity Providers and MFA solutions while providing real-time session monitoring to adapt security dynamically.

Supported Platforms & Systems

Endpoint Cloud Connector

- Windows
- macOS
- Linux
- ChromeOS
- iOS
- Android

Network Connector

- AWS
- Docker
- VMware OVF

Policy Enforcement Points

- iboss Global Cloud (100+ POPs)
- Azure
- Private Locations

Secure Remote Access

Replace legacy VPNs with modern ZTNA for enhanced security, visibility, and control—all within the unified iboss SASE platform.

iboss Zero Trust Network Access (ZTNA) is an integral part of the iboss SASE platform, providing secure, granular access to applications and resources in your offices and data centers. Replace legacy VPNs with a modern solution that reduces risk, enhances visibility, and simplifies management, ensuring users access only what they need while protecting your organization from modern threats.

Request a Demo Today

©2025 iboss. All Rights Reserved.

To speak with an iboss representative, please call: Americas: +1-877-742-6832 ext. 1 UK&I : +44 020 3884 0360 International: +1-858-568-7051 ext.

©2025 iboss. All Rights Reserved.