ISG-OPS

Zero Trust Network Access

ZTNA Solution

As enterprises progress on their digital transformation journey, they must enable secure remote access across their on- premises and cloud deployments.

75% of enterprises today are in some form of hybrid cloud deployment. Providing a seamless remote access solution that traverses this complex environment is a huge IT and security challenge. Network-centric solutions like traditional VPNs are not designed to meet the scale, performance, and usability needs of modern organizations, especially with complex hybrid cloud environments.

Legacy VPNs create a huge security liability as they offer overly broad access to sensitive corporate assets and permit the kind of lateral movement that adversaries use for ransomware and other illegal activity. With an increasing set of diverse users from employees and contractors to partners, access to these resources from a variety of remote locations and devices has made VPNs struggle to meet the demands of the modern hybrid enterprise.

The Zero Trust Network Access offering enables employees, developers, and third parties to remotely access on-premises, hybrid, and multi-cloud infrastructure and applications without needing to use legacy VPNs.

Our ZTNA enforces least-privileged access to applications and services in real-time, leveraging your existing enterprise identity and security tool investments. ZTNA transparently deploys in hybrid and multi-cloud environments, continuously enforcing trust-based access policies based on any combination of user, device, and application contexts.

KEY BENEFITS

- Application to User micro-segmentation.
- One platform replaces legacy VPN so that you can eliminate implicit network access risks in your network.
- Distributed Access Tiers or Global Edge Network to meet your connectivity needs.
- Integration with AD/IDP

  Integration with EDR

  Eliminate IP Whitelisting
- Support BYOD & 3rd Parties without VPN
- Continuous user & device trust
- Continuous Authorization
- Real-time User & Device Trust
- Least Privilege Access
- One-click access to infrastructure, intranet, or SaaS applications

CONTACT US

Why the urgency to move from VPN?

Massive Security Gap

- Traditional VPNs enable implicit access to your network. A compromised VPN allows lateral movement across networks leading to massive exposure.
- Legacy VPNs grant full access to a network's resources, allowing malicious actors with VPN access to move laterally across the corporate ecosystem.
- One-time authorization approach fails to provide real-time detection or enforcement of detected abnormal activity.
- Broad network-level access based on long- lived certificates, with lateral movement vulnerability especially for 3rd parties who can access any server on the network or in any Virtual Private Cloud (VPC).

Bad User Experience

- IT admins find legacy VPNs are expensive to acquire, maintain, and upgrade.
- Due to complexity in deployment, users experience performance delays and in many cases are unable to access applications due to VPN connectivity issues.

So Many Devices and Users

- No single device management solution provides complete coverage across all popular operating systems (Windows, MacOS, iOS, Android, Linux).
- Contractors, temporary workers, and third parties are usually unwilling or unable to use an organization's heavy- handed device management systems (MDM, UEM, etc.).

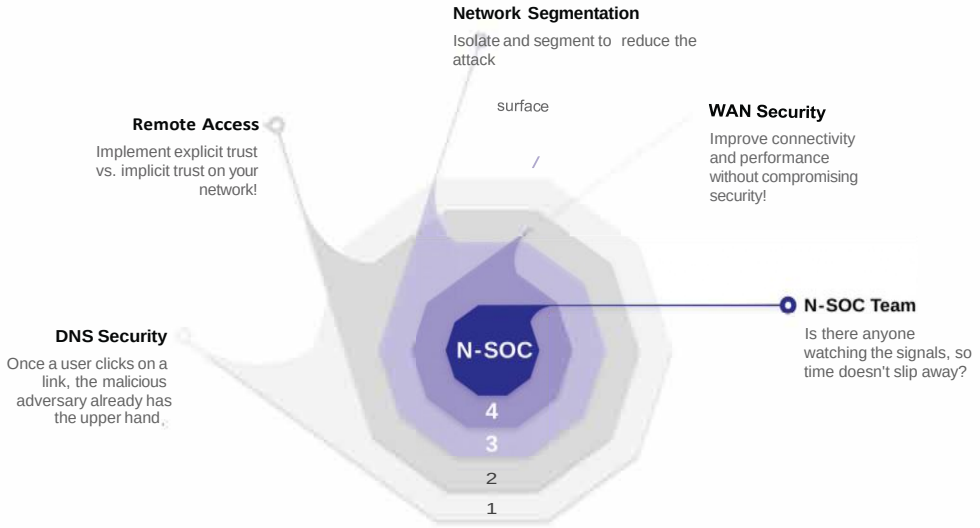
Management Nightmare

- No centralized way to secure IaaS, on-premises, and SaaS applications based on security posture of users and devices result in operational complexity.
- Complex network-level policies to segment access, which must be constantly updated to match dynamic user and application environments.
- Network-level controls hard to configure, especially due to ephemeral server instances on modern clouds.
- Painful process of updating end-point clients and VPN hardware and software patches.

Device Security & Enforcement

- User authentication and MFA systems do not register and authorize devices. Device Trust is a critical component of Zero Trust.
- There is no way to continuously know the security status of a device. Checks done only at the time of initial login are not effective when work happens 24x7x365.
- Device management silos and EDR do not integrate with access policy enforcement across users, devices, and resources.
- End-user frustration with multiple VPN and VDI clients and their complex security requirements hurts productivity.

Our zero-trust network security approach to #cyberresilience in a highly distributed world.



ZTNA Features

	Premium
Global SaaS Platform	
Secure, High Availability, Role-based Access	✓
24 x 7 x 365 Security Operations Center (SOC)	✓
Global SaaS edge network	✓
Simplify Secure Remote Access	
Desktop app with trust score integration	✓
Service catalog with one-click install	✓
One-click access to apps and infrastructure	✓
Mobile app (IOS & Android)	✓
UEM Integration	✓
EDR Integration	✓
UEBA integration	✓
Accelerate Compliance	✓
Zero trust policies	✓
Audit & reporting	✓
Enterprise SSO integration with IDPs	✓
Trust score customization to meet specific security requirements	✓
Self-hosted edge for access tier(s)	✓
Service discovery to know what is running on your endpoints	✓
Adopt cloud & PaaS securely	
Policies for SaaS applications to protect SaaS based business apps	✓
Cloud resource discovery	✓
Approval workflows to provided management oversight for access to key systems	✓
Tunnel capabilities to replace VPN	✓
Prevent rogue device access	✓
Secure Web Gateway	✓

Windows agents
All Windows workstation starting with 7 SP1 through Windows 11

All Windows Server starting with 2008 R2 SP1 through 2022

Mac agents
macOS Ventura, Monterey, Catalina, Mojave, High Sierra

Windows Legacy agents
XP, Server 2003 & 2008, 2009

Linux agents
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Container Support
Kubernetes self-managed v1.13+ [self-managed, AWS Kubernetes (EKS), Azure AKS]

Virtualization & VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V