# InstaSafe
# Solution Brief

celestix

# Table of Contents

Celestix InstaSafe

## What is InstaSafe Zero Trust?

InstaSafe leverages NIST and CSA Zero trust principles to extend secure and seamless access to users. The enterprise infrastructure is kept inaccessible from the external internet and is still accessible to the relevant users. InstaSafe helps to share application access alone, and not IP access at Layer 7 as a web solution at the browser. Hence the user can browse the applications and the IPs are masked.

## What problem is InstaSafe Zero Trust solving?

The issue with current VPN providers and technologies claiming to leverage Zero Trust is the simple fact that they not only expose IPs to the external internet but also fail to ensure that customer traffic remains private

### PRIVACY ISSUES

VPNs allow data traffic to flow through and be inspected by their servers, which can be compromised and lead to the exploitation of customer data

### EXPOSED IPS

VPNs do not completely hide all enterprise assets from the internet, which can lead to exposed IPs being exploited by malicious users

### FRAGMENTED ACCESS

The use of multiple access tools for accessing assets on-premises and on different cloud environments creates a web of vulnerabilities

## What are the features?

The features are as follows.

### 1. MAKE YOUR INFRASTRUCTURE INVISIBLE

Leverage SDP based principles and drop all firewall to ensure that visibility and the access to the applications and the infrastructure is limited to the authenticated users and authorized devices and the entire network is invisible to external users

- Any shared customer assets are kept on a local network behind a gateway unseen by the external users
- A drop all firewall at the gateway hides the presence of the gateway from the internet
- Each application/server access by a user creates a secure individual tunnel controlling the user access within the tunnel
- Only validated device/user combinations are given visibility to the network or the gateway
- The authentication process involves user credential validation, MFA, and device posture validation

## 2. KEEP YOUR DATA TO YOURSELF: PRIVACY FIRST

Customer Data belongs to the customer only. Your data traffic need not be inspected by your vendor machines. Any flow of your data through vendor machines exposes the risk of supply chain attacks. Ensure that data and authentication planes are separated, and your data remains confidential and secure with InstaSafe

- Separate Data Plane carrying critical data, from control plane where trust is established
- Data Plane doesn't go through vendor machines, ensuring privacy for your data
- Separation of planes protects against network-based attacks
- Your data is secured against supply chain attacks since enterprise data is inaccessible to vendor

## 3. LEVERAGE SINGLE MESSAGE AUTHORISATION FOR SEAMLESS ACCESS

Establish authorized encrypted application-specific tunnels seamlessly and instantly with Single Message Authorization.

- Any user trying to access enterprise apps must have visibility to the gateway
- InstaSafe's controllers communicate any incoming access requests to the gateways through a special messaging mechanism called SMA
- On validation of the message, the gateway allows port access, and a secure encrypted tunnel from the user to the apps is created
- All of this happens seamlessly and instantly in the backend, without the involvement of the end-user

## 4. ZERO TRUST. ONE ACCESS

Simplify access to all data, servers, and applications, hosted anywhere, with a unified access solution that can be managed from a single dashboard

- Allow for seamless integrations with IDP and AD for easier identity management
- Enable multifactor authentication capabilities along with SSO capabilities, with InstaSafe's own Authenticator applications
- Ensure advanced monitoring and reporting capabilities through easy integration with SIEMs
- Empower your security teams with Network Access and Control, IAM, and MFA capabilities from a single solution

## Use Cases

- VPN Alternative – Zero Trust solution is the best VPN alternative which is a cloud-ready and scalable on-demand
- Secure Remote Access – Empower your remote workforce to seamlessly connect and work securely, from anywhere
- Cloud Security – Simplifying controls and security of your multi-cloud environments with cloud access security solutions
- DevOps Security – Secure access to SSH/RDP and hosted applications like Gitlab and Jenkins for your DevOps team
- Clients Remote Access – Securely access your web application without the need to install a client, any OS, any browser
- Domain Joining – Extend AD/LDAP compliance to all your remote devices and ensure compliance
- Secure VoIP – Extend secure remote communications channels for remote VoIP users with a Zero Trust solution
- Multi-Factor Authentication – Inbuild adaptive MFA and SSO complements InstaSafe Zero Trust capability

Schedule a demo – Click here

## InstaSafe ZTA, Zscaler PA, Fortinet VPN Comparison

| Feature | | InstaSafe ZTA | Zscaler Private Access | Fortinet VPN |
|---|---|---|---|---|
| **Application Support** | Intranet Web Apps | ✓ | ✓ | ✓ |
| | SaaS Apps | ✓ | ✓ | ✓ |
| | Virtual Apps and RDP | ✓ | ✗ | ✗ |
| | Client Server App | ✓ | ✓ | ✓ |
| | VoIP (Call center applications) | ✓ | ✗ | ✗ |
| **Simplified Deployment and Management** | Centralized Security Management | ✓ | ✓ | ✓ |
| | Choice of Client and Clientless | ✓ | ✓ | ✓ |
| | Support for Windows | ✓ | ✓ | ✓ |
| | Support for Linux | ✓ | ✗ | ✗ |
| | Support for MacOS | ✓ | ✗ | ✓ |
| | Support for iOS | ✓ | ✗ | ✓ |
| | Integrated Management Tool available as bundled offering | ✓ | ✗ | ✗ |
| **Authentication Capabilities** | Inbuilt IDP | ✓ | ✗ | ✗ |
| | Inbuild SSO Capabilities | ✓ | ✗ | ✗ |
| | Support for third party IDP Solutions | ✓ | ✓ | ✓ |
| | Integrated SSO to all Web based Applications | ✓ | ✗ | ✗ |
| | Geo and Temporal Risk Assessment | ✓ | ✗ | ✗ |
| | ML Based Authentication | ✓ | ✗ | ✗ |
| | Integrated MFA with InstaSafe/Google/Microsoft Authenticator Support | ✓ | ✓ | ✓ |
| | Behavioral Biometrics based Authentication | ✓ | ✗ | ✗ |
| **Security Capabilities** | Split Plane Architecture | ✓ | ✗ | ✗ |
| | Single Packet Authorization | ✓ | ✓ | ✗ |
| | Segmentation at Application Traffic Level | ✓ | ✓ | ✓ |
| | User Activity Monitoring | ✓ | ✓ | ✓ |
| | Drop All Firewall | ✓ | ✓ | ✗ |
| | Role Based Access Control | ✓ | ✓ | ✓ |
| **Application Access Capabilities** | Access to L3/L4 protocols and applications | ✓ | ✓ | ✓ |
| | Support for RDP/SSH | ✓ | ✗ | ✓ |

## Celestix Contacts

Celestix Networks Inc. has a proven track record and is a trusted brand in the delivery of managed security appliances and security solutions. Celestix is leveraging its significant experience in the remote access and authentication markets to extend its portfolio into the Cloud managed appliance security market. Founded in 1999 and headquartered in Pleasanton, California, Celestix has delivered over 25,000 security appliances worldwide and currently offers support to over 5,000 customers. The company maintains regional offices in London, Singapore, and Tokyo. As the threat landscape constantly evolves, Celestix will never cease to protect our clients from risk. Our company provides market-leading technologies backed up by a global support network that ensures we meet and exceed the demands of our international customer base.

Celestix is a co-developer of InstaSafe Zero Trust Solution and is a deployment partner in North America, United Kingdom, and Asia.

### Americas HQ

Celestix Networks, Inc.
4125 Hopyard Road #225
Pleasanton, California 94588
United States
+1 (510) 668 0700
sales@celestix.com

### EMEA HQ

Celestix Networks UK
9 Greyfriars
Reading RG1 1NU
United Kingdom
+44 (0203) 900 3737

### Asia HQ

Celestix Networks Pte. Ltd
1 Paya Lebar Link
#04-01, Paya Lebar Quarter Singapore 408533
+65 6958 0822