







**InstaSafe**

**The Security Solution for  
the Hybrid Workforce**

# The Need to Rethink Security for your Remote Workforce

In the new normal, secure access of any corporate resource from anywhere is an indispensable necessity for maintaining the productivity of your workforce. That said, managing remote workforce access is not a simple task, and is further complicated by the presence of corporate assets in hybrid environments. Seemingly trivial tasks such as accessing your mail on an unsecured public network can compromise your entire network. And with obsolete legacy security systems in place, most organisations are often not ready to extend their security setup to the edge. Furthermore, these legacy setups serve to extend more access than necessary, leaving the scope for insider attacks and lateral movement.

## InstaSafe works on 4 core principles

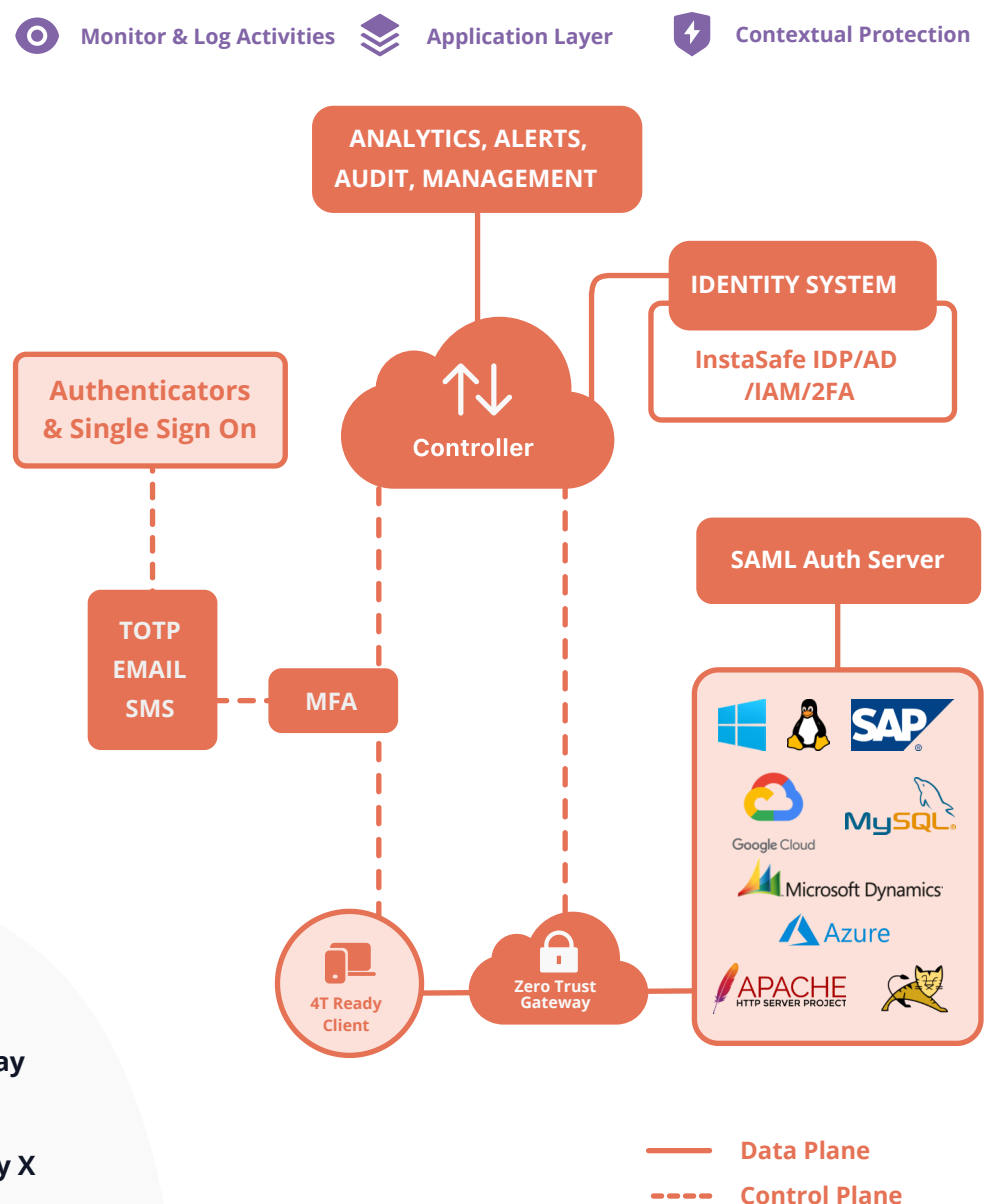
-  **Innate distrust, default deny:** Operationalise a system of continuous authentication and authorisation to provide least privilege, contextual access
-  **One Size doesn't fit all:** A complete visibility and control over user activity, allows for framing access policies on a granular level, and restricting access based on different levels of privilege for different users
-  **Align and Integrate:** Align to a broader security strategy and allow for easy integration with other security tools for better security posture
-  **Security based on Identity:** Pull the security perimeter from the network to the individual human users, and grant access based on identity as the single control point

# Zero Trust Remote Access: A Secure Solution for the Modern Workforce

The shift outside the perimeter, coupled with the shift to the cloud, is forcing companies to have a relook at their security setup and assess scalable, cloud ready alternatives that enable secure access of enterprise resources from anywhere.

Leveraging the Zero Trust precedent of 'NEVER TRUST, ALWAYS VERIFY' set across by Google's Beyond Corp model, InstaSafe's Remote Access solutions provide seamless secure connectivity of on-premise and cloud resources, to workforces situated anywhere in the world. InstaSafe leverages its three dimensional risk assessment methodology to assess the risk and trust associated with every user, device, and application. For every individual request to assess enterprise resources, the context of the request is assessed, and device and user checks are done using multiple parameters. Once this process of comprehensive authentication is complete, the user is granted access, but only to those applications that she is authorised to access, while the entire network remains inaccessible.

With InstaSafe's Single Pane Command Console, security teams get complete visibility into user activity, and are able to frame access policies down to the individual user level.



1. Endpoint provide device fingerprint by sending in a SPA request
2. Secure/Mutual TLS to controller
3. User Authentication + MFA
4. Receive Authorisation info
5. Request Access for Application via Gateway X
6. Check Authorisation and Relay message to Gateway X
7. Send SPA Request to Gateway X
8. Application Specific mTLS tunnel to Gateway X

## Secure Remote Access

- ✓ Protect and Enable Access for on-prem applications
- ✓ Integrated Single Sign On for a seamless access experience
- ✓ Natively secure all cloud applications
- ✓ Secure access to internal web applications
- ✓ Secure remote access to SSH/RDP
- ✓ Secure remote access to RDP
- ✓ Separate data and Control traffic

## Granular Access Control

- 🔒 Enforce role-based access policies
- 🔒 Geolocation and Geobinding - restrict access based on location of user and device
- 🔒 Enable behavioural biometrics for privileged users accessing critical data
- 🔒 Carry forth device posture checks before granting access
- 🔒 Set granular level policies for BYOD devices

## Endpoint Capabilities

- 🛑 Behavioural Biometrics based authentication
- 🛑 Device Posture and User Identity Checks
- 🛑 Dynamic Authorisation based on Geo-risk and Temporal (Time based) Risk Assessment
- 🛑 One click access to Applications on a single Dashboard
- 🛑 Disable Screen capture, Copy/Paste & Clipboard
- 🛑 Disable Screen Recording
- 🛑 Block downloads for sensitive applications

## All round visibility

- 👁️ Monitoring of user activity from Single Pane Command Dashboard
- 👁️ Disable Screen capture, Copy/Paste & Clipboard
- 👁️ Disable Screen Recording
- 👁️ Block downloads for sensitive applications
- 👁️ Multiple cloud based applications accessed through single click
- 👁️ Choose between agent based, agentless, and secure workspace browser options for deployment

## Seamless Integrations

- 🔗 Disable Screen Recording
- 🔗 Easy Integration with 3rd party applications
- 🔗 SAML/AD Integration
- 🔗 Seamless Integration with SIEMs and reporting tools
- 🔗 TOTP Authentication
- 🔗 Inbuilt InstaSafe Authenticator
- 🔗 Log streaming services
- 🔗 Inbuilt IDP with support for LDAP/AD

## Upgrade existing Security Posture

- 👉 InstaSafe Gateway only visible to user device
- 👉 Separate encrypted tunnel for each application connection
- 👉 Conceals itself, applications and devices from internet
- 👉 Secures against DDoS Attacks
- 👉 Separate user and group level access policies
- 👉 MTLS Encryption of traffic
- 👉 Drop All Firewalls



**Asia's fastest growing cybersecurity company is going global. InstaSafe is your trusted remote access security provider, catering to the remote access need of some the world's largest MNCs**

Representative Vendor-  
Gartner's Market Guide for Zero  
Trust Network Access- Global

Nikkei Asia Growth Champion-  
Fastest growing cybersecurity  
company of Asia

True Zero Trust Model, based on  
the CSA-NIST architecture

Representative Vendor- IDC's  
Guide for Software Defined  
Secure Access

Network and security support  
experts available around the  
clock

AWS Advanced Technology  
Partner

42 Points of Presence with 10  
million + endpoints

Customer presence in more  
than 70 countries

Customers in 120+ countries

## **The InstaSafe Experience Zero Trust. One Access.**

Scalable security that caters to the requirements of enterprises of any size. From onboarding and deployment within 4 days, to 24/7 support, at InstaSafe, we believe in leveraging identity to provide an integrated security experience

### **Problems? Talk to us**

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

✉ [sales@instasafe.com](mailto:sales@instasafe.com)

🌐 [www.instasafe.com](http://www.instasafe.com)