InstaSafe
Cloud. Secure. Instant.

Part of the Zero Trust Access Solution

INSTASAFE

ZERO TRUST ACCESS

BROCHURE

InstaSafe Zero Trust for Secure Remote Access

InstaSafe Zero Trust Secure Access is a unified security platform that empowers security teams to allow seamless security and management of remote access capabilities across multi-cloud and on-premise environments, while eliminating the need for VPNS and other obsolete security tools. InstaSafe's award winning Zero Trust methodologies allow IT teams to employ a model of continuous authentication and authorisation, and implement a least privilege access model on scale, while ensuring visibility over user activity. What differentiates InstaSafe's solutions is its ability to deploy both agent based or agentless models as per customer needs, and support multiple use cases within the organisation, ranging from secure cloud adoption, to remote access to on premise as well as cloud applications

Enhance your Remote Access Capabilities- Leverage Context Based Authentication and Authorisation

With InstaSafe's Zero Trust Solutions, we aim to providea seamless remote work experience for your entire workforce, while allowing easy management and control over who accesses what. We rely on a three dimensional, adaptive security framework which uses identity as the control point for allowing or disallowing access within your organisation.

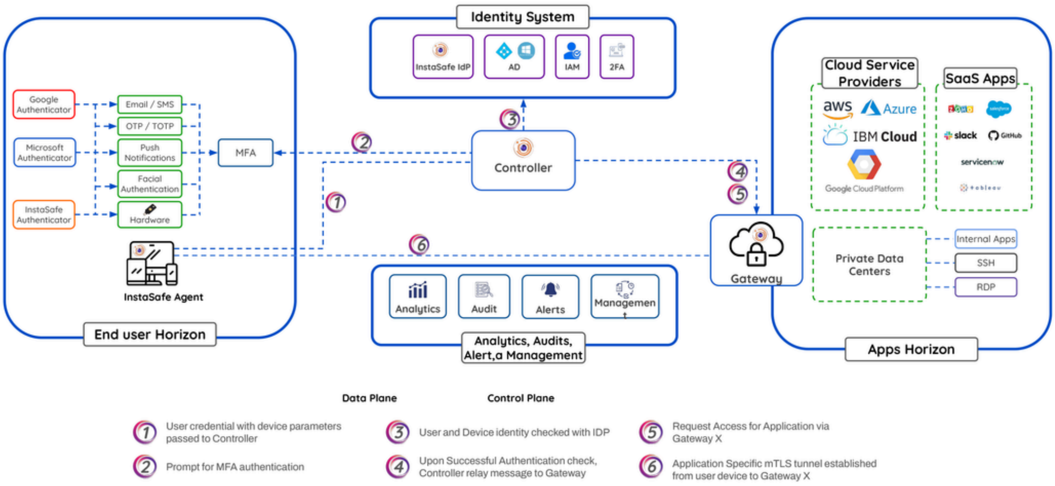
Simply put, with InstaSafe, users, be it remote or on- premise can only see and access the resources (cloud based or on-premise) that they are allowed to access, while all other resources are completely hidden and can't be accessed in any way, fair or foul. With InstaSafe, we eliminate the need for complex VPNS, and firewall policies, and empower your IT teams to implement access policies down to a granular level, while also allowing for complete visibility over network activity. By shifting access control from the network perimeter to the individual user, InstaSafe fulfils the promise of security designed to protect the modern enterprise network.

Security for Hybrid and Remote Workforces: An Endearing Challenge

It is now widely accepted that remote work is here to stay. The term 'new normal' may well be accepted as the only normal for a long time to come. And one of the major issues that is visible in the current context is not limited to the management of remote workforces, but extends to the security and management of hybrid workforces, which are much more complex in nature. With the modern enterprise leveraging the power of the cloud, remote access security solutions must cater to the needs of scalability, functionality in hybrid environments, and an ability to adapt to the remote work reality. Unfortunately, many companies are still dependent on legacy based solutions, which not only leave a larger exploitable attack surface, but are also incompatible with the cloud.

How it Works:

- Identity serves as the control point instead of networks, and access is moved from the network to the application layer.
- This means that users only get access to the applications they are authorised to see, through application specific tunnels, and the entire network is completely hidden from them and inaccessible, thus eliminating the scope for lateral movement.
- A system of continuous, three dimensional risk assessment of the users, devices, and applications are done, and access requests being handled approved on a contextual basis
- Access is given on a need to know basis, and for privileged users, additional layers of behavioural biometrics may be employed before granting access
- Security teams have complete visibility and a full audit trail of all user activity, with user level control over who accesses what. They can disable or enable certain activity depending on the risk assessment of the user



Key Features

Privacy First Approach: Split Plane Architecture

InstaSafe employs a split plane architecture to separate control and data planes and render network invisible to the public internet and prevent network based attacks. In addition, all data is end to end encrypted through Mutual TLS to prevent common MITM attacks

Black Cloud Approach, Least Privilege Access

A Zero Trust Solution should follow least privilege access policies, which means that users, irrespective of whether they are present inside or outside the network, should be given authenticated access to only those applications that they are allowed to use.

Advanced inbuilt authentication and integration capabilities

Integration support with 3rd party business process tools and policy managers for enhanced security management and easy policy orchestration. Inbuilt IDP and TOTP Authentication capabilities, with support for 3rd party integration. Integrated SSO for seamless secure access by end user. Additional Behavioural based Authentication for better security, required for critical users

Application Specific Access

With a view to limit access on a need to know basis, application specific tunnels are built from users to the applications they can access, which ensures that each connection for each of the users is restricted within a specific tunnel. This reduces the insider threats as no user is able to get to know about other users that are using the application or network. External attacks are restricted to a small tunnel or a single application.

Hyperscalable solution deployable in days

Instasafe has deployed solutions in multi cloud multi regions environments for more than 50,000 users in a matter of days.

Granular, Centralised Access Control

Simplified management of users, creation of groups and configuration of access policies for all applications, users, and devices directly through a single pane management Console

All Round Visibility

Complete, all round visibility into all user activity for better identification of threat vectors. Options to restrict or monitor user activity based on risk assessment.

InstaSafe Zero Trust Feature List

Network Access Controls

Features	Description
Least Privilege Access	Users are granted the minimum access necessary to perform their duties.
Access policies - User, group, devices, applications	Define specific access rules for users, groups, devices, and applications.
Role Based Access Control (RBAC)	Assign permissions to users based on their roles within the organization.
Client and Clientless Access	Using clientless access, user can access applications using web browser
Separate path for data and control traffic	Control traffic is established between user and controller. Once user authentication is successful, encrypted data traffic is directly established between user and gateway
Split Tunnel, Full Tunnel	Allow users to route traffic through a VPN (split) or all traffic through a secure tunnel (full)
Always On	Always ON ensures user device is always connected to corporate network whether user is inside or outside the office premise. Users can seamlessly access corporate resources anywhere
Azure AD Join	Push group policies to AD users
Windows Autopilot	Enabling Windows Autopilot for hybrid Auzure AD joined devices using Always ON connectivity

Identity and Access Management (IDAM)

Features	Description
Directory Services Support	
LDAP	Support Lightweight Directory Access Protocol for directory services
Auze AD	Integrate with Azure Active Directory for authentication and management
On-premise AD	Support on-premises Active Directory for user authentication
O365	Integrate with Office 365 for centralized user management and authentication
Google Workspace	Support Google Workspace for user authentication and management

Identity and Access Management (IDAM)

Features	Description
Multi Factor Authentication	
OTP via SMS / EMAIL	Send one-time passwords to users via SMS or email for authentication
Time based OTP	Generate time-sensitive one-time passwords for enhanced security
Fingerprint Authentication	Authenticate users through fingerprint recognition
Facial Authentication	Continuous facial authentication checks the liveness of the user by monitoring the face every 30secs.
Push Notification	Send push notifications on Mobile either to accept or deny
Hardware Token (Yubikey)	Use physical hardware tokens like Yubikey for authentication
Certificate based Authentication	Authenticate users with digital certificates
Form Based Authentiion	Authenticate users through web form credentials
Passwordless Authentication	Enable authentication without passwords using other authentication methods
Single Sign On for SAML based APPs	Single Sign on using SAML authentication
Single Sign On for Non-SAML based APPs	API based authentication to provide Single Sign On (SSO) to non-SAML web applications.

Authentication Protocols Supported

Radius Authentication	RADIUS is a client-server networking protocol that enables centralized authentication and authorization for a remote network.
TACACS Authentication	TACACS is a network security protocol that provides centralized authentication, authorization, and accounting services to access network devices and services.
OAuth Authentication	Enable OAuth protocol for secure authorization
SAML Authentication	Supports both IdP initiated and Service provider initiated SAML authentication
FIDO Authentication	FIDO authentication is based on public key crytography. FIDO allows users to sign in using passkeys.

End Point Controls

Features	Description
IP Restriction	Restrict access based on IP addresses
Geo-Location Restriction	Limit access based on geographic locations
Device Restriction	Control access based on specific device criteria
Time Restriction	Restrict access to specific times
Restrict Jaibreak device	Block access from jailbroken or rooted devices
Restict insecure password to be set	Enforce strong password policies
Device Binding/ Registry	Bind devices to users to ensure secure access
Disable Device Posture control check	16+ parameters can be checked including mac ID, System Serial number, OS Family, and others
Disable Delete (from keyboard)	Prevent deletion of data via keyboard shortcuts
Disable Shift + delete (from keyboard)	Block the use of Shift + Delete to permanently delete files.
Disable Ctrl+D (from keyboard)	Disable the Ctrl+D shortcut to delete items
Right Click & Delete Keyboard	Restrict right-click delete options
Shift + Dot of Num Pad (from keyboard)	Block Shift + Dot key combination
Hide Recycle Bin	Hide the Recycle Bin from users
Delete from Menu/Ribbon	Prevent deletion options in menus and ribbons
Delete from Virtual KeyBoard	Disable delete options on virtual keyboards
Run Disabled	Prevent users from running programs
Right Click Disabled	Disable right-click functionality
Control Panel Restricted	Restrict access to Control Panel settings
Date & Time and Time Zone Restricted	Restrict changes to date, time, and time zone settings.
Sleep Mode Disabled	Disable sleep mode on devices.

End Point Controls

Features	Description
Disable windows update	Prevent users from performing Windows updates
Disable screen saver setting	Restrict changes to screen saver settings
Disable change of IP address to user	Block users from changing IP addresses
Disable firewall setting	Prevent users from altering firewall settings
Disable folder share option	Block folder sharing capabilities
Cut, Copy and Paste Disabled	Restrict cut, copy, and paste functions
Task Manager Disabled	Prevent access to Task Manager
CMD disabled	Disable Command Prompt access
Windows Update Service Disabled	Block Windows Update services
Internet Restricted	Restrict or block internet access
Local Security Policy Access Restricted	Limit access to local security policy settings
Disable history of recently opened documents	Prevent tracking of recently opened documents
Local Drive disable (C,D,E as applicable)	Disable access to local drives
Remove Calculator	Disable access to the Calculator application
Disable access to notepad and word pad	Block access to Notepad and WordPad
Disable file/folder search option	Restrict file and folder search functionality
Auto shell or Auto login option	Enable automatic shell or login options for convenience

Data Loss Prevention

Features	Description
Block Copy and Paste	Prevent copying and pasting of sensitive data
Block Screen Capture and Screen Recording	Disable screen capture and recording features
Blacklist /Whitelist Domain or IPs	Control access to specific domains or IP addresses
Container based Browser	Use containerized browsers for secure browsing sessions
Watermark / Secure Overlay	Add watermarks or overlays for document security
Restrict SCRIPT / EXE File	Block execution of script and executable files
File Download Prevention	Prevent unauthorized file downloads
Blocking Apps like Anydesk, Teamviewer	Block remote access applications for security
Single Device Login	Allow only one device to login per user for enhanced security

Platform and Application Support

Features	Description
Windows Logon and RDP Access	Windows Login is a simplified, secure authentication solution that improves the logon security of Windows Desktops, Servers, and Windows Terminal Servers, ensuring a secure login experience for your users.
VPN - Radius Authentication	Use RADIUS for VPN authentication
Linux Logon and SSH Access	Provide secure Linux logon and SSH access
VDI (Virtual Desktop Infrasturcture)	Support virtual desktop environments
Web Based Applications	Secure access to web-based applications
Thick Client Applications	Support for thick client applications

Central Logging and Reporting

Features	Description
Audit logs for access, login, login failure	Maintain detailed audit logs for security events
Custom alerts for non approved devices	Create alerts for unapproved device access attempts
Historical and Compliance reports	Generate historical and compliance reports
Network Access logs	Log network access events for monitoring and analysis
Integration with SOC / SIEM tools	Integrate with Security Operations Center and SIEM tools for enhanced security

Network and Infrastructure Support

Features	Description
On-Premise/ Cloud Deployment	Offer both on-premise and cloud deployment options
High Availability	Ensure continuous availability of services
Load Balancing	Distribute traffic across servers for optimal performance
Auto Failover	Automatically switch to a backup system in case of failure

Benefits

- Upgrade your least privilege access capabilities: Leverage Zero Trust principles to provide granular access to enterprise resources, irrespective of where they are situated. Use continuous risk assessment and prioritisation to restrict access. Frame granular level policies for access to specific resources, and configure and manage access for applications belonging to different environments in a single dashboard.

- Connect Anything, Anywhere: Enable Remote access of applications situated anywhere to users situated anywhere. Allow secure and seamless Remote Desktop Protocol, Web Application, and SSH Access. Easy access of applications hosted on on-premise DCs as well as multi cloud environments, with a single platform

- Reduce Network based attacks and Insider threats: Secure your legacy servers as well as cloud servers from all forms of network based attacks. Enable Device Posture and User ldentity Checks using multiple parameters to prevent insider attacks. Restrict access based on location of users. Enforce policies to monitor and detect suspicious activity in near real time

- Gain Greater Visibility: Access complete audit trails of user activity. Leverage granular access to disable copy/ cut/paste functions and disable screen recording. Block downloads for sensitive apps. Integrate seamlessly with SIEMS for better insights

- Simplify Security Management: Manage and control access to all your applications from one place. Provision for agent and agentless access for your on premise and remote workforces. Deploy as you scale security that can be used for workforces of any size.

- Advanced Identity and Authentication Capabilities: Inbuilt Identity Provider with integration support for third party ldentity Providers for easier creation and management of user groups. Multifactor Authentication supported by inbuilt TOTP Authenticator Application for an integrated and unified security experience, with Support for 3rd party TOTP applications like Google and Microsoft. Integrated functionality for single click access.

Use Cases

- **VPN Alternative:** InstaSafe's Zero Trust Security solutions cater to the needs of the modern workforce, by enabling secure access to applications of any kind, to workforces situated anywhere. Compared to legacy solutions like VPNS, InstaSafe serves to minimise attack surface and through its process of continuous authentication and least privilege access, prevents malicious actors from gaining insider access to sensitive resources

- **Remote and BYOD Access:** Managing remote workforces is becoming increasingly complex, with many employees requiring remote access to a diverse set of resources, hosted in different environments. With InstaSafe, IT teams can manage access to all applications from a single vantage console. With granular level access control, every user, application, or device will be governed by specific sets of unique rules formulated by security teams, hence allowing for better management of BYOD devices as well

- **Third Party Access:** With advanced limiting features, that include geolocation and geobinding, along with all round visibility over all user activity, privileged access of resources to third party contractors becomes simple and easy

- **Secure DevOps Access:** For DevOps teams operating remotely, secure cloud based production environments are a priority. With its provision of least privilege access based on Zero Trust principles, and a complete audit trail of all user activity, DevOps teams can seamlessly operate in secure development and production environments.

InstaSafe
Cloud. Secure. Instant.

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 endor- 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 identityy 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

🌐 www.instasafe.com

You can connect us at:

/instasafe /instasafe /instasafe /instasafeZT