InstaSafe

Zero Trust Application Access

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 provide a 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.

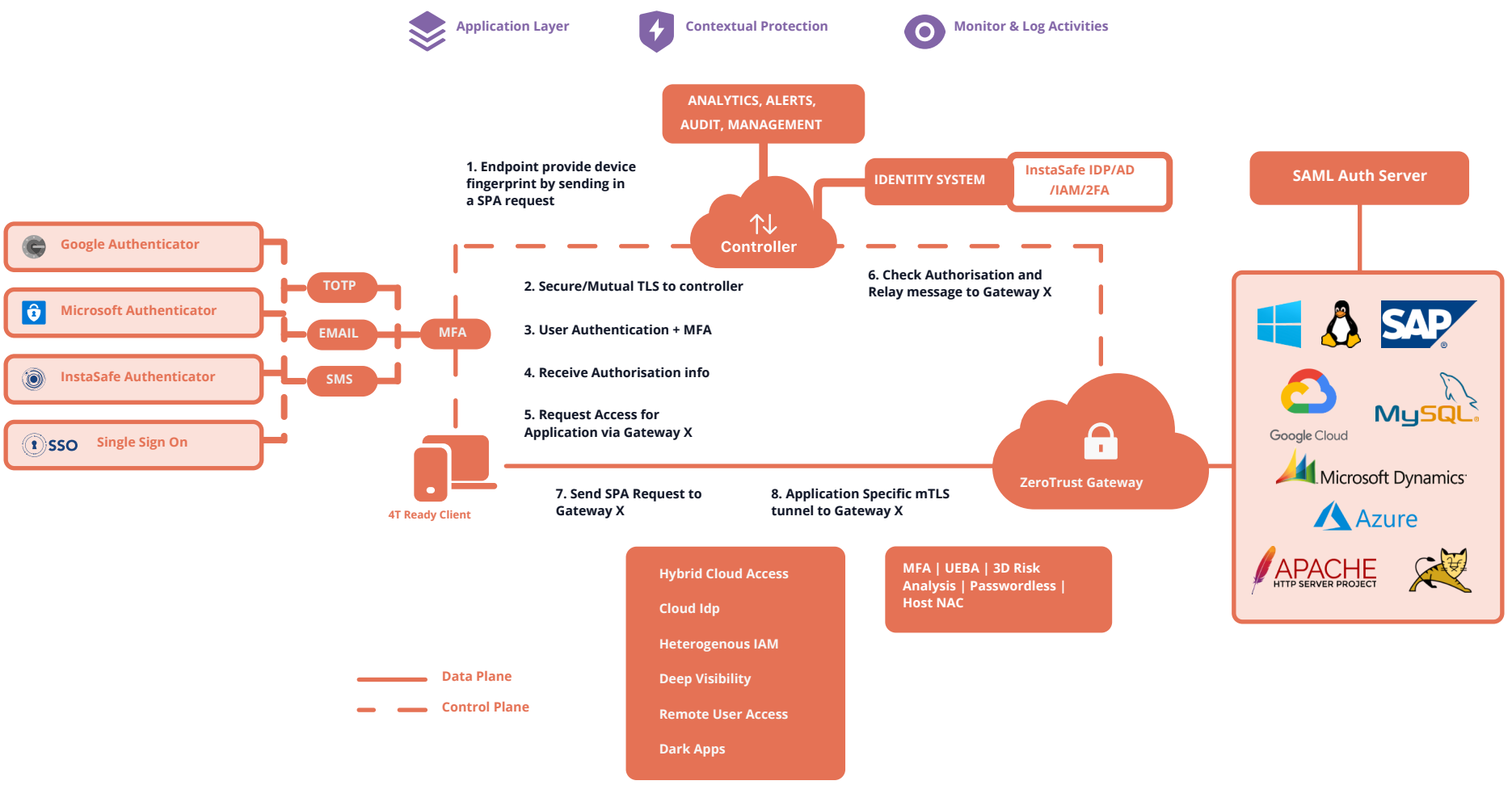
Simply put, with InstaSafe, users, be it remote or on-premise can only see and access the resources (cloud based or on-premise) that they are allowed to access, while all other resources are completely hidden and can't be accessed in any way, fair or foul. With InstaSafe, we eliminate the need for complex 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 and 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

Hyperscalable Solution deployable in Days

InstaSafe has deployed its solutions in multi cloud multi region environments for more than 50,000 users in a matter of days. With a choice to opt between agent based and agentless approach, and a completely hardware free deployment process, you can scale as you go.

Zero Trust, Least Privilege Model

Leveraging the Software Defined Perimeter, users are able to access only a limited number of resources based on permissions set by security teams. 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

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.

Centralized Control

Granular access control over and within each resource, based on the dynamic and contextual assessment of user attributes and device state. A rich set of rules can be enforced across all users, servers and enterprise data stores, including user commands and database queries.

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.

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 Identity 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 Identity 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 SSO 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 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

www.instasafe.com