Cloud. Secure. Instant.

InstaSafe

Frequently Asked Questions

June 2021 | v2.2 | www.instasafe.com

What does InstaSafe do?

InstaSafe's Zero Trust Access solutions enable organizations to provide access to internal corporate applications, without compromising the security of their networks. InstaSafe is easy to deploy, hyperscalable, more cost-effective, and a more secure alternative to VPNs. InstaSafe empowers IT Teams to give authenticated users policy-based secure access only to the internal apps that they are authorised to access, and that they need to work productively. InstaSafe's solutions provide application access without providing network access. Given its cloud agnostic, multi-environment functionality, InstaSafe operationalises Zero Trust in hybrid environments by decoupling itself from the physical network, which means that its software based solutions can be used to seamlessly access applications irrespective of where they are present, be it on-premises or in the cloud.

ZT Security Model	Network Protection	VPN Replacement	App Protection	Supports all Networks and Protocols	True Zero Trust
ZTNA	✓	✓	✗	✗	✓ ✗ ✗
ZTAA	✓	✓	✓	✗	✓ ✗
ZTA	✓	✓	✓	✓	✓

How does InstaSafe enable your organization to achieve Zero Trust at the network layer?

InstaSafe uses a combination of authentication, authorisation, segmentation, and monitoring to deliver Zero Trust security within the organisation. It begins with a comprehensive data and device classification process, wherein the devices are classified on the basis of multiple parameters. This is then fed into the solution's policy engine so customers can evaluate the security risks and frame requisite Zero trust Access policies. Based on multiple identity parameters of the device and the identity of the user, security teams translates the matching Zero Trust policy to the specific commands necessary to configure that policy on a broad range of network devices (switch, router, WAP, FW, SDN, etc.). This means that for every group of users, granular level access policies are configured. The commands are executed by InstaSafe and translate to remote access for each employee via either a client/clientless approach, and agentless approach enables easy deployment without IT administrators manually configuring each endpoint. Added to this, InstaSafe relies on the concept of Software Defined Perimeters. This means that in theory, microperimeters are created comprising of the user, device, and the applications that they are allowed to access. Every request for access is considered independently, and after assessment of the risk associated with the request, and the identity of the user and device, the Controller tunnels user traffic through application specific tunnels. In terms of monitoring and visibility across the network spectrum, InstaSafe relies on unique monitoring features like recording of session activity, and at the same time, integrates seamlessly with monitoring technologies like SIEMs. A continuous monitoring of devices, enables re-evaluation of risk in the event of change of devices, and thus enables easy enforcement of Zero Trust policies with minimal downtime

How does InstaSafe work in hybrid networks (cloud and on-premise)? Do we need additional implementation of different solutions for hybrid environment or multicloud usage?

As a cloud agnostic, heterogeneous solution, InstaSafe has been built with the aim of providing seamless functionalities across hybrid and disparate environments, including wired, wireless, virtualized on-premise data center, and cloud infrastructures. InstaSafe's solutions have been designed to operationalise Zero trust policies across all environments and provide a seamless and unified user experience across any platform being used. InstaSafe helps in the implementation of security policies defined by teams to a very large range of network infrastructure and security products.

What layers of the OSI model does InstaSafe function in?

InstaSafe's solutions operate at levels 3-7 of the OSI model for different levels of identification, authentication, and enforcement. The lower layers like L3 are utilised to inspect raw traffic and for data and device classification. What differentiates InstaSafe from other Zero Trust solutions is its ability to enforce application specific L7 tunnels that enable tunnels from user to authorised applications only. Endpoint device evaluation and inspection is done at the application layer using remote access guidelines and access policies. After successful authentication and verification of the user identity and device identity and evaluation of the Zero Trust policy applicable to that user, InstaSafe ensures application level access for the user concerned

How do InstaSafe's solutions map to the Zero Trust Models?

InstaSafe's Zero Trust Solutions are in line with the Zero Trust framework from the top down. InstaSafe enables IT teams to strategically implement Zero Trust across all portions of their enterprise networks. With powerful authentication and monitoring capabilities, InstaSafe starts with full visibility for all IP-connected devices across enterprise segments, including campus, data center, cloud and operational technology (OT) environments. The solution provides deep inspection of device security and configuration state to determine the device risk posture. The InstaSafe policy engine translates the enterprise's security policies and segmentation strategy into the rules applied by individual enforcement products based on the device's risk posture and the user identity, and on this basis they classify an access request made by a device as trusted or untrusted. Additionally, InstaSafe is easily integrable with monitoring and security tools like SIEMs and SAML/ADs, to simplify security management for teams.

How does InstaSafe simplify segmentation planning within the context of the Zero Trust framework?

Segmentation is a core tenet of the Zero Trust framework. It basically means segmenting and securing networks across hosting models. However, designing, applying and maintaining effective segmentation policies across distributed environments can be an arduous process. InstaSafe has substantially eased the process of designing, planning, testing and deploying dynamic network segmentation across the extended enterprise. Our Zero Trust model implicitly requires not only policy based authorization but also identity based authentication in the context of network micro segmentation, and distributed service connectivity and interconnectivity across hybrid private/public multi cloud scenarios. Since our platform can be used with an agentless approach, it is not only adept at discovering and profiling virtual instances and cloud-based workloads, but also facilitates easy IoT adoption through segmentation and permissions. This allows organizations to embrace Zero Trust principles for all IP-connected systems, while enabling security teams to have an omnipresent visibility across traffic flows and dependencies between users, applications, services and devices.

Does InstaSafe Zero Trust Access integrate with Active Directory or LDAP or RADIUS server?

Yes. InstaSafe ZTAA can be integrated with AD / LDAP / RADIUS servers. Integration with AD / LDAP allows you to directly import all or specific users from the directory and onboard them into InstaSafe ZTAA with a single click. What's more, InstaSafe has an inbuilt identity provider for simplified user group management

Does InstaSafe Zero Trust Application Access provide any hardware to be installed in my network?

No. InstaSafe ZTAA is a software only solution and does not deploy any hardware. The Gateway module that is installed in the customer network requires any generic hardware running a compatible OS such as Linux, Windows or Mac OSX

Does InstaSafe Secure Access support 2FA?

Yes. InstaSafe Secure Access has built-in support for 2FA using either SMS / Email / Google OTP. We also support other third party token based products such as RSA SecurID, Vasco etc. using RADIUS protocol.In addition, InstaSafe's own Authenticator Appplication, which has capabilities ranging from TOTP based authentication to biomteric enabled access, adds to the security of your enterprise

Does InstaSafe ZTAA work without an agent?

Yes. InstaSafe ZTAA can be used with both an agent based or agentless approach, and also supports secure workspace browser. InstaSafe's flexible security functionality makes our solution unique and more secure than the others and can be used for multiple use cases

Can I connect multiple clouds using the InstaSafe ZTAA solution?

Yes, InstaSafe Secure Access solution was designed to be cloud-independent. Using the Secure Access Gateways you can connect your deployments on different clouds or hybrid environments.

Does InstaSafe save any of my data that is passing through it?

No. All data from the endpoint Client to the Gateway is tunnelled through the AES 256 bit encrypted tunnel. The tunnel is not terminated on the wire in our cloud and hence no data is decrypted nor stored in our cloud. We only store activity, access and other related logs for a specified period of time. Such logs are accessible only by authorized personnel of InstaSafe based on their role.

What are the main benefits of using InstaSafe Zero Trust Application Access?

InstaSafe Zero Trust Application Access helps you protect your applications against many network based attacks by allowing you to hide the applications, while at the same time allow access to the applications to only authorized users accessing with registered / authorized devices. The benefits can be outlined as follows:

Better Security: Secure access for users to access corporate applications across multi cloud environments, or on premise, without the need of switching agents

Better Access Control: Role based access to business applications on a need to know basis

Deploy Anywhere: Supports all user devices and all operating systems

Better Visibility and Analytics: With a single dashboard for all private Business Applications with complete visibility into network traffic, for a simplified enhanced user experience

BYOD security: Protect BYOD Users from unwarranted Cut, Copy, and Screenshot Capture

Rapid Deployment and Scalability: Solutions can be deployed for large workforce and across multi cloud environments in days. It can be scaled as per your need on just one click.