InstaSafe
Cloud. Secure. Instant.

Better Security through the Privacy First Approach

Why InstaSafe Zero Trust is a better VPN alternative than Cisco Duo Security

Jan 2022 | v1.1 | www.instasafe.com

The Need to Rethink Remote Access Security for your Modern Network

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 Zero Trust Access: A Secure Access 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.

Zero Trust is a holistic approach to security that addresses these changes and how organizations work and respond to threats. The Zero Trust model and philosophy incorporates the need for borderless networks. Whether inside or outside of the corporate network – nothing should be trusted automatically. With Zero Trust, this trust is established but is constantly re-evaluated. Hence temporary.

Leveraging the Zero Trust precedent of 'NEVER TRUST, ALWAYS VERIFY' set across by Google's Beyond Corp model, InstaSafe's Zero Trust 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 prior to establishing the connection. 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 s/he is authorised to access, while the entire network remains inaccessible.

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, where identity includes the user and the device.

The Privacy First approach: Split Plane Architecture

InstaSafe follows a Privacy First approach. To put it across in simple terms, InstaSafe builds its technologies on the fundamental assertion that the data belonging to the company should be handled by the company itself, and not by any intermediary vendor.

Cisco Duo Platform steers all internet bound traffic, without segregating or differentiating the traffic, to the Cisco Cloud for inspection. Now, this essentially increases the risk of supply chain attacks, wherein, when the security provider is compromised, and access to the Cisco cloud is attained, it results in company data being compromised as well. It can also act as a bottleneck and be a reason for latency. InstaSafe believes that a vendor managed device should not get the visibility to the data consumed by the users of the organisation.

InstaSafe Zero Trust Access was designed to create an architecture for positive identification of network connections through single packet inspection prior to accessing sensitive data. And one of the inherent underlying principles in designing InstaSafe Zero Trust Access was the principle of a Split Plane Architecture. A split plane architecture is the separation of the control plane, where trust is established, from the data plane where actual data is transferred. The control plane carries forth the processes of user authentication and authorisation, while the actual data is transferred through the data plane. Separating the control from the data plane renders protected assets "black," thereby blocking network-based attacks. It also ensures that the customers' data directly flows from the user device to the application without driving it through to the vendor's machines. The method helps to avoid the network latency as well. The data in question flows to and from the user device and application server owned by the company. While ensuring proper authentication through the control plane, the direct flow of data to the application server ensures data privacy for the company. In addition, this removes the vulnerabilities inherent in TCP and TLS termination as well.

	Feature	InstaSafe ZTA	Cisco Duo
Application Support	Intranet Web Apps	✓	✓
	SaaS Apps	✓	✓
	Virtual Apps and RDP	✓	✗
	Client Server App	✓	✓
Simplified Deployment and Management	Centralised Security Management	✓	✓
	Choice of Client and Clientless Approach	✓	✓
	Support for Windows	✓	✓
	Support for Linux	✓	✓
	Support for macOS	✓	✓
	Support for iOS	✓	✓
	Integrated Management Tool available as bundled offering	✓	✓
Authentication Capabilities	Inbuilt IDP	✓	✗
	Inbuilt SSO Capabilities	✓	✓
	Support for third party IDP Solutions	✓	✓
	Integrated Single Sign On to all Web Based Applications	✓	✓
	Geo and Temporal Risk Assessment	✓	✓
	ML Based Authentication	✓	✓
	Integrated MFA with / Google/ Microsoft Authenticator Support	✓	✓
	Behavioural Biometrics based Authentication	✓	✗

	Feature	InstaSafe ZTA	Cisco Duo
Security Capabilities	Split Plane Architecture	✓	✗
	Single Packet Authorisation	✓	✗
	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	✓	✓
	Support for RDP	✓	✗
	Simplified DDoS Protection	✓	✓

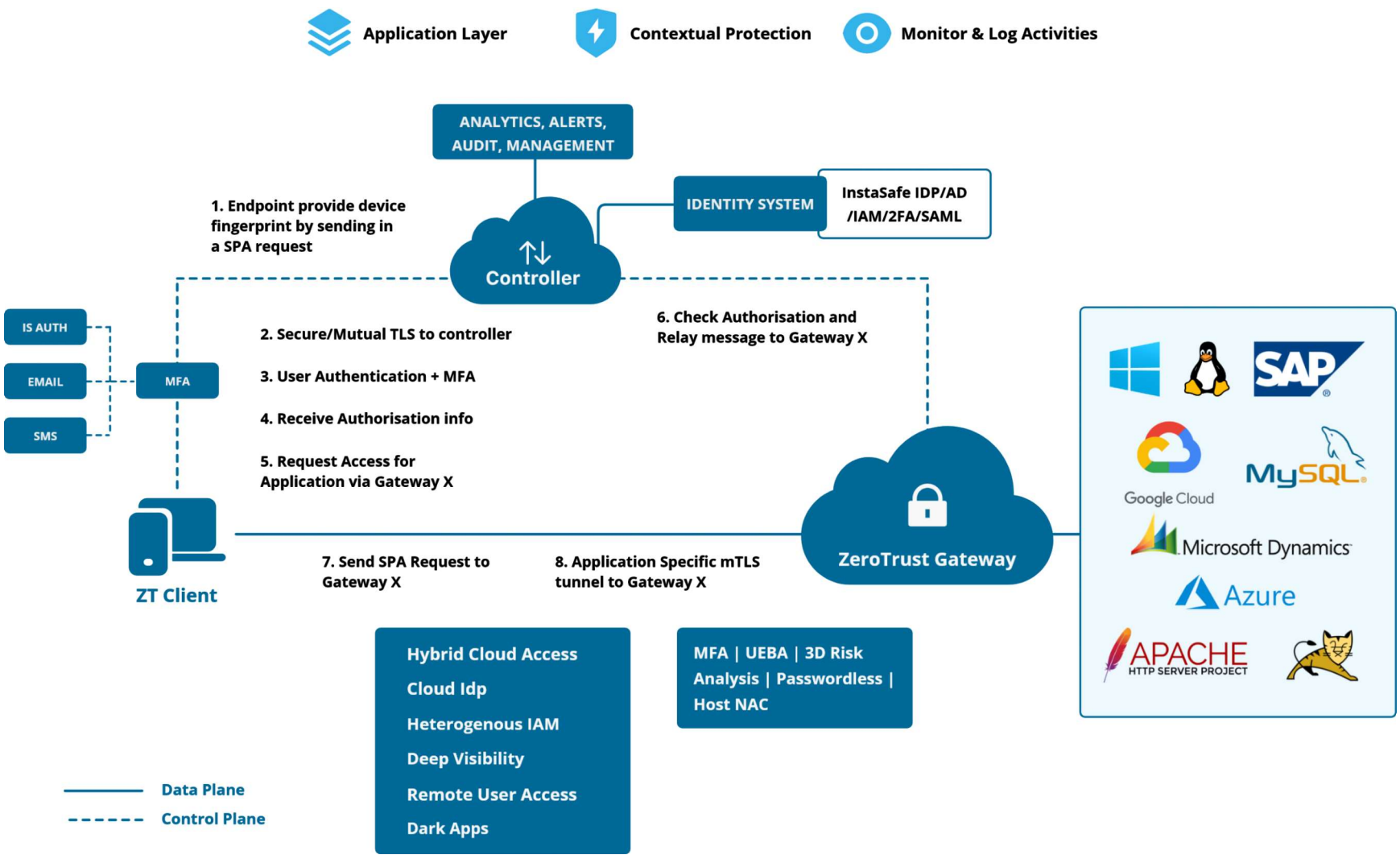
Ease of Deployment

InstaSafe Zero Trust believes in offering customers the choice of a true VPN less, seamless, clientless approach that ensures security without affecting productivity. InstaSafe ZTA's support for client and clientless deployment enables a flexible onboarding for the customer, and allows access via any web browser on any platform without downloading the Zero Trust Client. This makes sense especially when it comes to ensuring quick deployment for a large distributed workforce.

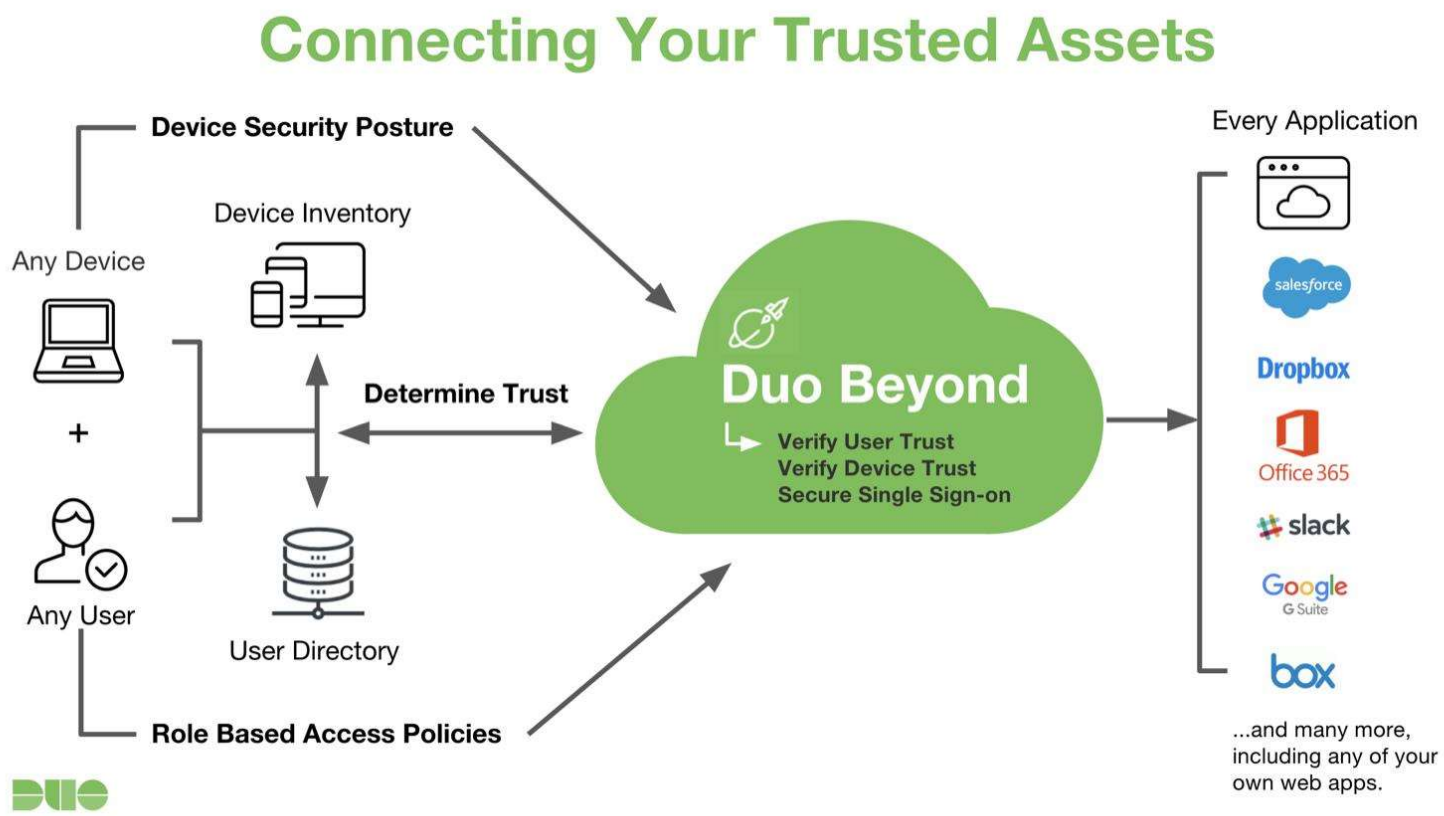
Clientless Zero Trust: InstaSafe ZTA provides a choice for agent based and agent less approach for accessing enterprise applications. Once the security team defines the access policies, the user may access web and SaaS apps using any native browser. This provides a web isolation solution, that launches any web, SaaS or virtual app while also maintaining an air gap between the device and the app.

Client-based Access: When accessing enterprise apps from the lightweight InstaSafe Zero Trust client, InstaSafe launches the requested application after authorisation in a Chromium browser embedded in the ZT Client. InstaSafe supports iOS, Android, Windows, macOS, and Linux platforms and provides a seamless user experience.

Clientless Access: InstaSafe also empowers secure clientless access through any native browser, by executing remote browser isolation, which allows for secure access to web based applications while also securing the network from browser based attacks.



InstaSafe's Zero Trust Architecture showcasing split plane architecture (Data plane and control plane)



Cisco Duo Zero Trust : **Single Plane Architecture (Authentication and Data in same tunnel)**

Zero Trust, One Access: Integration and Authentication Capabilities

One of the key defining features of InstaSafe is its versatility, not only in terms of deployment or onboarding, but also in terms of single click access to applications by end users. With support for L3/L4 and L7 layers of protocols and applications, InstaSafe also enables an easy 5 step onboarding process for web based and protocol based applications for admins:

1. **Create Users**
2. **Create Application**
3. **Create Policies**
4. **Create Gateway**
5. **Add applications to gateway**

What makes InstaSafe different from other major Zero Trust providers is the quest for eliminating gaps in security infrastructure, not only through seamless integration capabilities, but also with the additional inbuilt security capabilities. Thus, InstaSafe ZTA extends beyond support for integration with customers' third party IDP solution providers such as AD, Azure AD and includes an inbuilt IDP, which helps create and manage the users and user groups.

InstaSafe Zero Trust also enables single sign on functionality for all web based applications. The single sign on feature works closely with SSO enablers such as Google SSO and SAML solution providers.

InstaSafe's Geo and temporal Risk Assessment features enable security teams to control the user access based on working hours and location. This feature ensures that the access to the user device will be provided only when it adheres to conditions such as location of the device, time of access and security posture of the device.

The Multifactor Authentication Functionality of InstaSafe is powered by SMS, EMAIL and TOTP providers such as Google and Microsoft. In addition, InstaSafe has its own InstaSafe Authenticator which can be used to enable MFA functionality.

Future Proof Security: ML Based Authentication

Strengthening the precepts of a Zero Trust model by involving elements of machine learning and behavioural biometrics for privileged users can result in a further tightening of network defences against common attacks like identity and credential theft. While all the authentication mechanisms focus on validating an information that's present with the user, Machine Learning(ML) focuses on the behaviour of the user. When another user impersonates the original user, the way he types or uses the device is different. The solution identifies the impersonation of the end user based on the usage of keystrokes and other history based approaches and block access. This feature is available for high priority privileged users in a company to secure access to highly confidential information.

About InstaSafe

InstaSafe Cloud. Secure. Instant.

As an industry pioneer in Zero Trust, human-centric solutions, we, at InstaSafe have backed the belief that at the center of security for businesses, lies the ability to enable workforces to unleash their potential, irrespective of where they are. Which is why we help organisations in fulfilling their goal of productivity on scale, by simplifying the challenge of ACCESS.

With our hyperscalable and modular solutions, we aim to make the cloud and remote journey for businesses and workforces, much simpler, and much more secure

Recognised by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access and InstaSafe Zero Trust Application Access follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. Spread across 5 continents, we secure 500,000 endpoints for more than 100 Fortune 2000 companies, with our cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

sales@instasafe.com www.instasafe.com