celestix

White Paper

Why InstaSafe Zero Trust is a better security alternative to VPNs

Zero Trust Application Access

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.

Traditional castle-and-moat security models of VPNs, in essence, don't hold good when it comes to security for the modern workforce, with both applications and workforces moving outside the traditional perimeter. InstaSafe Zero Trust Access provides a 100% hardware-free, zero configuration, VPN-less solution to access all intranet web, SaaS, mobile, and virtual applications—whether using managed, unmanaged, or bring-your-own devices (BYOD) over any network. This solution brief explores why Citrix Workspace is a better choice than VPN to meet security, performance, and scalability requirements for remote workers.

The Problems with VPNs:

Sans today's broadening horizons of technological reach, and the resulting dissolution of geographical boundaries, providing access to enterprise applications would have been a simplified process, given that all users would have resided in predictable locations, and would have used enterprise issued devices.

However, with the advent of the cloud generation, access on the go has become paramount for the effective operation of any organisation. This, in turn, creates multiple complexities, exposing the vulnerabilities that can be easily be exploited in traditional technologies like Virtual Private Networks:

1. A majority of existing corporate networks operate on the basis of a traditional hub and spoke model. They are flat, in the sense that there is a minor, and in most cases, no distinction of data and user networks. In this scenario, traditional network access technologies, like VPNs, tend to extend trust to anyone in an internal network, allowing for lateral movement attacks and exploitation of vulnerabilities, including MITM (Man in the Middle), and PtH (Pass the Hash) attacks.

2. Additionally, when VPN users are present on the network, VPNs end up providing network level access to data centres, potentially placing the entire network at high risk. Malicious actors may exploit minor vulnerabilities to gain access to the entire network, and wreak havoc.

3. While organisations traditionally use remote access VPNs to extend their networks to remote users, the costs involved in deploying full VPN gateway appliance stacks are significant, and additionally, they require resources to manage on a consistent basis. In essence, handling data centre based hardware technologies like this is an expensive and cumbersome affair.

4. In the context of today's enterprises, it becomes imperative to grant varying levels of access, and assign different levels of trust to different users. In this aspect, VPNs fail to make a mark. Traditional VPNs are unable to provide granular segmentation along with varying levels of access.

5. The entire process of having a user's traffic routed through VPN gateways that are located within different data centres, sometimes not in the same geography as the user, tends to increase latency, slow down the process, and effectively downgrade user output and user experience.

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:

1. Innate distrust, default deny: Operationalise a system of continuous authentication and authorisation to provide least privilege, contextual access
2. 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
3. Align and Integrate: Align to a broader security strategy and allow for easy integration with other security tools for better security posture
4. 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.

	Feature	InstaSafe ZTA	Legacy Solutions
Application Support	Intranet Web Apps	✓	✓
	SaaS Apps	✓	Partial
	Virtual Apps and RDP	✓	X
	Client Server App	✓	✓
Simplified Deployment and Management	Centralised Security Management	✓	X
	Integrated Management Tool available as bundled offering	✓	X
	Choice of Client and Clientless Approach	✓	✓
	Support for Windows	✓	✓
	Support for Linux	✓	Limited
	Support for Mac	✓	X
	Support for iOS	✓	X

	Feature	InstaSafe ZTA	Legacy Solutions
Authentication Capabilities	Inbuilt IDP	✓	X
	Inbuilt SSO Capabilities	✓	X
	Support for third party IDP Solutions	✓	Y/N
	Certificate based authentication	✓	X
	Integrated Single Sign On to all Web Based Applications	✓	X
	Geo and Temporal Risk Assessment	✓	X
	ML Based Authentication	✓	X
	Integrated MFA with InstaSafe/ Google/ Microsoft Authenticator Support	✓	Partial
	Behavioural Biometrics based Authentication	✓	X
Security Capabilities	Split Plane Architecture	✓	X
	Single Packet Authorisation	✓	X
	Segmentation at Application Traffic Level	✓	X
	User Activity Monitoring	✓	Partial
	Drop All Firewall	✓	X
	Role Based Access Control	✓	X
Application Access Capabilities	Access to L3/L4 protocols and applications	✓	✓
	Application Access without Network Access	✓	X
	Support for RDP/SSH	✓	X
	Simplified DDoS Protection	✓	X
Monitoring	Continuous health monitoring Application health is continuously monitored to ensure that ports are available and users can connect to the app.	✓	X
	Integrated access portal for web apps, hosted apps, SAAS Apps	✓	X

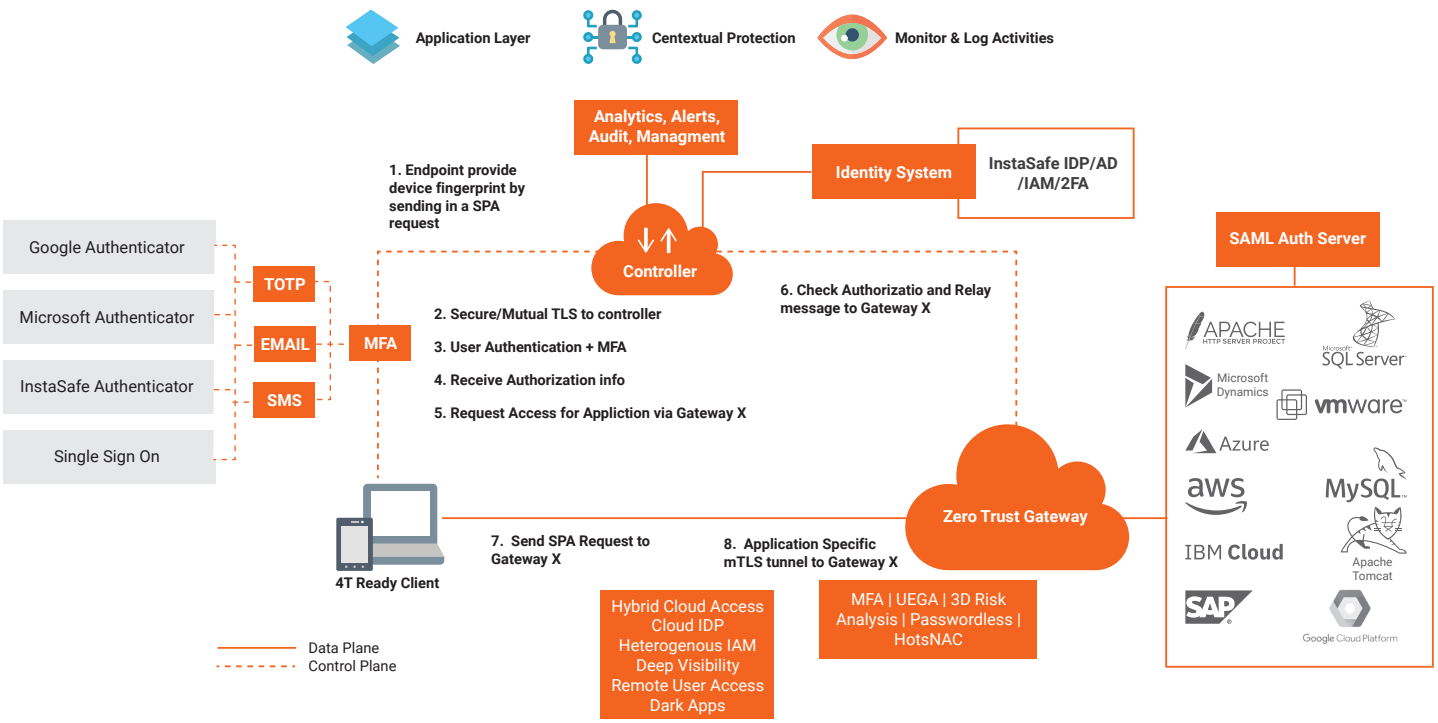
The Privacy First approach: Split Plane Architecture

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.

VPNs steers all internet bound traffic, without segregating or differentiating the traffic, to their server for inspection. Now, this essentially increases the risk of supply chain attacks, wherein, when the security provider is compromised, and access to the server 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.



Instasafe’s Zero Trust Architecture showcasing split plane architecture (Data plane and control plane)

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. On the other hand, VPNs do not support Linux platform effectively.

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.

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.

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.

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.

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.

The Latin adage "Tempora Mutantur"- Times have changed, and we have changed with it; is precisely apt to describe the constant state of flux that the IT industry is in. As the maxim suggests, Information Technology transformation is the only constant. With the advent of the

cloud, we are witnessing a rapid broadening of the "edge of network". Sadly, this brings with it greater opportunities for attack and exploitation of data. Given the widespread migration of internal enterprise applications to the cloud, for use by both on premise users and more importantly, remote users, traditional network security models might turn up to be woefully inadequate in preventing malicious attacks

Cloud based solutions are today proving to be a silver lining that are a key driver in maintaining business continuity in the midst of an impending pandemic. While the future of the outbreak and its impending ramifications remain vague, it is apparent that there is a need to revamp corporate capabilities in line with increased adoption of cloud technologies. Companies may have to go back to the boardroom to discuss, re-evaluate, and re-assess the impact of such disasters on their functional capabilities, and may have to accept the utility of remote work, and the adoption of its associated technologies as the norm.

In this scenario, InstaSafe endeavours to make your transition easier with cloud based security and disruptive innovations like those of Zero Trust Network Access. By enabling extension of remote access capabilities on cloud, securely, and instantly, we empower organisations to maintain business continuity. With traditional security perimeters becoming redundant and somewhat dissolving into oblivion, every organisation needs to shift their focus from a network centric approach, to a user and application centric one. Only then can an organisation's business processes be distributed workforce friendly, flexible to sudden changes, and supportive of digital transformation. So the question arises, how ready are you to be a part of the long impending work from home revolution, the wheels of which are already in motion?

celestix

Celestix Networks, Inc.
4125 Hopyard Road #225
Pleasanton, CA 94582
www.celestix.com

Americas : +1 510.668.0700
EMEA : +44 (0203) 900 3737
Asia : +65 6958 0822
sales@celestix.com