InstaSafe Zero Trust

Secure Access to Office 365 Applications

A Zero Trust Security Model employs concepts beyond the traditional confines of network security, relying on the basic assumption that trust is not an entitlement; trust, and by extension, access, needs to be gained through a comprehensive process of verification, authentication, and visibility.

WHAT DOES ZERO TRUST ENCOMPASS?

The traditional security model uses network perimeters which divide users and devices into 2 groups: those on the ‘inside’, deemed to be ‘trusted’, and gaining unrestricted access to resources within the network, and those on the ‘outside’ which are untrusted. This system of assigning excessive trust by default, as an entitlement, has an inherent problem. Once the network perimeter is breached, attackers can move laterally through the network, accessing and exploiting all critical resources.

In an increasingly mobile world, where fast and secure access to applications, both cloud and on premise, has become an imperative, implementing a perimeter-based security model becomes even more impractical and presents a myriad of security risks. One can no longer unilaterally assign trust to a user, since users are mobile and enterprises have migrated to the cloud. Thus, organisations need to consider a better approach towards securing access while facilitating modern digital transformation.

The rise of a novel and innovative new approach to these security challenges has arisen very recently. Known collectively as a Zero Trust Security Model, this approach doesn't assign trust to any user or device by default. Instead, this model lays emphasis on the authentication of every user and the verification of the security posture of every device, as apart of a comprehensive risk and trust assessment process, for every single access request that is sent. Only after a multilevel process of authentication, is the user granted access, that too only to those application that the user has been allowed to use.

Organisations today have started moving en masse towards the adoption of a zero trust model, using technologies like a Software Defined Perimeter, since they guarantee better security along with constant monitoring and 360 degree visibility of all network traffic.

Irrespective of the scenario, Microsoft applications have been indispensable to the functioning of innumerable organisations. With the increasing adoption of the cloud, operationalising and implementing zero-trust access models can not only reduce the challenges of lateral movement, and data breaches, while at the same time ensuring all round visibility and enhanced user experience. In this solution brief, we will showcase how InstaSafe's Zero Trust Solutions ensure zero-trust access security for the Office 365 suite.

DIRECT INTERNET CONNECTIVITY FOR OFFICE 365 – DIRECT INTERNET CONNECTION USING APPLIANCES

Office 365 was built to be accessed securely and reliably via a direct Internet connection and Microsoft has invested in a CDN to deliver a fast experience. Deploying appliances at each branch is better for the user experience, but it is expensive to buy, deploy and maintain.

CHALLENGES WITH APPLIANCES

- Requires constant firewall updates and missing an IP or URL update will cause connectivity issues
- Requires appliance capacity assessments to ensure they can handle the high number of long lived connections.
- Requires security tradeoffs in branches with only UTMs or firewalls for security.
- Requires local DNS.

HOW DOES IT WORK?

With its simple to use interface and features that ensure enhanced productivity, Microsoft Office 365 ensures a profitable and cost effective experience. That said, there may occur multiple security risks that security teams must consider while moving their critical data to the cloud. In this scenario, implementing a model that considers each access requests uniquely using a risk and trust assessment methodology, and enforces granular level access policies for better control over who sees what.

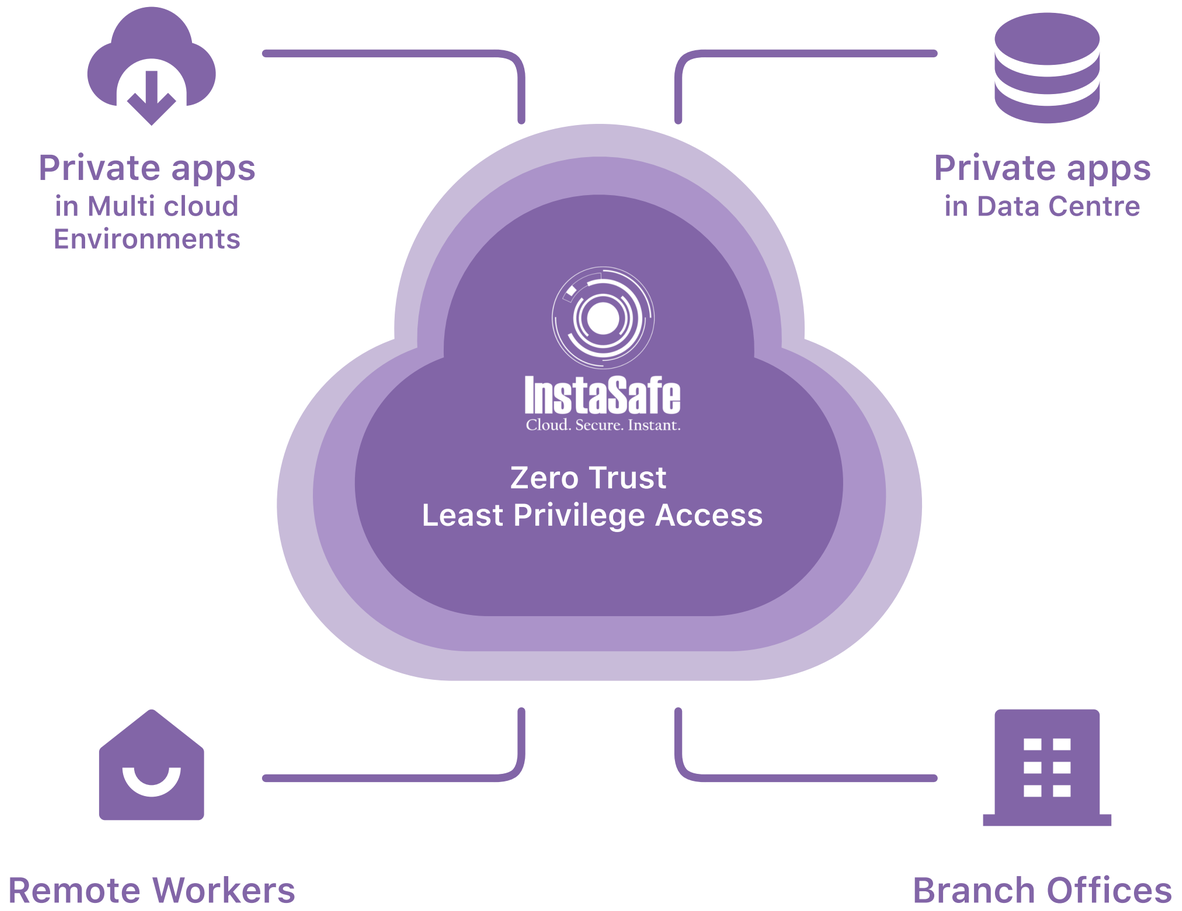
InstaSafe's Zero Trust Solutions makes Office 365 deployment easy. InstaSafe provides your users with a fast Office 365 experience, while maintaining the highest level of security for Internet traffic. Simply point your Internet and Office 365 traffic to the closest InstaSafe data center. There is no hardware to deploy and manage and since traffic is routed locally, you can reduce your MPLS spend.

HOW INSTASAFE ZERO TRUST ACCESS SECURES OFFICE 365

- Never Trust, Always Verify: Using a combination of multifactor authentication, geolocation, device checks, and behavioural biometrics, InstaSafe ensures that every user, and her device is authenticated for every request to access applications. Through this comprehensive authorisation process, InstaSafe secures users against a variety of attacks, which may include credential theft or DDoS attacks. Given that Office 365 is implemented across the organisation, InstaSafe offers a variety of authentication modes, based on the role of the user and her presence in the stack.
- Granular, Role Based Access Control: InstaSafe uses microsegmentation and Software Defined Perimeters, empowering companies to implement role based access policies, so as to ensure that users get access to applications that only they are allowed to access, and that too only after their device's trust level is assessed and authorised.
- Visibility across managed and unmanaged devices: Since remote workforces are able to access Office 365 from anywhere in the world, there arises a need for all round visibility into all network traffic, for better identification of threat vectors. InstaSafe ensures complete monitoring and insight over all the devices which are logging into Office 365. With these security insights, administrators can assess if devices logging in are potentially vulnerable to exploits and attacks. In addition, InstaSafe Zero Trust Access is compatible across all end user device platforms, thus empowering organisations to gain visibility into BYOD as well.
- Support Across Multiple Cloud based Apps: Companies use multiple cloud applications and platforms which they utilise for various use cases. With InstaSafe, your organisation can easily extend security policies for Office 365 to other cloud applications. In addition to this, the Continuous Adaptive Risk and Trust Assessment Framework followed by InstaSafe helps in customising access policies for each of these cloud based applications

THE INSTASAFE APPROACH

- Use InstaSafe portal to group all the applications (Skype, Yammer, Mail and OneDrive) with respective public subnet.
- After user on boarding to InstaSafe Zero Trust Portal, the respective administrator has complete control to create customised access policies for each user
- Administrator can also determine and define the device specifications and geographic specifications for user access
- Once the access policies have been created, the user can login and download the InstaSafe agent to connect office 365 applications outside his/her office network.



FEATURES OF INSTASAFE ZERO TRUST ACCESS

- No requirement for VPN Access. Works on Zero Trust Principles.
- Support for SAML/AD integration
- Integrated Single Sign On (SSO)
- Geolocation and Geofencing for targeted devices and users
- Multilevel, Multifactor Authentication (SMS, Email, google Authenticator, QR Code, etc)
- Behaviour based Authenntication for advanced use cases, using neural networks
- Supports Intergration with all popular SIEMs, including QRadar, ArcSight, Splunk
- Can be used to enable screen recording, do time based checks, and disable screen capture.

ABOUT INSTASAFE

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. 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. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

CONTACT US

InstaSafe Inc,
340 S Lemon Ave
#1364 Walnut,
CA 91789,
United States
+1(408)400-3673

InstaSafe,
Global Incubation Services,
CA Site No.1, Behind Hotel
Leela Palace Kempinski,
HAL 3rd Stage, Kodihalli,
Bengaluru – 560008

/InstaSafe
/instasafe_diaries
/InstaSafe
/company/instasafe

hello@instasafe.com | www.instasafe.com | +1(408)400-3673