Getting Started with Zero Trust

InstaSafe's Zero Trust Whitepaper

GETTING STARTED WITH YOUR ZERO TRUST JOURNEY

The Latin adage “Tempora Mutantur”: Times have changed, and we have to change with it; is precisely apt to describe the constant state of flux that the IT industry is in. 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. With the adoption of the cloud, users, applications, and devices have moved beyond the confines of a traditional network perimeter, organisations need to move beyond a network-centric approach to security, focusing instead on individual users’ identities, and the applications they access.

In the light of the ever evolving nature of the IT industry, it is surprising to see that certain technologies have continued to be stagnant in terms of metamorphosing to match industry needs. Foremost among these are remote access VPNs. Though they were considered revolutionary when first introduced in the 1990s, with the development of the cloud, the traditional conception of extension of complete enterprise networks to the remote user, on which remote VPNs work, has become a cumbersome and particularly risky affair. With the deployment of network centric security solutions in a dynamic, cloud based environment becoming an increasingly complicated process, and hindering cloud adoption, the need for a versatile cloud based alternative that provides enhanced security, and better scalability at lower costs is imperative.

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, need to be gained through a comprehensive process of verification, authentication, and visibility.

In this Whitepaper, we explore the evolution of Zero Trust as a security concept, and how enterprises can leverage InstaSafe’s solutions as a foundational step in their Zero Trust journey.

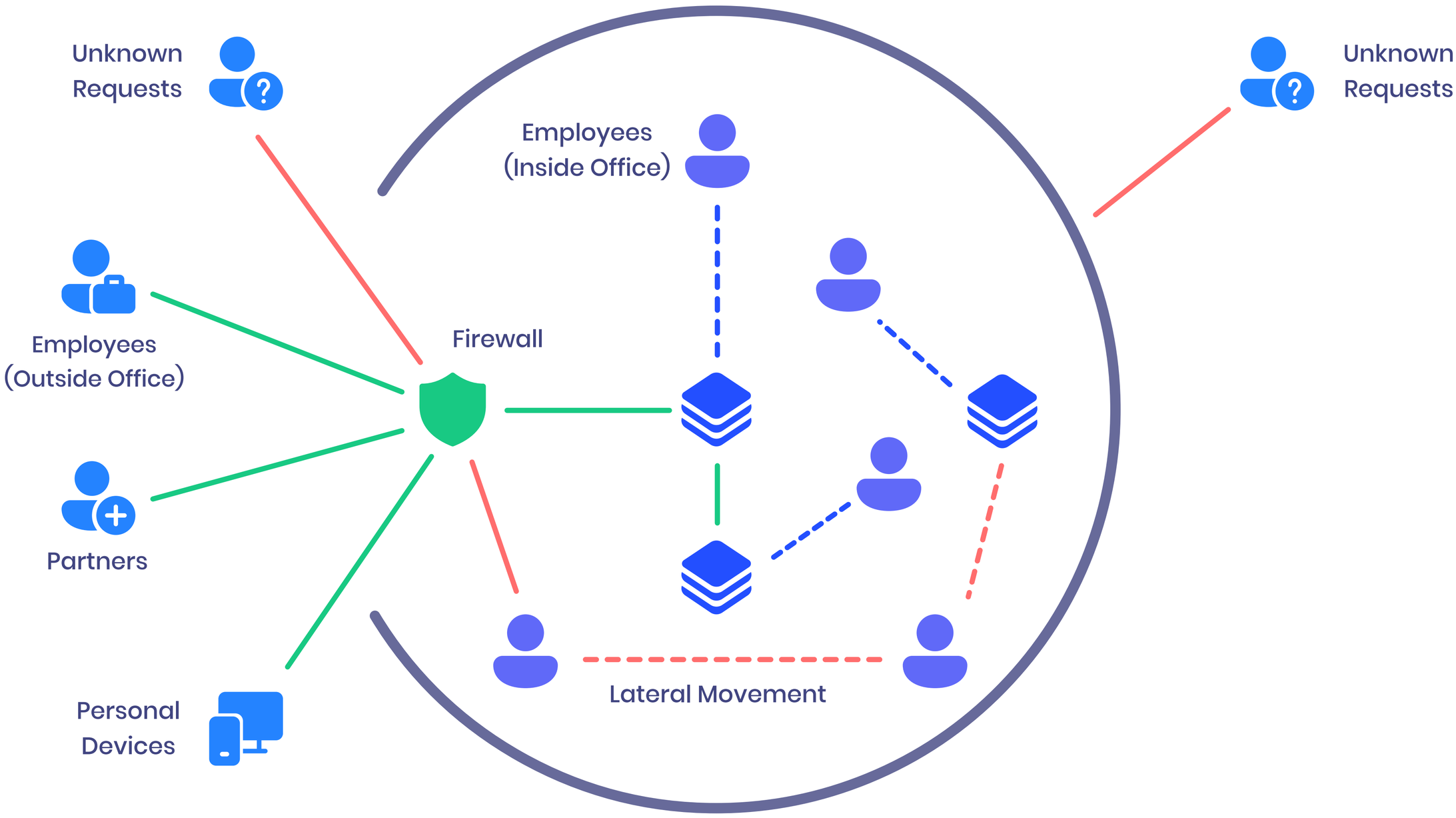
MOVING BEYOND THE CASTLE AND THE MOAT

The invention of the internet had a single purpose in mind: that of connecting users and devices to form a highly interconnected ‘network of networks’. Thus, we had an open system based on unfettered trust, where any device/user could talk with anyone. This system of perimeter based security was analogous to a castle with all of the enterprise assets, protected by gates, moats, and walls, with its entry points being guarded by security technologies, and thus known as the castle and moat approach to security.

In essence, 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 tend to extend trust to anyone in an internal network, allowing for lateral movement attacks and exploitation of vulnerabilities.

With users becoming mobile and applications moving to the cloud, 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.

This system of unfettered trust, however, was exploited by hackers on a large scale, who leveraged the absence of security checks to intercept and siphon off critical data. To keep a check on this, enterprises chose to implement firewalls and other security tools to create a ‘perimeter’, effectively dividing assets into ‘trusted’, present inside the perimeter, and ‘untrusted’ present outside the perimeter. The issue of remote connectivity and access to 3rd party contractors was solved by using technologies like Virtual Private networks (VPNs). The external facing resources moved into DMZs, exposing them to attackers as well.



Security enforced at the network perimeter

In essence, the traditional approach to security has long involved network perimeters that divide users and devices roughly into 2 groups: those on the inside of the perimeter were deemed to be ‘trusted’, having unrestricted access to resources within the network, and those on the outside were untrusted. This system of assigning excessive trust by default had an inherent problem. Once the network perimeter was breached, attackers could move laterally through the network, accessing and exploiting all critical resources.

THE EVOLUTION OF ZERO TRUST

Although the buzz around Zero Trust Security architectures is fairly recent, Zero Trust Network Concepts have been around since the early 2000s. The early conceptions of Zero Trust Networks were devised by the United States Department of Defence while working on their black core routing architecture. Zero Trust Networking concepts were leveraged by leading market research and IT advisory firm Forrester, into a security concept that could be implemented by enterprises.

Among other observations, Forrester recommended that instead of focusing on conventional network perimeters, enterprises should consider all network traffic untrusted. Access should only be granted on a need to know basis, after a process of authentication, and complete visibility over all network traffic should be maintained, for better identification of threat vectors.

Zero Trust Models draw upon the following ground assertions:

1. Distinctions between “inside” and “outside” the network perimeters no longer stand true. Network locality can’t be a lone factor in determining trust.

2. Malicious threats exist on the network at all times, and may be internal or external in nature

3. Every user, device, network, and data, is to be validated and authenticated before granting access

4. Zero Trust Policies are to be dynamic in nature, taking into account multiple sources of data, and continuous monitoring of data is to be done for garnering new insights regarding any new vulnerabilities that may crop up

In essence, ZTNA cannot be divined to be just a single network architecture, but is rather a set of guiding principles in terms of both network design and network operation that dramatically revamps the security infrastructure of an organisation, while at the same time increasing visibility and the scope for analytics across the network.

Gartner also recently published a new Market Guide for Zero Trust Network Access, laying down the need for companies to adopt Zero Trust projects. The report, while delineating on the types of Zero Trust Access, included a list of representative vendors, which offer Zero Trust capabilities. InstaSafe features in the coveted list of 24 vendors, offering Zero Trust access. Among other observations, Gartner recommends phasing out legacy VPN-based access for users who don’t need full network access and begin phasing in ZTNA. This reduces the ongoing need to support widely deployed VPN agents and introduces agentless identity- and device-aware access, which can facilitate access from managed and unmanaged devices.

Zero Trust Network Access (ZTNA) is an evolved response to changing enterprise security trends, which especially include those relating to remote users and cloud based assets, that are not present within enterprise owned network realms. Given that traditional perimeters are dissolving in the light of new and unprecedented expansionary trends, ZTNA concepts shift the focus from protection of network segments, to the protection of resources. A network location is not considered to be the primary component of the security posture of the enterprise anymore.
ZTNA approaches stress on providing a consistent security strategy of users accessing data from any location in any way. By adopting a “Always verify before you trust” stance, ZTNA flips the entire traditional trust calculation, asserting that all transactions, users, and data, whether on-premise or remote, are not to be trusted from the outset.

While framing an all-encompassing definition of a zero trust architecture requires touching upon multiple aspects of network architecture, a brief operative description of a zero trust architecture may be as follows:

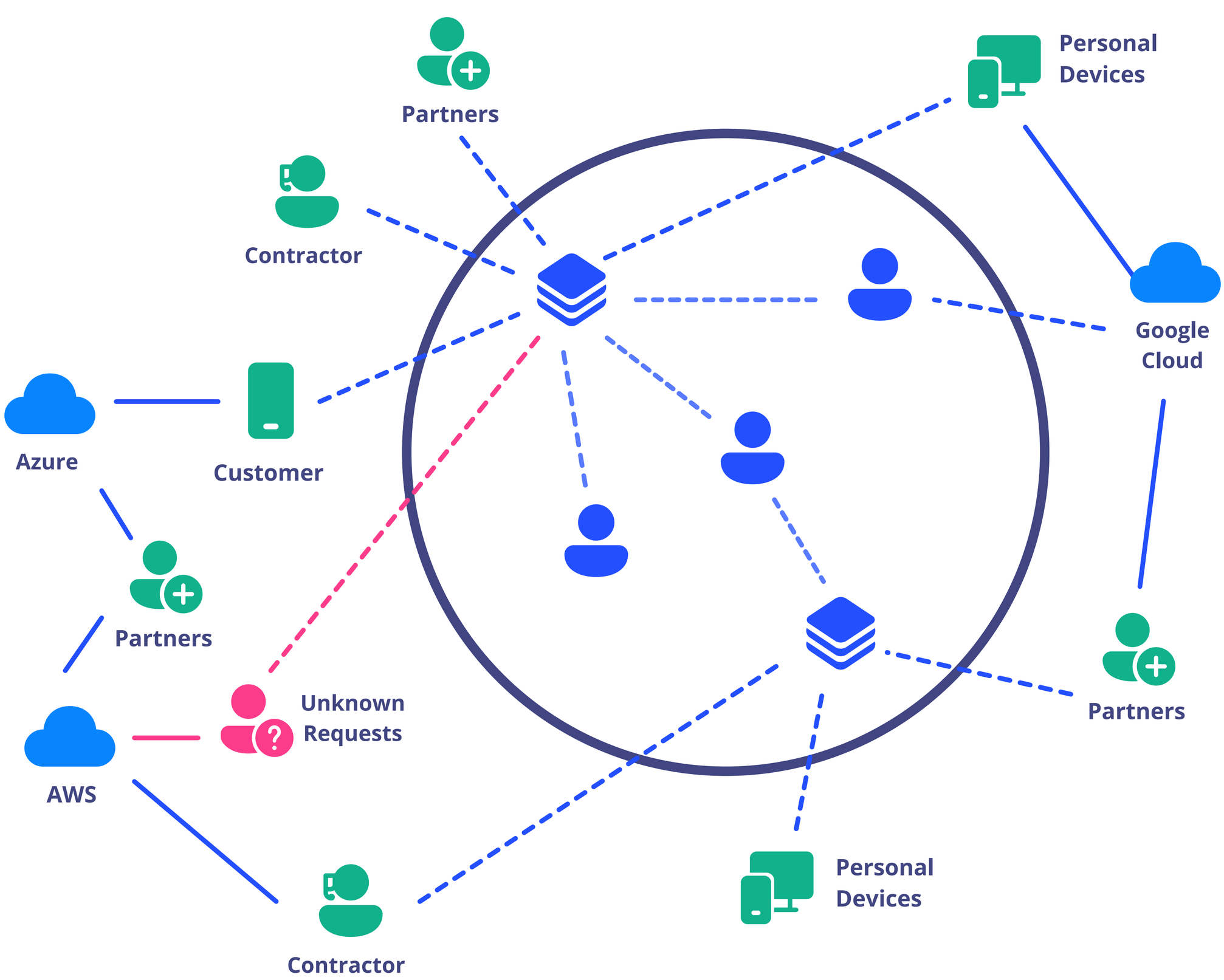
Forrester’s work was taken further by Gartner’ CARTA framework, which called for a continuous adaptive risk and trust assessment process for enterprises to secure access to their resources. The Zero Trust concept was put into practice by Google in its Beyond Corp program, and has today gained ground as a preferred security architecture that companies seek to implement.

Zero Trust Architecture is designed to lay down an aggregation of principles, concepts, and component relationships, that serve the primary purpose of effectively eradicating any uncertainties that may arise while enforcing decisions relating to access to enterprise systems and applications. In retrospect, the zero trust model would require an adaptive deployment model that lays a special emphasis on Continuous Diagnostics and Mitigation. The primary aim of the architecture is making access control as granular as possible, and at the same time, completely eradicating any form of unauthorised access.to enterprise resources. In essence, following a Zero Trust philosophy marks a shift from a focus on networks to a focus on identity and applications. InstaSafe focuses on these core philosophies to design people-centric solutions for secure access.

ZERO TRUST ARCHITECTURE

A Zero Trust security policy essentially means providing secure access of resources to the right people, irrespective of where they are situated, while providing complete visibility and insights into their activities. Implementing and operationalising Zero Trust is not a simple process. Your security infrastructure needs to go through multiple steps of maturity before you start adopting a Zero Trust security posture.

The InstaSafe Zero Trust Maturity Model helps in better understanding the steps involved in transitioning to a Zero Trust security architecture.



Need: Simple & Flexible Secure Access during this Digital Transformation Journey

1. ***Audit Security Posture*** - The first step towards operationalising Zero Trust is to analyse whether your organisation has a relevant and pragmatic Identity, Credentials, and Access Management strategy, which is in synchronisation with the business needs of the organisation. Organisations need to review whether or not all resources are being accessed securely, and at the same time, carry a complete audit to identify and highlight the security vulnerabilities that are created due to the use of multiple security vendors. In order to integrate the functions of these technologies, it is necessary to consolidate their functionalities under a single Identity and Access Management System

2. ***Inventory connected devices*** - Update your asset inventory, to log all managed as well as unmanaged devices that have had access to your critical assets. Design a context based access policy deigned to urge all device users to update their devices in line with current security requirements. Access policies should be designed in a manner as to measure the risk associated with, and the context of each access request. This extends to verification of the user profile and device profile, assessing the context of the request, and the risk associated with granting the request. On the basis of these contextual insights, and the accompanying access policies, access may or may not be granted.

3. ***Classify, Identify, Catalogue*** - To garner a granular view of what occurs in the network, it is of paramount importance that enterprises classify, identify, and catalogue all traffic without distinction based on encryption or hopping. This step serves to stress on the “verify before you trust” tenet that Zero Trust Network Access adheres to.

4. ***Create Zero Trust Architecture and Policy*** - While it is conventional for a network design to have creation of its architecture as the first step of its design, it must be understood that zero trust is not a universal design, but highly customised, depending on the organisation adopting it. Further, given that it is improbable for an organisation to undergo migration to a ZTNA network in a single technology refresh cycle, it is absolutely necessary to perform the aforementioned surveying steps in order to ensure a successful deployment. The entire Zero Trust Policy may be designed using Ohno’s ‘Why?’ method

5. ***Continuous Monitoring and Visibility*** - Perform a deep dive analysis of all incoming and outgoing traffic, to garner new insights for improvement. A Zero Trust model relies on constant monitoring and logging of all network traffic, both North- South and East-West

InstaSafe’s identity centric solutions allow organisations to frame customised access policies to secure and enhance the end user authentication and usage experience. By moving beyond adaptive multifactor authentication and including the option to include AI driven behavioural biometrics as an authentication factor higher up the security stack, IT administrators have the choice of implementing more stringent security controls for critical assets. InstaSafe’s identity driven security approach utilises user and device identity along with access policies to derive and verify the context of each access request, assess the risk associated with granting access for that request, and authenticate the user and device profile before granting access on a need to know basis.

While enterprises today are only beginning to scratch the surface in terms of implementing a Zero Trust approach, InstaSafe continues to create additional features that can empower and operationalise a company’s Zero Trust journey.

THE BENEFITS OF USING A ZERO TRUST MODEL

Zero Trust Solutions provide multiple security and business benefits that organisations can leverage to secure their assets and improve business productivity.

1. Protect Customer Data : InstaSafe’s Zero Trust Security Solutions secure critical assets and infrastructure by employing split-plane architecture. This means that the access control plane, where trust is established and the data plane where actual data is transferred, are separated. This helps in blocking network based attacks, since each of the planes is rendered invisible to external actors.
In addition, a Zero Trust approach serves to secure better protection for your cloud application, by virtue of centralised connectivity and a default deny gateway that verifies the identity and context of each access request.

In essence, this ensures that only authorised users are able to access the data and applications that they are allowed to access. This, in turn, helps in preventing breaches and data exfiltration, among other benefits.

2. Provide an integrated security infrastructure : As has been discussed, one of the major problems while implementing a zero trust model is that a single point of trust for network connections is an uphill task to visualise and implement. Integrating identity management before granting access is a highly resource intensive task.. Providing individual applications the ability to control their security posture is a stretch. In other words, it is simply difficult to integrate access control, identity management, session management, and other security controls as an integrated security architecture. InstaSafe's Zero Trust approach serves to not only integrate user aware applications and client aware devices, but is instrumental in integrating other security controls as well. InstaSafe's solutions integrate across a wide variety of security solutions to provide an umbrella approach to your zero trust journey. Security that empowers digital transformation: With mobile and remote connectivity becoming ubiquitous, and a migration towards the cloud becoming the norm, it is necessary for security technologies to facilitate cloud adoption and digital transformation.

Traditional technologies have never been upto the mark when it comes to securing and facilitating cloud adoption. Since the perimeter based approach to security becomes ineffective in this scenario, legacy based solutions are not viable as an answer to secure cloud adoption. A Zero Trust approach to security, on the other hand, empowers and simplifies the digital transformation journey of organisations by helping them securely adopt cloud architectures while ensuring a significant reduction in the costs and complexities involved in designing security models that support multi cloud deployments. In addition, the use of micro segmentation of networks and multi layered authentication facilitates the secure adoption of Internet of Things and other neoteric digital transformation technologies. By using microperimeterisation to segment workloads, and centralising control for companies, a Zero Trust approach serves to deploy applications at a faster pace, with better security controls

3. Simplified Security and an Enhanced User Experience : The use of convenient multifactor authentication based access and Single Sign On helps in delivering a secure and more enhanced user experience. Add to that the significant reduction in latency as compared to traditional technologies, and we are assured of simple and hassle free usage. InstaSafe's Cloud-based zero trust solutions additionally serve to enhance application performance for the users, allowing them to access only what they need to access, and deliver a seamless user experience across different device types, locations, and network conditions.

4. Complete Visibility into network traffic : A core principle and advantage of Zero Trust Networks is 360° visibility and monitoring of all network traffic for better identification of threat vectors. By enabling continuous monitoring across the network, it becomes easier for system administrators to fulfil compliance requirements and frame customised access policies.

In the light of an increase in remote workforces, and an increasing adoption of digital transformation processes, security becomes critical. Traditional solutions are often found to be inadequate in dealing with security challenges associated with the increase in employees working from home.
In this scenario, Zero Trust solutions are flexible, and provide an enhanced level of security without compromising on the user experience. Many enterprises have recognised the fallacies associated with traditional solutions, and have chosen to shift to a more neoteric model of security, and primarily, Zero Trust Solutions.

INSTASAFE'S VISION FOR A VIABLE ZERO TRUST SOLUTION

A Zero Trust Solution needs to facilitate the migration of workforces to remote locations, and the migration of applications to the cloud. Using a continuous risk and trust assessment process, InstaSafe's zero trust security model involves the following:

1. Least Privilege, Black Cloud Approach : A Zero Trust Solution should follow least privilege access policies, which means that users, irrespective of whether they are present inside or outside the network, should be given authenticated access to only those applications that they are allowed to use.

2. Scalable on Demand, Cloud based implementation : The solution that operationalises a zero trust approach should be cloud based to facilitate perimeter less security on scale.

3. Granular Level Access Control : System administrators need to have complete control over who accesses what and have the ability to frame granular level access policies to enforce a zero trust model

4. Continuous Visibility and Monitoring : As discussed, a core necessity of a zero trust solution is the constant monitoring and logging of all network traffic, to enable identification of threat vectors and framing of granular access policies.

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