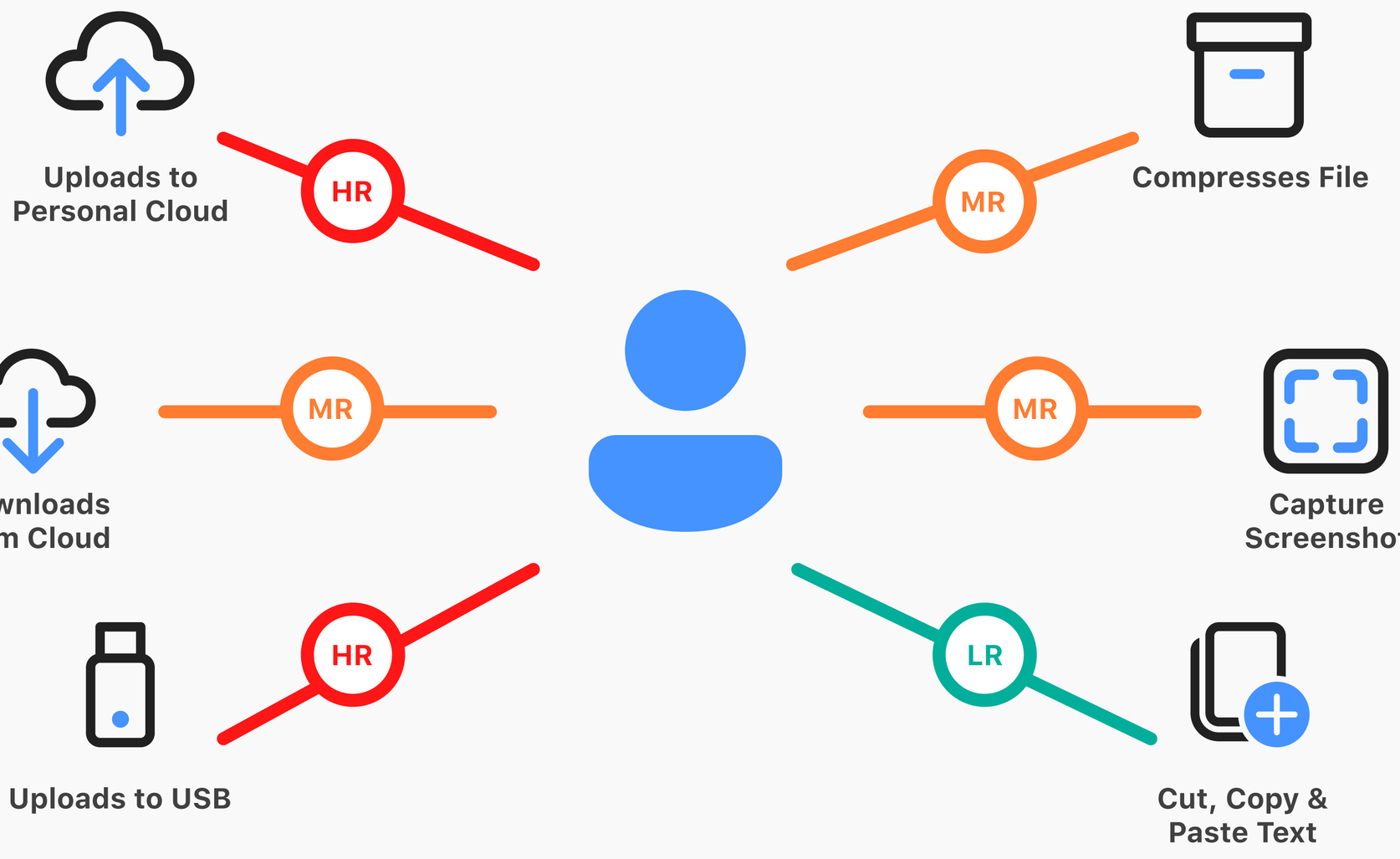
Solution Brief

Enabling productive and secure work from home experience

The greatest asset which an organisation can possess is that of its human capital. It is every organisation's duty to ensure the protection of its employees and resources. In the light of the coronavirus outbreak, we, at InstaSafe, pursue this vision. We commit to helping organisations maintain business continuity, and ensure the health and well-being of their employees on priority.

As we wade through uncertain times, many organisations have been unwittingly pushed into extending their remote access capabilities without ever being prepared for it, and without having the necessary security infrastructure in place. That said, it becomes imperative for organisations to retain their productivity in order to maintain business continuity, while at the same time, ensuring the safety and security of their employees.



CONTINUOUS MONITORING AND RISK ASSESSMENT

ISSUES WITH CURRENT TECHNOLOGIES

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:

INCREASE IN ATTACK SURFACE

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.

INCREASE IN RISK OF LATERAL ATTACKS

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.

COST AND TIME REQUIREMENTS

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.

LACK OF GRANULAR ACCESS

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.

INADEQUATE USER EXPERIENCE

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.

In essence, a key takeaway is that the over reliance of current network access technologies like VPNs on a network-centric model, becomes a serious bottleneck in securing networks, making it imperative for cloud based alternatives to take centerstage.

INSTASAFE SECURE ACCESS FOR A SECURE, SAFE, EASY REMOTE ACCESS USER EXPERIENCE

There has been an exodus of organisations from traditional hardware based applications to cloud based security applications. This is primarily because of the agility, ease of deployment, and greater scalability associated with cloud based security. InstaSafe takes it one step further by providing a level of security that is a notch above traditional solutions. By employing the concepts of Zero Trust Network Access and Software Defined Perimeters, InstaSafe assures organisations of complete secure access, be it to on premise users, or a large remote workforce.

As a cloud agnostic security solution, InstaSafe was built with the aim of empowering organisations in their transformative migration to the cloud. Recognising the lacunae in the traditional perimeter based approach in network security, InstaSafe has come up with its neoteric cyber security offering, InstaSafe Secure Access (ISA), based on the Zero Trust Network Access framework, which shifts access controls from the perimeter to individual devices and users. Our SDP based interface is a hardware free, zero configuration solution that accords granular level access control to the enterprise, and is a highly cost effective, practical, and prudent solution for any organisation looking to strengthen their security architecture. By using ISA, an enterprise can extend secured access to both remote and on-premise users, with an assurance of uncompromising security. Using Secure Access's Software Defined Perimeter architecture, the whole enterprise Network is placed behind a dark cloud. Given that hackers cannot attack what they cannot see, enterprise networks come to be secured against an array of credible threats, including man in the middle attacks, credential thefts, and server exploitation.

DIMENSIONS OF A ZERO TRUST FRAMEWORK

HOW ZERO TRUST WORKS

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.

ZERO TRUST MODELS DRAW UPON THE FOLLOWING GROUND ASSERTIONS

- Distinctions between “inside” and “outside” the network perimeters no longer stand true. Network locality can’t be a lone factor in determining trust.
- Malicious threats exist on the network at all times, and may be internal or external in nature
- Every user, device, network, and data, is to be validated and authenticated before granting access
- 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.

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

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.

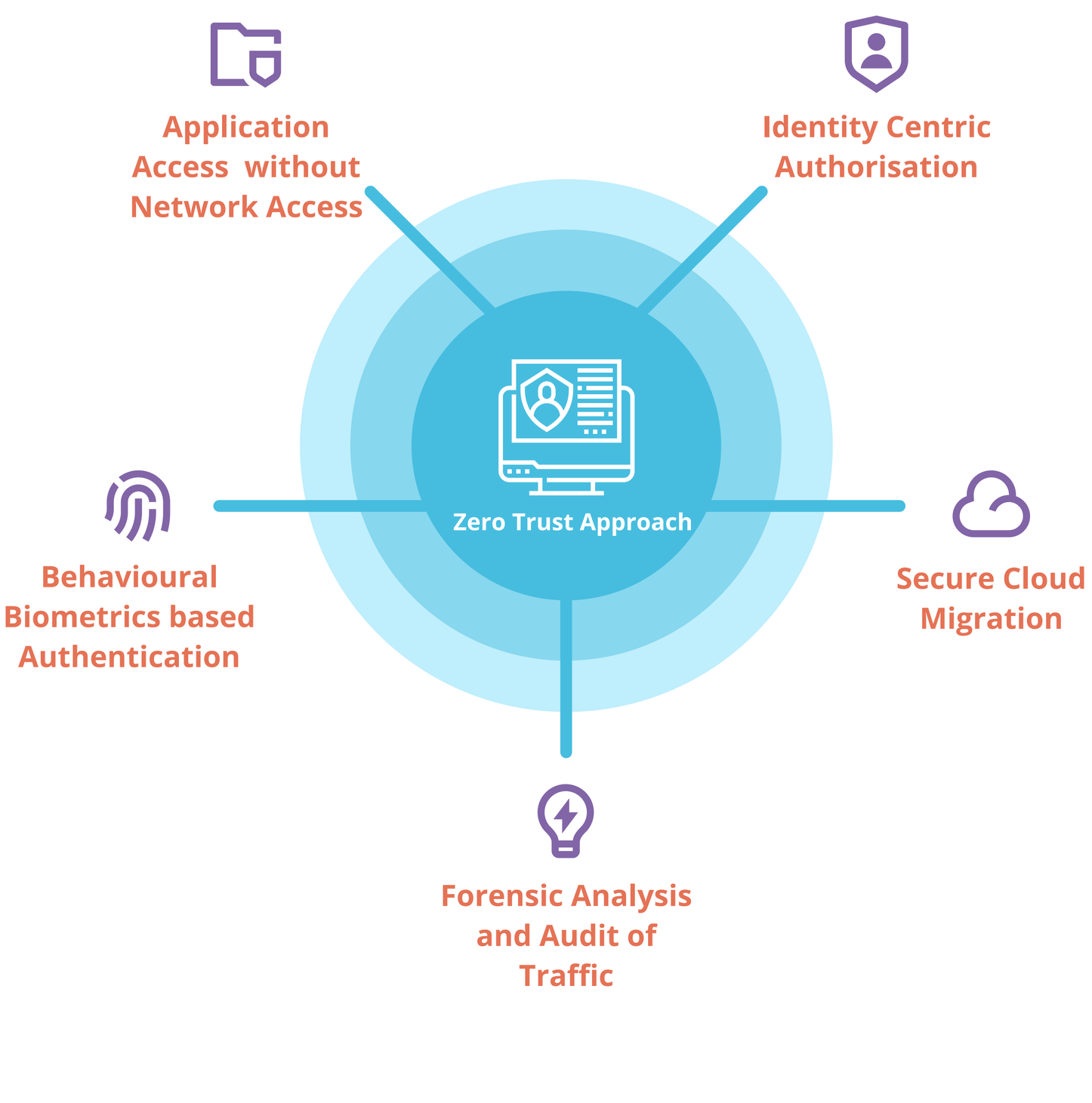
In retrospect, the zero trust model would require an adaptive deployment model that lays a special emphasis on Continuous Diagnostics and Mitigation. The primary aim of the architecture is making access control as granular as possible, and at the same time, completely eradicating any form of unauthorised access.to enterprise resources.

INSTASAFE SECURITY PRECEPTS

Given the inherent issues and challenges that are presented by the application of legacy based systems like VPNs in cloud based environments, it becomes imperative to address these issues. The InstaSafe team garnered market research data and did an insightful analysis of the current lacunae in the cloud security market, to recognise that some important precepts need to be kept in mind while designing security solutions that keep up with the broadening horizons of enterprises that use them. By capitalising on the areas of concern where VPNs or other traditional perimeter forms couldn't keep up, an all encompassing security solution could be drawn up which drew inspiration InstaSafe's major mission of providing seamless cloud security services that are both secure to use and instant in their installation and usage experience.

But before that, our team decided to pinpoint the most important canons that needed to be kept in mind before coming up with such a solution. Our vision for a next gen cloud based remote access solution stood on 3 pillars, which we refer to as the InstaSafe Security Precepts. Our belief is that any solution that is drawn up keeping the broadening realms of enterprises and dissolution of traditional perimeters in mind should belay its foundations on these 3 precepts.

WHAT DOES ZERO TRUST ENCOMPASS?



ISOLATED, SEGMENTED ACCESS EQUALS SECURE ACCESS

By isolating all network resources from the internet, and at the same time, microsegmenting access on a ‘need to know’ basis, security solutions can endeavour to heavily restrict the occurrence, and effect of potential exploitative attacks. Blacking, or rendering invisible the enterprise resources effectively creates a near impenetrable intranet within the internet, preventing malicious actors from accessing your resources

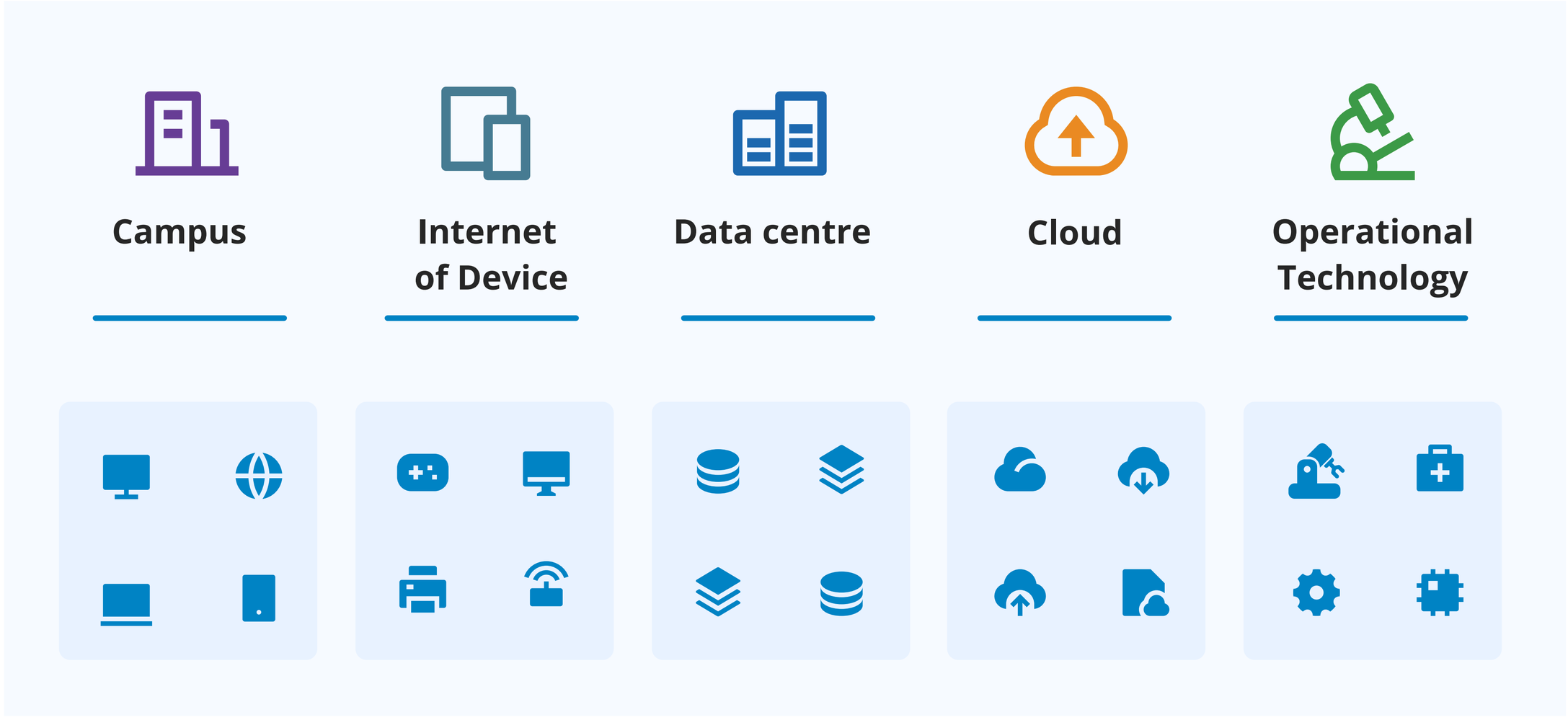
ALWAYS VERIFY BEFORE YOU TRUST

A system of innate distrust must be the norm if an enterprise wishes to achieve a higher level of security. Further, using this ‘default deny’ approach to frame your security policies, with regards to what assets you have to protect and secure, what applications are to be isolated, and how you will segment traffic, tends to further mitigate chances of exploitation. Further, the entire user authentication process should be dynamic, and cyclic, in that the entire process of assessing threats, adapting, and continuous authentication is to be followed for every user.

ONE SIZE DOESN’T FIT ALL

Given that each user in an enterprise is allowed access to different quanta of resources, each of them needs to be assigned a different level of trust. This further reinforces the need for microsegmentation, i.e. the framing of granular level security policies, which may go down to the workload level, or the device level. This will enable micro perimeters, segmenting the user traffic into contextual lanes, and practically realising the 1st precept.

THE STANDARD FOR DEVICE VISIBILITY ACROSS THE EXTENDED ENTERPRISE

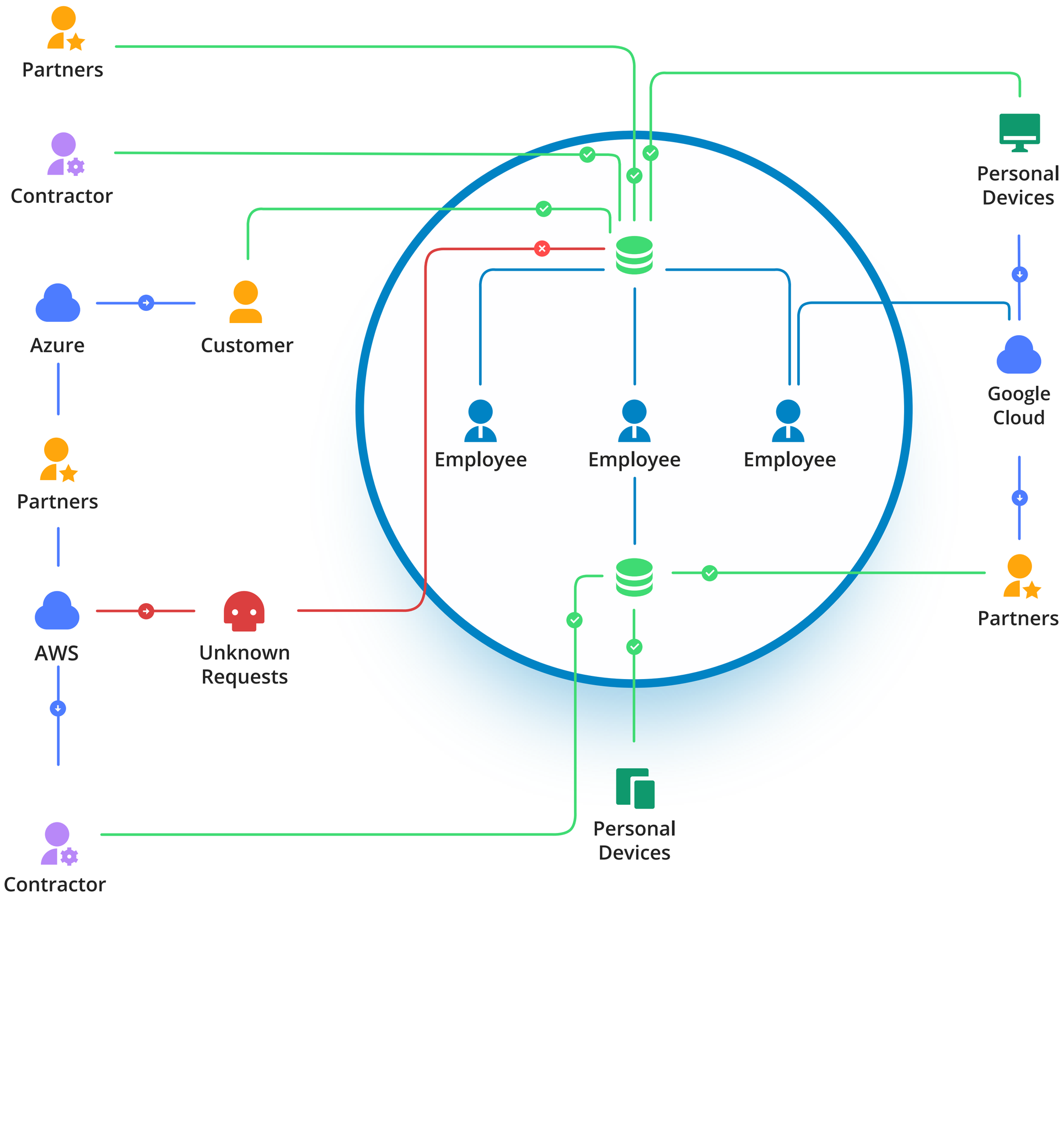


INSTASAFE PROVIDES A DEVICE AND CONTROL PLATFORM FOR THE EXTENDED ENTERPRISE

INSTASAFE SECURE ACCESS: HOW IT WORKS

The prospects associated with Zero Trust Architecture has thrown up a window of opportunity that has been suitably exploited with the introduction of a neoteric offering, Software Defined Perimeters. Contrary to the ineffectiveness, unscalability, and cost heavy nature of traditional network security constructs, Software Defined Perimeters provide a viable, scalable, highly productive alternative that secures your network infrastructure with greater accuracy. With a view of upending cybersecurity infrastructures, SDPs serve to offer flexibility in security policies, in conjunction with granular level access control. As a result, InstaSafe significantly minimises the attack surface on offer, resulting in fewer exposable vulnerabilities in the network.

Operating on an ‘inherent distrust’ model, InstaSafe’s dynamic and context-dependent trust validation system seeks to restrict access to resources based on credential policy thresholds. The SDP architecture further expands upon the “need to know” security model, providing additional layers of security like the Mutual Transport Layer Security. By extending protection beyond traditional perimeters with a hardware free configuration, InstaSafe ensures that both the device and the user are able to access only what they are authorised to access. Further, InstaSafe endeavours to secure all critical resources by separating access control and data planes, thus rendering them invisible to external unauthorised users.InstaSafe® Secure Access (ISA) works by having a client agent on the user’s device that helps to connect the user to the controller, where the user is authenticated and the device is verified; and have an agent running in the data center to connect to the Controller and tunnel all user traffic to the data center applications.



HOW INSTASAFE MAKES REMOTE ACCESS PRODUCTIVE AND SECURE

EASE OF ACCESS

By providing for a cloud based, neoteric approach to secure access, and not compromising on user experience that is oft overlooked as an implication of backhauling traffic in VPNs, InstaSafe's SDP based solutions provide for a seamless user experience and at the same time, are protected by disruptive Identity access management systems and multi factor authentication. This implies that even while working from home, users get to have a productive and seamless experience, even while their access is secured by a myriad of security measures.

EASE OF DEPLOYMENT

InstaSafe Secure Access can be deployed within minutes owing to it being hardware free and zero configuration. Given that for a productive work from home experience, your employees need complete, unhindered access to all business applications, InstaSafe's solutions are scalable on demand, allowing for complete coverage of all users, whether on-premise, or remote.

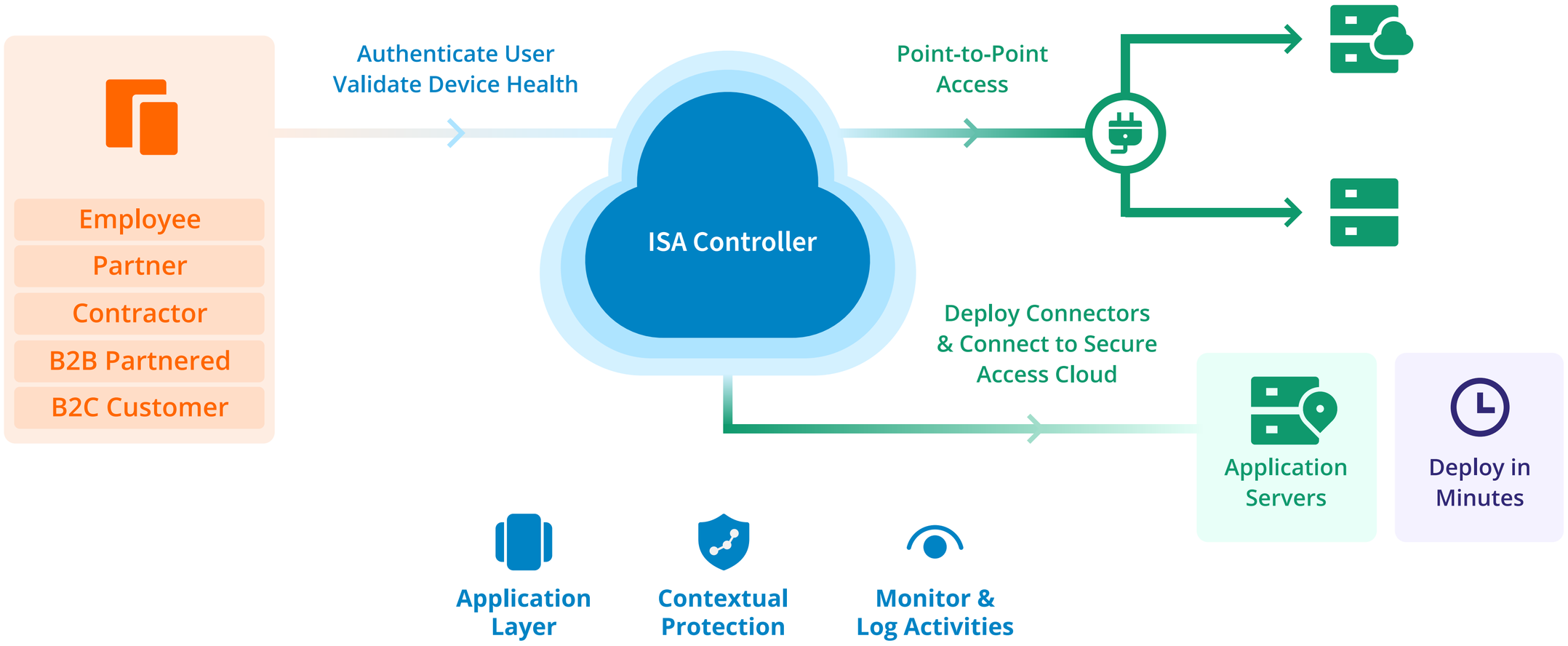
EASE OF OPERATION

With a Single Pane Management Console to control all access permissions, InstaSafe's solutions provide for complete ease of operation and management. In addition. InstaSafe provides for granular level of control based on the need to know model. This allows access only to those applications that an employee is allowed to use, thus providing for the extra layer of security.

EASE OF OPERATION

Given that much of the enterprise data and applications will be on the cloud, organisations need a solution that provides for ease of monitoring, by effectively centralising authentication services, and in turn, providing your infosec teams with greater control over access management. InstaSafe Secure Access helps in providing this granular level of control over all user, and in constant monitoring of user access and user activity. By integration of behavioural biometrics into the powerful InstaSafe Secure Access program, we ensure complete securing of identities, even in the event of credentials theft.

HOW INSTASAFE'S ZERO TRUST APPLICATION ACCESS WORKS



REMOTE ACCESS, THE ZERO TRUST WAY

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?

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.

Learn more about InstaSafe products and offerings that empower your organisation’s business processes through easy and secure extension of remote access capabilities

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

/InstaSafe /instasafe_diaries /InstaSafe /company/instasafe