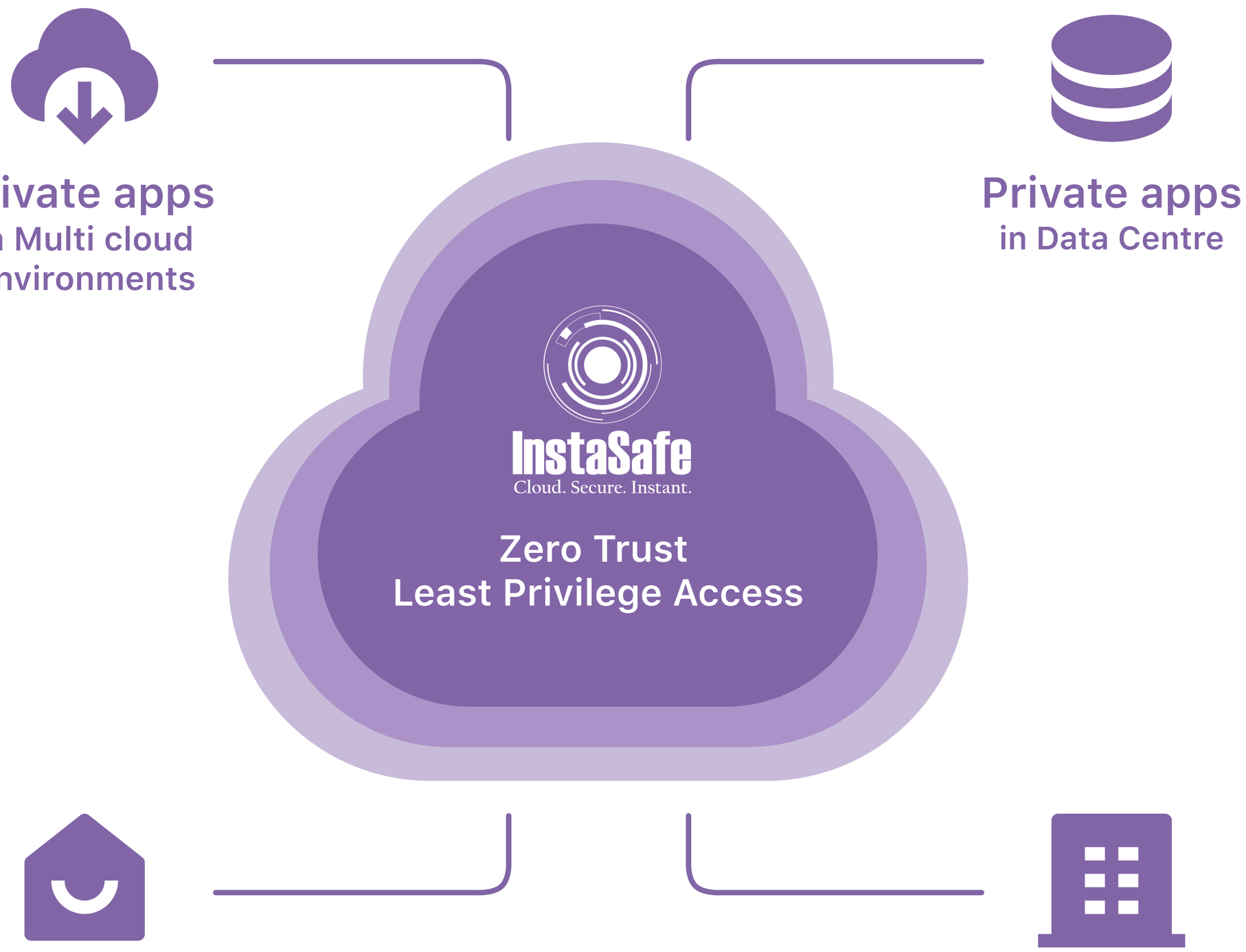
Total Visibility with InstaSafe : The Master Key to Zero Trust

InstaSafe provides the device visibility platform for Zero Trust security

Visibility is the key to gaining a deeper and granular knowledge of the network and all the functions that happen inside and outside the network. Without granular visibility, it will be impossible to understand and fully differentiate normal network patterns from irregular communication patterns. Hence, the more visibility you have, the better you can detect threats and stop them at the right time



NEVER TRUST ALWAYS VERIFY

The concept of Zero Trust begins with the idea that nothing is to be trusted by default, whether internal or external to the network. Every asset is verified to the absolute endpoint of every user, device, service, or application on the network before trusting any network. InstaSafe provides strong security and ensures both ends are doing what they are supposed to be doing.

PERIMETER SECURITY IS NO LONGER SUFFICIENT

According to Gartner, as a result of digital transformation efforts and a rapid and unprecedented adoption of the cloud, most enterprises will have more applications, services, and data outside their enterprises than inside. Technology is evolving day by day, as technology grows and upgrades, there will be a constant barrage of attacks from threat actors and motivations that put data, assets, applications, and services at constant risk.

A single organization may work under internal networks or remotely or mobile individuals and cloud services. The implantation of the traditional method of perimeter-based network security has increased the complexity to such an extent there is no easily identified perimeter or single network for the enterprise. Hence, there are more chances of attacking or threats to the network. Perimeter-based network security is considered to be not sufficient and it is only a matter of time before a bad actor can breach it.

The systemic failings of perimeter-focused security resulted in InstaSafe developing its Zero Trust Solutions, based on the Software Defined Perimeter Model, as an alternative. First used in the corporate world by Google, as part of Beyond Corp, Zero Trust is a conceptual and architectural model which approaches networking and security differently, enabling security teams to:

- Redesign networks into secure micro-perimeters
- Strengthen data security using obfuscation techniques
- Limit application access to need to know basis and enable admin to customise user privileges and access.
- Improve security detection and response with analytics and automation.

INSTASAFE ZERO TRUST: IMPLEMENTING ZERO TRUST ARCHITECTURE

It is important to know how the InstaSafe Zero Trust architecture helps in ensuring better control and visibility over all network traffic, and in effect, helps in better threat detection and response. At InstaSafe, we help businesses by delivering comprehensive and uncompromising protection to mobile and remote workers, enabling them to safely and securely access enterprise apps, email, and web from anywhere on any network. Zero Trust is an iterative process that starts with what you know, and as you tend to go deep through the process you gather information at a granular level which leads to having a clear understanding of the design.

For more understanding, we can divide Zero trust into five basic elements:

1.DEFINE PROTECT SURFACE

This means protecting data and applications that are inside and outside the network and also it includes protecting all service such as connectivity protocols i.e. LDAP, DNS, etc

2.ARCHITECT ZERO TRUST NETWORK

Networks are designed based on the business initiative at InstaSafe zero Trust secure access which provides comprehensive and uncompromising protection to mobile and remote workers enabling them to safely and securely access enterprise apps, email, and web from anywhere on any network.

3.MAP TRANSACTION FLOWS

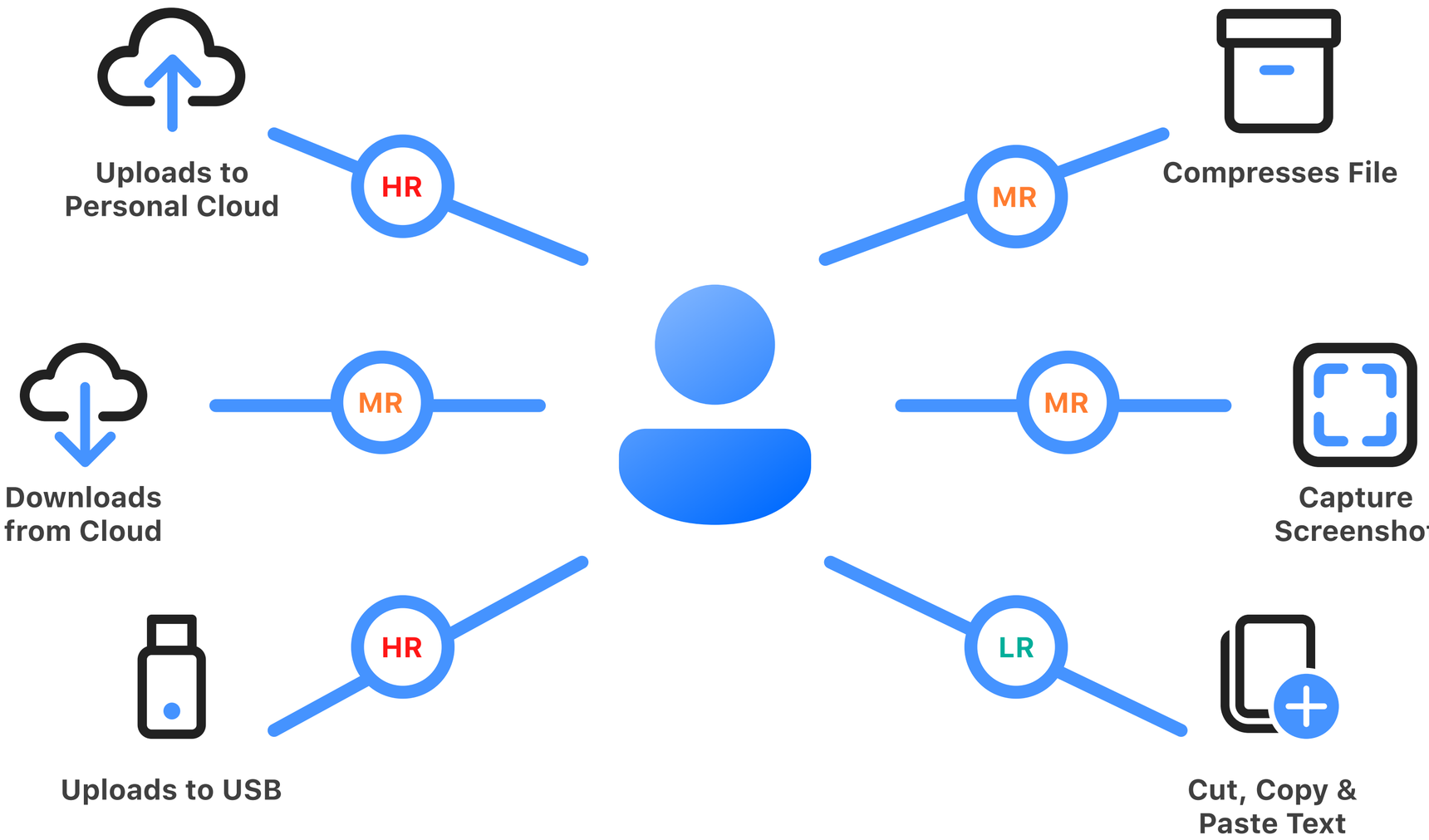
In order to design a network it is always important to understand how the system should work. Without having a proper understanding, it is not possible to design anything. This understanding of the system can be achieved by mapping and scanning the traffic flows inside the network to protect the surface of the network. Once the system is understood this map will explain where to insert controls in order to protect data, applications, services, and networks. Zero Trust has an iterative workflow, which starts with what you know, and as we move forward we start understanding data and traffic flow at a granular level.

4.CREATE A ZERO TRUST POLICY

Once the architecture is completed it is very important to create supporting policies to the created architecture around it because, for one resource to communicate with another resource, a specific rule must explicitly allow that traffic. Hence creating policy enables granular enforcement, so that only known allowed traffic or legitimate application communication is allowed in the network. This process significantly reduces the attack surface.

5.MONITOR AND MAINTAIN NETWORK

The final step refers to monitoring the network and maintaining it and more importantly it refers to how to improve the Zero Trust network over time. The more your network is improved, the stronger it will become, with greater insight into making policies more secure. Hence it is important to do a continual improvement approach.



TOTAL VISIBILITY : THE MASTER KEY TO ZERO TRUST

InstaSafe provides the device visibility platform for Zero Trust security

WHAT THE TERM “VISIBILITY” DOES AT INSTASAFE ZERO TRUST

The First step of InstaSafe Zero Trust is to have completely discovered and understood the devices that are connected to the network. Once all the devices that are connected to the network are discovered at the granular level it is classified in order to have a clear picture of what it actually does to the network.

InstaSafe gives more importance to the term visibility- that means the more visibility you have the better you can detect threats and stop them at the right time. It is always impossible to protect the invisible or without having a proper understanding of either devices or network, it is impossible to save it from happening attacks or security breaches.

The main responsibility of the security company is to protect networks and devices that are related and surrounded by it. In order to achieve this InstaSafe uses a strategy called ‘visibility’ which enables us to have a deeper and granular knowledge on the network and all the function that happens inside and outside the network.

InstaSafe Zero Trust provides Secure access which provides comprehensive and uncompromising protection to mobile and remote workers enabling them to safely and securely access enterprise apps, email, and web from anywhere on any network. It quickly determines and has clarity about the user, owner, and operating system, as well as device configuration, software, services, and the presence of security agents. After gaining visibility, InstaSafe provides remediation, control, and continuous monitoring of these devices.

INSTASAFE ZERO TRUST NETWORK CAPABILITIES

InstaSafe's dynamic microsegmentation continuously monitors suspicious behaviour inside and outside the network, such as irregular traffic patterns and suspicious URLs. In microsegmentation you should always do what you are supposed to be doing.

Micro-segmentation takes the traditional zone-based VLAN design and further segments within the VLAN, enhancing security. Microsegmentation set very specific and granular policies in order to protect your application environment. Micro-segmentation gives administrators the control to set granular policies. The policies will restrict communication to hosts that are only allowed to communicate.

This offers a one-to-one mapping. If a bad actor gains access to one segment in the zone, they are prevented from compromising any of the networks within that zone. They simply can't see them. It is impossible to attack what you cannot see.

Microsegmentation only allows communication that is completely necessary This reduces the attack surface and protects networks and systems very carefully by providing security.

FOR INSTASAFE ZERO TRUST SUCCESS, START WITH TOTAL DEVICE VISIBILITY

InstaSafe offers many ways to gain greater insight into the InstaSafe platform, including:

TAKE A TEST DRIVE

Experience the before-and-after difference of the InstaSafe platform with a hands-on test drive.

REQUEST A DEMO

Visit the InstaSafe demo page to request a personal demo and access a full complement of on-demand demos and video options.

CONTACT INSTASAFE CONSULTING SERVICES

Are you in the process of architecting your environment to the Zero Trust model? InstaSafe consultants are thoroughly trained, experienced, and certified in product implementation, process development, and systems integration, as well as network access and endpoint compliance best practices.

THE STANDARD FOR **DEVICE VISIBILITY** ACROSS THE EXTENDED ENTERPRISE

Campus

Internet of Device

Data centre

Cloud

Operational Technology

INSTASAFE PROVIDES A DEVICE AND CONTROL PLATFORM FOR THE EXTENDED ENTERPRISE

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