celestix

# InstaSafe Product Overview

Zero Trust Application Access

## Overview

Organizations are rapidly evolving and embracing digital transformation on the go. With more and more enterprise applications moving to the cloud, and remote access and distributed workforces rapidly becoming the new normal, information security teams need to think beyond protection of traditional perimeters and move to a more evolved approach while securing critical assets.

While a migration to the cloud and rapid digital adoption have caused business processes to be simplified and more productive, they have simultaneously led to the erosion of the traditional 'castle and moat' approach to network security. The conventional approach of placing your assets behind a firewall and focusing on keeping intruders out has become obsolete with the advent of mobile workforces, and omnipresent Internet services. This has led to the development of an approach popularly known as 'deperimeterization'.

Deperimeterization downplays the role of hardened perimeters in the age of the cloud and advocates the development of open and secure standards which act as enablers in the boundaryless flow of information.

## The Challenge of Implementation of Integrated Controls

One of the primary challenges that Security teams face while implementing security controls is ensuring Visibility and transparency of network traffic across the entire network. Today integration of controls is performed by SIEMs, which are used to collect data for audit, logging, and forensic analysis.

Determining a single point of trust for network connections is a Herculean task. In additions, individual applications cannot be given the ability to control their security posture; it would result in an impossibly intricate security architecture. All in all, it is not an easy task to integrate access control, IAM, session management etc. as an integrated whole.

## The Challenge of Disolving Perimeters

The approach of a fixed network perimeter, with trusted internal network assets secured by network appliances such as firewalls, has been long made obsolete by virtualized networks, and the increasing inadequacy of traditional solutions, which are not secure-by-design. The existing network protocols have several vulnerabilities which may be exploited to obtain critical information. The very notion of a traditional security perimeter is brought into question with the unprecedented increase in remote workforces, and an increasing adoption of BYOD models, IoT technologies, and other transformation processes.

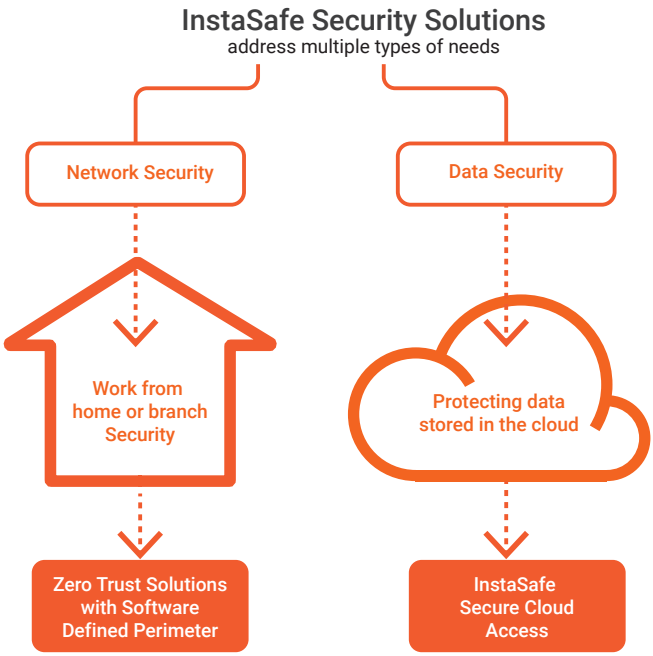
In a traditional approach, a Demilitarized Zone acted as a sub-network, which contained the organization's exposed, outward facing services. That said, the migration of enterprise applications to the cloud renders the conception of a traditional perimeter obsolete

The above transitions in the way organizations work has forced IT teams to consider alternatives which will not only accommodate, but drive digital transformation. While virtual DMZs are an option to be considered, they are often found to be extremely resource consuming, while adding to the complexity of a security architecture that is often already bursting at the seams. In this scenario, there is a dire need for a solution which not only seamlessly becomes a part of existing security infrastructures, but also tends to the needs of cloud security and remote workforce security.

# InstaSafe ZTAA: Reimagining Secure Access, the Zero Trust Way

InstaSafe ZTAA (Zero Trust Application Access) is a cloud security solution that utilizes Software Defined Perimeters to ensure zero trust access to critical organizational resources. InstaSafe's 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 organization looking to strengthen their security architecture. By using ZTAA, an enterprise can extend secured access to both remote and on-premise users, with an assurance of uncompromising security. Using the 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.

Through an application centric approach, access to critical IT assets no longer needs access to the network. This enables the applications to be accessible to the users through inside out connectivity. Our vision for a next gen cloud based remote access solution stand 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:




## ISOLATED, SEGMENTED ACCESS EQUALS SECURE ACCESS:

By isolating all network resources from the Internet, and at the same time, micro-segmenting access on a 'need to know' basis, security solutions can endeavor 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 quantum of resources, each of them needs to be assigned a different level of trust. This further reinforces the need for micro-segmentation, 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 realizing the 1st precept.

# Implementing A Zero Trust Strategy

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.

## 1. AUTHENTICATION BEFORE ACCESS

Using VPNs and Firewalls to establish Zero Trust allows the user to connect to services (eg. a mail server). Firewalls can be set up to ban IPs and services can be set up to figure out which IP addresses are good or bad. VPNs can be set up to only let the users on the network who have the authorized VPN client and the appropriate keys suggesting a Zero Trust has been implemented. However, unauthorized users who clone the VPN client and steal the keys can also access the mail server and then guess other user names and passwords and perform malicious acts such as DDoS, credential theft etc.

The VPN allows you to log into the network and not allow you to use other services (eg. SharePoint) that are not on the mail server network segment. But, because unauthorized users are already in the network, they can get to the SharePoint server by using hacking techniques. Allowing users access to the network and then access to services and then letting the service determine whether the user can access the service, is an issue. Access before authentication allows users (good and bad) to have access to all the services - not login, but access.

In order to ensure authentication before access, there is an implied requirement: a control plane for authentication that is separate from the data plane. To ensure acceptable response times, a mechanism for immediate authentication is also required.

## 2. CAPABILITY TO LIMIT NETWORK CONNECTIVITY AND EXPOSURE

Public/private clouds do configure perimeter network security. They provide a layered approach to security, stream logs to monitoring tools providing insight and configure hybrid service control policies. However, this does not address authentication prior to access.

Strong supporting measures for cloud native platform and application services include inbound/outbound security configuration and corporate network policy configuration. The industry standard practice for authentication and authorization is mTLS certificates. The best approach, however, is to drop or forward packets at the network layer with traffic management provided by an SDN controller interfacing to an SDP Zero Trust Deployment. With this architecture, the SDN infrastructure can drop network connections if authentication fails.

## 3. GRANULAR TRUST AUTHENTICATION MECHANISM

Network Layer VPNs and firewalls and application layer firewalls and SSL VPNs do not have explicit fine-grained access control. A Zero Trust deployment implicitly requires not only policy-based authorization but also identity authentication in the context of network micro segmentation, and distributed service connectivity and interconnectivity across hybrid private/public multi cloud scenarios.

Let's examine firewalls specifically. Firewalls are static so user groups are used to provide granular trust. It's not unusual to have a group of users, from a variety of departments with different roles needing access to the same service with the same IP address. Firewalls rules are static and rely only on network information. Firewalls don't dynamically change based on levels of trust required for a given device. Consider these situations. A frequent situation has a user moving to a "more risky" location like an Internet café. Unbeknownst to the user the local firewall or anti-virus software has been turned of by malware or by accident. A traditional firewall will not detect this.

A case can be made for IPSec VPNs, which do not access identity attributes for authentication prior to allowing access. Instead IPSec VPNs are reliant on tokens and credentials that may have been intercepted. Add to this the likelihood that SSL VPNs have vulnerabilities.

In light of these limitations, Zero Trust deployments must address the granular trust authentication mechanisms and policy-based authorization using integrative approaches.

## 4. MONITORING SUSPICIOUS ACTIVITY

Consider what happens when authentication of identity attributes fail. The capability to forward suspicious activity based on packet inspection to endpoint logging and monitoring services provides really useful inputs to the security orchestration, automation and response (SOAR) as technologies that enable organizations to take inputs from a variety of sources (mostly from security information and event management (SIEM) systems, see SDP Architecture Guide for details). Automation refers to the workflow processes that are initiated to gather data into an Artificial Intelligence (AI) model, to be integrated and orchestrated, providing operational intelligence and visualization graphs and dashboards. Zero Trust implementations can forward useful intelligence for input to SOAR AI models and the proper monitoring of suspicious activity.

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