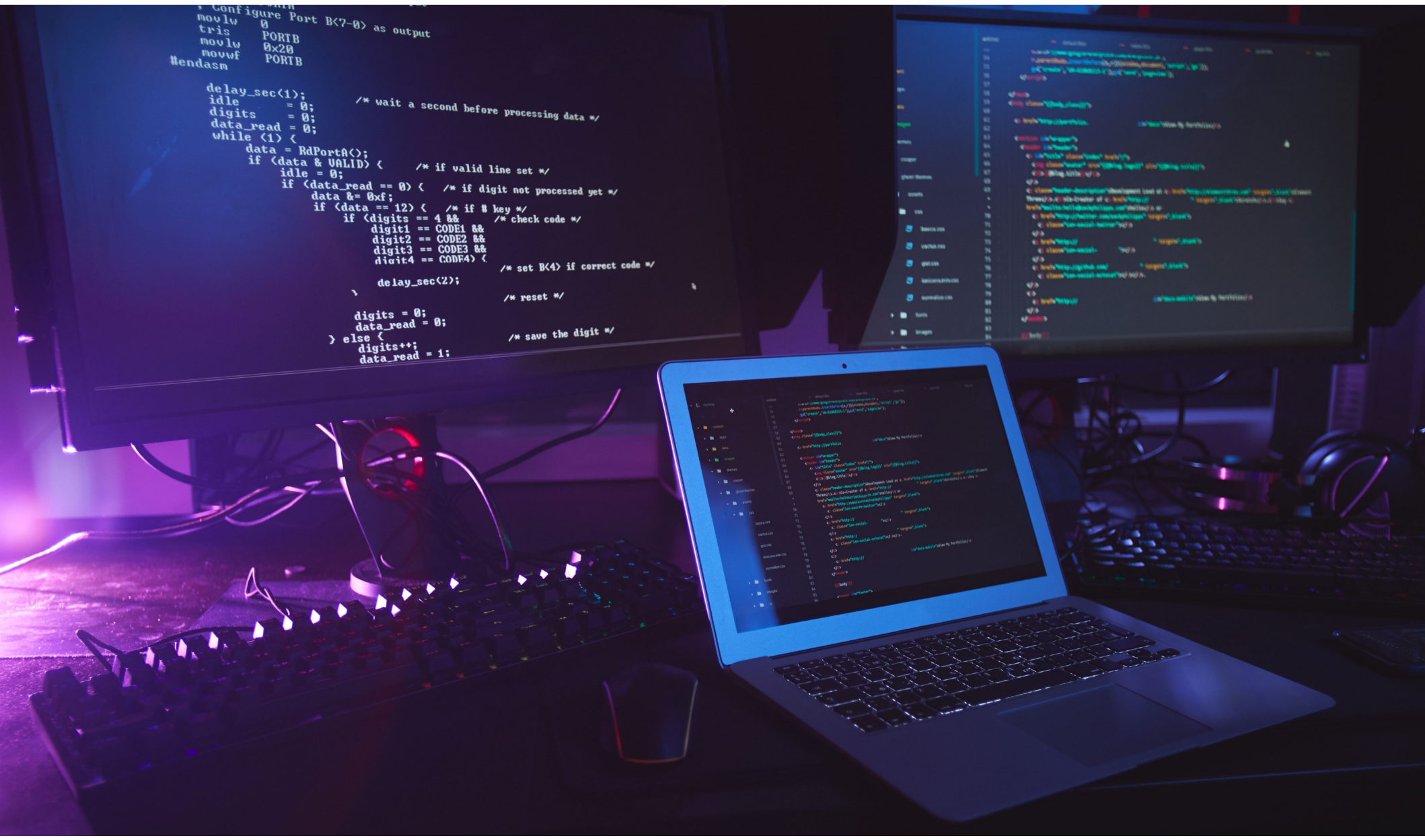
InstaSafe
Cloud. Secure. Instant.

WHITE PAPER



Secure Access to Your SAP Applications with InstaSafe

Zero Trust Network Access 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.

What Is Zero Trust?

Zero trust is a strategy that helps stop successful information breaches by removing the idea of trust from the network architecture of an organization. Founded in the concept of Never Trust, Always Verify, Zero Trust was created to secure modern digital environments by limiting and negating lateral movement, according granular control over access, offering Layer 7 threat prevention, and monitoring all network activity actively.

As a concept, Zero Trust is founded on the insight that legacy based security frameworks tend to assume that everything within the organization's network is trusted by default. Under this ineffective trust model, it is believed that a user acts in good faith and should be trusted, and that the identity of the user is not compromised. When legacy based security users are present on the network, they 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.

Zero Trust takes this vulnerability into account while designing security systems, and introduces a system of innate distrust. Zero Trust Access 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, Zero Trust 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.

Zero trust is not a matter of making a system trustworthy, but rather of eliminating trust.

Benefits of InstaSafe Zero Trust for securing your SAP Applications

As is the case with a majority of distributed organisations belonging to retail, healthcare, logistics, manufacturing, and multiple other verticals, they leverage SAP ERP applications to manage and streamline their business functions. As such, there is a large scope for some or most of the endpoints remaining exposed to the open internet, or the servers in which ERP applications are hosted may be left unprotected.

A Zero Trust setup secures the network from both outside and inside, by leveraging the concept of least privilege access. This means that any user, once authorised, is granted access only to those applications that are needed by them to complete authorized tasks. The rest of the network is completely invisible and inaccessible to them.

At the same time, by leveraging a system of continuous authentication and authorisation every time the user requests to use an asset, zero trust models ensure that no threat actors have access to data that is valuable, even if they are present in the network.

Some of the important benefits that an enterprise can derive by operationalizing Zero Trust Access to SAP Applications include:

Secure, Containerised SAP Connectivity

In the modern network setup, identity and applications may be considered the crown jewels, most sought after by criminals. By amalgamating least privilege access for every user irrespective of their location, with a system of continuous authentication, authorisation, and monitoring, InstaSafe's zero trust model makes sure that malicious actors are unable to access any critical data or tamper with the so called crown jewels.

Containerised Access to SAP ERP Applications ensures that even when a single endpoint is compromised, it won't expose the entire network or the entire scope of data to the malicious actor. Zero Trust, in essence, believes in providing application access without providing network access, which is achieved by drawing application specific tunnels between the authorised user and the applications they are allowed to access only.

Better, More Productive SAP Performance

One of the key tenets on which Zero Trust models work is the scope for high flexibility. Since a Zero trust model does not demand an additional network layer, like legacy based solutions. Rather, it may be put into effect on an existing network. The light nature of Zero Trust models ensure that performance is always maximized, without compromising on security.

Supports SAP Agility and Scalability

The provision of granular access controls from a single Admin Dashboard, which allows security teams to add users, remove users, modify permissions, and restrict access with ease, enables high scalability with low effort, allowing organisations to scale their security as they grow. Modern Zero Trust Solutions like InstaSafe provide the option for users to have an agent based or agentless model, as per their scaling needs. This means that in some cases, end-users wouldn't need to install software on their computer or other devices.

Thus, any user can be given controlled access to systems and resources regardless of where they are located.

Secure Remote Workforces When Using SAP

By securing workforces and extending remote access to ERP Applications irrespective of the location of the workforce, InstaSafe ensures a productive experience for remote workforces. Transparent and smooth connection to SAP Apps for remote employees and third-party users minimizes time, reduces frustration and overheads and increases productive work.

Key Steps to Implementing Zero Trust in an SAP Environment

Audit Your Protect Surface and your Attack Surface

The first step towards operationalizing Zero Trust is to identify the scope of your network and elucidate your exposed attack surface and protect surface. 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.

- Locate where the protect surface is
- Isolate and classify applications, data, services and assets
- Increase contextual and visibility awareness—this includes awareness of the application and identification of users

Inventory connected devices and Classify, Identify and Catalogue

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.

- Utilize automated tools to map data over all forms of traffic
- Identifying how applications, data, networks, and systems interact
- Categorizing all traffic and recording the findings

Develop a Zero Trust Network

Define Your Trust Policy and Develop a Zero Trust Architecture with InstaSafe

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.

- Establish a policy to outline a micro-perimeter by linking the protect surface to a segmentation gateway
- Ensure your zero trust strategy is consistent and unified by implementing a centralized management system
- Apply scalable security solutions to reduce bottlenecks
- Automate and develop application rules according to best practices
- Incorporate a multi-layered security approach to scan for threats and mitigate them
- Ensure the policy addresses details such as:
    - Who can access what
    - When is access granted or restricted
    - Where the user is located
    - How the resource is accessed
    - Why the user requires access

InstaSafe helps in being the vital cog in the Zero trust Architecture, by helping define granular level access policies, making it easy for security teams to identify traffic flows and detect threat vectors, and using segmentation to create individualised micro perimeters that rely on identity as the control point.

Simplify Zero Trust Access for your SAP Applications with InstaSafe

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.

InstaSafe's security controls help in contributing to this framework and help organizations develop their zero trust approach.

InstaSafe Zero Trust Access is a redundant, cloud based SaaS application created to extend secure access of SAP applications, web apps, on premise applications and public cloud infrastructure users to users anywhere across the world. It allows you to extend zero trust to the cloud and SAP applications

Context-Based Access Control

The zero trust method demands strict verification of all devices and individuals that try to access the resources of an organization. InstaSafe's contextual access control function lets users broaden their authentication process and develop access approaches according to user contexts, including citizenship, geo-location, employment type, department and the like.

Rather than providing users with access to applications according to, for example, password and ID, the access decision may rely on the particular characteristics of a user (e.g. geolocation).

Least Privilege, Zero Trust Access

Leveraging the Software Defined Perimeter, users are able to access only a limited number of resources based on permissions set by security teams. Containerised Access limits attack surface and negates the scope for lateral movement as well

Centralised Management and Visibility

Granular access control over and within each resource, based on the dynamic and contextual assessment of user attributes and device state. A rich set of rules can be enforced across all users, servers and enterprise data stores, including user commands and database queries. In addition, the security teams get insights and ensure continuous, on the go monitoring over all user traffic and all access requests from a single pane management console.

About InstaSafe

InstaSafe - Trusted cybersecurity provider that offers innovative security solutions and technology backed by crowdsourced vulnerability discovery to protect and keep organizations and businesses safe.

InstaSafe's mission is to secure enterprises from the misuse 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.

Let’s talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

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