ITES Case Study

Delivering Remote Access for IT/ITES sector with InstaSafe Zero Trust Solutions

The customer in question is one of the largest Business Process Outsourcing and IT Management firms in the world. With a client base covering more than 400 multinational firms worldwide, the firm has more than 40000 employees working across multiple geographies. They deliver a wide array of Business Process Management solutions across the verticals of accounting, human resources, customer interaction, and multiple such areas.

THE CHALLENGE: MAINTAINING SECURE ACCESS IN AN INCREASINGLY REMOTE WORLD

With an increase in remote workforces due to Covid-19, the customer wanted to evaluate secure access solutions to various applications hosted in multiple Data Centers across the Globe. They were primarily looking out for a Cloud based Zero Trust Access solution for their private Applications and softphones hosted across their India, South Africa, Philippines, Ireland, and US locations, to access their applications remotely and securely. Given the requirement of Business Process Outsourcing firms to extend continuous access of their soft telephony services to their remote workforces, it was critical that our customer was able to provide uninterrupted secure access to their workforce.

The firm also needed to be prepared for unprecedented situations wherein they might have to operate with employees working from home, and might have to extend the calls from their OSP sites to their agents' soft phones at home, using viable cloud security solutions. In other words, while converting the calls to VoIP and connecting to agents' phones within their local network, the extension process required a secure connection, which could be achieved by a viable cloud security solution.

In essence, the agents, while working from locations across both hemispheres, needed secure access to all their applications and to the VOIP's, be it on premise at their OSP sites, or remotely. The secure access solution needed to seamlessly integrate with existing network infrastructure to ensure an unhindered customer experience and efficient functionality. Accessing applications through an unmanaged device introduces an element of risk, which is why many organizations often require device enrolment to deploy a traditional VPN solution. Information Security teams often have no means to monitor the health of a personal device, which may be infected with keylogger or similar malware.

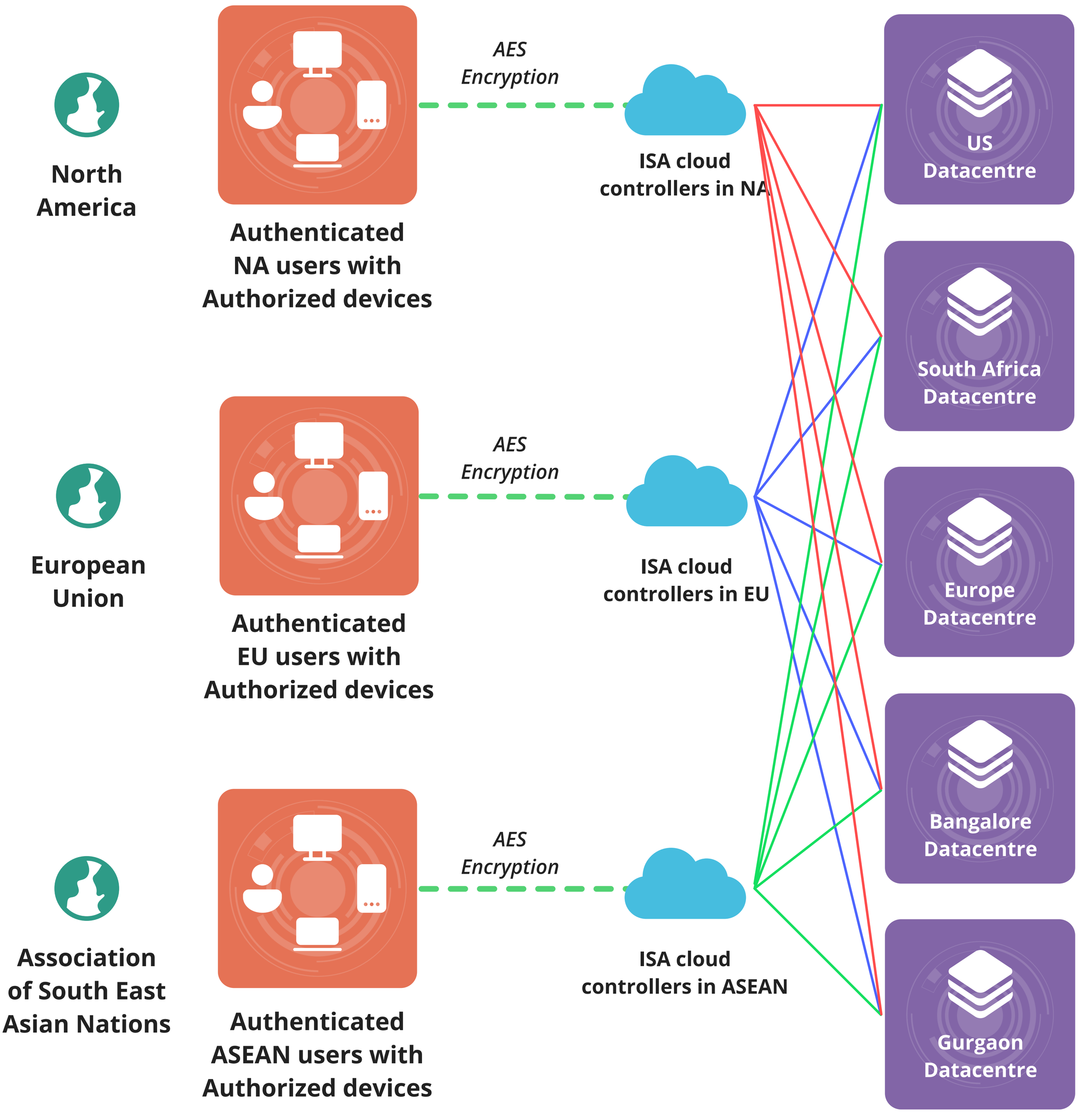
In this scenario, InstaSafe reached out to the prospect to pitch how its solutions would be a perfect fit for secure Business Process Management operations and remote access, and started the process of a longstanding partnership.

> **Our existing security systems were extravagant in terms of expenditure, and we were faced with handling hardware-based solutions with complex interfaces that were tough for our remote workforce to comprehend. In addition, it was tough to manage an array of agents accessing applications across different continents with multiple dashboards, said the CISO of the organization.**

USING INSTASAFE ZERO TRUST ACCESS FOR BETTER, SECURE, REMOTE ACCESS

To enable its diversified workforce to conduct business and ensure full productivity in a cloud-first world, and secure all data that is accessed remotely, the company chose InstaSafe Zero Trust Access to secure traffic from remote locations through Zero Trust Security, and for data loss prevention by using the cloud.

The Information Security team at the firm sought to refer to trusted vendors of the neoteric Zero Trust Network Access architecture by referring reports by market research authorities like Gartner. The security and business benefits derived from adopting InstaSafe Zero Trust Access were manifold, as elucidated in the following representation:



EASE OF OPERATIONS

The entire deployment process for 500 users was completed within one week. A later extension to more than 30000 users during the coronavirus outbreak took the same amount of time.“InstaSafe had all the necessary capabilities that we required from a security solution. Given that we wanted to ensure that our entire workforce had to have access to critical assets, we had to also ensure that all privileged access was segmented, and each resource had access to applications that they were allowed to see, to prevent lateral movement .The CISO of the firm commented.

GRANULAR LEVEL ACCESS CONTROL

Granting contextual access to applications, a feature that InstaSafe provided, enabled the firm to implement a ‘need to know’ model. Through a single pane management console, the InfoSec team had an unprecedented level of ease in managing all remote users, and monitoring threat visibility across the networking.

GREATER SECURITY

By isolating all network resources from the internet, and at the same time, micro segmenting access on a ‘need to know’ basis, InstaSafe restricted the occurrence, and effect of potential exploitative attacks. Blacking, or rendering invisible the enterprise resources effectively created a near impenetrable intranet within the internet, preventing malicious actors from accessing or attacking the customer’s resources. This allowed easy extension of calls from OSP sites to remote employees as well.

ZERO TRUST ACCESS, FROM ANY LOCATION

Using InstaSafe’s inbuilt multifactor authentication helped only pre-authorized and registered devices to have access, effectively geobinding the device to the user. The multiple Gateways helped to authenticate with the local Active Directory servers. Users could now access any private applications hosted on the on-premise and cloud data centers [RDS, Citrix Outlook Web Access, Exchange Client, Shared Drive, VOIP, and respective third-party custom-built applications]to deliver IT support from any location on any device.

COMPLIANCE REQUIREMENTS

As per the mandatory compliance requirements set forth by the Department of Telecommunications (DoT)for BPOs and KPOs, all the Logs are streamed and archived to SIEM hosted in data centers for future audits. Application logs furnished by the InstaSafe Zero Trust tool also have the capability of providing endpoints with Static IP addresses for VPN connectivity, as per DoT compliance requirements. The internal HR team can use this report to monitor the employee login and logout mechanism as a productivity tool as well.

RELYING ON THE ZERO TRUST WAY DURING THE COVID-19 OUTBREAK

“We were the one of the very early adopters of Zero Trust Secure Access for about 500 critical users in 2016. We had been planning an expansion to a larger number of users in 2021, through a gradual digital transformation process” says the CISO. “However, the outbreak of the COVID-19 pandemics had us accelerating our processes, and transitioning our security setup dramatically, and we had to suddenly find ourselves having to extend secure remote access to more than 30000 users within a very short period of time.”

The company decided to reach out to their existing hardware vendors alongside InstaSafe and evaluate their options available in the respective regions. However, with lead times of up to 6- 8 weeks in certain regions for VPN hardware to be shipped, the strain on the global supply chain, and given that support organizations weren’t allowing staff to travel to help with deployment in data centers, the option to expand their existing remote access platform would certainly, have been an economic and social risk for the company, its clients, and its employees.

InstaSafe set up a special COVID deployment technical task force for immediate deployment of its solutions to the entire workforce. A Safehats Team, for vulnerability assessment of security setups, along with an InstaSafe team of engineers, was at the disposal of the company, working together on daily calls for a week through dedicated social forum groups.

On these calls every day, the InstaSafe team walked them through all the configurations for applications, access, Static IP's, Global Console configuration, Multifactor, QR code integration, ACL rules, DNS Configurations, and Multiple Gateway rollouts across multiple AWS regions until they got to a stable position. Usage of Zero Trust Access required with minimum bandwidth and a seamless user experience, a necessity, since users use home internet connection broadband & sometimes even hotspots to connect to the corporate network. "Despite the time and demand constraints, InstaSafe has been instrumental in deploying its solutions instantly, and helping us maintain business continuity."

RELYING ON DISRUPTIVE INNOVATION

The information security team was forward looking in moving beyond traditional solutions like VPNs to secure remote access for the organization in question. "Relying on cloud based Zero Trust solutions not only helped us secure a granular level monitoring of our entire security architecture, but also helped in having access to a solution that was both flexible and scalable on demand" said a solutions architect at the firm.

CUSTOMER FIRST

Aside from the instant deployment and higher security provided by InstaSafe, what set it apart was the continuous customer support provided by the team. As one of the top advocates of our offerings in the company puts it, "The team is dedicated in fixing any issues we face. Not only that, they go to great lengths to ensure that you are utilizing their offerings to their fullest potential. They look at you not as a customer to sell to, but one to build a business relationship with"

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