Deploying Zero Trust BYOD Security for an NBFC

Company: **A leading NBFC-MI based out of India**

Industry: **Financial Services**

No of Employees: **2500**

Revenue: **~USD $35mn**

Company Footprint:

The Company in Question is one of India's prominent microfinance institutions with a strong presence in North India, providing low cost financial products and services to underserved low income households, and helping them achieve financial stability

Deploying Zero Trust BYOD Security for an NBFC

Introduction

One of the fastest growing segments in India in today's times is the Fintech industry. With the demand for loans growing from across MSME & Retail segments spread across the hinterland, NBFCs are growing faster than expected.

However, though technology has enabled and empowered for reaching out to the last mile users for NBFC, the CIOs and CISOs of these organisations are grappling with the challenge to provide a strong, reliable and secure access solution that ensures seamless access to the Central Server by the widespread network of Financial Advisors that these companies have

The Customer Story

The customer in question had similar problems associated with secure access of the Central Server by financial advisors, using unmanaged mobile devices and tablets. These 2500+ users were spread across Tier 3 towns and villages across the country, and furthermore, were not acquainted with basic cybersecurity hygiene.

Unmanaged devices using the central datacenter to access enterprise applications posed a risk of being exploited. So, the security team was assessing various secure access solutions to resolve the challenges.

Key Challenges

- Restricting access of applications hosted in public cloud only to pre-authorised users
- Allowing encrypted, secure, and seamless access for applications hosted in public cloud over standard internet
- Managing secure access to unmanaged mobile devices and tablets
- Cloud based web security for endpoints (Linux OS/Android)
- Central management of end points with an SIEM tool

Why was the InstaSafe way chosen?

InstaSafe's Zero Trust Solutions, with their unique secure access solution provided all users with secure and encrypted access to applications hosted on the public cloud, while ensuring that only pre-authorised users get access based on need to know basis across roles and responsibility of users

InstaSafe's solutions enabled easy and simplified configuration of access policies for each of the users, and hence enabled secure and easy access to enterprise applications without compromising on security.

Deployment of InstaSafe's Zero Trust Agent on unmanaged devices was a fairly simple and uncomplicated process that involved low technological know-how, and complete deployment of solutions was achieved in a remarkably short period of 7 days.

Device Posture checks and Device binding features helped in assessing the risk associated with the unmanaged devices and ensuring that they were not compromised

InstaSafe's Unified Single Pane Management Console helped the company's Security team to monitor and manage the users (remote user, small branch user etc) from a single dashboard, while also enabling group policy deployment with just a few clicks.

With lower latency and efficient IT infrastructure replacing the traditional legacy based solutions that the company was using, the users were assured of seamless access from anywhere, even on lower bandwidth networks in remote locations.

Key Benefits of InstaSafe Zero Trust

- Secure, Restricted access to enterprise applications without granting access to network
- Granular access control with simplified configuration of access policies for all types of devices
- Increased security through Device Posture, Device binding and User Identity checks
- Increased employee productivity with secured & encrypted access to public cloud applications.
- Simplified Visibility and Management of all users, devices and applications from one single dashboard.
- Hyperflexible, scale as you go solution that cut deployment time by 80% and could be deployed for any number of users

InstaSafe
Cloud. Secure. Instant.

Asia's fastest growing cybersecurity company is going global. InstaSafe is your trusted remote access security provider, catering to the remote access need of some the world's largest MNCs

Representative Vendor- Gartner's Market Guide for Zero Trust Network Access- Global

Nikkei Asia Growth Champion- Fastest growing cybersecurity company of Asia

True Zero Trust Model, based on the CSA-NIST architecture

Representative Vendor- IDC's Guide for Software Defined Secure Access

Network and security support experts available around the clock

AWS Advanced Technology Partner

42 Points of Presence with 10 million + endpoints

Customer presence in more than 70 countries

Customers in 120+ countries

The InstaSafe Experience Zero Trust. One Access.

Scalable security that caters to the requirements of enterprises of any size. From onboarding and deployment within 4 days, to 24/7 support, at InstaSafe, we believe in leveraging identity to provide an integrated security experience

Problems? Talk to us

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

sales@instasafe.com

www.instasafe.com