Executive Summary

Retail businesses have adopted technology to optimize operations and reduce costs on various fronts. They are the favourite targets of all hackers due to the lure of the PII and card data they hold providing immediate benefits to the hackers. This has led to large investments in IT security by the retail businesses, yet they face increasingly complex attacks leading to costly data breaches. Apart from the security challenges, retail businesses face operational challenges in managing the widely distributed POS systems, ERP access and other systems in stores that are either owned / operated by the company or through a franchisee. The ability to strike a balance between reducing risks and reducing costs while maintaining high level of operational agility to ensure great customer experience is a continuous challenge for all retail businesses.

POS systems are the basic minimum systems required in each store to run the business. The ability to secure them and their access to the applications, located in the retailer’s Cloud, while also ensuring that the end user of the POS systems can get timely help to troubleshoot any issues are typically the core concerns of all retailers.

InstaSafe Secure Access is a Software Defined Perimeter (SDP) solution, that secures the POS systems access to the data center, while also simplifying your IT staff ability to manage and support the IT infrastructure in stores. Our SDP solution creates a ‘dark-net’ of the applications in the DC / Cloud, effectively making them invisible to everyone. This invisibility of applications makes them significantly secure against hackers as the hackers cannot probe and discover these applications. While the hackers cannot ‘see’ nor access any of the applications, business users can access the applications as, InstaSafe Secure Access establishes a level of trust of the User and the device by pre-authenticating all users and preauthorizing all devices. Based on the trust level of the User and their device, access to specific applications is granted based on the role of the user.

Beyond the security benefits, we enable agility for retail businesses to use a hybrid infrastructure of legacy systems and new age systems, both at the store as well as in the data center or Public Clouds and the connectivity between them. Irrespective of the connectivity, protocols, or the systems used across the enterprise, our solution enables you to stay confident of the network access control and data security in transit.
**Simplifying Security and Accessibility for Retail Businesses**

InstaSafe Secure Access is a software only solution delivered as a service. Retail businesses get various benefits, such as:

- Secure connectivity from POS systems to applications in the Cloud or DC
- Secure and simple remote support for IT staff to troubleshoot in-store systems
- Requires just simple internet connection using any type of connectivity - broadband, 4G/LTE, fiber, MPLS etc.

The InstaSafe solution is made up of three components - the Controller, Gateway and Client.

- Controller is the heart of the solution, enforcing the security policies and is hosted in InstaSafe’s secure cloud.
- Gateway is installed on a generic server in every data center or customer cloud. It acts as the gatekeeper to protect all applications behind it and to connect the Users to the applications.
- Client is installed on all POS systems and staff laptops to secure their access from the device to the application using any available network.

This is depicted in the diagram below.

The InstaSafe Controller creates a private network of all the POS systems and the applications, ensuring they are not visible to the internet.
### Functions and Benefits

<table>
<thead>
<tr>
<th><strong>Zero Inbound Firewall Ports Required</strong></th>
<th><strong>Mutual TLS connections with AES 256-bit encryption</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>All applications in the cloud or DC are invisible to all users and the internet resulting in lower security incidents.</td>
<td>All connections from POS to the cloud or DC are authenticated and encrypted ensuring data confidentiality and integrity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Device Identification</strong></th>
<th><strong>Multi-factor Authentication</strong></th>
</tr>
</thead>
</table>
| Device identity is verified using a fingerprint made of the MAC address, serial number and UDID of the device and is checked against registered list of devices. This ensures that only registered devices can be used to connect to applications reducing attack vectors drastically and helps comply to PCI DSS requirements. | • Certificate based authentication using our managed PKI (default and always on)  
• Password authentication using any directory  
• OTP using SMS / Google Authenticator OR  
• 2FA using 3rd party solutions  
All of the above can be enabled to identify Users and comply to PCI DSS requirements. |

<table>
<thead>
<tr>
<th><strong>Device Binding</strong></th>
<th><strong>Device Checks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>All devices are bound to Users ensuring that the user credentials will only work on registered device. Effectively prevents attacks due to stolen or shared passwords and helps comply to PCI DSS requirements.</td>
<td>Allow / deny endpoint connection to applications based on device status compliance with PCI DSS and/or corporate policies. E.g. anti-virus running, OS patch level, disk encryption enabled, domain membership etc.</td>
</tr>
</tbody>
</table>

**Identity-based Access Policies**

Post user and device authentication and authorisation, the identity-based access policies are required to specifically grant access based on the role of the User and not based on source IP addresses. E.g. ‘Allow John access to CRM application on port 443’ ‘Allow Sarah access to POS application on port 8443’ ‘Allow Tim access to POS terminal on port 22’ This ensures that the network is ‘dark’ to the users and their devices until pre-authenticated and pre-authorized and then ONLY allowed limited access to specific services based on their role requirements.
Simplifying Security and Accessibility for Retail Businesses

Many of our customers in the retail industry such as Infinity Retail, Madura Fashion and Lifestyle, Vishal Mega Mart, Sangeetha Mobiles and others have benefited by way of not just significant reduction in risks, but also in terms of operational efficiency and simple end user experience.

A Large Retail Chain Deployment Plan

After considering the concerns and inputs from the Retail Chain IT Team. Following deployment proposal is mutually agreed between the Retail Chain and InstaSafe Technologies.

Each and every store will be deployed two InstaSafe gateway agents in two servers which are placed in the Retail Chain’s store network.

InstaSafe gateway agent will identifies MPLS network status and routes the traffic to datacentre. For all the POS machines at the store, InstaSafe gateway agent installed machines IP address need to be added as gateway IP of POS machines with priority because of high availability.

POS machines requests will come to InstaSafe gateway agent installed machines and according to the MPLS status traffic will be routed via MPLS or InstaSafe cloud in case of MPLS link down.

Deployment architecture Store Level:
Scenarios to be Tested

When MPLS is down?

IP configuration for POS1
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx

IP configuration for POS2
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx

When Primary Server and MPLS is down?

IP configuration for POS1
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx

IP configuration for POS2
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx
**When MPLS is up and primary or secondary server is down?**

IP configuration for POS2
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx

Primary Server
IP: 192.168.xx.xx

**When primary and secondary servers both are down and MPLS is up?**

IP configuration for POS2
IP: 192.168.xx.xx
Mask: 255.255.255.0
Gateway: 192.168.xx.xx
Secondary gateway: 192.168.xx.xx

Primary Server
IP: 192.168.xx.xx
Effort Required for Day-to-day Operations

Normally the support issues that occur in the field are very few. An L2 resource is deployed to perform the below minimal task.

- For every new store opening new InstaSafe gateway needs to be created in InstaSafe management console by entering the store name and store network.
- Access control rule needs to be created after gateway creation in InstaSafe management console.
- Needs to download and install the InstaSafe Gateway agent when deploying servers.
- For any reason if server OS is reinstalled InstaSafe gateway agents needs to be installed.

Operational Efficiency and Simple User Experience

Security is generally seen as a blocker to simple user experience and we at InstaSafe have consciously ensured, by design, that our software is easy to use for the end user. A retail store staff is generally not tech savvy and hence requires a solution that is simple to use. To reduce the friction for the end user to login and access the applications, we made our Client to run in the background as a service the moment the POS system starts. The Client on the POS system starts upon boot-up and if connected to the internet, will connect to the InstaSafe Controller. It provides its certificate, which is the first level of authentication and if the certificate if found valid, the TLS encrypted connection is established after which the user can be prompted for a password and an OTP or just directly an OTP making it very simple for the User to login. All the other checks of the device fingerprint, compliance checks etc. are all done behind the scenes without bothering the user ensuring a smooth experience.

The IT staff at the retail business, while generally located at a central place, may also be spread across regions, based on the diversity and complexity of the infrastructure. Many of our customers have realised significant benefits of centralising all IT management of store infrastructure by using InstaSafe Secure Access. As we create a single encrypted virtual private cloud, all the Clients are accessible from the central location allowing the IT staff to manage them remotely and securely, resulting in faster turn-around times for closing tickets and significant savings on travel costs.
Summary

InstaSafe Secure Access, a Software Defined Perimeter solution is unique in its ability to provide simple yet effective security, ensuring a military-grade network security for the retail businesses. We enable retail businesses to manage a heterogeneous infrastructure effectively while reducing data breach risks irrespective of the location of the users, devices, applications or the connectivity, apart from compliance to various PCI DSS requirements. Importantly, InstaSafe Secure Access solution being delivered as a service helps reduce the overall TCO, due to zero hardware requirements in each store, and improve ROI, through faster ticket resolutions and lower costs of managing the distributed infrastructure.