Securado
A Phoenix Company

1. Background

Organizations are proactively opting to implement work from home (WFH) strategy for all or most of its employees to curb ongoing COVID19 pandemic and ensure safety of their employees. Management's primary concern over here is cybersecurity while they are allowing employees to connect to the enterprise applications from anywhere.

2. Problem Statement

Work From Home (WFH) shall definitely ensure employees' health and safety, at the same time, make sure that the organization is operational, productive, and cater to their customers' needs and demand. However, WFH strategy comes with certain challenges, some are listed below:

1. How do we manage security on unmanaged computers, and the Spread of Viruses, Worms, and Trojans from Remote Computers to the Enterprise Network.?
2. How to ensure the agility in providing one door identity-based access to enterprise URLs, files, networks and applications?
3. How effectively can we allow users to access their office desktops from home and ensure no data leaves the corporate network?
4. How do we ensure hassle-free user experience across multiple OS platforms (Windows and Mac) giving users the flexibility to use devices of their choice with minimal or no IT intervention?
5. How do we ensure the scalability of the solution with increasing number of business demands that need to be catered to users working from home without compromising information security and still be agile?

3. Solution – SecureConnect (Powered by Securado)

SecureConnect is a comprehensive solution offered in a Managed Service model, where organizations could opt for this service and once deployed, they could simply roll-out work from home strategy overcoming the above-mentioned challenges, which are, limitations of a traditional Layer 3 VPN.

Any Device, Any Application: SecureConnect ensures enhanced business productivity from outside Organizations' perimeter with support to any devices (Laptops, Desktops, Tablets, Smart Phones, Windows & Mac, iOS & Android) and any applications (Mobile Apps, Web applications, Published Applications, Physical and Virtual Desktops, Client Server Applications, Network and File Share) as good as from within the enterprise network.

Access Method: SecureConnect ensures that the remote user has the flexibility to access their authorized resources via Layer-4 secure connectivity, application-level client-server access and Layer-7 Web access via a single door web portal that provides a superior mix of flexibility, control and security.

Authentication, Authorization, and Auditing: Organizations' can ensure Authentication, Authorization, and Auditing (AAA) for the employees working from home via SecureConnect enhanced AAA services with Device-based pre-authentication, dual and multi-factor authentication using Duo Security coupled with per-user policy engine for identity-based access to URLs, files, networks and applications.

End to End Security: Organizations', without any hassle and operational overhead can roll out end to end security high performance 2048-bit SSL encryption, endpoint security including device-based identification, host-checking, cache cleaning and adaptive policies. SecureConnect will ensure the traffic leaving from a remote user's computer reaching the Organizations' network is free from malicious traffic, by passing it through SecureConnect's Next Generation Firewalls and analyzed against Antivirus, Antispyware, and IPS.

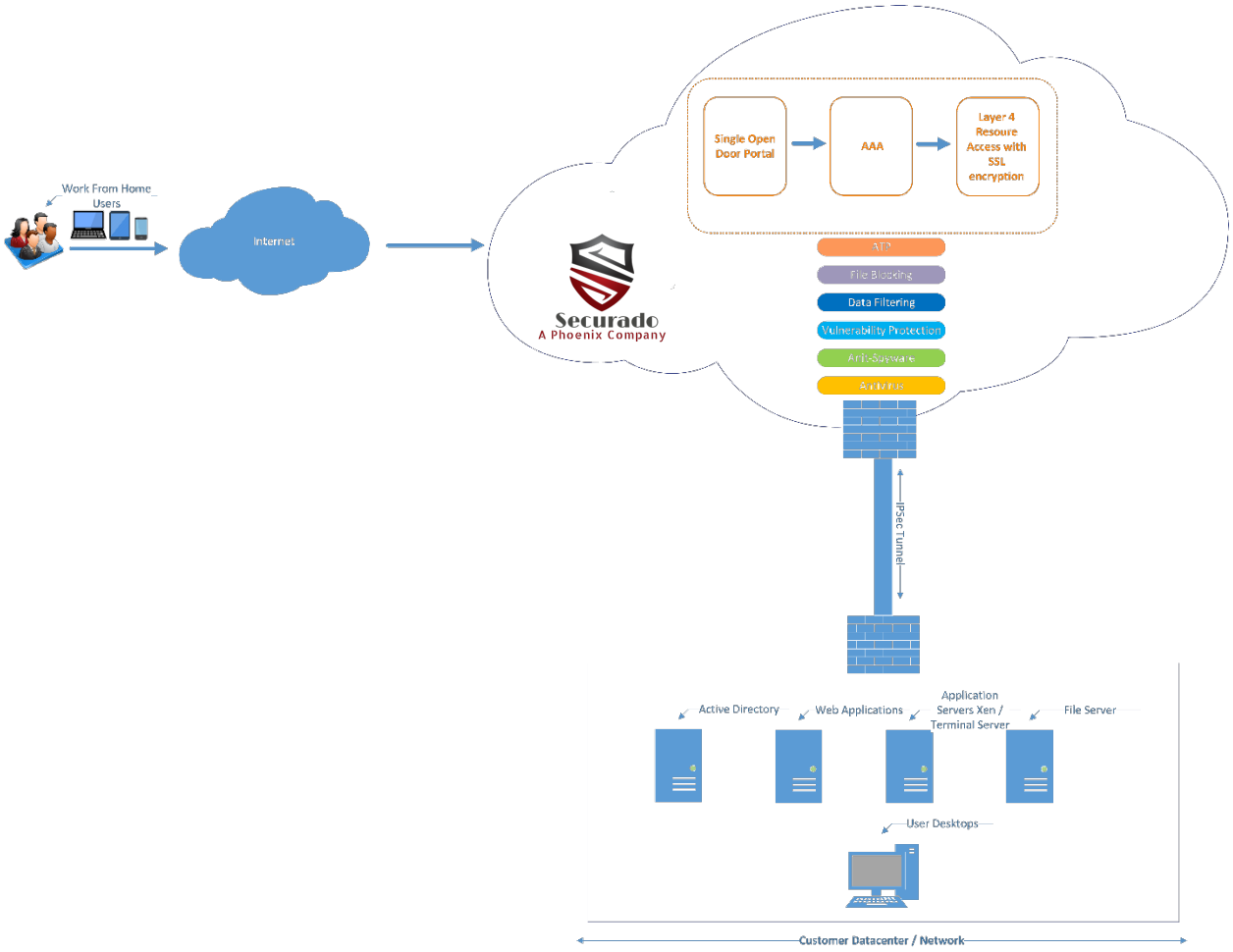
User Experience: SecureConnect service will enable Organizations' to provide their employees working from home to have an 'easy to access' user experience with its 'single door web portal' which is presented to the employees once they are authenticated, where-in they will have access to all their IT resources (Applications, File Shares, Remote Desktops, and Web Applications) as per their authorization.

Desktop Access: SecureConnect services will enable the Organizations to give access to their employees's office desktop with flexibility while they are working from home along with servers that they need access to, with security policies remaining in effect data never leaves the corporate network; building on advantages inherent to RDP, data leakage is significantly mitigated to enable a greater degree of compliance and accountability.

Published Application: SecureConnect services will enable the organization with a flexibility to give access to their core applications leveraging Citrix XenApp and Terminal Services.

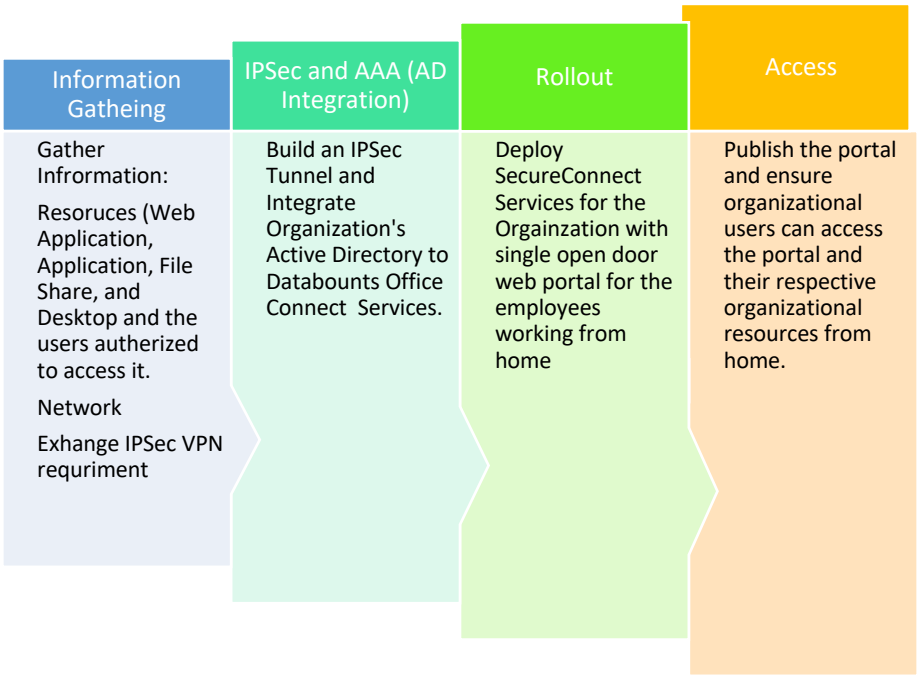
Operation Centers: Securado's Network and Security Operation Centers will monitor and ensure Office Connect Services used by an organization is operational without downtime and without security risks, by 24x7 proactively checking on the services from Operational and Security standpoint.

4. Solution Architecture



1. SecureConnect architecture consists of an IPsec Tunnel between the Organization and Secure Cloud Datacenter (Locally hosted), explicitly allowing traffic to resources that will be accessed by users working from home.
2. A Portal deployed with the one door access to resources (Web Application, Application, File Share, and Desktops) that will be accessed by users working from home, along with AAA.
3. Users working from home will access SecureConnect Portal, Login into it, and once authenticated they get access to all resources as per their individual authorization in the organization.
4. The user's traffic travels via Secure datacenter though multiple layers of security, analyzing the traffic for malicious content and applying relevant security counter measures against malicious traffic, ensuring a clear Pipe down to the organization's datacenter / Network.

5. Implementation Workflow



6. Inputs from the customer

1. Information regarding Resources i.e. Web Application, published application via Terminal services / Xen App, File Share, Desktops and Servers and the user / user group authorized to access these resources or a resource.
2. In case, organization needs its employees working from home need to access Client-Server application, and these applications are not published via Terminal services / Xen App the customer may provide Secure with Terminal Server or may avail the terminal server services from Secure Cloud.
3. Collaborate with Secure Cloud Infrastructure Lead Engineer and build IPsec VPN Tunnel as per the parameters described by SecureConnect between Secure Cloud Datacenter and the organization.

6. Securado, a Phoenix Company

Securado, a Phoenix Company (Phoenix Technologies & Solutions LLC) which is a leading information security solution provider and a pioneer in providing secured infrastructure, data centric security, Security Operation Center in a box, and Adaptive Cloud Security Stack.

Founded and managed by Information Security and IT infrastructure veterans who have more than a Five decades of combined experience in providing information security and IT infrastructure solutions and services to many business verticals including Banking, Financial Institutions, Insurance Companies, and Governments in the Sultanate.