REMOTE WORK CONSIDERATIONS: SECURING THE NEW CORPORATE NETWORK

EVOLVE IP

BACKGROUND

Having provided virtual desktop and infrastructure solutions for over a decade we've seen a massive shift take place in the way IT provides applications to end users. Eleven years ago, customers were utilizing 90% client-server based software. Meaning companies would acquire a server, whether physical or virtual, install the application, and then install the client on each user's desktop.

Now, fast forward to today. It is estimated that the percentage is down to around 25%. So, where are all those applications moving; Software as a Service (SaaS). Companies like Salesforce.com, ADP, Concur, Outreach and more are all delivered via a browser with no software to install.

For the purposes of this document, we'll be using the term "before" to describe how applications were delivered to end users in the "old days" and "after" to describe how applications are delivered now. We will cover the four main differences and what IT has to be cognizant of regarding these dynamics.

Finally, we will look at a way to provide enterprises with the security they need while still enabling employee mobility, BYOD, and helping businesses compete for top talent via remote work in today's increasingly competitive job market.

Access Control	
Before	After
Active Directory(AD)	Per Vendor - Independent of Corporate Controls

As networks matured over time, IT realized they needed "rules of the road". Active Directory (AD) was put in place to control which network resources users could access. By creating user groups with permissions, IT could enable a user with one set of credentials and off they went.

Unfortunately, SaaS providers are all independent of each other. Therefore, there is no common framework IT can enable in order to control access to SaaS providers. In theory, you could control access from the corporate network to decide which SaaS providers your users could reach, but as with many ideas on how to lock down security, that would prove to be completely inflexible in practice.

The result? IT is forced to not only provide AD credentials for corporate legacy access, but then enable, manage and finally disable access to all SaaS providers individually.

For enabling and managing access, this equates to a massive commitment of time from IT. An even larger consideration is when employees are offboarded. IT must first figure out which applications users were provided when they started, then what applications they added throughout their tenure, and finally what other applications do they have access to that IT may not even know of – also known as Shadow IT. When this is an amicable parting of ways, it's more of an annoyance, but when it's a sensitive or negative offboarding, this can present huge business risk if not done quickly and accurately.

Defense Tactics	
Before	After
Defense in Depth	Wild West

Up until the explosion of SaaS, the industry best practice was what IT referred to as "defense in depth". At its most basic level this meant placing a firewall at the edge of the network, then monitoring at the network level for illegitimate traffic, and then finally leveraging a variety of security tools at the server or desktop level. Basically, build big castle walls and keep the bad guys out.

However, the new corporate network doesn't stop at HQ's walls. It also doesn't stop at the VPN connections. It's everywhere. Users need to access resources from different SaaS providers around the globe and those connections are all public.

For corporate assets, IT still maintains anti-virus (AV) and other protections on those devices which certainly helps. Some companies have turned to Cloud Access Security Brokers (CASB) in an effort put a man in the middle act as a relay to protect the enterprise while enabling a more flexible environment for their employees. Unfortunately, to date, these solutions have proved very costly and complicated to implement.

Devices	
Before	After
Corporate Owned	BYOD

For years, when it came to device acquisition, the business ruled. IT would provide a spec to purchasing who would go out to Dell, HP and Lenovo in search of 2 things; the best price and the most standardization. This was done to make ITs life easier. The fewer drivers the better. Everyone gets the same device … office worker or road warrior, accountant or marketer, you were getting the same exact device. Which made sense back then.

Today, the explosion of SaaS, and resulting lower dependence on IT-provided resources, is shifting the power of choosing devices to the user. What was forecasted for years is now finally here and mainstream – the BYOD revolution. Users are demanding to be able to do their jobs from their favorite devices whether iPad, desktop or personal laptops. And what's shocking, is that according to Gartner, this choice is increasingly affecting whether top candidates take or stay in a position within a given organization. Thus, forcing the business to push even more for a BYOD stance.

For the last few years, virtual desktops (VDI) or desktops as a service (DaaS) have provided a band-aid in this department. IT figured out a way to give users access to a desktop OS from pretty much any device that has an Internet connection while still being able to enforce some of those corporate controls mentioned above. This was a great step in the right direction but it still didn't provide the native experience users desired for Mac devices, tablets etc.

Applications	
Before	After
IT has to build	Credit card

When it came to application implementation, similar to devices, IT held all the power. If Marketing wanted a new CRM, IT would need to technically bless the app, deploy it and then finally provide credentials to each user. This was an inefficient process and one of several reasons for the explosion of SaaS-based applications.

Application provisioning has dramatically changed with the explosion of SaaS. Today, that same Marketing team can deploy an entire tech stack in an afternoon with a credit card. Because there is little if any dependence on IT, organizations are finding more and more instances of "shadow IT". In essence, functional areas are going out and utilizing applications without oversight from IT which leaves the organization extremely vulnerable.

Organizations have begun writing policies to try and curb this approach but increased pressures on results from the business have caused employees to resort to a 'by any means necessary attitude' to achieve their specific needs; losing sight of the overall impact to the business. Training and education workshops help, but IT leaders are left scratching their heads on the best way to deter this behavior.

Let's face it, IT is being forced to figure out a way to support and protect devices they don't own or perhaps aren't even aware users are utilizing. On top of that they now need to control access to applications that can be deployed without their involvement. IT has gotten out of the data center business and into the integration business … unfortunately, at the same time as the rest of their tech-saavy employees. We have reached the tipping point in SaaS adoption and as a result, Internal IT is being forced to become more strategic than ever.

Bottom line … many organizations have increased their security risks and have lost (or are losing) control of some critical functions of IT. The good news is that there is a single, simple, cost-effective solution.

Enter Workspaces

Evolve IP has developed a comprehensive solution that addresses the needs of the IT and the business. Workspaces enable mobility and security and give employees the tools they need to do their jobs in ways that make them more productive than ever.

Evolve IP Workspaces include:

- **Active Directory Integration** – Control access to legacy line-of-business and SaaS applications through AD
- **SSO and Self-Service Password Resets** – Users adopt, and adhere to technologies that make their lives easier
- **Multi-factor Authentication** – Increase security posture requiring a second form of authentication
- **BYOD Friendly** – Allow employees to use any device while maintaining security controls
- **Custom Toolbelt** – Users get just the tools they need, the way they want them, increasing efficiency
- Full DaaS capabilities for power users

Visit www.evolveip.net/workspaces for more information or give us a call at 855-481-3798 for a demo.

Why Business Choose Evolve IP

At Evolve IP we **Make Work Better™**, ensuring employees are more productive, more mobile, more secure and less dependent on IT resources. We design Purpose-Built® solutions, tailored just for your business, that unify workspaces, collaboration and communications, and contact centers. Integrating blue-chip technology partners like Microsoft, Cisco, Citrix and VMware, with our intellectual property, Evolve IP's analyst-acclaimed solutions have been deployed globally to 500,000+ users and into the world's most well-known brands. All Evolve IP associates are focused on driving successful client outcomes and that has resulted in our scoring at the top of verified analyst and client satisfaction rankings.