celestix

Improved User Experience for Remote Access

In the “Always On” world of today, the user expects technology services to work in a seamless fashion with little or no effort required to access corporate resources. This is especially true in the case of increased mobile and remote workers who are rarely, if ever, in the corporate office and yet depend on company applications, information, and resources to be effective in their role.

Legacy VPNs have presented a number of problems to both the end user and the IT support organization that are translating to considerable loss of operational dollars. While operational improvements are always a key focus area for IT, most support organizations have begun to understand the importance of running IT as a service business with the goal to provide the best possible user experience and value.

Due to the antiquated nature of traditional VPNs, users are confronted with a number of problems logging in because of connection, password, or application compatibility issues, resulting in an increase in help desk calls. It is not uncommon for the Help Desk to receive multiple calls throughout the day to address relatively simple but time consuming VPN issues, potentially creating chokepoints in the service delivery model. There are always those users whose limited use of VPN technologies means that they are more likely to require support while working remotely, potentially causing spikes in service requests and increased, unplanned demand on the support group.

Next generation remote access solutions are just now starting to make an appearance in the market. Despite being available, new Remote Access solutions represent a slight barrier to entry due to the lack of knowledge as to what’s available and how it benefits the organization, as well as the technical complexity of the deployment and implementation process.

Finally, creating an “Always On” experience for the user immediately exposes security risks to the corporate intranet. The trends in data theft indicate that criminals are increasingly well versed in circumventing traditional authentication and password methods while more actively targeting mid-market and SMB companies based on the fact that these targets represent fewer security protocols to beat in order to gain access.

It is estimated that the average cost of a data breach is over $5M to the business and the use of traditional login and password policies have proven to be ineffective in protecting companies from data theft as evidenced by the increase in the number of security breaches across all industry verticals, regions, and business type. Password policies that do not require a second factor of user authentication are all but useless when considering the sheer number of free and low cost password hackers, key loggers, and other tools available to help thieves steal sensitive data.

Combined with the increasing skill and sophistication of the modern data thief, the availability of free or low cost password hacking tools, and the uselessness of traditional password policies, the threat to any organization providing an “Always On” remote access solution is compounded exponentially.

In order to protect your organization from a breach of your most sensitive customer, employee, and partner data, a Two-Factor Authentication solution is no longer a “nice to have” but a requisite for doing business in this era of increased threat. Whether providing an “Always On” remote access solution or not, the need to ensure only authorized users are accessing your network is a business imperative for the security conscious IT organizations.

Companies are achieving a better user experience, reduced administration costs, and a reduction in Help Desk calls while improving their security posture by implementing Celestix DAX DirectAccess with Celestix HOTPin Two-Factor Authentication. The combination of an IPv6 Always On VPN connection and Celestix HOTPin Two-Factor Authentication provides an improved user experience and adds an additional layer of security to ensure the safety of your corporate network. Because the user is no longer required to logon to Legacy VPN technologies, the need to offer support for password reset, connection, or VPN application is all but eliminated.