Clear2there®
CLEARLY CONNECTED

Clear2there Reports Its Smart Premise Service Delivery Architecture Is Not Affected By Heartbleed Bug

Fundamental architecture of Viewbiquity Cloud Application Suite delivers security without relying on Open SSL or other vulnerable elements

Oklahoma City, Oklahoma, April 29, 2014 -- Clear2there LLC, a leading provider of advanced video surveillance, smart-home, smart-business, and smart-farm applications, and M2M solutions for service providers and enterprises, is stating that its Viewbiquity Cloud Application Suite (VCAS) platform is not susceptible to the Heartbleed bug that has been affecting the operations of computing and communications services worldwide. The Clear2there platform has been deployed by some 80 telecommunications service providers across the US to deliver smart home, business, farm, healthcare, and access control services to broadband subscribers.

According to Clear2there chief technology officer Tom Shafron, the VCAS platform employs a unique architecture that assures system security and integrity while limiting access to the intelligent devices used in smart premise deployments. The solution assures that inbound queries and connections are only possible from its secure server, and outbound connections are not permitted.

“The Viewbiquity Gateway located at the customer premise secures all information and data between the host datacenter servers and the customer’s site using strong VPN and encryption technology,” noted Shafron. “This approach eliminates the exposure of individual smart devices such as thermostats, video cameras, sensors, and control devices, to the Internet. Even if some of these devices were to be susceptible to the Heartbleed bug, they are not exposed to the Internet, and therefore the bug cannot be exploited.”

The VCAS platform does not use the Open SSL stack in any of its components, and the robust architecture helps to prevent any devices attached to the system from becoming an unintentional entry point to a network.

“For any device that uses the Open SSL stack and shares data across the Internet, there is a risk, Shafron continued. “And if you extend this same scenario to the millions or even billions of sensors, controllers, smart thermostats, appliances, and smart-premise gateways connected by telecommunications and security service providers, remediation of Heartbleed may not even be practical. But if solutions are architected to anticipate and block Internet-based attacks, the problems can certainly be mitigated.”

About Clear2there: Clear2there is an innovative, full-service provider of market-leading smart-home, smart-business, smart-farm and smart-healthcare solutions for service providers, including broadband operators, regional telephone, data and mobile communications providers, cable operators, and electric utilities. Clear2there’s broad solutions portfolio includes feature-rich video surveillance, advanced communications, and M2M technologies that are targeted for both business and consumer use. Based in Oklahoma City and Deerfield Beach, Florida, Clear2there works with national distribution partners, and offers a team of dedicated support staff to assist in all phases of implementation. For additional information, visit www.clear2there.com.

PR Contact:
John Stafford for Clear2there
Parallel Communications Group
515-708-1296
jstafford@parallelpr.com