Dental Group Gets Improved Security and Cost Savings.

A national franchised multi-site dental group, with thousands of users – staff, dentists, clinicians, anyone with access to EMR (Electronic Medical Records) or email – required a security upgrade for their systems/network. A centralized corporate office provides operations and IT, including support, for all locations. They experienced a small hack, which caught their attention, and the Mitre Attack Report made them further aware of their vulnerability. The Report also introduced the many leading solutions available, after contacting Providers, their options looked to be costly and required additional demands.

CUSTOMER PROFILE:

• Franchised multi-site dental group
• Thousands of users
• National organization

OBJECTIVE:

The client wished to reduce their vulnerability as affordably as possible. They had a low-level security solution in place and needed to replace it with a stronger more encompassing product. They considered buying the licenses and managing the improved solution(s) themselves, while hoping to find streamlined options that were less costly. The client requested we only put forward known brands, for their piece of mind.

DISCOVERY:

Other technology experts who approached them were primarily pushing different categories of solutions, and not listening to their security concerns. We approached with security as job one. Licensing directly would have resulted in a high cost per seat, plus the self-managing requirement. Resellers, large Providers, buy large numbers of licenses at a discount and pass on the savings to customers, in this case, cutting the cost almost in half, without additional expenditure for deployment, IT staff, and acquiring adjacent technology/solutions.

SOLUTION/ DEPLOYMENT:

We went deep looking at a variety of Providers, all big players in the industry. Our Sales Engineer helped us identify a large Security Provider who could provide the desired security solution at a steep discount (almost half of the original quote). Additionally, the new Provider would manage the nextgen endpoint software – deployment, ongoing maintenance/upgrades, and even a SOC (Security Operations Center) from the same Security Provider. This saved the client the need to hire staff to execute the deployment, and a high-level IT person to maintain their network (who, in this competitive market, would demand several hundred thousand dollars in annual compensation). In addition to the security solution, we updated their organization to a hosted voice platform and superior connectivity approach. After contracts were signed, the solution was deployed within a month, with the Partner also paid within a month.