****

**Encryption Alone Does Not Defeat Insider Threat**

***How Vanguard CS Maximizes Your Protection by Adding an Additional Layer of Security and Providing a Front-Line Defense Against Attacks***

***There is always a point of vulnerability***

In most network architectures containing encryption, there is a defined point of vulnerability in the infrastructure where the encryption reaches a demarcation point, allowing un-encrypted sections of the infrastructure to be exposed. At these points, even when they are in a secure IDF closet or an area deemed “Secure Open Storage”, there is a risk of an insider threat having access to and stealing the data. In addition, encryption does **not** detect or prevent physical attacks on critical network infrastructure or critical pathways that could damage the infrastructure.

Network Integrity Systems’ ***VANGUARD™ CS Fiber Optic Monitoring System*** detects and prevents physical attacks on network infrastructure by performing continuous analysis of the cables, pathways and points of vulnerability and looking for intrusions that occur as a precursor to a physical attack (tapping, theft of data) or damage that could degrade network performance or availability. Protecting the physical network infrastructure with VANGUARD CS will maximize the security and protection of your distributed assets. Therefore, Encryption should be considered a parallel solution to VANGUARD CS***,*** notan alternate solution.

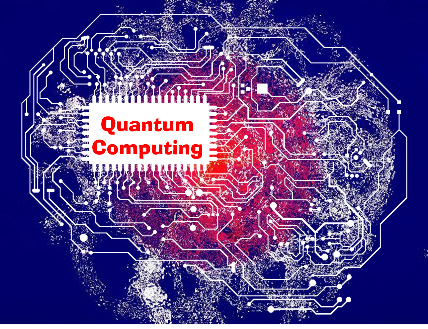
***What if my encrypted data IS tapped and stolen?***

What if a physical optical tap was placed on your critical data infrastructure without you knowing it? How long would the intruder have access to your data? How much time would the intruder have to break the encryption code or steal a key? In most cases it is not likely that a day-to-day hacker can achieve this, but with a more sophisticated and well funded intruder (ie China, Russia, etc.), your probability increases dramatically; especially when you have no idea you have listening devices or optical taps residing on your infrastructure.

When encrypted data is stolen or compromised, with enough time and resources, an assailant or “hacker” has a high probability of cracking the encryption and obtaining the critical data.  Therefore, it is imperative to know if your encrypted infrastructure has been tapped or sabotaged. By monitoring or alarming the physical aspects of your infrastructure with VANGUARD CS, you will know that the tap is being attempted before the assailant is able to obtain the encrypted data.

In the figure below, a simple Google search produced real, recent headlines confirming that there are constant efforts to defeat encryption.

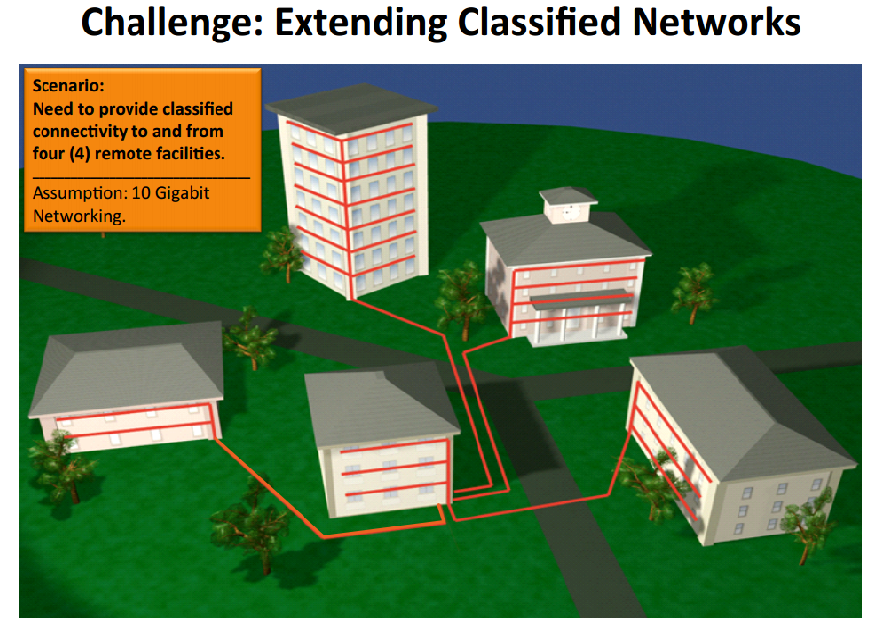
Ensuring that your physical layer of critical infrastructure is protected, even if encrypted, should be a no-brainer. You need the capability of knowing if someone is unlawfully handling your network infrastructure.

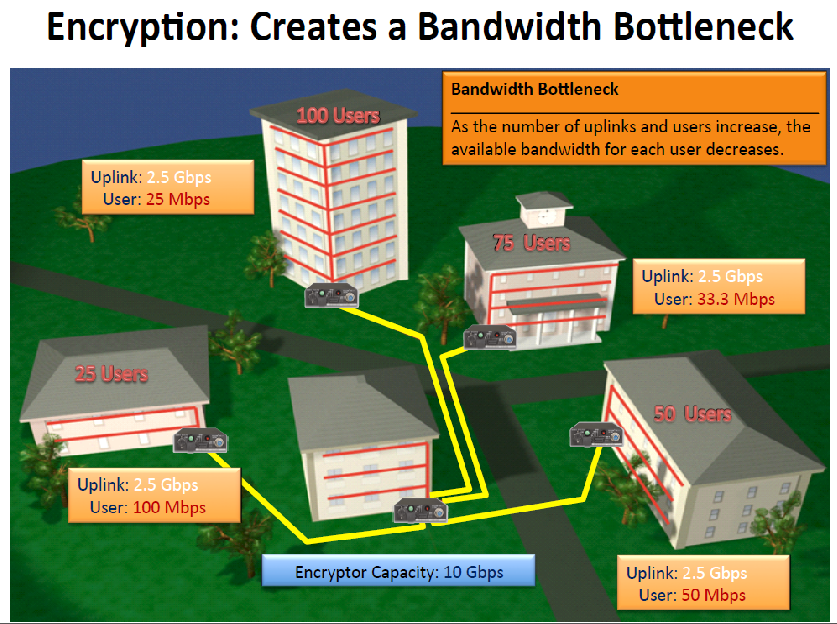
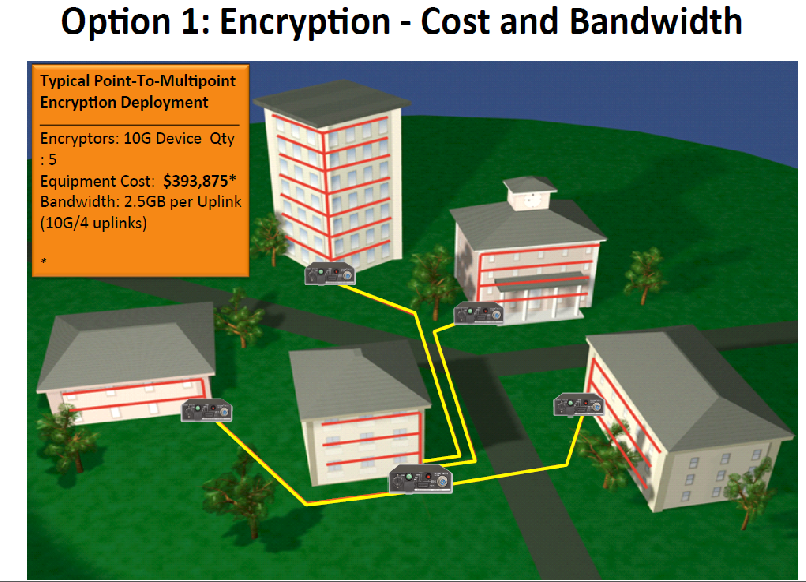
***Will the emergence of Quantum Computing cost you more in the end?***

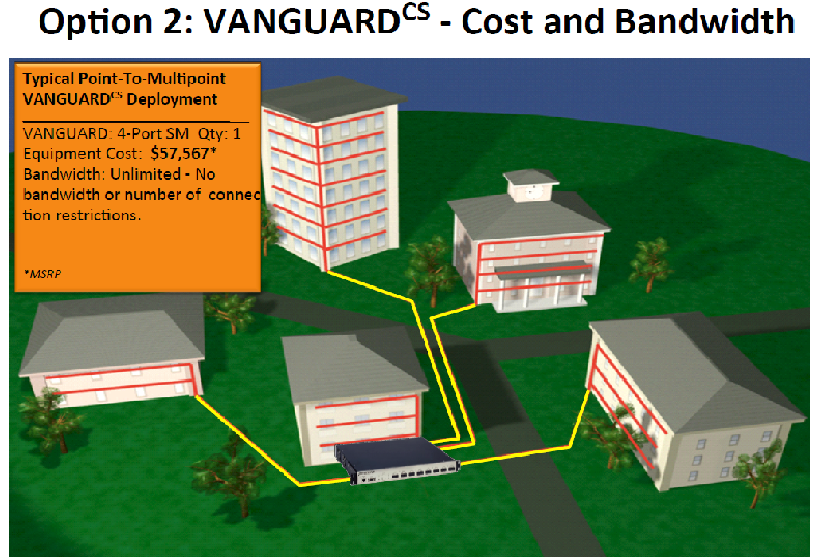
Quantum Computing is right around the corner, and just by reading the headlines in the image above, you can see that quantum computing poses a serious threat to encryption. So the question is; if you invest in millions of dollars to implement best-of-breed encryption into your network, what happens when it’s compromised by an up and coming Quantum computing feature? Does this mean you now must re-invest in a new product or robust firmware updates every time your encryption product is compromised? This potentially could be a CAPEX/OPEX trap and could cost you millions of dollars.

***Is Network Bandwidth Important to you?***

Perhaps the number one business case against using Encryption revolves around network bandwidth. Encryption can cause a severe constraint to your bandwidth capabilities. Depending on the required speed your critical infrastructure needs to operate, major hurdles can present themselves when implementing encryption. For example, if your newly installed data center fiber optic network is running at a 40 GIG or higher, encryption most likely will not follow suit. If your Encryption devices are only capable of 10 GIG, the constraints are obvious. Not only will the performance of your network be affected, the principle of spending the moneys for a 40+ GIG speed network is now in question. VANGUARD CSwill protect your new 40+ GIG network infrastructure without touching the active data, hence having zero effect on the bandwidth you invested in.

******As an example of this, reference the ***Encryption vs. VANGUARD CS*** slide-deck images below taken from a recent business case by a major defense contractor. You will not only see the significant difference in bandwidth allowance, but also the cost savings between the two options. Although encryption products vary in cost, especially between government and commercial sectors, the principle remains the same.

******

******

The 4th slide depicted here shows the direct comparison of VANGUARD CS to Encyption for this particular business case. Almost all cases are similar.

***Adding VANGUARD CS to protecting your critical network Infrastructure is the answer***

Using only Encryption to protect your critical data presents risks and vulnerabilities. It simply cannot prevent physical attacks on your network infrastructure. In addition, encryption has a high risk of being defeated by “time” and Quantum Computers. It also impacts the speed of your network.

In contrast, the VANGUARD CS ensures protection from an assailant by protecting individual cables or network pathways throughout your facility and/or campus. Time and Quantum Computers cannot defeatVANGUARD CS because it is a passive device that does not touch or process the data being transported throughout the network. Finally, since VANGUARD CS has zero effect on you network bandwidth; it does not alter network performance.

For more information about the ***VANGUARD CS*** solution, contact Network Integrity Systems or visit [www.networkintegritysystems.com](http://www.networkintegritysystems.com)