Blue Horizon BUSINESS GROUP | TriSquare Cyber

Design Rational

The whole of the competitive landscape is divided into three parts: Established firewall vendors “flexing” into verticals, industrial players creating firewall products (with or without established firewall vendors), and lone wolves pursuing security devices that can fit into a variety of applications. **It is important to note that there is not an obvious competitor specifically supplying firewall-style security devices for use with IP camera networks.**

We believe, based on our experiences, that an in-network FW would provide benefit to both the industrial and physical security sectors. Indeed, both of these vertical share similar characteristics in that both are industries where a variety of analog communication technologies were codified and standardized over a period of decades; both industries have transitioned to network protocols for this communication; and both industries do not appear to place great credence in using IT network professionals.

Because both industries already employed communication standards, neither were really early adopters to the digital revolution because the benefits of switching to digital IP–based networks were not immediately better than the existing standards. As benefits have accrued, both industries have moved to a digital world, but they are late adopters and un-supported by the technology experts we would expect in other industries.

This can perhaps be best exemplified by the terminology used to describe higher tech offerings. In the physical security world, digital cameras are called “IP (Internet Protocol) Cameras”. Few individuals in an office setting would refer to their computer as an “IP Typewriter”. Likewise, the industrial sector refers to the ability to network machinery as a function of “OT” (Operational Technology). Both industries are insulated from the standard office environments, terminology, and IT security functions we would expect in 2021.

Likewise, both industries are specialized in that the main technologies employed are not just servers, PCs/laptops, printers, etc. Industrial automation is its own beast with a wide variety of technologies from Programmed Logic Controllers (“PLC”s) to entire automated systems that perform specific machining, welding, slitting, and other processes.

Enterprise grade Physical Security faces a slightly different categorization in that the home user now has familiarity with intrusion detection (burglar alarms), cameras, and other sensor sets. Professional installations employ higher-grade equipment, but all of this equipment can be grouped into the IoT “Internet of Things” terminology. At the most basic level, we are really addressing the difference between home networks and business networks.

While average users feel comfortable with technology, it is readily apparent that the average user has little real knowledge of the risks posed from IoT nor what is required to mitigate these risks. Indeed

Professional Installers of Physical Security equipment, known in the industry as “integrators”, display decent specialized knowledge of the equipment involved in physical security – cameras, sensors, access control systems, network video recording servers. Such integrators, however, have demonstrated significantly less robust “cyber security” knowledge.

Given these technology limitations, it is not surprising to see established names in the firewall industry market product lines that cater to these two sectors. Unlike other efforts to be discussed below, however, these products are the exact same firewall products already available – the names are the same but the marketing is changed. In this regard, these products are most likely aimed at the IT professional responsible for protecting networks who would have heard of the brand through common IT channels and is now encouraged to use these products to protect industrial or security infrastructure. Instead of this being a true product offering, it is better to view this as a “flex” to cover more industries - a “yeah we can do that, too” approach to covering the specialized nature of industrial automation and camera networks.

Industrial Firewalls

As noted earlier, we do not see a specific “Physical Security” Firewall Device, but we do find niche hardware being marketed, sold, and installed in the Industrial sector. An internet search on the term “industrial firewall” will get instant results. The more complex industrial systems have embraced cyber security as a way to protect large-scale industrial installations. Since industrial systems rely on a combination of Ethernet, fiber, SCADA, and other specific connectivity standards, industrial firewalls utilize complex hardware with dedicated ports for all of these types of connections. In this sense, industrial firewalls serve a wider function – most likely translating signal types amongst the various protocols; translating IP addresses where IP bands are shared; and serving as true firewalls scanning and controlling traffic across the business networks and the machine networks. It should be noted, that many of the physical devices present in this market look surprisingly similar – suggesting common suppliers for the hardware itself. In these types of industrial settings, the firewall is positioned as one tool in a largest array of hardware and software designed to both improve operations and guarantee security.

There is a stratification amongst these devices. While the key players in this space represent some of the largest global producers of industrial equipment on the planet, the use of the devices differ in two ways. First, there are industrial firewalls that are clearly brand-specific and designed to operate within the confines of a larger system. Second, we find more generic firewalls (still produced by large manufacturers) that are not positioned to be another piece of a larger end-to-end installation.

A brief note on all-in-one boxes: The integrated switch elements are indicative of non-sophisticated network users and are a staple of home-use routers, for instance. More sophisticated network professionals will want each device to serve one function. In some respects, the marketing strategy of the all-in-one box approach implies that the end user may not see the value of a firewall… but could totally use more switch ports. For comparison, the Physical Security Industry is replete with all-in-one boxes that mix servers, recording, and switching all into a single magic box. Please see the slide show […] for more details.

Non-Traditional Firewall Offerings

The final sector of the industry is what we are calling “non-traditional” offerings. If the first segment are name-brand firewalls that flex into new markets, these players are the off-brand offerings that specialize in not being name-brand. By this, we mean there appears to be enough uncertainty about what exactly the box is doing, that it appears to be more than it really is.