White Paper

All-in-One Versus Distributed (Conventional) Security Systems

When selecting home electronics, appliances, and equipment, many consumers are sold on the simplicity of devices that combine several functions in one. Multi-function office equipment is a perfect example. Rather than purchasing a separate copier, fax, scanner, and printer, they will choose an all-in-one device that combines them into a single piece of equipment. In the security market, this approach is represented by the all-in-one security or self-contained system that combines the panel, keypad, and siren in a single unit. These types of systems may offer apparent benefits; however, there are also some distinct drawbacks. In this white paper, we compare the all-in-one systems to the traditional, distributed security system having multiple, separate components.

Section I. Physical Attacks

The ability of the system to withstand physical attack is possibly the most significant difference between all-in-one and distributed systems. “It's possible for completely unskilled intruders to physically rip these systems out of the wall and smash them to bits,” according to Daniel McKimm, founder and owner of ProTech Security in North Canton, Ohio. Prior to launching ProTech over 30 years ago, McKimm was in law enforcement, giving him first-hand experience in responding to alarms for burglaries and intrusions.

With all of the elements in one package, he says that brute-force attacks are all too easy. These types of attacks are made easier because an intruder either is drawn to it by the noise of the siren or knows the approximate location of the system. Intruders, able to recognize the type of security system, will be able to identify it as an easily attacked all-in-one.

At least one manufacturer has compensated for that fault with a bit of programming. When an alarm is tripped, there is typically an entry delay before the alarm signal is sent to the Central Station. In some systems, a tentative alarm signal is transmitted immediately to the Central Station and held there. When the user enters the code to disarm the system, it sends a cancellation to the Central Station. If the system is attacked and disabled during the entry delay, no cancellation signal is sent, and the tentative alarm signal is activated. Most all-in-one systems lack this feature.

Distributed systems are inherently more resistant to physical attacks. The visible and readily accessible peripheral components could all be attacked, but the panel is typically concealed and protected. If the system is tripped or if any of the peripheral components are attacked, the panel maintains its ability to transmit the alarm signal to the Central Station.

Section II. Simplicity of Installation and Operation

Programming all-in-one systems used to be the simpler option for the installer during initial setup because of the absence of numerous devices to interconnect (panel to sensors, sirens, etc), allowing for "plug-and-play." Installers appreciated this feature, because it allowed them to make more installations during the day. This is not as big an advantage as it once was. The increasing dominance of wireless systems like the DMP XTL™ allow for very rapid installation. A distributed, wireless system can be installed in less than an hour, due to time-saving features like Walk Test and Survey LED, that allow a single installer to quickly place and set up system components. The simplicity offered by an XTL system is equal or better than most all-in-one systems.

Once installed, basic operation is comparable for both types of systems. Routine activities like arming and disarming are very similar. Distributed systems have some additional consumer programming options, and therefore, the added potential to tailor the system to meet the end user’s needs. However, these can be limited by the alarm company to create an extremely simple system to sell and install.

As with the multi-function office device, the all-in-one security system means there's a single device. There may be fewer things to go wrong. However, when something does go wrong, it typically requires replacing the **entire** system.

With a distributed system, if an individual component should fail, it can be replaced easily and cost effectively. It's not necessary to go to the higher expense of purchasing an entirely new system. The distributed approach also provides the opportunity for the consumers to selectively upgrade components or to add new devices and features to their system.

Section III. Cost

Price is always a consideration for consumers. In the case of all-in-ones, you would expect that their simplicity of design and reduced number of components would make them more affordable. In fact, there's little or no cost advantage when purchasing these systems.

For system dealers, the all-in-ones put them at a potential disadvantage in terms of profit. The inability to modify or expand these systems makes it impossible to incorporate add-ons or upgrades that the consumer may want. In addition, these upgrades provide additional revenue opportunities for the dealer.

The expansions, upgrades and add-ons that are easily incorporated in distributed conventional systems, such as mobile services and video monitoring, create many potential RMR opportunities.

Section IV. Summary

All-in-one systems are a simple and low-cost approach to security and a good example of getting what you pay for. Their simplicity limits them from being customized or updated. They are what they are. Distributed systems are both customizable and updateable. As new features and functions become available, they can be added. Software upgrades can also be applied to add features and improve operation. Most importantly, the vulnerability of all-in-one systems to attack means that they are not able to provide the same level of protection as a distributed system.

The decision is ultimately the consumers, but dealers like Dan McKimm, who want to provide their customers with a strong and reliable security systems, consistently recommend distributed systems.