News

Examining the continuing allure of smart technology in 2019

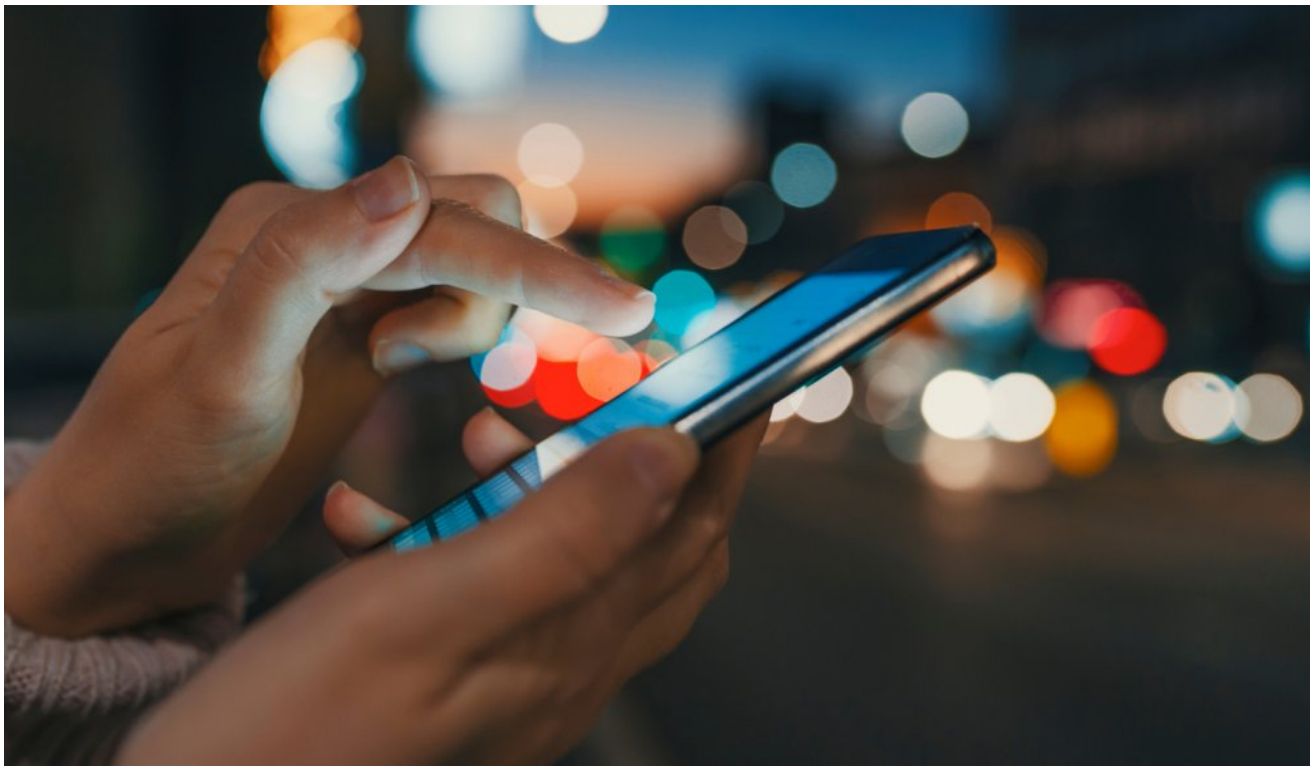
It seems the positive possibilities for smart technology is endless, and the general public certainly appears to be onboard. For instance, Cambridge-based tech company, Arm, commissioned research firm NorthStar to survey 2,000 global consumers. It wanted to discover consumer insight on 2018 technology trends and their expectations for 2019. It also asked its technology experts and futurists what they think will happen within IoT technology over the next year and beyond. The convenience of smart technology is the main reason to "love" (26 percent) or "like" (37 percent) the technology. One in five respondents appreciated what the technology was doing for their city experience.

Most cities already deploy many technological devices that fall under **the IoT blanket** . For instance, industrial control systems (ICS) exist to run day-to-day necessities like water, power, traffic, and transportation. It is common knowledge that IoT devices are built

for functionality, with security coming in second, and with this, enters the growing presence of cyberattacks. For example, traffic control systems could be exploited to cause jams or crashes. Other risks include subways grinding to a halt, or water supplies being contaminated.

Smart Technology: Where We're Leading

One of the obvious drawbacks of IoT devices is that they are based on the concept that everything is accessible. And when it comes to security, it can only take the weakest domino in your defensive lines to fall before your security is comprised.



The Rise of Smart Cities

Vanderbilt tackles this IoT issue through a slightly different approach. Instead of making everything accessible, we try to securely allow access to additional devices through a gatekeeper system. For instance, communication with an **SPC Wireless** PIR sensor is facilitated directly through the main SPC system itself.

So, through the SPC cloud platform, you can securely login and adjust the settings of your SPC Wireless PIR securely and safely through a system built from the ground up with cybersecurity in mind. The SPC system acts as a gatekeeper to protect all individual devices working in conjunction with the SPC panel. This also expands out to other

downstream connections, such as third-party integrations working on different buses.

SPC Cloud Devices

This is because **SPC** has built-in protection mechanisms whereby if the system is attacked, it will go into protection mode. The system will remain operational and it will still be able to communicate out, but it will start to shut down elements of itself to protect the system from the attack. While no system is invincible, SPC has been designed so that should an attack penetrate, the system has multiple communication paths available as backup. Therefore, if one server is taken down the system can immediately switch to a backup server and then switch communication paths to bypass the attack and ensure messages still operate successfully. This makes the SPC system a secure gatekeeper to facilitate communication between Vanderbilt's IoT devices such as the SPC Wireless range.

Cloud Security Whitepaper: A Brief Journey through the Revolutionary Technology

So, the Vanderbilt approach to IoT is to provide a very secure platform that applies uniformity, allowing system users to see and access the status of all their devices securely from a single app. This provides the benefits of IoT without exposing the devices to all of the risks associated with IoT, in turn maximizing functionality of the product.

Download our White Paper