THE SWITCH E-BOOK

The Builder's Guide to Smart Home Security

www.primex.com

primex Fit everything. Together.

Smart home builders – do your customers dream of living in a futuristic home with AI-enabled security? Or maybe they want to keep it simple?

Learn how to integrate all types of smart home tech in new home construction. This e-book gives you the latest research so you can inform your customers about data security.

Contents

Why Home Security is a Must-Have Smart Home Feature

Smart home builders, prepare to get busy. The global smart home market is expected to be worth $9.4 billion by 2021.

Smart home automation is among the fastest growing categories on Yelp, a consumer-based recommendations web service. The driving force behind much of this growth is a desire for improved home security. What does that mean for you?

It means more fiber-to-the-premises internet installations because customers will be using more bandwidth than ever before. And it means that if you want to stay competitive and get positive Yelp reviews, you'll need to stay on top of smart home security developments.

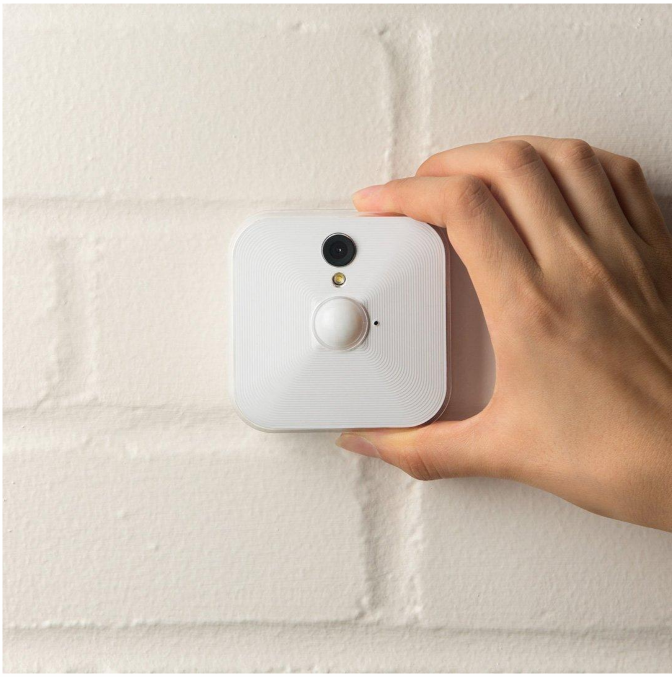
If you want evidence of the importance of home security to the smart home ecosystem, just look at how many options are out there – and which companies are investing in home security. Two of the world's largest companies, Amazon and Google, are funding heavily in security features as they compete for dominance in the smart home market.

Nest is part of Google again after three years as an Alphabet subsidiary. Alphabet is Google's parent company, and the move is being viewed as evidence of Google's intention to compete with Amazon in the smart home market.

***What sets Nest apart?** A tag that allows residents to tap in and out of the home, eliminating the need for them to memorize codes!*

Why Home Security is a Must-Have Smart Home Feature

Last year Google spent half a billion dollars establishing Nest Secure Home in the home security market. The nest security system is made up of a hub that connects to a network of sensors, cameras, smart locks, and a smartphone app.



Amazon's investment in home security includes Blink, a wireless security system that sends alerts and video to the homeowner's smartphone. Blink's latest product, a video doorbell offers two-way audio, infrared night vision, and two years of battery life.

Amazon closed a purchase of another video doorbell company, Ring. The sale was a reported $1 billion. Ring founder and CEO, Jamie Siminoff, in an interview with The Guardian, said that the deal makes smart home security more accessible because Amazon's scale allows for a price decrease. Siminoff also said that the deal gave Ring access to additional resources, including the intellectual property associated with Blink.

Big tech firms are not the only players competing for smart home market share. Smaller companies are finding creative ways to compete in the smart home market as well. Notion, a startup that sells sensors that monitor doors and windows, water leaks, and smoke, is partnering with insurance companies to find ways to help homeowners decrease their insurance bills.

Notion is also exploring ways to use the data collected through the smart home security platform to find ways to predict behavior in a way that enables homeowners to reduce losses. Notion CEO Brett Jurgens, in an interview with Forbes, said that he believes that “one day it could very well become a requirement to have certain smart home technologies installed in your home to get insurance coverage.”

Homeowners are getting creative too, and many are discovering additional benefits to their smart home security products. A Notion customer set up a sensor near her front door and added temperature sensing only because the option was available. When the system started to alert her to temperature drops near the doorway, she realized her weather stripping needed to be replaced.

The future of smart home security

As video technology evolves, video security will change too. For example, facial recognition software can be used to configure security systems to disarm when they recognize the face of the homeowner. Similar technology can be used to monitor neighborhoods, alerting residents when vehicles with unknown plates are in the area.

Amazon and Google are both investing heavily in artificial intelligence (AI), which means AI integration with smart home security may be coming soon.

How Secure is Your Internet?

Whether your customers want to live in a futuristic home with AI-enabled security or they want only simple features like programmable lighting that will deter intruders, they have lots of options.

Do you consider your internet connection an essential service?

Many commercial and residential users do! For most businesses, a loss of service could stop them from being able to function. Residents could lose their phone service and the ability to work from home as well.

For years internet security has meant protection against computer viruses, malware and malicious code on websites. Most computers today are protected by firewalls and anti-virus software but even some of the most sophisticated networks can be defeated by cyber attacks.

Cyber attack categories include:

- *Cyber crime hacktivism*
- *Cyber espionage*
- *Cyber warfare*

A number of universities across the U.K. lost their internet connections when their network was brought down by a Distributed Denial of Service (DDoS) attack. Other examples include Target being hacked and the Ashley Madison data breach.

The website Hackmageddon.com categorizes cyber attacks into cyber crime, hacktivism, cyber espionage and cyber warfare. The majority of cyber attacks are by criminals trying to obtain personal information such as credit card numbers and other banking information but the next most common is hackers often with some type of political agenda.

But it isn’t just the virtual world that can be a threat. The actual physical connection can be damaged by weather, accident or deliberately. The entire internet is mostly connected through cables whether by fiber or copper, which may be above ground, underground or beneath the sea.

Protecting fiber and cable

Some cables are extremely important. If you use a highway system as an analogy, then the major freeways would be called backbones. These backbones are usually high capacity fiber cables that carry thousands of internet connections.

Other than weather-related issues most cable damage is caused by accident. The most common is from construction companies that don't check on the presence of underground cables before they dig. Because backbones are so important they are often buried underground and if damaged a huge number of customers may be affected.

Other culprits include squirrels who love to chew through the protective coating around fiber cable and vehicles that collide with utility poles bringing down overhead cabling. But not all damage is accidental.

Copper cable is quite valuable and thieves will steal large quantities of it. They sometimes mistakenly think fiber is valuable if cut into segments. Although a single fiber strand is capable of carrying a huge amount of data, it does so through a pencil-thin cable that is relatively simple to cut.

Vandalism and sabotage accounts for some of the deliberate damage. It's important to protect the termination point of an internet cable by installing it in a secure lockable enclosure that will also protect it from the elements. Burglars may also seek to cut the internet cable as it often carries security signals as well as communications.

There's also concern about the presence of Russian submarines and spy ships in areas where there are vital undersea cables. If these cables were attacked it could cripple global internet communication. With tensions building for some time, the worry is the Russians may sever cables at the most difficult-to-access locations. Meaning the damage could take quite some time to repair.

Terrorist attacks can come in the form of cyber warfare or damaging critical infrastructure. Although a lot of effort is put into protecting data, essential cabling requires the same attention.

Smart Homes and the Dark Web

How do you ensure your customer's smart home is protected beyond the physical boundaries of their house? Simple. Send them to the dark web.

The dark web is part of the deep web, and your customers use it almost daily. The deep web is a part of the internet that you can't find with search engines like Google or Yahoo. Anything that isn't indexed is part of the deep web. Any site or application that requires a password to access or that exists behind a paywall is part of the deep web. Your customer's bank account, for example, is in the deep web. Your customers access the cloud controls for their smart home in the deep web.

The dark web, also known as the darknet, is part of the same deep web that protects your customers' banking information. But your customers can't find dark websites using standard web browsers. And that's a good thing because there are many, many sites on the dark web conducting illegal business.

What is the dark web?

- *Part of the deep web*
- *AKA darknet*
- *Not indexed by search engines*
- *Requires a password to access*

Not all activity on the dark web is criminal, though. Journalists and activists use the dark web to share information, particularly in states where personal freedoms are restricted.

One of the elements of the dark web that's going mainstream is anonymous internet activity. Many of your customers have installed Virtual Private Networks (VPN) to protect their privacy. One of the most popular VPN options, Tor, is the main tool for accessing and populating the dark web.

Tor allows users to set up servers or websites without revealing the IP of the provider. Tor also allows internet users to conceal their location so they can access information that might be blocked in their home country and so they can share information freely.

Tor is used by businesses wanting to keep their procurement practices private, NGOs wanting to protect the safety of their volunteers and even by a branch of the US Navy.

And Tor can hide your customer's smart home from would-be attackers.

Recently, the Guardian Project, a Tor partner, announced the development of a technique to use Tor to protect internet of Things (IoT) devices.

Tor can be installed on a Smart Home Hub running HomeAssistant, an open-source home automation platform. Nathan Frietas, director of the Guardian Project told Wired Magazine that this transforms an "internet-of-things hub into a hidden service."

The Tor setup for Smart Home hubs goes a step further by turning the hub into an authenticated hidden service.

With an authenticated hidden service, no user, no hacker, not even Tor’s intermediary computers, can be routed to the server without a passcode. This means your customer’s smart home hub is protected not only with passwords and encryption, but it is also invisible. Intruders can’t breach what they can’t see.

Tor provides instructions for anyone interested in employing Tor for IoT security setup, and the organization is hoping to work with IoT vendors to provide safe hubs for IoT devices.

The drawback to the Tor system is that it is more complicated to set up. And, let’s face it, your customers may not like the idea that their best protection is to hide in the same location criminals are using. But the added security may be worth it. The idea is definitely worth checking out.

How Virtual Private Networks Protect Your Customers

These days, internet security is a top concern for your customers. As their broadband installer, you provide their first line of defense by supplying lockable enclosures that secure the network against physical threats. You also connect them to online protection provided by their internet service provider. But some of your customers need additional security tools like Virtual Private Networks (VPNs).

As more people work remotely, run businesses from home and use mobile devices to access smart home controls, more information travels the public internet where information is vulnerable to a variety of attacks.

A VPN is a virtual version of a secure physical network. VPNs use encryption and other security measures to protect your customers' data. It will also hide the IP address of the user, sharing only the IP address of the VPN.

VPN setup:

- *On a single device*
- *On a network using a PC*
- *Using a dedicated VPN router*
- *Delivered via a 3rd party*

VPNs can be set up on a single device, on a network using a PC or a dedicated VPN router, or they can be delivered via a third party. To make the right choice, your customers should know a little about how VPNs work.

The most important feature in selecting a VPN is the encryption protocol. Some VPNs use proprietary protocols. The rest will use one of the following methods:

Point-to-Point Tunneling Protocol (PPTP)

PPTP has been around since dial-up networks were common. Supported by all of the common PC and mobile operating systems, it's easy to set up. It doesn't use a lot of processing power, so it's fast. But, this is the least secure protocol.

Layer 2 Tunneling Protocol (L2TP) internet Protocol Security (IPSec)

L2TP is usually paired with IPSec for encryption. This protocol pairing works with all major operating systems, and no known weaknesses exist. It's relatively fast, but it has difficulty operating with firewalls.

OpenVPN

This technology combines protocols. It’s considered very secure, and is widely supported by third party software. OpenVPN is slower than other protocols, and it’s complicated to set up.

Secure Socket Tunneling Protocol (SSTP)

SSTP is a proprietary protocol developed by Microsoft. Considered as secure as OpenVPN, it’s a good option for anyone working in a Windows environment.

How to choose?

Your customers first need to consider whether they need a VPN at all. If they use their devices on public Wi-Fi in hotels or cafes, they should consider a VPN.

If they access home files from these locations, a VPN is a must. The same goes for your customers conducting business over the internet.

For personal use, L2TP/IPSec may offer enough protection. OpenVPN is better, but your customers may compromise on speed. For a Windows machine, SSTP is a solid option that requires no additional software purchase.

Business internet users should work with their IT department to select the right VPN. They should avoid PPTP, and L2TP/IPSec is not an option if their business network uses a firewall.

VPNs can spy

A VPN service is a great option for many of your customers, but one thing they need to keep in mind is that a commercial VPN will protect them from outside attacks, but nothing is stopping their VPN from spying on them.

Whether your customer opts for a VPN or not, make sure their network is protected against wear and tear by using the best structured wire management and network housing options.

Data Security and the Smart Home

High-profile events like the WannaCry Ransomware attacks get people thinking about the safety of their personal data. Those who live in smart homes – or are considering buying smart products – may be worried about the potential security threat.

Their concerns are valid. Smart devices are typically part of the home WiFi network, utilize cloud software and connect to your customer's phone. While cyber criminals are unlikely to be interested in your customer's temperature control data, if they can use that data pathway to access financial or other sensitive data, they will.

According to a report by Accenture, 47% of consumers cite security and privacy concerns as a reason to not buy smart devices. Given that the global cost of cybercrime is more than $600 billion in 2017, it's in everyone's best interest to work toward more secure devices and processes.

How to protect home data:

- *Secure the home network*
- *Segregate devices*
- *Use security software*
- *Secure smartphones*

Fortunately, people in a position to actively protect data are also thinking about security. Businesses are always striving to enhance their security, of course, but legislation helps to ensure that their efforts continue. The European Union (EU) seems to think so.

The EU established Data Protection Act (DPA) in the 1990s, but that legislation was drafted in a time when only large corporations had the resources to process or transport personal data. To deal with the increase in data use, they are replacing the DPA with the General Data Protection Regulation (GDPR).

The GDPR took effect in May 2018. What's important about the GDPR is that there are serious consequences for data processors responsible for a breach. The fines can be as high as 5% of global revenue or €100, whichever is higher. Any company that touches personal data has a responsibility to protect it under this law.

The fines are scaled based on the type of breach and how the company handles it. So a company with the appropriate measures in place would receive a lesser fine for a breach.

This is great news for the smart home, and not just the EU smart homes. This law will affect any company that touches EU data, so it will impact everyone. Any organization that offers online services will need to be compliant, as will any company wanting to do business with the EU market. Consumers in the rest of the world will benefit from improved security measures.

Improved security should generate greater levels of consumer confidence in terms of smart home features. And that's good for anyone delivering smart home services.

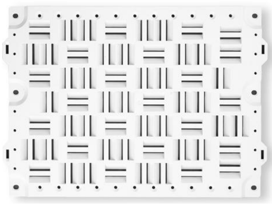
But your customers should not depend on others to protect their data.

Here are some things they can do to protect their home data:

1. **Secure the home network**
   Use a router with a firewall and set up WiFi protected access (WPA2) encryption protocol. Change the pre-set user name that comes with the router.
2. **Segregate devices**
   Your customer's WiFi gateway may allow for different network identities. It's a good idea to have the devices used to access banking and other sensitive information on a different network than smart home devices that may be vulnerable.
3. **Use security software**
   Even if the network is secure, your customers should use security software to protect their laptops, tablets and smartphones.
4. **Secure smartphones**
   Your customers use apps for their smart home and their banking. These devices need to be secure. The first line of defense is a good passcode and setting for the phone to lock after a few minutes of inactivity.

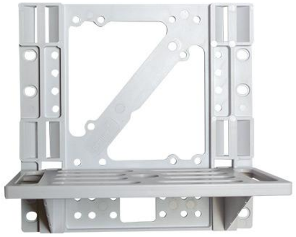
Resources

Smart Home Mounting Systems



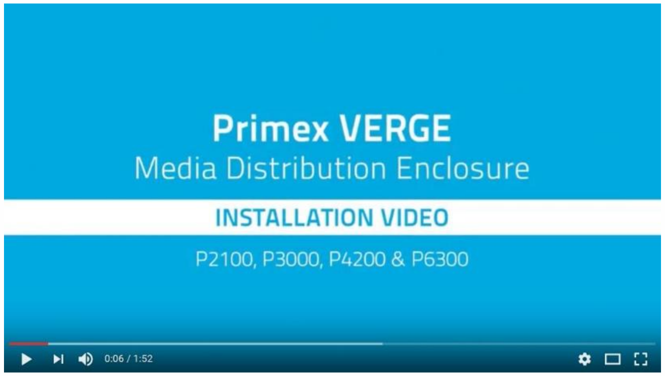
Universal Mounting System

Rail Mounting System



Shelf Mounting System

Watch Installation and Demonstration Videos



Primex VERGE
Media Distribution Enclosure
INSTALLATION VIDEO
P2100, P3000, P4200 & P6300

Blog THE SWITCH BLOG

eNewsletter Sign up for The Switch

Social:

Website: www.primex.com

Contact: www.primex.com/contact

Toll Free Tel: 1 (877) 881-7875

primex Fit everything. Together.