WHITE PAPER

McAfee
Together is power.

Protecting the Home Front

Defending the variety of devices in increasingly connected homes

Protecting the Home Front

Defending the variety of devices in increasingly connected homes

You Are Not Home Alone

McAfee® Secure Home Platform is the guardian of the home galaxy, protecting every device in a home network from Internet threats. Not just another home improvement appliance, Secure Home platform is integrated with the customer's home router, and combines the best of router-based gateways, cloud-based threat intelligence, and mobile management. Attacks are blocked locally, informed by real-time global threat intelligence, and controlled by a mobile app that makes security approachable.

Can you identify every connected device in your home? Starting the list is easy. There are some computers, several phones, a tablet or two, and a game console. Then you add the smart TV, streaming video box, and a cable company's set top box. There is of course a router connecting all of these to the Internet, one or more Wi-Fi access points, and maybe a network-connected backup disk or two. Don't forget the webcam, thermostat, and video doorbell. Maybe your alarm system is Internet-accessible, the garage-door opener, or a door lock? The count is probably 10 or more connected devices in many homes, and we haven't even started on the toys yet.

In the next few years, the average number of connected devices is going to more than quadruple, as manufacturers add Internet connectivity to everything from faucets to fridges, and introduce new devices we have not yet thought of. Many manufacturers are adding connectivity with little or no experience in networking or cybersecurity, releasing products with multiple vulnerabilities and painfully re-learning the cybersecurity lessons of the last 20 years. As a result, the likelihood of a successful exploit against a connected home is rising to almost 100 percent.

The good news is that, unlike almost every large organization, homes are not being constantly hammered by attacks. The bad news is that most home networks have only a minimal set of defenses enabled, and attackers only have to find one vulnerable device to gain entry. That could be anything like a default admin password on a webcam, an open Bluetooth link, older software on a router, or an accessible command line on something you did not even realize was sending data back to the manufacturer.

Guardians of the Home Galaxy

Protecting the connected home means protecting each and every device at home from a wide range of attacks. In addition to the well-known threats of computer malware, there are digital peepers trying to gain access to your video feeds, simple hacks that can open your digital door lock, and privacy snoops that want to know if you are home based on your thermostat or alarm-system.

There is also a large and growing group of adversaries that want to take control of any accessible devices in order to amass a legion of bots capable of attacking organizations and disrupting their business. Installing, configuring, and maintaining security against these threats is well beyond the capabilities of most consumers, and they are looking for someone or something that will help keep them secure. While many organizations are working on this, from software start-ups to traditional cybersecurity vendors, it is often the home's Internet service provider that is the first point of contact.

Making House Calls

Malware often slows down infected devices, and compromised devices that have been turned into bots can consume a significant portion of a home's bandwidth. Either way, when things are not working as expected, consumers see this as an Internet problem and will call their ISP's support line for help. Some may do a speed test, and note that their measured network speed is nowhere near their subscribed rate. The ISP support agent looks at the modem or router, sees that it has normal signal strength, but cannot see past the router into the home network. Maybe they try a reset or dispatch a technician for a house call, but either way they cannot diagnose the problem with their available tools. Even if the ISP has network-based equipment that can detect whether something in a home is compromised and participating in a botnet, because they see the home as only a single IP address, there is no way for them to tell which devices are affected.

An Internet Home Companion

With these concerns, why are more people not using existing security controls? Firewalls are built into most routers, and parental controls that enable blocking of malicious or suspicious websites have been around for at least 10 years. Sure, most people have some type of security defenses on their computer, but even that is usually left on the default configuration. The reason, of course, is that effectively configuring these tools is very complex, and beyond the knowledge of most consumers. While parental controls can be complicated to set up, the major reason parents found them ineffective is they did not cover all devices (e.g. game consoles), and children could circumvent, uninstall, or work around them. These are addressed by putting the control in the router. What's more, none of these configurations are effective if they are treated as a one-time, file and forget activity. Malicious websites are constantly changing URLs and IP addresses, new attacks are emerging every day, and the list of software vulnerabilities is frequently updated. Large organizations have multiple full-time staff dedicated to keeping track of cyber threats, an option that is simply not available to consumers.

Defending the Homeland

Effectively defending the home requires a mix of abilities to detect attacks, protect devices that are unable to protect themselves, and quickly correct intrusions or infections before they can cause serious harm. On traditional computer devices, security software has been reasonably effective at providing the necessary defenses, assuming it is correctly installed and frequently updated.

But it is not possible to install security software on most of these new devices, such as cameras, TVs, and home automation gear, and most people do not even get around to changing the default admin password.

Since most manufacturers of these smart devices are not incorporating advanced security functions into the software, and there is little or no capability to install 3rd-party software on them, it is critical to protect them at the home network level. This method delivers several important benefits to everyone and everything in the house. First, protection is immediate, detecting and preventing attacks at the earliest possible point in the home network. Second, it applies to all devices, from the smallest home sensor to smart TVs, game consoles, tablets, and smart phones. Third, it has a very low impact on users and home network performance, using the processing capabilities of the home router and the cloud to inspect and evaluate traffic.

Home and Away

These protections also need to extend away from the home, as people go out with their smart phone, tablet, and laptop. On-device security acts as a valuable complement to network security, creating a unified solution for the home user, regardless of location.

Why Secure Home Platform?

The McAfee Secure Home Platform is directly aimed at bringing enterprise level security into the home and protecting the entire home from attack. This product and service combination follows three key principals of usability, intelligence, and cloud-based performance.

Home Improvement

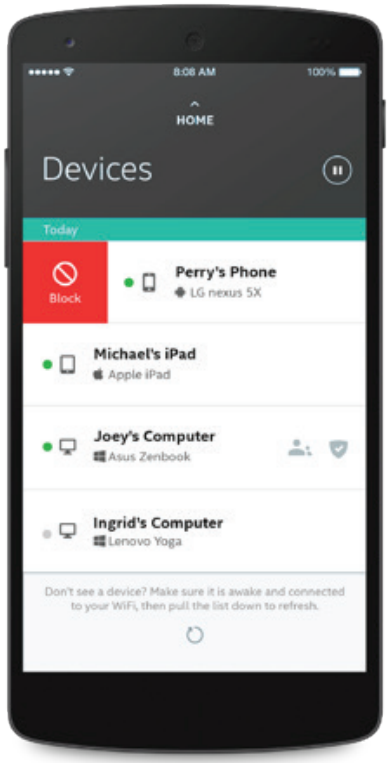
Since there is no home IT department, and since security is not a one-time activity, the Secure Home Platform has to be usable by virtually everyone. We considered the needs and abilities of a wide range of people when designing and implementing the controls, and focused on removing the typical headaches that security management can create.

Not Another Home Appliance

First, these functions are incorporated directly into the home router, precluding the need to install yet another box at home and reducing support complexity. McAfee has partnered with several router manufacturers and ISPs to add Secure Home Platform directly to their products. We specifically did not want to add another layer of complexity to the system, preferring to work with existing experts to produce the ideal combination of routing and security.

Home Button, not Home Page

Second, the configuration must be readily accessible, so we did away with complex router screens in favor of a mobile app. With the Secure Home Platform Mobile App, consumers have easy access to a variety of features such as parental controls, device identification, and internet pausing. People can quickly see what is on the network, provide nicknames for regularly connected devices, and the system will even suggest a name as it learns the behavior of a newly-authorized device. They can also receive real-time alerts through the app about things like potential vulnerabilities, new connected devices, and parental control violations.



Getting Engaged at Home

Third, since security is not a file and forget activity, the tools have to keep the user engaged. So, if something new shows up, you get prompt notification that a new device has joined the network, along with some identifying characteristics such as the manufacturer's name, model number, and device type. You can change the name right away to a more representative nickname, like "doorbell camera". If you don't provide a name, as time goes by the system will get a better idea of what the device is and assign a category to it, for example webcam or thermostat. Regular engagement like this, through timely notification of events, keeps users actively aware of and regularly updating their network security. This is a valuable tool for identifying if unauthorized people are using the home network, or when a family member adds a new device.

Home Intelligence

The Secure Home Platform continually monitors traffic from all of the devices on the net, establishing a "fingerprint" for each one based on its regular activity. This helps to identify suspicious or malicious activity early, before something is compromised.

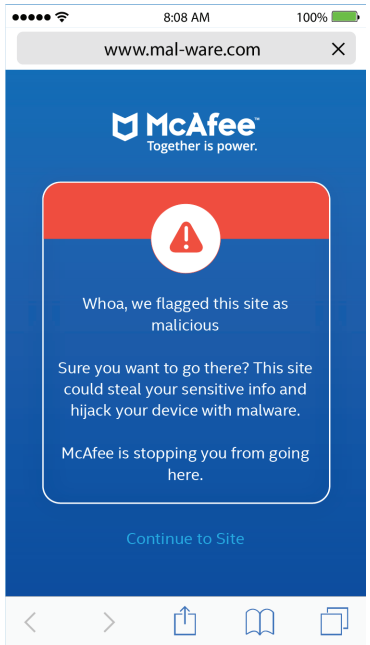
Fingerprinting starts when a new device is first detected, and this works for any device that uses an IP address. There is no need for the Secure Home Platform to test or pre-certify devices to improve their security. McAfee is working with router manufacturers to gather as much data as possible about the device and expand this fingerprinting capability, using common protocols such as Universal Plug and Play (UPnP) and Bonjour.

For example, Apple iOS is pretty good at blocking malicious activity, so most people do not install additional security on their iPad. However, a phishing email attempting to capture a banking password will often get through to the mail app. Our research shows that 33% of people are still opening phishing emails, and 13% of those actually click on the links. This is a better click through rate than many marketing campaigns! Secure Home Platform will block the link with a clear visual that tells the user "you shouldn't go there".

Behaving at Home

Another risk point is the flood of Internet of Things devices being added to the home. Many of these devices do not have their own screen to display a warning. Luckily, most have very simple and predictable behavior. For devices, such as a nanny cam or video doorbell, Secure Home Platform will get to know the regular usage pattern – what sites or addresses it talks to, what type of traffic does it usually send, and how much? If these change suddenly, or if the device attempts to connect to a known malicious site, Secure Home Platform will block the traffic and send an alert. The mobile app will pop up a warning that "your nanny cam has been compromised", automatically block the device, and quickly allow the user to keep it blocked or allow the device back on the Internet.

There are currently no widespread standards for these devices, and the rapidly growing IoT population makes protecting them a big challenge. McAfee Secure Home Platform's protections are based on the device's IP address, removing the need for interoperability tests or certifications. If a device uses an IP address, Secure



Home Platform will see it as soon as it joins the network, start to fingerprint it, build a profile about it, and determine normal behavior. If or when an anomaly is detected, the device is immediately isolated from the network to minimize the potential damage.

No Home Bots

Compromised devices being used as bots is probably the biggest threat to most connected homes. Many people are more concerned about ransomware attacks or privacy violations, but bots are a big concern for router manufacturers and ISPs. The average upload speed for North American homes is about 7.6 Mbps. The average upload speed during a bot attack is 7 Mbps, or more than 90% of the home's available bandwidth. Secure Home Platform will be able to detect this sort of activity, isolate the devices that are compromised, and notify the user through the mobile app to take appropriate action.

With so many different devices, there is a wide range of distribution methods and attack vectors for malware. Preventing all devices from all attacks is not feasible, so the focus is on rapidly identifying compromised devices, stopping them from infecting any other devices, and preventing any further harm to the home, the ISP's network, or the general Internet. These actions serve to protect the entire chain, from home owner to router manufacturer to ISP from the potential damage and liability of a rampant botnet using their devices and networks to attack others.

Home in the Clouds

Since the threat of attack is primarily from the Internet, and the router is always connected to the Internet, it made sense to put the primary security functions in the router. Since effective security requires a continual stream of up-to-date intelligence, and also requires more processing capability than most home routers have available, it made sense to put the supporting functions in the cloud.

Many routers include firewalls and filtering rules that are rarely used, and even less rarely updated. They also require the occasional firmware update to fix a vulnerability or add a new feature. Unfortunately, very few people even know this capability exists, let alone how to update the firmware. And without proactive notification of updates, fewer still even know when an update is available.

Up-To-Date Security

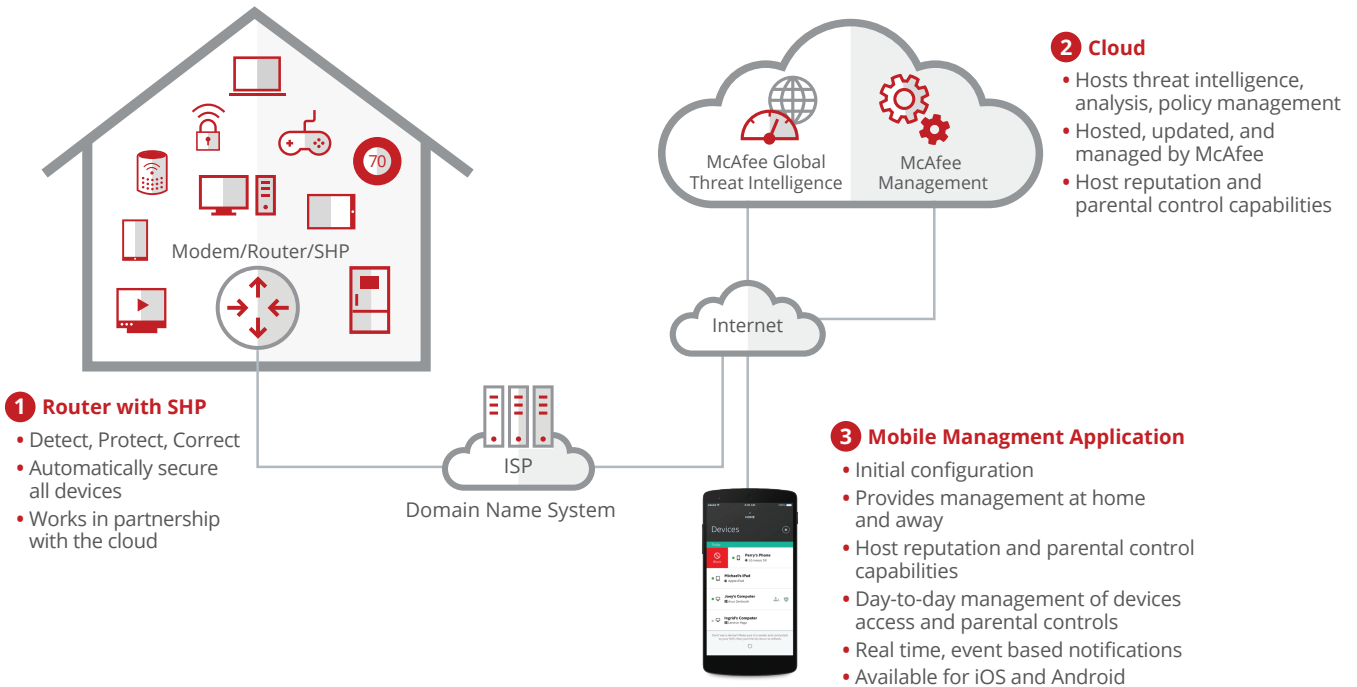
Moving this functionality to the cloud removes the requirement for updates, as the McAfee Global Threat Intelligence (GTI) database provides up-to-the second security for everybody. This McAfee service is the newest thing that you have been using for years, as it has been delivering threat information to consumer and enterprise security products for more than eight years. Global Threat Intelligence is at the core of McAfee's enterprise products and services, and benefits from a broad set of sensors and services at large organizations, many of which are under constant attack. Details on evolving and emerging threats are instantly available and applied to everyone, so that the home now has the same security benefits

as a large government organization or major financial institution. To give you an idea of the scope of this service, Facebook gets about 43 billion visits per day, while GTI processes more than 47 billion queries each day.

Secure Home Platform is made up of three components working together to deliver the best combination of local security, cloud services, and mobile management. The code on the home router is responsible for identifying local devices, fingerprinting behavior and identifying suspicious activity, and enforcing the desired restrictions. Cloud services provide threat intelligence and parental controls, using enhanced DNS to find out the security status and classification of sites from McAfee Global Threat Intelligence. The mobile management app enables easy configuration, day-to-day management, and real-time notifications. Since the app is connected to the cloud, the user can monitor and control their home network security anywhere in the world that they have an Internet connection; they do not have to physically be at home.

Three Components Working Together

Combining the best of gateway, cloud-based security, and mobile management



1 Router with SHP

- Detect, Protect, Correct
- Automatically secure all devices
- Works in partnership with the cloud

2 Cloud

- Hosts threat intelligence, analysis, policy management
- Hosted, updated, and managed by McAfee
- Host reputation and parental control capabilities

3 Mobile Managment Application

- Initial configuration
- Provides management at home and away
- Host reputation and parental control capabilities
- Day-to-day management of devices access and parental controls
- Real time, event based notifications
- Available for iOS and Android

Performing at Home

These cloud services offload much of the security workload from the home router, enabling enhanced security without impacting performance, and adapting to new threats and zero-day attacks without requiring firmware updates or database downloads. Looking up threats in the cloud database, evaluating suspicious traffic, and other network security functions typically require high performance devices, which are not feasible for a home or even for most ISPs. Putting these functions in the cloud ensures that there is little or no performance hit to the home router or the ISPs equipment, and the service can scale up or down as needed, based on demand. Many enterprises are adopting this model of cloud-enhanced security, and the same benefits are now available to consumers.

Home, Sweet Home

Secure Home Platform automatically protects internet-connected devices on your home network from a variety of threats. Attacks are blocked at the router level, delivering robust security features that can be controlled from an easy-to-use mobile app. Regular engagement makes everyday users security experts for their own home, and gets people thinking about security in a positive way. The mobile app makes security more approachable, giving users a sense of control over their home and its connected devices.

Placing multiple layers of security between you and hackers or cyber criminals significantly increases the level of protection. Secure Home Platform also automatically identifies devices on the network that do not have antivirus functions installed or turned on. Combining McAfee Secure Home Platform with device-based protection, such as McAfee Antivirus, helps to create defense-in-depth for the home, a security best practice followed by most enterprises. With Secure Home Platform, consumers can enjoy enterprise-level security without the cost and management requirements.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

3661_1017_us_wp-protecting-the-home-front
OCTOBER 2017