wightfibre
because we care

WightFibre Smart Home Guide

A Different Kind of Broadband • Full-fibre • Ultrafast • Future-proof

Executive Summary

WightFibre has created one of the best broadband networks in the world providing domestic and business customers with future-proofed ultrafast, full-fibre, internet access.

With such fast broadband speeds, expanding WiFi coverage throughout the whole home or business premises has never been more critical. But more than that, the explosion of wireless portable devices, smart appliances, home automation and the “Internet of Things” (IoT) not only need to be connected but they also need to be looked after and monitored for reliability, safety and security.

This white paper explains how WightFibre’s state-of-the art network, combined with the facilities offered by Plume HomePass which is available to all WightFibre customers, create the very best and secure environment not only for PCs, laptops, tablets and phones, but all of the smart devices in a customer’s home.

Introduction

Smart homes are no longer just the dream of “early adopters”, but now almost everyone can buy affordable smart home devices, from lighting, heating, speaker systems, digital voice assistants like Amazon Alexa and Google Home, smart TVs, kitchen appliances and even toys.

This brings challenges to the home as you now need good WiFi everywhere in the home coupled with first class broadband for the smart devices to work reliably and you also need confidence that they are operating safely and securely.

This is where the WightFibre eco-system combining future-proofed ultrafast full-fibre broadband coupled with Whole Home WiFi becomes essential together with the HomePass App for monitoring and controlling access.

Section 1 describes the rapid growth and diversity of smart home devices and their demands on the WiFi they are connected to.

Section 2 describes the solutions available to deliver WiFi to all the smart devices wherever they are in the home and how Plume HomePass from WightFibre can deliver WiFi throughout the home.

Section 3 looks at the often overlooked subject of Smart Device Security and how Plume HomePass from WightFibre can secure your home network.

SECTION 1
- The State of Play of Smart Home Technology

Smart homes are no longer just the dream of “early adopters”, but now almost everyone can buy affordable smart home devices, from lighting, heating, speaker systems, digital voice assistants like Amazon Alexa and Google Home, smart TVs, kitchen appliances and even toys.

This brings challenges to the home as you now need good WiFi everywhere in the home coupled with first class broadband for the smart devices to work reliably and you also need confidence that they are operating safely and securely.

This is where the WightFibre eco-system combining future-proofed ultrafast full-fibre broadband coupled with Whole Home WiFi becomes essential together with the HomePass App for monitoring and controlling access.

Section 1 describes the rapid growth and diversity of smart home devices and their demands on the WiFi they are connected to.

Section 2 describes the solutions available to deliver WiFi to all the smart devices wherever they are in the home and how Plume HomePass from WightFibre can deliver WiFi throughout the home.

Section 3 looks at the often overlooked subject of Smart Device Security and how Plume HomePass from WightFibre can secure your home network.

Challenges for Internet Service Providers

The soaring growth in smart technology is leading to a change in expectations of customers and coupled with the surge in technology use during the COVID lockdowns, customers are discovering more ways to use their broadband and their in-home WiFi. They’re using new and more devices to access voice, video and data services and adopting new technologies that stretch the traditional broadband and WiFi router solutions.

At the same time the growth of cloud-based services including cloud-based services coupled with smart devices is increasing the demand still further.

Meanwhile, customers are less reliant on traditional phone lines with mobile and Voice over IP (VOIP) providing more flexibility and ease of use, whilst traditional cable and satellite TV are being displaced by streaming services.

Challenges for WightFibre's Competitors

Traditional Communication and Internet Service providers (CSPs and ISPs) have built their business on hardware and infrastructure; in fact in the UK, most are relying solely on re-selling the legacy Openreach infrastructure with their own WiFi router, customer services and price as the only differentiating factor. This platform arguably isn't flexible and agile enough to adapt to the rapidly changing demands and growth in the smart home market and as issues become more device specific, their customer services become less able to give the support required.

Additionally, many of these resellers offer a basic WiFi router which often can only provide a good signal in the immediate vicinity of the router itself leaving the customer to find WiFi extender solutions. Even where the provider does offer "whole home" guarantees this is often through the provision of basic WiFi mesh devices rather than smart WiFi systems.

WightFibre's partner Plume has noted the challenges to traditional operators have lead to more competition fighting for the same pool of customers, declining earnings, lower returns on investment and a continued battle to control costs and optimise existing business systems rather than to upgrade to the new age.

What are the Solutions?

A real solution to these challenges requires new models and strategies built on digital, smart home thinking. Such an approach demands putting a priority on technologies that can achieve the following:

Achieving these goals offers obvious and dramatic benefits which WightFibre can pass on to its customers:

- Improved business efficiency and innovation.
- Transformation with a new focus on software-defined services.
- Flexible, network-agnostic technologies for smarter and more reliable connectivity.
- Data-driven insights into networks, devices, and customer usage.
- Personalization of products, services, and customer experiences.
- Open-source software that can scale rapidly across both deployed and new hardware.

Achieving these goals offers obvious and dramatic benefits:

- Better efficiency means more resources for building the business and benefiting the customer
- Digital business brings flexibility, agility, and scalability. Smarter connectivity makes services easier for customers to deploy and use.
- Data-driven insights allow customer support teams to identify and resolve technical issues more quickly.
- More data on user behaviour and usage patterns also allows customers to be offered better, more tailor-made, personalized offerings.

Why WightFibre is the Choice

WightFibre combines its new, future-proofed, ultrafast, full-fibre, internet access network with an intelligent Whole Home WiFi Product powered by partner Plume.

WightFibre's Smart Home WiFi ecosystem is powered using Plume's OpenSync technology and products meaning WightFibre can deliver an entire suite of world-class Smart Home Services at scale, whilst continuing to add the latest services almost instantly.

Customer support is improved through Plume's Customer Experience Management Platform which provides back-end analytics, machine learning and AI to not only spot problems before customers notice them but also provide support tools and rapid troubleshooting.

HomePass, an award-winning Smart Home Services Suite, is managed by the Plume Cloud, a data- and AI-driven cloud controller currently running the largest software-defined network in the world. With HomePass, WightFibre can quickly and easily deliver a wide range of Smart Home Services to customers:

- **Adapt:** Flawless, self-optimizing WiFi that responds to usage patterns.
- **Control:** Seamless guest access including custom passwords, parental controls, and the ability to freeze internet access when appropriate
- **Guard:** AI-powered cyber-security that monitors online activity in real time, protecting against hacks, filtering suspicious data, and automatically blocking and quarantining suspicious content.
- **Sense:** Transforms network-connected IoT devices into home-based motion sensors for whole-home awareness.

Adapt provides the foundation for the WIghtFibre suite of Smart Home Services. Unlike traditional mesh WiFi systems, **Adapt** is deeply distributed throughout the home, and delivered as a cloud service that continuously adapts to the needs of the home and its occupants. Powerful and self-optimising, it provides continuous monitoring to avoid interference with other nearby networks and uses multiple channels for increased network capacity. Routing algorithms also help to balance network loads and optimize the performance of applications on every device, in every room of the house.

As a cloud-based service, **HomePass** can deliver new features and upgrades to customers as soon as they become available.

The HomePass mobile app makes it easy for customers to get set up and enables them to monitor and control their home network and devices remotely.

SECTION 2
– Smart WiFi for Smart Homes

People are transforming their homes into smart homes. They're adding smart devices of all kinds: from voice assistants and connected home hubs to smart thermostats, security systems, door locks, lights, doorbells, appliances, and more. With so many more networked devices in the average home, people need reliable, high-capacity WiFi more than ever. They want all their smart devices to work and deliver their favourite services as expected, whenever they're needed. But even the most advanced smart devices won't deliver on their promises if WiFi connectivity isn't up to the job. After all, what's the use of having multiple state-of-the-art devices—4K smart TVs, internet-connected exercise equipment, advanced gaming consoles, webcams for teleconferencing, etc.—if they can't all work in harmony?

WiFi's Smart Home Challenges

While WiFi isn't the only way to connect devices in a home, it's the most common. There are, however, many potential obstacles that can prevent WiFi from working as effectively as needed for smart home applications and so t's critical that WiFi is built on a rock-solid foundation that can support such services.

Physical barriers

WiFi signals can be weakened or even wholly blocked by objects or structures between a wireless router and a smart home device. These can include everything from brick or concrete walls, modern insulation, large mirrored surfaces, heavy doors, or even radiators and heating systems and microwave ovens.

Distance

The greater the distance between a traditional wireless router and a device, the weaker the WiFi connection is likely to be. A larger house, or one with several floors, is likely to experience unreliable smart device connections. Enabled devices outside, whether these are lights on a garage or security cameras in the garden, or even Electric Vehicles being charged can also struggle to maintain WiFi connectivity.

Interference

WiFi signals in one home can also interfere with signals in neighbouring homes, creating performance issues affecting a large number of residences. This is especially prevalent in the "old" 2.4GHz band where there are really only three fully separate channels available that don't overlap with other channels. Even in the 5GHz band the Isle of Wight has special challenges as many 5GHz channels can suffer from interference from marine radar near the coast.

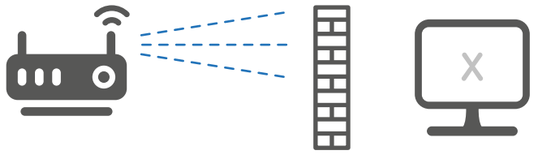
Technical issues

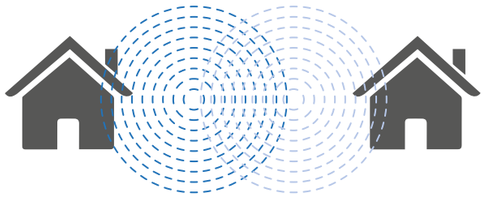
A wide variety of technical problems can prevent WiFi from performing as well as it should in a home. With some cheap routers, for instance, WiFi signals in the 2.4 GHz band can bleed over into the 5 GHz band, reducing capacity in both.

Security

Another challenge is ensuring that all connections across a smart home are secure, so no device is at risk of being hacked.

WightFibre's partner Plume quotes a US report that says "just over 30% of computing and entertainment device owners report experiencing loss of wireless connectivity, with home network routers identified as the most common source of the problems.". UK domain registrar Nominet found that only 46% of adults say their home internet connection can "easily" meet their needs.





The Impact of these Challenges on Smart Home Systems

WiFi problems are annoying enough when they affect computers, laptops and smart Phones and when they affect home entertainment like Smart TVs, but they become more troublesome when they affect the performance of household infrastructure, such as appliances or heating and cooling systems.

A very common experience, for example, is the frustration of installing smart light bulbs that keep going offline when you need them, or not being able to control the heating when you need it. And what about when WiFi problems impact critical systems related to safety, like smart security devices? Just imagine the potential for connection or security failures in devices such as smart locks. Customers who use smart home devices to safeguard their homes and families need assurance that those devices will stay online and functional no matter what.

There are also configuration issues as many cheaper smart devices may only be compatible with the 2.4 GHz band. This can cause problems during the initial setup – the device is looking for a 2.4 GHz network, but there are issues because the smartphone with the App to control the device is connected to the 5GHz network with the same name – even in 2022 there are some smart devices that recommend renaming 2.4GHz and 5GHz networks to keep them separate!

Attempted WiFi Fixes

Not only has there been an explosion in growth in Smart Home devices but also due to the pandemic, many people have been working from home videoconferencing using tools such as Zoom, Microsoft Teams, and Google Meet and this has meant more people have been coming up against the limitations of their home network. WightFibre's partner Plume reports an increase of more than 100% in time spent online at home since pre-pandemic levels and load and congestion has risen even more by as much as 252%.

A common impression many people have (perhaps because traditionally the broadband connection and the WiFi is provided in one "router") is that they need to increase their broadband speed when in fact it is the WiFi that is the problem. However, when you have a fibre connection from WightFibre you can have as much broadband connectivity as you need, this can really show up weaknesses in the WiFi.

Another common approach is to opt for a relatively cheap option such as WiFi extenders. Whilst they are a relatively cheap option, they are cheap for a reason and so basic WiFi extenders can yield quite disappointing results. To work well they need to be positioned to receive a good signal from the main WiFi router as otherwise they will simply relay a poor signal (a common mistake is to put them in the part of the house you want to improve the signal in rather than bridging the gap to that part of the house). The other issue is that part of the available bandwidth is used to relay the signal and in cheap devices each "hop" typically halves the bandwidth available.

A next step beyond a basic WiFi extender is to use a "powerline" extender. These plug-in devices attempt to use your mains network instead of high-speed network cables. In small properties with a single ring main these can work fairly well, but it needs to be remembered that clever as they are, domestic wiring simply isn't designed to carry the high-speed signals that proper twisted pair network cables are and, despite the claims of some of the newest adaptors, in practice they are found to deliver maybe half of their claim and even then only on a clean modern ring circuit. Many larger and older properties may have multiple rings and signals may not cross well between them (or even at all) and interference from other powerline systems or even things like plug in rodent deterrents can scramble the system.

More recently "mesh" systems have become available from multiple vendors. Many of these go some way to solve the problems above, for example using the 5GHz band as the "back channel" to avoid halving bandwidth in the 2.4GHz space, but aside from being expensive, most mesh systems are still static with each node acting independently and not coordinating with the other mesh nodes and rest of the network. This can lead to inconsistent and unpredictable performance.

Ideally what you need is an intelligent network with mesh components that are constantly learning and improving and this is where the HomePass and PlumePod solution from WightFibre's partner Plume comes in.

WiFi Quality of Experience

Traditionally, network and WiFi quality is measured by the Quality of Service or "QoS" metric. This metric uses technical data to form a view of the QoS, based on bandwidth, latency (often known as ping), jitter (the variations in latency) and error rate. Whilst this is valuable it doesn't recognise that different devices have different requirements and actually user perception of experience of using a device is arguably more important.

WightFibre's partner Plume has developed a more comprehensive metric called Quality of Experience (QoE). QoE takes into account a much wider range of data points and recognises that not every smart home device has the same requirements. For example, scrolling through social media feeds or dimming a home's smart lights requires a lot less bandwidth than video conferencing; and keeping a smart speaker connected and available puts much different demands on a home network than does streaming a full-length UHD movie.

Without some way to manage all of those devices and connections intelligently, it's more likely that performance glitches will be encountered if there are multiple demands at the same time—say, reading tweets and asking Alexa to adjust the living-room temperature while watching Netflix on a laptop. Traditional WiFi extender solutions described above can't ensure such glitches won't happen.

WightFibre's suite of smart home services powered by Plume and back-end services are underpinned by Adapt, Plume's self-optimising WiFi to address these challenges.

Adapt by Plume from WightFibre

WightFibre's partner Plume developed its adaptive WiFi technology with the future of smart homes in mind. With **Adapt**, WightFibre can easily and quickly solve traditional home WiFi problems without the downsides of other solutions like repeaters or static mesh paving the way to providing customers with a great ecosystem for running their smart home devices.

What it Does

Adapt uses intelligent algorithms to ensure that device connections throughout the home adapt continuously to changing conditions and user behaviour. With non-stop monitoring and channel-hopping, as well as band-steering capabilities, **Adapt** prevents interference with nearby networks and increases a home's networking capacity. It also optimises traffic loads and application performance based on each device's specific requirements and QoE score.

This is enabled by **OpenSync**[2] , cloud-agnostic software for delivering, curating, and managing home connectivity and entertainment services. Originally developed by Plume, OpenSync7 was made open source in 2018 through a silicon-to-service framework founded by Samsung, Comcast, Bell Canada, Liberty Global, and Plume.

By communicating intelligently with every Plume Pod or OpenSync-enabled access point (AP) in the home, **Adapt** ensures that every node works as efficiently as possible. And it directs each device in the home network to the appropriate pod or AP for the optimal route topology.

In this way, **Adapt** ensures the high performance of connections and devices throughout the home, no matter when those connections are needed and no matter where those devices are located.

How It Works

Unlike the traditional solution using a single WiFi router, **Adapt** provides distributed WiFi coverage via a variety of access points such as Plume Pods placed around the home. This enables each AP to be optimally placed, resulting in the overall network being able to reach every device, no matter where they are and no matter what the home's size.

Plume Pods are smaller and lower-power than a traditional router and can be readily plugged into any convenient power socket reducing the distance between nodes and meaning that they can operate at a lower power, whilst still eliminating WiFi dead zones and zones with degraded signals.

Because "Adapt" is delivered by WightFibre through the Plume Cloud, software updates and security patches are fast and seamless.

Advantages over other WiFi systems

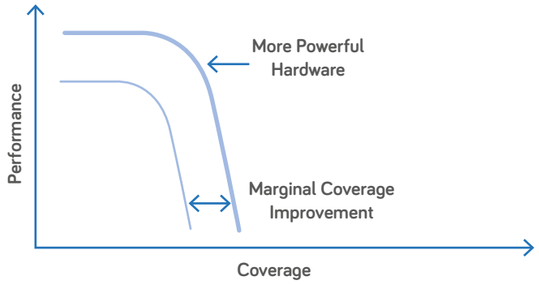
There are many advantages of Plume from WightFibre:

- Intelligence: All the Plume nodes are managed through a cloud-based system that uses AI, data analytics, and optimization algorithms to keep home networks as fast, secure, and efficient as possible.
- Adapatability: Plume's system continuously monitors a home's network and connections for changing conditions and demands, and adjusts accordingly to keep devices online and performing as they should. This reduces problems with interference, overloaded channels, latency, and other issues.
- Flexibility: Because Adapt makes smart home management simple via the Plume Cloud, you can easily install, add, and manage services on their own, without the need for technical support (though it is there if you want it).

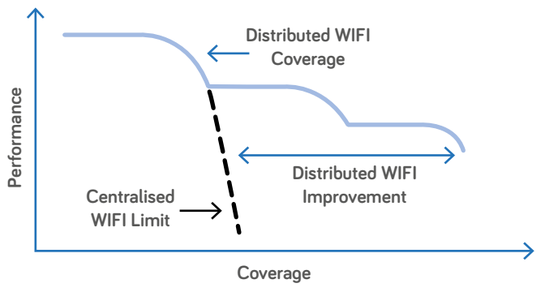
WiFi repeaters and extenders can't match any of these capabilities. Even advanced mesh systems don't provide these levels of intelligence and cloud-based control.

With Plume from WightFibre, WiFi becomes more than just a by-product of your internet connection and unlike other solutions, rather than just extending WiFi from the main router in the home, WightFibre's WiFi ecosystem powered by Plume enables you to distribute intelligent, self-monitoring, self-optimising WiFi everywhere you need.

Coverage Improvement with single WIFI Router HW Improvement



Coverage Improvement with Distributed WIFI System



SECTION 3 – Smart Security for Smart Homes

Home network security has never been more important. Customers are enhancing their homes with an increasing number of smart home devices, many of which present unknown security risks. At the same time, the nature of work is changing, with more people than ever using their homes as offices.

A home network is effectively an interconnected series of devices which requires robust protection. Unlike a corporate network, there is no professional (or team) dedicated to keeping that in-home network secure. Providing protection therefore presents challenges because of the large number of home networks, their small scale, the multitude of device types and operating systems, and the limited resources and capabilities of end-users.

Using data from its cloud-based system, WightFibre's partner Plume says that on average households have 21 devices connected to the home network. The mix varies, but, for a typical family, that number may comprise multiple smartphones, several computers (including company or school laptops used to work or study from home), tablets, video game consoles, and a video streaming device, stick, or TV.

If that family adds a smart doorbell, smart thermostat, voice assistant (estimated to number 8.4 billion globally by 2024), smart speaker, smart lights, and a home security system, the number can quickly increase. Health devices—including connected fitness equipment, such as the Peloton exercise bike, or even small ones like the Fitbit fitness tracker, or Apple Watch—are adding to the network load as they grow in popularity.

All those Internet of Things (IoT) devices connected to home WiFi represent possible points of compromise. Home users, many of whom do not have in-depth technical knowledge, are concerned about the security of their home network, but don't always know what to do. A recent survey found the leading concern about smart home privacy is hacking, at 75%. But while many customers want to protect their security and privacy, 40% of respondents said they didn't feel knowledgeable on the subject.

Consumers' top smart home security concerns

Hacking	Government spying on in-home smart cameras	Smart speakers
75%	53%	52%

Source: ADT Survey: Consumers ant cyber protection for smart homes

The Challenge to Secure your Home Network and WiFi

Broadband alone is no longer enough. As well as fast and reliable broadband, customers want and need a seamless WiFi experience in which everything they need is available.

Customers typically aren't IT experts, but they know they need a secure digital environment to protect themselves and their families. Home networks are now becoming increasingly complex and so many users don't feel qualified to implement and oversee security themselves, and although many people feel comfortable and familiar with installing virus protection on devices with screens like PCs and laptops the situation has been exacerbated by the huge growth in smart devices.

Working from home during and after the pandemic has also created a new slew of challenges and it looks like it is set to stay with many staff now being offered increased flexibility and continued home working as an option. WightFibre's partner Plume quotes CISO magazine which says:

- 30% of people working for a company at home don't use a Virtual Private network (VPN), to access the company network.
- 40% use a company-provided "dongle" to connect, whilst the others rely on home WiFi or mobile phone data for access
- The average household already using Plume devices has 21 devices connected to the home WiFi network, each one with its own vulnerabilities

This means that many people are doing business-critical work, possibly including accessing sensitive customer data, on machines connected to a network with unknown security weaknesses, and which may be populated with unvetted devices.

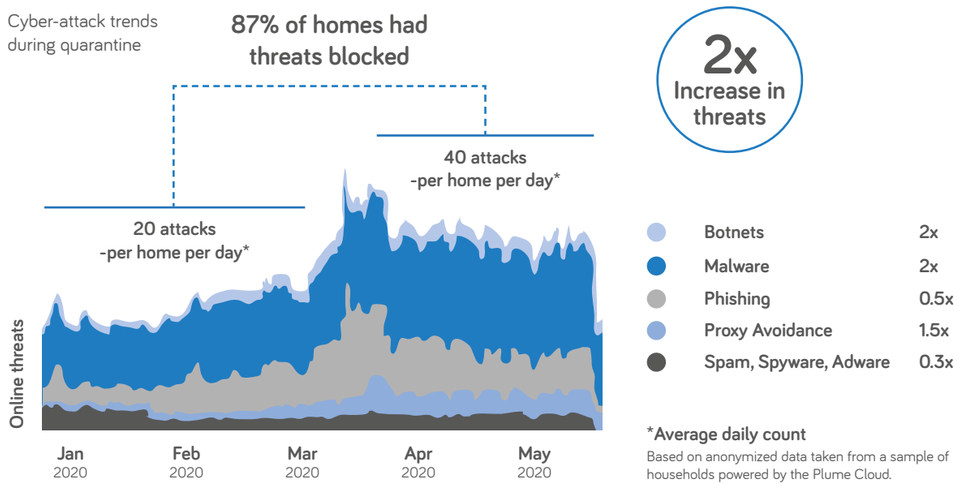
Both the UK National Cyber Security Centre and the US Cybersecurity and Infrastructure Security Agency have highlighted that the surge in working from home has encouraged an increase in "bad actors" looking to target individuals and organisations.

WightFibre's partner Plume predicts that by 2024 connected devices could grow from the current 21 or so to exceed 38 devices across all categories—computers, mobile phones, tablets, set-top boxes, voice assistants, smart TVs, printers, surveillance cameras, game consoles, and more. Each of these devices opens a unique door to potential attacks. These attacks could be from websites and the servers they connect to. They could be the result of exploiting weak or reused passwords and unpatched software, and they could take the form of targeted phishing, spam, fraud attacks, and more.

IoT devices bring a new level of threat to home networks for several reasons:

- Devices don't run through browsers but connect directly to networks
- Many manufacturers do not frequently issue patches for their devices
- Customers don't always update software, even when patches are available
- Customers don't always set secure passwords or change default passwords

Cyber-attack trends during quarantine



*Average daily count

Based on anonymized data taken from a sample of households powered by the Plume Cloud.

The WightFibre Whole Home Network Securing your WiFi

This is where WightFibre can help. Not only does WightFibre bring you reliable, ultra-fast, futureproofed broadband but using HomePass from Plume WightFibre can bring you whole home WiFi and help create a secure home network environment giving customers and their families more control and visibility of their personal IT security. All of this is powered by advanced AI and machine learning.

Using it's OpenSync framework Plume has multi-layered security and the Guard service provided as part of HomePass collects and analyses data and uses AI to predict and neutralise threats. The system is easily deployed throughout the house via Plume Pods or OpenSync enabled gateway.

Guard's AI-Powered security provides a range of features that together provide comprehensive protection:

- **Advanced device typing (ADT):** ADT technology classifies 95% of devices within minutes and ensures cloud-customized performance for each device.
- **Whole-home device protection:** AI-based global threat intelligence protects every connected device in the home from visiting known malicious destinations, as well as infection from malware, spyware, ransomware, and phishing attacks.
- **Intrusion detection and blocking:** IP-based online protection stops outside attackers from gaining access to home networks and notifies users of any attacks on exposed devices.
- **Behavioural analysis and anomaly detection: Guard's** anomaly detection uses machine learning to understand normal IoT device activity and develop a whitelist of allowable behaviours. Anomalies are reviewed and high-severity potential threats are automatically blocked.
- **Remediation and isolation:** When high-severity anomalies are detected, **Guard** automatically blocks connections and quarantines devices on local networks to prevent the spread of malicious code.
- **Security dashboard:** See what's happening in the network through various lenses, including by activity, time period, and threat type.

In addition to the tools directly available to customers through HomePass, WightFibre's Customer Services have Plume Dashboards that enables them to monitor threats and provide user support down to device level.

The great thing about **Guard** is that it provides technology-agnostic security, meaning customers can use the IoT hardware of their choice—even mixing brands—while remaining protected, thanks to Guard's Advanced IoT Protection features. These features specifically address threats to IoT devices, using behavioural analysis and anomaly protection to detect behaviour that's out of character for any device on that network. It can even quarantine the device until the anomaly can be investigated. The monitoring of IoT devices on the network, combined with intrusion protection and outbound IP protection offerings, automatically blocks high-risk IP-based interactions to and from connected home devices.

This data, in aggregate, goes into the full intelligence of the solutions, making it smarter for everyone who has Plume HomePass installed. This intelligence helps the technology better understand both user behaviour and the threats that exist online, as well as their distribution, their prevalence, and their targets. And better understanding means better, faster responses to threats. That means HomePass members get better protection every day.

From March 2020 to May 2020 (the start of the Pandemic) there was a 120% increase in home network usage. During this time, 87% of homes with Plume had threats blocked. Furthermore, the number of attacks against those homes doubled from the previous months, increasing from 20 per day to 40 per day, with malware topping the charts.

The Plume HomePass App from WightFibre alerts customers to issues and allows configuration of options to address those issues.

HomePass also includes several value-added features, for example:

- **Sense** allows users to turn their existing home WiFi-enabled devices into a motion-sensing network, providing them with enhanced home awareness
- **Access** provides secure WiFi guest access without the need for a separate guest network and allows users to control usage and content access levels in their household. This same service allows parents to set rules for children and filter the content they can access. Simple network administration options ensure the customer maintains control of how their network is used, protecting both their network and their loved ones.

Helping protect homes against these threats adds real value for customers and is available with many WightFibre broadband packages.

In Conclusion

In a world of always-connected devices, security concerns continue to grow for end-users. WightFibre really stands out from the crowd, offering a secure, convenient, intelligent, all-in-one solution to not only provide WiFi all around the home but holistically safeguard a customer's home network. WightFibre provides Plume's cloud-based delivery platform, hardware, HomePass app, support, and other tools make that possible, to do more to help their customers and provide excellent customer support.

wightfibre
because we care

01983 300 000

www.wightfibre.com