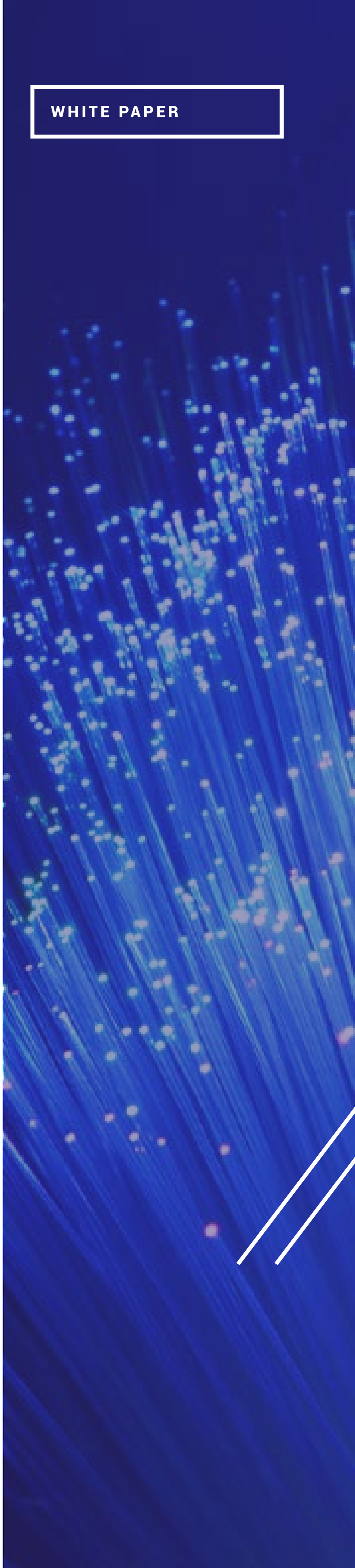
Calix


WHITE PAPER

Addressing Subscriber Security Challenges with Comprehensive Gateway Security Controls

INTRODUCTION

Service providers are increasingly focused on improving the quality of experience for their broadband subscribers. Fast connection speeds, competitive pricing, superior Wi-Fi performance and coverage, value-added services, the quality and responsiveness of customer care—all of these play a major role in keeping subscribers happy.

Providing Managed Wi-Fi services is one approach service providers are adopting to improve the quality of the home Wi-Fi experience for their subscribers. These value-added offers bundle premium Wi-Fi equipment and customer support to ensure the best possible Wi-Fi coverage and performance. However, despite the initial success of these (and similar) initiatives, many service providers are not yet stepping up in one key area where their subscribers are looking for help: home network security.

With smartphones, laptops, tablets, and wearables for every family member, along with smart speakers, locks, doorbells, thermostats, and many other devices for home automation, home Wi-Fi networks have become more complex than ever before. They have also become more susceptible to cyberattacks and increasingly sophisticated forms of malware, such as phishing scams, code injections, cryptojacking, cross-site scripting attacks, and more. As the number and frequency of these threats increase, subscriber devices, personal data, and privacy are all at risk, and the average broadband subscriber is not well equipped to fend them off.

New research from Parks Associates finds that more than three-quarters (76 percent) of broadband subscribers are very concerned about their privacy and security. They don't want anyone getting unauthorized access to their connected devices and their personal data. The research also finds that services that protect devices from unauthorized access and malicious activity are ranked number one in terms of appeal, with more than half of consumers (51 percent) finding this type of service very appealing. [1]

These findings highlight a significant opportunity for service providers to help their subscribers address a key challenge. By complementing high-speed Internet services and existing Managed Wi-Fi services with a home network security solution that's robust, reliable, and easy-to-use, service providers can improve the quality of the subscriber experience, generate incremental revenue, reduce costly support calls and truck rolls, and create differentiation in the market.

[1] Changing Dynamics of the Smart Home: Opportunities for Service Providers, Parks Associates, 2019.

OPTIONS FOR SMART HOME NETWORK SECURITY

There are several different options for securing the smart home against damaging malware, cyberattacks, and inappropriate or dangerous content.

Endpoint security software

By installing endpoint security software on their laptops and desktop computers (and in some cases their smartphones and tablets), subscribers can be protected from viruses, adware, spyware, ransomware, and other forms of malware.

While these solutions can be effective for individual devices, endpoint security software is not available for the majority of smart home devices. When combined with the fact that many smart home devices—from security cameras and baby monitors to thermostats and doorbells—have limited security protections and are therefore vulnerable to attack, endpoint security alone does not provide protection across the entire network.

Home security hubs

Standalone home security hubs are another option for subscribers looking to protect their home networks from malware and other external threats. While feature sets vary by manufacturer, home security hubs typically provide protection by scanning incoming traffic and blocking security threats before they reach any of the devices in the network. Some of these systems also offer parental controls, so that subscribers can protect their children and other users from inappropriate or harmful content.

Unlike endpoint software, security hubs are capable of offering protection for all the devices connected to the home network. Still, hubs tend to be expensive and some require subscribers to pay an annual fee for software that works in combination with the hub and must be installed on each connected personal computer, smartphone, and tablet. For subscribers already struggling to manage multiple smart home devices, security hubs represent one more device that they need to understand, install, configure, and update. In addition, since all network traffic must be routed through this extra device for scanning, subscribers will experience degraded performance.

Residential gateway with integrated security protection

A third option for subscribers—and one which service providers are best equipped to provide—is a residential gateway that is equipped with its own integrated software-based security capabilities. A key advantage of managing security at the gateway is that it provides security protection at the perimeter of the network while minimizing any impact to overall performance. It identifies threats as they enter the network and then neutralizes them before they can cause harm at the device level, for example by installing malware, stealing personal data, taking control of smart home devices, etc.

With security embedded in the residential gateway, all personal and smart devices in the network are protected from external threats. Subscribers are provided with whole-home protection with no additional devices to manage. Subscribers can also use a mobile app to easily manage controls on a per-device basis, monitor security activities, and set parental controls to protect children from visiting websites with inappropriate and harmful content.

For service providers looking to offer a comprehensive managed security solution for their subscribers that is integrated into the residential gateway, security protection needs to be provided in three keys areas:

- **Secure network authentication:** The residential gateway has to be equipped with advanced security technology that enables it to be securely authenticated on the service provider's network.
- **WPA3™ Wi-Fi security:** The gateway must support WPA3, the latest Wi-Fi security standard from the Wi-Fi Alliance, to ensure that subscriber Wi-Fi networks are protected with the highest available level of Wi-Fi security.
- **Integrated network security and parental controls:** The gateway must also be equipped with specialized software that protects subscribers from malware and cyberattacks and enforces parental controls which protect children and other family members from harmful content and applications.

SECURE NETWORK AUTHENTICATION

Before any residential gateway can connect to the service provider network, the network must first be able to verify its identity and, based on this identity, securely authenticate it on the network. This is an essential security function that prevents unauthorized, and potentially compromised, devices from gaining access to the network.

There are different methods for authenticating devices on the network, but the IEEE 802.1x standard is currently considered the most secure method available and is being widely adopted by service providers globally. It provides an industry-wide security mechanism for service providers to identify and verify the identity of the connected system.

As with any form of authentication, 802.1x depends on knowing the identity of any device that tries to connect to the network. This identity is based on a cryptographic root key which uniquely identifies the device and is stored in a trusted execution environment (TEE) on the chip. The root key is typically installed on the gateway during root key provisioning (RKP), which occurs during the device manufacturing process.

Because the network authentication process uses the root key to determine the identity of the device, it's incumbent on device manufacturers to provide the highest level of security possible to prevent it from being obtained by a hacker.

Securing the root key with the physical unclonable function

To date, residential gateway manufacturers have typically relied on one of two methods for storing the cryptographic root key. The first uses one-time programmable (OTP) memory, such as fuse or anti-fuse memory, for storing the key. The second method uses non-volatile memory (NVM), such as EEPROM or Flash memory. A more recent technology solution—known as the physical unclonable function (PUF)—provides a substantial improvement over these existing methods for securing cryptographic key storage on the device.

The PUF provides a highly reliable method of key generation and storage for the device, acting as an unclonable "digital fingerprint," which is derived from the unique, intrinsic physical characteristics of the chip used on the device. As such, there are no root keys to inject so the zone of human trust in the supply chain and manufacturing flow is greatly minimized.

During the silicon manufacturing process, variations occur that give each chip slightly different physical properties. These physical differences result in each chip having unique electronic properties, such as the transistor threshold voltages and the gain factor. As a result, the chip's identity is considered "unclonable" because it is virtually impossible to access and duplicate.

Using SRAM PUF for residential gateway authentication

The PUF can be implemented using different methods. One such method, known as SRAM PUF, involves using the static random-access memory (SRAM) on the chip to generate the device's identity.

The unique physical variations on a chip that occur during the manufacturing process can be measured by reading out the start-up values of the uninitialized SRAM. Each SRAM cell has a preferred startup state of either 0 or 1. This value is based on the relative variation in transistor threshold voltages and is unique to the chip.

The value that is read from the uninitialized memory is known as the SRAM PUF response. This response is used to generate a reliable cryptographic root key that is unique to the device. By deploying residential gateways that implement this technology, service providers can be assured of the identity of the devices authenticating on their networks and limit their exposure to malicious activity.

WPA3 SECURITY SUPPORT

In addition to providing a secure method for authenticating on the service provider network, residential gateways must also support the latest security standard that governs how subscribers and devices authenticate securely on their home Wi-Fi networks. Known as Wi-Fi Protected Access 3, or WPA3, this new standard was released by the Wi-Fi Alliance in mid-2018 and is an update to the WPA2 standard, which has been used in Wi-Fi networks since 2004.

In the context of consumer Wi-Fi deployments, WPA3 improves on the security of its predecessor by providing better cryptographic consistency, which reduces the susceptibility of the network to attacks. In addition, by replacing Pre-Shared Key (PSK) used in WPA2 with Simultaneous Authentication of Equals (SAE), WPA3 provides more robust password-based authentication and stronger security protections.

SAE is a key exchange protocol that authenticates two peers using only a password, resulting in a shared secret between the two peers that can be used for secret communication while exchanging data over a public network. This method of authentication provides a secure alternative to using certificates.

The WPA3 method of authentication using SAE provides protection from offline dictionary attacks, in which hackers attempt to get unauthorized access to a Wi-Fi network by trying passwords from a dictionary file. Because these types of attacks are ineffective on gateways that support WPA3, subscribers can choose passwords that are easier to remember and easier to enter while still retaining a high level of security.

By providing subscribers with residential gateways that implement the WPA3 standard, service providers can ensure they are protected by the highest available level of Wi-Fi security.

GATEWAY-BASED NETWORK PROTECTION AND PARENTAL CONTROLS

A security application that provides protection from cyber threats at the perimeter of the network is the third requirement of a comprehensive gateway-based security solution. Installed on the residential gateway, this application would provide malicious website protection, anti-virus and anti-ransomware packet inspection, and intrusion detection. Any threats would be identified as they enter the subscriber's network and neutralized before they could get access to devices and personal data. As well as reducing the need for endpoint software on personal devices, this solution would also provide a high level of protection for potentially vulnerable smart home devices.

To keep subscribers informed on an ongoing basis of any security-related events in the network, subscribers could be provided with a network security smartphone app. Each time a threat is detected in the network and then neutralized, subscribers would receive a notification in the app providing them with the relevant details and advising them of any required action.

APP-BASED PARENTAL CONTROLS

While protecting the many connected devices in subscriber homes is critical, no whole-home security solution would be complete without extending protection to the people who are using these devices. With a network security application installed on the residential gateway to proactively monitor traffic to identify various cyber threats coming into the network, subscribers would also need the ability to protect children and other family members from accessing inappropriate or harmful content.

A full-featured managed security solution would include an easy-to-use smartphone app that would give subscribers the ability to block and filter specific types of inappropriate content and applications on a per user basis. From a network security perspective, content filtering also prevents users from accessing malicious websites that could be hosting malware which could then infect one or more devices on the network.

Parental controls could also include time-of-day management capabilities to prevent children from accessing the Internet during specific times of the day. The app could also be used to block Internet access completely or to limit children's access to specific applications. For example, children could be prevented from accessing social media apps like Instagram TikTok on their smartphones while they are supposed to be doing their homework.

KEY BENEFITS OF GATEWAY-BASED SECURITY PROTECTIONS

- Reduce help desk calls by empowering users with easy-to-use tools to protect their networks from destructive malware
- Improve the subscriber experience
- Generate additional monthly revenue from subscribers by offering security service as a chargeable add-on
- Provide protection for the entire network, not just individual devices and network layers
- Ensure the best balance of security and performance by implementing security capabilities in the residential gateway
- Reduce the possibility of malware infecting devices in the network, by enabling subscribers to proactively block malicious websites that could be hosting malware

CAPITALIZING ON THE SECURITY OPPORTUNITY

The growing complexity of home Wi-Fi networks has left broadband subscribers more exposed than ever to a wide range of security threats that threaten their devices, their personal data, and even their physical security. While there are various security solutions that subscribers can purchase, such as endpoint security software and standalone cybersecurity hubs, these options come with significant limitations.

Given these limitations, service providers have an opportunity to position themselves as the trusted protector of their subscribers against current and future cyber security threats. By integrating best-in-class technologies like PUF, WPA3 and software-based security controls in the residential gateway, service providers can ensure complete protection at the network perimeter while minimizing the impact on performance and maximizing the subscriber experience. Coupling these capabilities with an easy-to-use mobile application provides a high degree of control by subscribers, enabling them to monitor their network security and apply parental controls to keep their family members safe.

SECURITY FEATURES IN CALIX PRODUCTS

As part of its Revenue EDGE solution, Calix offers EDGE Suites, specialized applications which help broadband subscribers manage, automate and secure their home networks. Calix also offers several cutting-edge Wi-Fi systems—the GigaSpire BLAST portfolio—which feature PuF and WPA3 functionality.