Protect Your Subscribers from Cyber Threats with Calix Comprehensive Security Controls

Calix has equipped its products with a comprehensive set of security features that ensure subscribers are given the highest levels of protection.

As consumer Wi-Fi networks continue to be the target of a growing list of ever more sophisticated cyber threats, your subscribers are becoming increasingly worried about their online security and privacy. Recent research sponsored by Calix backs this up, with nearly three quarters of respondents reporting that they, a friend, or a family member has had a computer virus or been affected by a malware attack.¹

¹ Security and Privacy Controls are an Unequivocal Requirement in Today’s Smart Home - Calix, June 2020.
Their concerns are well-founded. From botnets to ransomware and phishing to cryptojacking, cybercrime is on the rise. And, as broadband subscribers connect more and more devices to their Wi-Fi networks, malicious actors have an expanding selection of potential weaknesses to exploit. Consumer smart home devices, many of which have limited security protections, are especially vulnerable to attack.

Recognizing the risks to subscribers and to service provider networks, Calix has equipped its products with a comprehensive set of security features that ensure your subscribers are given the highest levels of protection—so they can enjoy the best possible quality of experience. These include the Calix portfolio of GigaSpire BLAST systems and EXOS, which together form the foundation of the Calix Revenue EDGE solution.

Give your subscribers superior protection with GigaSpire BLAST systems

Poorly secured residential gateways are easy targets for would-be attackers. If hackers are able to get access to a residential gateway, they can engage in a wide range of malicious activities that put subscribers and their data at risk, including:

- Redirecting them to a web page that phishes for their login credentials;
- Trick them into installing malware on their personal and smart home devices;
- Spying on them or harassing them through their IoT devices, such as security cameras or baby monitors;
- Changing their DNS server to easily steal their passwords; and
- Using their gateway as part of a botnet to launch large-scale cyber-attacks.

Referencing the Open Systems Interconnection (OSI) model, the attacks can come from any one of seven different layers. In response, a comprehensive security solution needs to address all layers.
The Calix portfolio of GigaSpire BLAST systems, with EXOS, offer cutting-edge security protections for all 7 layers of the OSI model, keeping unauthorized users out and your subscribers safe.

**Secure Wi-Fi authentication with WPA3-Personal**

The GigaSpire BLAST systems support Wi-Fi Protected Access 3 (WPA3), the latest security standard from the Wi-Fi Alliance. WPA3-Personal offers several significant security improvements for individual users compared to WPA2, the previous version of the standard. These improvements are specifically designed to help your subscribers authenticate securely on their Wi-Fi networks, while preventing access by unauthorized users.

Overall, the new standard reduces the susceptibility of subscriber networks to attack by providing better cryptographic consistency. A key advantage of WPA3-Personal is that it provides more robust password-based authentication for subscribers even when they choose passwords that don’t meet complexity requirements. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2. SAE protects subscribers from offline dictionary attacks in which a hacker uses a dictionary file to try possible passwords to log into the GigaSpire BLAST. Because BLAST systems make these types of attacks ineffective, subscribers can choose passwords that are easier to remember and easier to enter while still retaining a high level of security.

**Secure network authentication with physical unclonable function (PUF)**

In addition to ensuring your subscribers can connect to their Wi-Fi network securely, it’s critical for you to be able to verify the identity of each residential gateway that attempts to authenticate on your network. The most common network authentication protocols typically use a device’s unique cryptographic root key to verify its identity before allowing it to connect to the network. To prevent this root key from being obtained and exploited by a malicious actor, device manufacturers must provide the highest level of security possible.

There are several methods that can be used to generate and store the root key on a device such as a gateway, including one-time programmable (OTP) memory or non-volatile memory (NVM). A recent technology solution, known as the physical unclonable function (PUF), provides the most secure method. PUF security uses the unique physical characteristics of the chip on the gateway to generate its cryptographic root key—it’s unique digital fingerprint—which can’t be obtained or copied by a third-party.

The Calix portfolio of GigaSpire BLAST systems employs PUF technology so you can be sure that only authorized residential gateways are able to authenticate on the network.

**REVENUE EDGE SUITES: PROTECTIQ™ AND EXPERIENCEIQ™**

As part of the Revenue EDGE solution, Calix offers two EDGE Suites that provide advanced security capabilities for your subscribers: ProtectIQ and ExperienceIQ. Both of these applications are available to subscribers with the CommandIQ™ mobile app.
Protect your subscribers from malicious online threats with Calix ProtectIQ

ProtectIQ is a network-level security application that provides malicious website protection, anti-virus and anti-ransomware packet inspection, and intrusion detection. It proactively monitors network traffic coming into your subscribers’ homes, automatically blocking anything that looks suspicious. Installed inside a BLAST system, ProtectIQ is the optimal point at which to establish and enforce a home perimeter layer of security and privacy.

Calix ExperienceIQ: Empower your subscribers with flexible parental controls

ExperienceIQ provides your subscribers with an extensive set of parental controls that allow them to easily create and enforce online rules for the users and devices in their home networks. It also gives them peace of mind by protecting their children from inappropriate or harmful content.

When enabled inside the Calix CommandIQ app, ExperienceIQ allows subscribers to create a profile for each member of the household and then associate specific devices with it. With the profiles created, subscribers can then take various protective actions from the convenience of the app. These include pausing the Internet connection for individual devices, blocking and filtering content and applications, and scheduling specific times of day during which Internet and application usage is limited or blocked for individual users.

ADVANCED SUBSCRIBER SECURITY CONTROLS WITH EXOS

Calix EXOS is a hardware-independent, modular, always-on, intelligent OS that enables you to bring new services and applications to market more quickly, while also reducing testing and integration times. EXOS features a multi-purpose traffic flow inspection engine called the classification engine, which has visibility into the packet header data for all traffic that flows through the Calix GigaSpire BLAST systems. The classification engine scans the packet’s metadata, which it uses to determine:

- source and destination IP address, packet type, packet size, etc.
- device fingerprinting, including manufacturer, make, model, operating system, and MAC address
- mapping of applications (e.g., Netflix) to devices (e.g., Samsung Smart TV)
- network traffic and control protocols (e.g., DNS requests)

The EXOS classification engine is coupled with the GigaSpire BLAST forwarding engine, which provides information via APIs to ProtectIQ and ExperienceIQ. This shared architecture results in improved flexibility, efficiency, privacy, and security.

KEY BENEFITS

- Provide protection for your subscriber’s entire network, not just individual devices and network layers
- Reduce costly help desk calls by proactively reducing cyber threats in your subscribers’ networks
- Empower subscribers to take control of their own security with easy-to-use tools that protect their devices and family members
- Generate additional monthly revenue from subscribers by offering ProtectIQ and ExperienceIQ as chargeable add-ons
- Reduce the odds of malware infecting devices in the network, by enabling subscribers to proactively block malicious websites that could be hosting malware