A blue-tinted photograph of a man and a woman looking at a screen together. The man is wearing glasses and a dark shirt, and the woman is also wearing glasses and a dark shirt. They appear to be in a collaborative work environment.

Enhance home network security and generate revenue with app-based network and content controls

EDGE Suites provides service providers with access to a growing ecosystem of partners that deliver valuable applications for subscribers.



Broadband subscribers are connecting more and more devices to their home Wi-Fi networks. By 2022, it's estimated that there will be 13 connected in-home devices per person in North America¹. Most households today already have multiple connected devices—from laptops and tablets to smartphones and wearables. And as smart home devices like smart speakers, thermostats, security cameras and light bulbs continue to grow in popularity, home networks will become increasingly complex and challenging for subscribers to manage.

What's more, with each new device the risk of exposure to online threats grows. Poorly secured residential gateways and smart home devices are known targets for hackers looking to create botnets and launch distributed denial-of-service (DDoS) attacks. And your subscribers are vulnerable to a whole host of cyber threats, including phishing scams, ransomware, spyware, data interception and malicious code injection.

Not surprisingly, broadband subscribers are worried. In a recent study sponsored by Calix, 76% of broadband households in North America expressed high levels of concern about security and privacy when using their connected devices at home. They're particularly concerned about their children's safety, and are looking for effective parental controls to monitor and limit their screen time and protect them from inappropriate and harmful online content and applications.

GENERATE NEW REVENUE WHILE SECURING THE SUBSCRIBER NETWORK

These trends represent a challenge for service providers, but also an opportunity. The challenge lies in providing subscribers with effective, easy-to-use tools and capabilities to give them visibility into the devices in their networks, ensure the online safety of family members and mitigate the constantly evolving online security risks they face. As web-scale and over-the-top (OTT) players move aggressively to stake their claim in the connected home, addressing your subscribers' security challenges presents an opportunity to fight back. It helps you create differentiation by addressing your subscribers' highest-priority challenges. And it enables you to take the subscriber experience to new heights by eliminating complexity in the management of Wi-Fi, network security, parental controls and home automation. In short, you can offer your subscribers a value proposition that OTT consumer solutions simply cannot match.

INTRODUCING CALIX EDGE SUITES

With ExperienceIQ™ and ProtectIQ™, Calix helps you address your subscribers' home network security and monitoring challenges directly, while also enabling you to generate additional monthly revenue streams with new, value-added capabilities. These new application suites help you solve and support the rapidly-growing management and security complexities of your subscribers' home networks. While ExperienceIQ empowers your subscribers with industry-leading parental controls, ProtectIQ enables them to protect themselves and their families from a wide array of malicious security threats in their home networks. ExperienceIQ and ProtectIQ are the first two applications of Calix EDGE Suites, a component of the Calix Revenue EDGE solution. Both applications are accessed from the Calix CommandIQ app.

¹ Source: Cisco Visual Networking Index (VNI): Forecast and Trends, 2017–2022 (<https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>)

EXPERIENCEIQ: EMPOWER YOUR SUBSCRIBERS WITH FLEXIBLE PARENTAL CONTROLS

ExperienceIQ empowers 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.

Content filtering

Using ExperienceIQ, subscribers can use content filtering to ensure the online safety of their children and other family members. They can restrict access to inappropriate content for individual users based on numerous preset categories, such as pornography and nudity, violence, P2P file sharing, online shopping, social networks, and many more. In addition to filtering by category, subscribers can block access to specific websites or applications for some or all users.

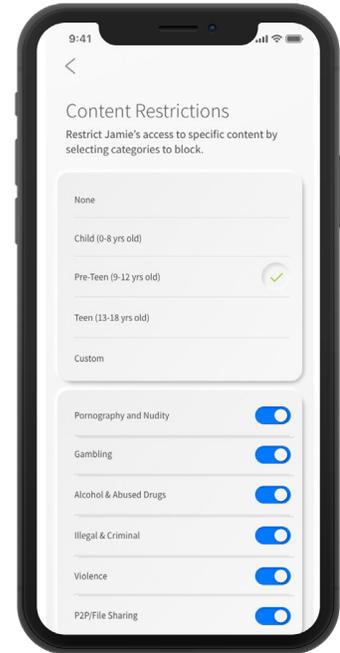
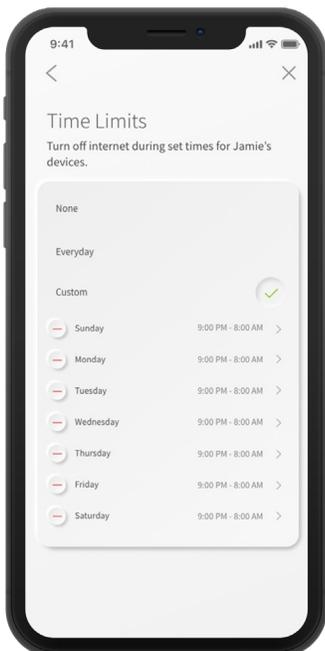


Figure 1: ExperienceIQ Content Filters, found in the CommandIQ mobile app, allow users to restrict access to inappropriate content for individual users based on numerous preset categories.



Time limits and restrictions

ExperienceIQ allows parents to schedule times during which children are prevented from accessing the Internet at all or during which individual applications cannot be used. For example, access to social media apps like Snapchat and Instagram could be blocked during the evening when children are doing their homework, and Internet access could be completely blocked after 10:00 pm and then unblocked at 7:00 am. Subscribers can control this for each user and each device associated with that user.

Figure 2: ExperienceIQ Time Limits allow users to schedule times during which children are prevented from accessing the Internet or specific applications.

Usage reporting

ExperienceIQ also gives parents a view of the approximate time each user spends on different applications, so they can better understand their children's online activities. Per-user usage reports are available on a daily, weekly or monthly basis. For example, a parent could view how many hours each of their children spent on TikTok during the past week.

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. When enabled inside the Calix CommandIQ app, ProtectIQ proactively monitors network traffic coming into your subscribers' homes, automatically blocking anything that looks suspicious. Installed inside a Calix GigaSpire BLAST system, ProtectIQ is the optimal point at which to establish and enforce a home perimeter layer of security and privacy.



Figure 3: ExperienceIQ Online Usage reports allow users to view the approximate time each user spends on different applications and web sites.

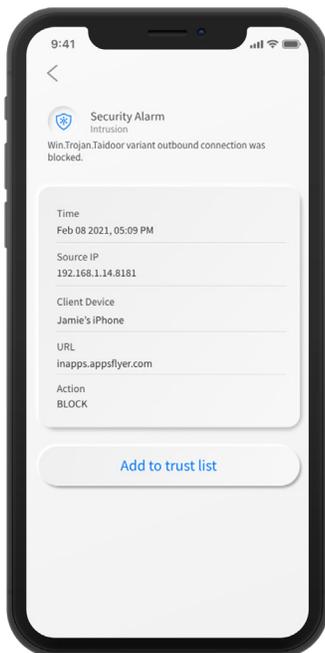


Figure 4: ProtectIQ sends notifications to users whenever a security issue is triggered.

Malicious website protection

This service monitors devices attempting to visit known websites that could be harmful to your subscribers' network and devices. ProtectIQ blocks all attempts to visit these websites and presents users with a browser message indicating that the website is not available or that the connection was terminated.

Anti-virus and anti-ransomware packet inspection

ProtectIQ provides an active security monitoring service that uses a large database of known threats. By looking for the specific signatures of these threats in real time, ProtectIQ can terminate the transfer of data before a malicious payload is delivered to any vulnerable network devices. The database of threats is constantly growing as new threats emerge and the application's database is kept up to date weekly in the cloud.

Security alerts

For each of its network security features, ProtectIQ sends notifications to users whenever a security issue is triggered. Alerts will include details about the device that was attacked, where the attack came from, and when the attack occurred.



KEY BENEFITS OF THE CALIX EDGE SUITES

- 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 ProtectIQ and ExperienceIQ as chargeable add-ons
- 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 Wi-Fi system
- Reduce the possibility of malware infecting devices in the network, by enabling subscribers to proactively block malicious websites that could be hosting malware