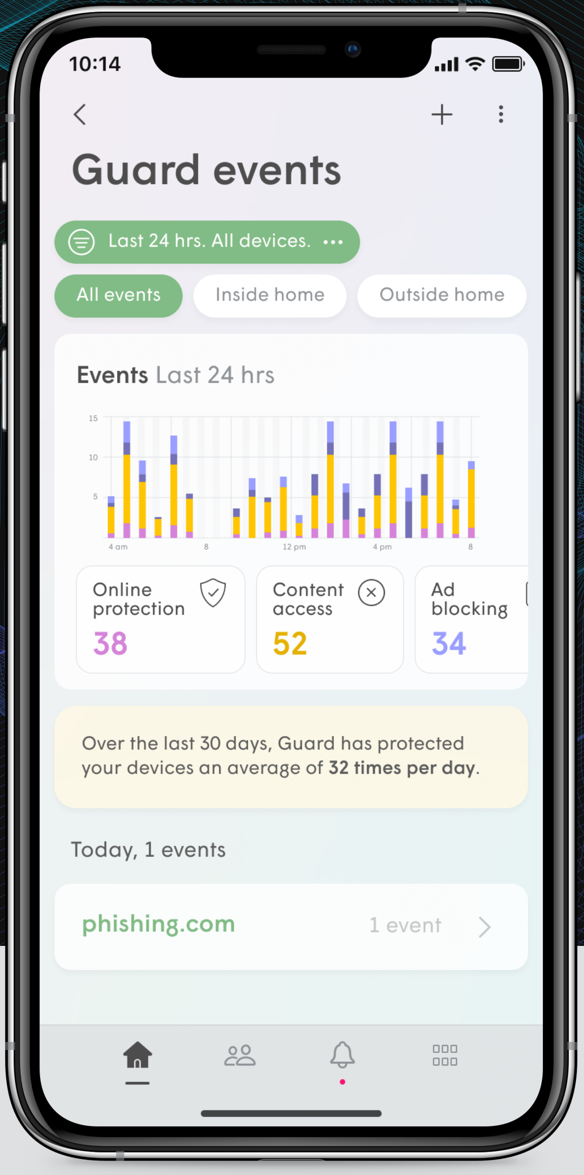
Plume

Guard

Protect your customers' devices from cyber-threats at home and on the go

Cyber-threats persist beyond home networks

Today's customers rely on their many smart devices for work and play, all of which are vulnerable to cyber-threats within and outside of home networks. Traditional device-specific solutions, however, may require device-specific updates and generally provide no overall network visibility, control, or protection to their end users.


10:14

Guard events

Last 24 hrs. All devices. •••

All events | Inside home | Outside home

Events Last 24 hrs

Online protection 38

Content access 52

Ad blocking 34

Over the last 30 days, Guard has protected your devices an average of **32 times per day**.

Today, 1 events

phishing.com 1 event

Provide greater peace of mind with security that follows the device, not the network

Powered by cloud-based, real-time protection algorithms and machine learning-based intelligence, in partnership with Akamai, Plume's Guard protects your subscribers from cyber-threats down to each device. It neutralizes threats in- and out-of-home, and is user-managed through a simple mobile app. Whether their device is on their home network, another WiFi network, or a cellular network, your subscribers will have control over their devices. In addition, with Guard, your subscribers will have outside-the-home security and setting migration on their smart devices.

Key features

Advanced device typing (ADT)

ADT technology classifies 95% of applicable connected devices (by brand, model, and firmware) within minutes to ensure cloud-customized performance for each device. These details are made available to Providers enabling smart home managed services.

Online device protection

AI-based global threat intelligence prevents all connected devices from visiting known malicious destinations. This protects the connected devices from infection or attack by malware, spyware, ransomware, botnet servers, and phishing. Guard is also compatible with DNS Encryption to provide protection and content filtering even if Guard cannot see DNS due to encryption (DoT/DoH).

Intrusion detection and blocking

IP-based online protection stops outside attackers from gaining access to home networks and notifies users of attacks on exposed devices.

Privacy Controls

Built-in ad-blocking features allow your subscribers to enjoy a privacy-first browsing experience with minimal ad interruptions.

Behavioral analysis and anomaly detection

Guard's anomaly detection uses machine learning to understand normal IoT device activity and develop a whitelist of allowable behaviors. Anomalies are reviewed, and high-severity outliers are automatically blocked to prevent the spread of infection to other connected IoT devices.

Remediation and isolation

When high-severity anomalies are detected, Guard automatically blocks connections and quarantines devices to their local networks to prevent the spread of malicious code to other networks.

Network-wide security dashboard

See what's happening in your network through various lenses, including by activity, time period, and geographic distribution, so that you can respond quickly to infrastructure threats.

Multi-layered security

Guard equips subscribers with multi-layered security, including a DNS layer to protect against domain-based attacks, IP-based prevention for inbound and outbound cyber-threats, and anomaly detection.

Outside home protection

With the HomePass app, subscribers can personalize policies and control settings to apply even when their devices are connected to another WiFi or cellular network.

Key benefits

Monitor

Visualize your customer network down to the device level from a comprehensive dashboard. Filter, track, and analyze cyber-security events as well as active threats.

Protect

Safeguard customer privacy and data, as well as your network, from malicious attacks. Meanwhile, subscribers can stop unwanted ads and filter content by user and device.

Prevent

Stay ahead of emerging threats with Guard's machine learning ability, which updates device profiles continuously and stops intrusions before they can start. Enhance zero-trust security by autonomously blocking all malicious incoming connections.

Correct

Correlate threats across your network for faster response to wide-scale attacks. Isolate compromised devices and notify users and manufacturers of exposed devices.

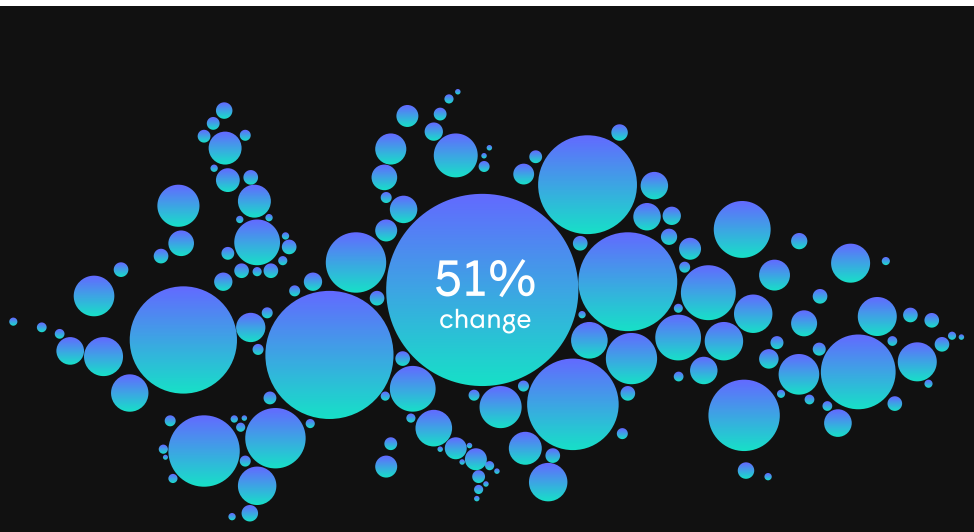
Outside home protection

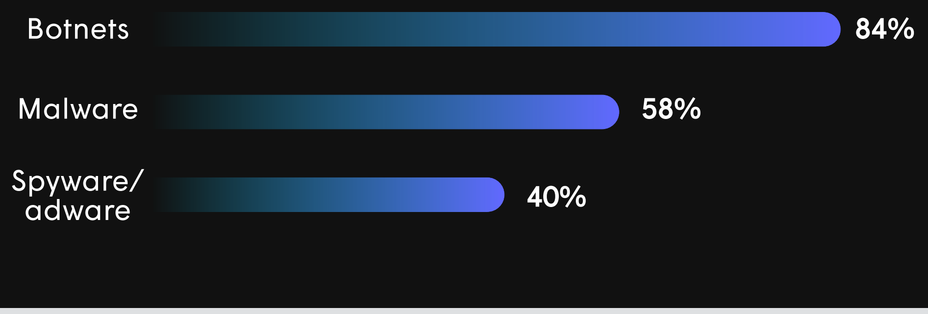
Keep your subscribers' devices safe from adware, malware, phishing, botnets, ransomware, spam, and fraud, even when they're on the go. Guard also keeps activated parental settings and freeze schedules enforced—even when devices are disconnected from the home WiFi network—to protect children from accessing inappropriate content.

The relentless threat of cyber-crime

Globally, the average number of cyber-threats blocked in Plume-powered homes has significantly risen by 51% in 2022, as compared to the year before, with the top three highest growth cyber-threat categories being botnets (84% increase), malware (58% increase), and spyware and adware (40% increase).*

(*Source: Plume IQ 1H 2022 report)





Why partner with Plume?

Plume's solutions help CSPs reduce costs while increasing operational efficiency.*

▲ 60+ NPS

▼ 67% Truck rolls

▲ $15 Monthly ARPU

▲ 200% ROI

*Data based on an average taken across Plume's deployed CSP customer base.

Let's get started

Offer your customers the next level of home network protection.
Contact **partner@plume.com.**