Avira

AVIRA SAFETHINGS™

SECURING THE CONNECTED HOME

Avira SafeThings™ empowers home router manufacturers and Internet service providers (ISPs) to create a secure environment for their customers' smart homes.

SafeThings protects the end user's home network from attack by placing their IoT smart home devices beyond the reach of hackers. It delivers control, visibility and peace of mind.

SafeThings also protects the service provider network from misuse, and provides insight to the aggregated usage of connected devices in their customer base. It delivers analysis, enables trends to be predicted, and creates an opportunity to cross-sell value-added services.

IMPLEMENTATION

Avira SafeThings is a cloud-based behavioral threat intelligence platform which interfaces with a service provider's home router. It enables a connected home to operate securely without fear of compromised IoT devices. Service providers benefit from comprehensive report management options though the SafeThings Insights and Management Centre API. Consumers gain visibility and complete control over their home devices through a custom developed mobile app.

A powerful machine learning / AI engine lies at the heart of Avira SafeThings. When combined with lightweight software on the home router, the AI performs behavioral analysis to discover connected home devices and profile their normal behavior. Together, they identify unusual behavior, block vulnerabilities, protect privacy, guard against IoT-specific malware, and prevent malicious misuse of smart home devices, all without the need for additional hardware.

Service Providers and Router Manufacturers can:

- Safeguard customers' smart homes against hijack, misuse and intrusion and keep their data private
- Gain aggregated data and statistics into IoT device use across their network
- Generate new revenue streams and increase market share
- Protect the service provider network infrastructure from emerging IoT threats
- Strengthen their brand reputation as a protector of the connected home

AVIRA SAFETHINGS COMPONENTS

Avira

AVIRA SAFETHINGS SENTINEL

Avira SafeThings Sentinel is the collection and enforcement point on the home router. Running on top of the router's firmware, it provides the functionality to enforce highly granular security policies under the control of the SafeThings Protection Cloud. Unlike more traditional approaches that rely on deep-packet inspection, SafeThings uses next-generation behavioral analysis algorithms to identify anomalies. It also helps to secure the router by scanning for known vulnerabilities.

To ensure that SafeThings has no performance impact on the home network, the Sentinel software runs in the user space at a lower priority than other applications (e.g. DHCP server, DNS server, etc.). To comply with privacy legislation, it only collects anonymized metadata and generates minimal additional traffic on the access network.

Above all, Avira SafeThings Sentinel maintains consumer data privacy because it only monitors packet headers and records how traffic flows through the smart home network. It does not monitor what is in the payload.

SAFETHINGS SENTINEL

- Installs on the home router
- Discovers the devices connected to the home network
- Inspects high level information on traffic flows
- Enforces security policies on the router

AVIRA SAFETHINGS PROTECTION CLOUD

Avira SafeThings Protection Cloud uses big data and machine intelligence to profile devices, detect and control anomalies in real time.

The SafeThings Protection Cloud is the central store for all the detection, classification, categorization and traffic information reported by the SafeThings Sentinel. It uses advanced machine learning algorithms and behavioral analysis techniques to learn normal activity, classify usage patterns and detect anomalies. The SafeThings Protection Cloud also acts as the management, insight, and rule definition interface. It works with the Sentinel on the home router to apply security policies that ensure privacy and the correct function of devices in the connected home..

SAFETHINGS PROTECTION CLOUD

- Detects anomalous patterns in the behavior of IoT devices
- Delivers proactive security profiles to the Sentinel agent on the home gateway
- Monitors and suppresses network attacks

AVIRA SAFETHINGS USER INTERFACE

The Avira SafeThings User Interface enables the end user to manage their home security directly through an app on their mobile device.

Smart home owners get an overview of all the devices connected to their home network, monitor vulnerabilities and set custom rules. When events happen in the network the end user receives a notification within their mobile app, and can control their SafeThings protected network in real time.

SAFETHINGS USER INTERFACE

- Device security assessment report
- Network traffic report
- Real time notifications and alerts
- Parental Controls – rules for the family's devices

Avira

AVIRA SAFETHINGS INSIGHTS AND MANAGEMENT CENTRE

Avira SafeThings Insights and Management Centre is an optional custom developed reporting tool for Internet Service Providers. It enables a wide variety of data reporting from Avira SafeThings which can be provided via API or as a full tailored solution.

SAFETHINGS INSIGHTS

- Comprehensive customer support
- Unparalleled visibility to smart home networks
- A single consolidated view

AVIRA INSIGHTS AND MANAGEMENT CENTRE FOR ISPs

OUR AWARDS

FIND OUT MORE

Website: oem.avira.com
Email: oem@avira.com
Blog: insights.oem.avira.com
Social Media: @AviraInsights

Europe
Middle East, Africa

Avira
Kaplaneiweg 1
88069 Tettnang, Germany
Tel: +49 7542 5000

Americas

Avira, inc
c/o WeWork, 75 E Santa Clara Street
Suite 600, 6th floor San José
CA 95113 United States

Asia/Pacific and China

Avira Pte Ltd
50 Raffles Place
32-01 Singapore Land Tower
Singapore 048623

Japan

Avira GK
8F Shin-Kokusai Bldg
3-4-1, Marunouchi Chiyoda-ku
Tokyo Japan 100-0005