Allot EndpointSecure

The Challenge

There are multiple occasions and reasons for your customers to connect to 3rd party Wi-Fi networks. They might want to save data on their service plan, or they might simply be in a location where mobile connectivity is not strong enough. Whatever the reason, you should protect your customers when they are offnet just like you do on your network. It only takes one mistake for a device to become infected by malware, so it is crucial to offer constant protection, regardless of connectivity.

The same holds true for parental control. Your customers' children should be prevented from accessing the wrong content even when they are guests on a different network. And your customers should not have to configure these settings more than once.

The Solution

Allot EndpointSecure leverages award-winning Bitdefender security technology to provide protection and parental control, even when the user is not using your network. The security policies are defined once and enforced the same way by all the other solutions in the Allot Secure family. For example, Johnny's parents only need to create one policy to protect him from online threats, block social networks and make sure he is not online during study time. This policy is automatically propagated by Allot Secure to NetworkSecure, HomeSecure and EndpointSecure for enforcement on any device assigned to Johnny, regardless of how he is accessing the internet.

Benefits

Add Value to your business with a unique, unified Security-as-a-Service (SECaaS) solution

o   Increase revenue
o   Brand differentiation through custom EndpointSecure logos and texts
o   Easy promotion using Allot Secure engagement tools

Add value for your customers through comprehensive, easy-to-use security

o   Constant protection for the entire family, even when offnet
o   Run malware scans on the device itself, in addition to network-based protection
o   Additional, device-based functionality, such as location tracking, sending alarms to the device and wiping it in case it is stolen.

Easy add-on to your Allot Secure platform

o   Leverages the existing deployment
o   Provides the same unified interface as the other solutions
o   Seamless integration

allot   See. Control. Secure.

Advantages

EndpointSecure, in conjunction with other Allot Secure products, provides 360° security for the mass market, unifying three security layers to protect subscribers at home, at work and on the go.

Allot Secure products include:

o   NetworkSecure - for protecting customers across all devices connected to your network

o   HomeSecure / BusinessSecure - for securing IoT devices, smart appliances, and end-user devices, in the home and office

o   EndpointSecure - for extending network-based security and controls to customers when offnet

The Allot Secure platform allows you to easily create a company-branded, user-friendly management app for your subscribers. Alternatively, our out-of-the-box management app can be used. In either case, parents can configure one-time security settings and parental control, and access unified reporting for all of the Allot Secure modules. Your subscribers will enjoy anywhere, any device, any threat protection over fixed, mobile, and converged networks. EndpointSecure is available for Android, iOS, Windows and macOS platforms.

EndpointSecure Enforcement Sample Notifications - can be branded to your look and feel:

All is good, your device is protected.

Malware was detected by device scan.

Downloaded malicious app was automatically detected

Specifications

Threat Protection

Feature	Android	iOS	Windows	macOS
Malicious Website Protection (identification and blocking)	✓	✓	✓	✓
Real-Time Scanning (new files on the device)	✓	N/A (not allowed by iOS)	✓	✓
Device Scanning (find existing threats)	✓	N/A (not allowed by iOS)	✓	✓

o   Malicious Website Protection: Identifies and blocks access to malicious websites using market-leading detection techniques.

o   Real-Time scanning: Scans downloaded files, such as apps, to identify those that have malicious intent.

o   Device Scanning: User-initiated scans to find existing threats on your device.

Content Filtering

Feature	Android	iOS	Windows	macOS
Category-based Filtering (identification and blocking)	✓	✓	✓	✓
White & Block Listing (creating exceptions)	✓	✓	✓	✓
Quiet Time (time-based blocking of all device traffic)	✓	✓	✓	✓
App Blocking (blocking specific apps from being opened on the device)	✓	N/A (not allowed by iOS)	✓	✓ (planned)

o   Category based filtering: A parent can choose which website categories should be blocked for the child.

o   White & block listing: Creation of specific exceptions for websites to be allowed or blocked.

o   Quiet Time: Block all device communication during predefined time periods or based on a schedule.

o   Application blocking: Identify apps installed on the device and block those that are not suitable for the child.

Other features

Feature	Android	iOS	Windows	macOS
Device Remote Actions (tracking and theft protection)	Block, Alarm and Wipe	Alarm	N/A	N/A
Locate (showing the device on a map)	✓	✓	N/A	N/A
Reporting (blocking events)	✓	✓	✓	✓

o   Remote Device Actions: Block the screen to stop further device usage, play an alarm sound on the device to know where it is or wipe the device content if you lose it.

o   Locate: Identify the current location of the device on a map.

o   Reporting: Blocking events are reported back to the Allot Secure platform for the parent to receive an aggregated activity view across all the solutions.

Powered by

Bitdefender®

Sep 2020

See. Control. Secure.