Allied Telesis

React Less. Defend More.

Automated edge security for an easier, faster threat response.

SELF-DEFENDING NETWORKS

Automated Edge Security Solution

As cyberattacks evolve and spread, the cost of keeping your business safe increases. Complexity and constant vigilance require specially trained staff able to take immediate action to defend your network.

Ideally, your network would defend itself—enter the Allied Telesis Self-Defending Network solution. We created this solution to instantly respond to threats and automatically decide the appropriate reaction for any detected attack.

The Self-Defending Network

Most threat protection solutions are only capable of blocking suspicious traffic as it passes through the firewall, so only external threats can be detected and blocked. However, the Self-Defending Network can isolate traffic anywhere in the network, such as those introduced inadvertently by staff with USB sticks via BYOD and insider threats.

The major benefits of the Self-Defending Network are:

- Immediate and accurate threat response, without any manual intervention.
- Protection from suspect user devices without the need for software agents to be installed and maintained.
- Defense against wireless users. We control the network, not the device so we can protect you from threats on ***any*** device however it is connected to your network.
- Compatibility with your existing firewall solution without the need for reconfiguration or software updates.

The Self-Defending Network is an innovative security solution that monitors traffic entering and traversing your business networks, without extra complexity and costs. When partnered with our network management automation solution, the benefits are magnified, and ROI is increased.

To learn more visit **https://bit.ly/2JYQ33z** or contact sales on **1-800-428-4835.**

SELF-DEFENDING NETWORKS

"Companies that had security automation technologies deployed experienced around half the cost of a breach ($2.65 million on average) compared to those that did not have these technologies deployed ($5.16 million average)."

2019 Cost of a Data Breach Report – IBM

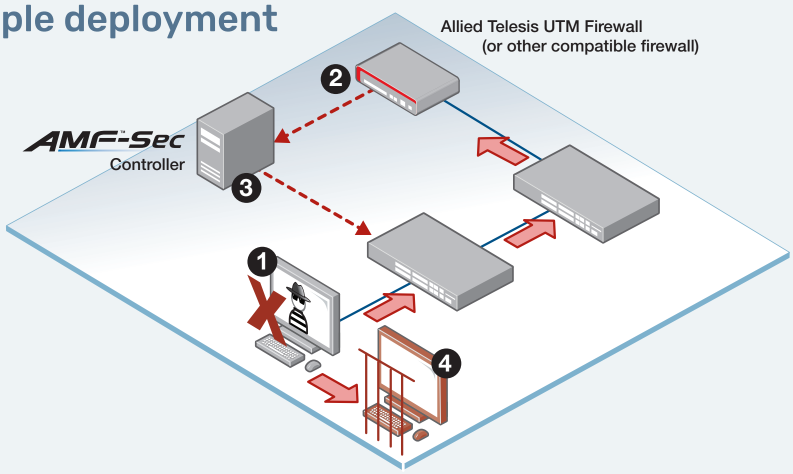
The Self-Defending Network comprises three components:

AMF-Sec Controller
The brain of the automated Self-Defending Network integrates with your firewall to respond to threats.

Autonomous Management Framework (AMF)
The automation engine that controls the network and provides additional management cost savings by automating everyday admin tasks.

AMF-Capable Network Switches
Networking devices that AMF controls to isolate suspected threats.

Example deployment



1. Targeted attack inside the network! Threat information sent upline
2. Firewall sends threat notification
3. AMF-Sec instructs switch to shut down threat source
4. Infected device sent to quarantine

The Self-Defending Network provides effective protection for small branch offices and for corporate headquarters. Our flexible licensing and pricing models enable cost-effective solutions to be built to suit any application.

Branch office with up to 100 users

This example assumes 2 connections per user (PC + VoIP phone) + 10 WLAN APs = 210 edge ports.

Product	Description	Qty
AT-FS980M/52PS	5 x 48-port PoE+ switches	5
AT-x530-28GTXm	24-port gigabit core switch with 10G ports for server uplinks and a built-in network management application (Vista Manager mini)	1
AT-FL-x530-AM20	AMF software license for x530 switch	1
AT-FL-SESC-BASE	Self-Defending Network application license	1

The cost is less than you think and will save more than you expect. Talk to us to find out more.

Contact us to get started:

Allied Telesis™

AlliedTelesis.com