PANDA ADAPTIVE DEFENSE 360: SECURING REMOTE USERS

By Marios Tsimaris – Junior System Consultant

Introduction

Guarding the endpoint against assault is hard. Insurance must incorporate a wide scope of protections counting conventional antivirus/against malware, individual firewall, Web and email separating and gadget control. Furthermore, any protection must give extra defends against hard to-recognize zero-day and focused on assaults. Up to now, IT has expected to procure and keep up various items from various sellers to protect the endpoint.

Adaptive Defense 360 is the only solution available that offers the full insurance of a conventional antivirus, whitelisting, and assurance against cutting edge dangers across the board. Truth be told, it joins the entirety of the capacities of two item classifications in one – EPP (Endpoint Protection Platform) and EDR (Endpoint Detection and Response).

Adaptive Defense 360 additionally computerizes abilities diminishing the weight on IT. Adaptive Defense 360 starts with Panda's best-of-breed EPP solution which includes Simple and centralized security, Remedial actions, Real-time monitoring and reports, Profile-based protection, Centralized device control, and Web monitoring and Filtering.

Differences between Adaptive Defense 360 and a traditional antivirus

1. An antivirus needs proactive discovery and doesn't order the entirety of the applications. Rather, it just characterizes those which it has recently recorded as malware while Adaptive Defense groups every single running application, be they goodware or malware, known or obscure.
2. An antivirus implies a specific degree of work for the manager – the executives of the isolate, managing bogus positives, and so forth. Then again, Adaptive Defense is an overseen administration and these sorts of undertakings are dealt with naturally by Panda.
3. An antivirus doesn't offer recognizability for the activities taken by a malware, implying that it doesn't give any scientific insights concerning the assault. Versatile Defense, be that as it may, offers point by point criticism on each activity taken by a risk.

Functionality

The functions in the Endpoint of Panda Adaptive Defense 360 are based on three principles:

1. Continuous monitoring of applications and servers of the company.

2. Automatic classification using Machine Learning techniques in Panda's Big Data platform.
3. Analysis and manual classification, by PandaLabs' technicians, of applications that are automatically unclassified to know the behaviour of what is running.

With this kind of protection and response in the Endpoint, you achieve a complete solution to fight against malware as well as prevent it.

Along these lines, the new arrangement consolidates all the benefits of a customary antivirus – anticipation and hindering of assaults, and remediation of infections – with cutting edge security and full discernibility, which means we get the chance to examine 100 % of the running applications.

The new arrangement gives an endpoint identification administration that can precisely order every one of the association's applications with the goal that it just runs what is legitimate. This is absolutely what separates Adaptive Defense 360 from regular antiviruses.

Another bit of leeway of being on the endpoint is that Adaptive Defense 360 distinguishes dangers in a genuine situation paying little heed to source, including USB. This is something which doesn't occur with most ATD (Advanced Threat Detection) arrangements, as they just find dangers that enter the system and virtualized conditions.

The only solution to guarantee the security of all running applications

1. Complete and robust protection guaranteed
2. Forensic information
3. Protection for vulnerable operating systems and applications
4. Full EPP capabilities
5. Continuous status information on all endpoints in the network
6. SIEM available
7. 100% managed service

At the point when everything is said and done, we can see that Adaptive Defense 360 is route in front of different choices accessible available. It exceeds expectations against conventional dangers as well as with powerless applications and propelled dangers.

Adaptive Defense 360 constantly examines the framework's movement in order to decide how to arrange each procedure being done as goodware or malware, without leaving space for uncertainty, and shuts the hover of discovery with the arrangement worked in.

www.ibs.com.cy

Marios Tsimaris is our Systems Consultant, and he is working for IBSCY for the last 2 years. He is a member of our IT department which consists of 5 people and it is responsible for the day-to-day support and maintenance of our clients. His team is also fully responsible for the implementations of new and existing clients in Cyprus and internationally. He holds several certifications from Microsoft, Fortinet, VMWare and other vendors.