Adaptive Digital Defense for OT environments / OT Visibility & Profiling

Adaptive visibility, the perquisite for digital security

"Industrial companies have begun to engage in a digital race...
A 2017 report released by Morgan Stanley analysts provides further evidence of the trend favoring the increased use of technology: Digital Manufacturing has reached the tipping point, and is now going mainstream.

... originating a complex and growing problem":
According to 2018 Gartner report "Strategic Roadmap for Integrated IT and OT Security": OT networks have been unmanaged, from a security and risk perspective, for many years. They are flat, with a mix of OT protocols, unidentified assets, legacy systems and devices with unsecure communications.

Despite growing security risks and increase in regulatory pressure industrial firms do not have a centralized, real-time view of all assets connect to the organization; IT, IoT / IIoT and OT.

Manufacturing and other industrial related companies require a 360º real-time view of everything that is connected to the network both locally and remotely (third party vendors etc.), in IT & OT networks.

The solution needs to be easy to adopt to the infrastructure and business logical and guarantee zero impact on uptimes.

VISIBILITY AND CONTROL OF ASSETS IS THE Nº 1 SECURITY CONTROL. CIS*

A SIMPLE, ADAPTABLE SOLUTION:

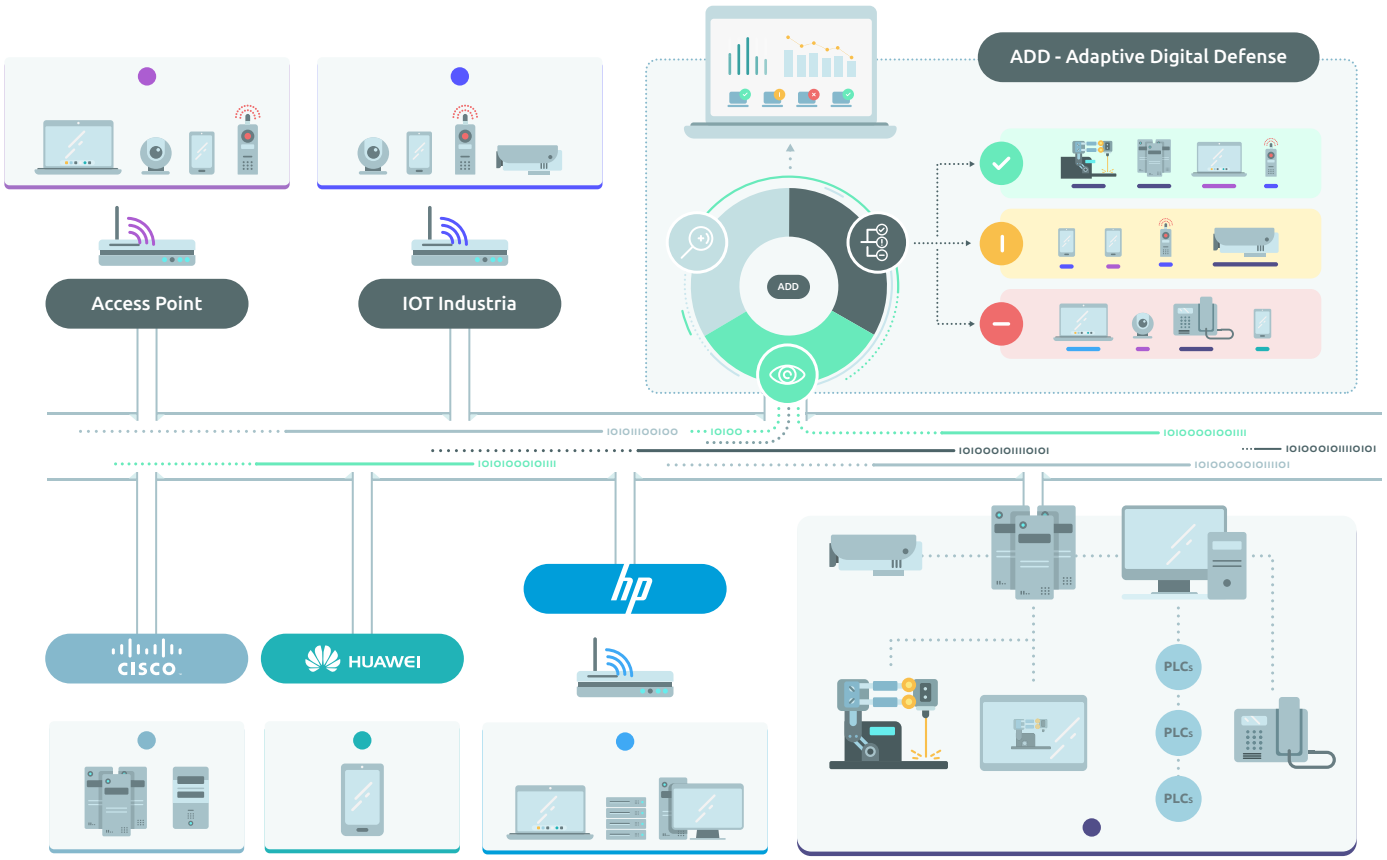
Adaptive Digital Defense for OT environments / OT Visibility & Profiling is a software-based solution that enables companies running all kind of industrial processes to gain 100%, accurate, real-time visibility of all assets connected to OT networks.

Via non-intrusive techniques and a modular approach organization can achieve a centralized view of their networks assets and establish their mission criticality to determine the appropriate security controls while guarantying zero impact on uptimes.

WITH SO MANY SOLUTIONS ON THE MARKET WHY ARE ORGANIZATIONS STILL FAILING THE VISIBILITY TEST; THE PREREQUISITE FOR DIGITAL SECURITY?

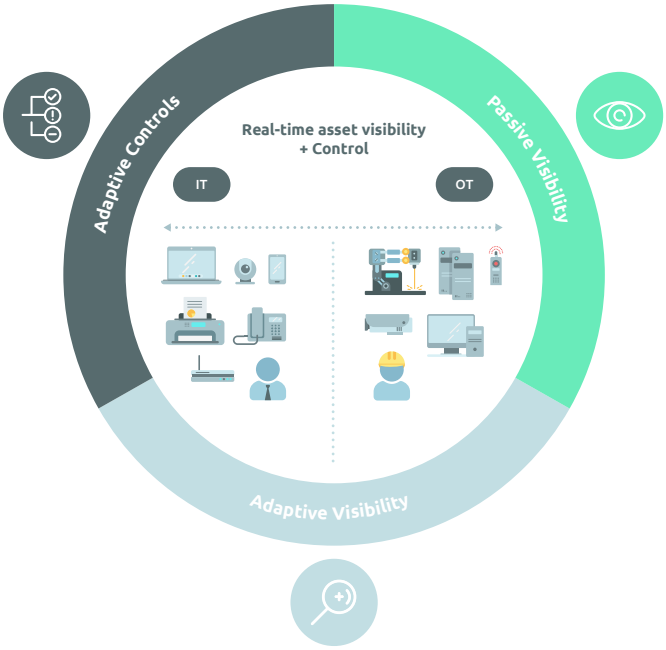
* Center for Internet Security https://www.cisecurity.org

opencloud factory
Industrial cybersecurity



THE ADAPTIVE SOLUTION:

Adaptive Digital Defense for OT environments / OT Visibility & Profiling is software-first technology guaranteeing an agnostic, flexible solution that can quickly adapt to the organizations existing infrastructure and security stack, reducing barriers to adoption and guaranteeing quicker results.



Adaptive Digital Defense for OT environments / OT Visibility & Profiling works off an extendible tag system for categorization. Assets are automatically discovered and categorized using available asset information but organizations can extend that information to apply the organizations own logic and mission criticality etc.

VISIBILITY IS GAINED IN A PHASED, LESS TO MORE, APPROACH WHICH ENABLES TEAMS TO GAIN QUICK WINS AND MATURE AS THE TECHNOLOGY IS IMPLEMENTED.

1. Passive Visibility

Passive discovery and profiling of every asset that is connect to the OT / IT network is achieved automatically using multiple techniques via a non-intrusive port-span probe

2. Adaptive Visibility

OT teams can establish the mission criticality of the assets and if they can be exposed to active profiling to extend passive asset information. The tool is based on RESTful API it can integrate rapidly with third parties

3. Adaptive Controls

With a complete picture of all assets and their mission criticality organizations can define what controls should be established; segmentation, alerts, compliance reports / base lines.

Level 1. Production	Level 2. Supervision	Level 3. Operation Management	Level 4. Deal
BACnet	6LoWPAN	CC-Link	DCOM
Beckoff EtherCat	CC-Link	DDE	DDE
CANopen	DNP3	GE-SRTP	FTP/SFTP
Crimson v3 (Redlion)	DNS/DNSSEC	HSCP	GE-SRTP
DeviceNet	FTE (Fault Tolerant Ethernet)	ICCP (IEC 60870-6)	IPv4/IPv6
GE-SRTP	HART-IP	IEC 61850	OPC
IEEE 802.15.4 + ZigBee (ECC)	IEC 60870-5-101/104	ISA/IEC 62443 (series IACS)	TCP/IP
ISA/IEC 62443 (series IACS)	IPv4/IPv6	MODBUS	WiFi (IEEE 802,11I)
ISA SP100	ISA/IEC 62443 (series IACS)	NTP	
MELSEC-Q (Mitsubishi Electric)	OPC	Profinet	
MODBUS	NTP	SUITELINK	
Niagara Fox (Tridius)	SOAP	Tase-2	
Omron Fins	TCP/IP	TCP/IP	
PCWorx			
ProConOs			
Profibus			
Profinet			
Sercos II			
S7 Communications (Siemens)			

*ADD`s final goal is to address all main OT protocols without limiting to the ones mentioned in the table. The table is used as a reference and the on-boarding of additional protocols with done via a step by step collaboration with customers based on their priorities, needs and timeline.

We are located

SPAIN

HEADQUARTERS
IMDEA Software Institute
Campus Montegancedo
S/N, Pozuelo de Alarcón

BRAZIL

Market Place Tower
Av. Dr. Chucri Zaidan, 920
9º andar Cordeiro, São
Paulo, CEP: 04583-904

USA

Independence Wharf 470
Atlantic Avenue
Boston, Massachusetts
02210

SPAIN

OCF Industrial Cybersecurity
C/ Zugasti 12, Bajo.
Despacho 5 48610 Urduliz,
Bizkaia

MEXICO

Presidente Masaryk 111
Piso 1, Miguel Hidalgo
Polanco V Sección
11560 Ciudad de México

Source: Main protocols of levels of communication.
A look at industrial cybersecurity CESICAT*

* Centre for Information Security of Catalonia