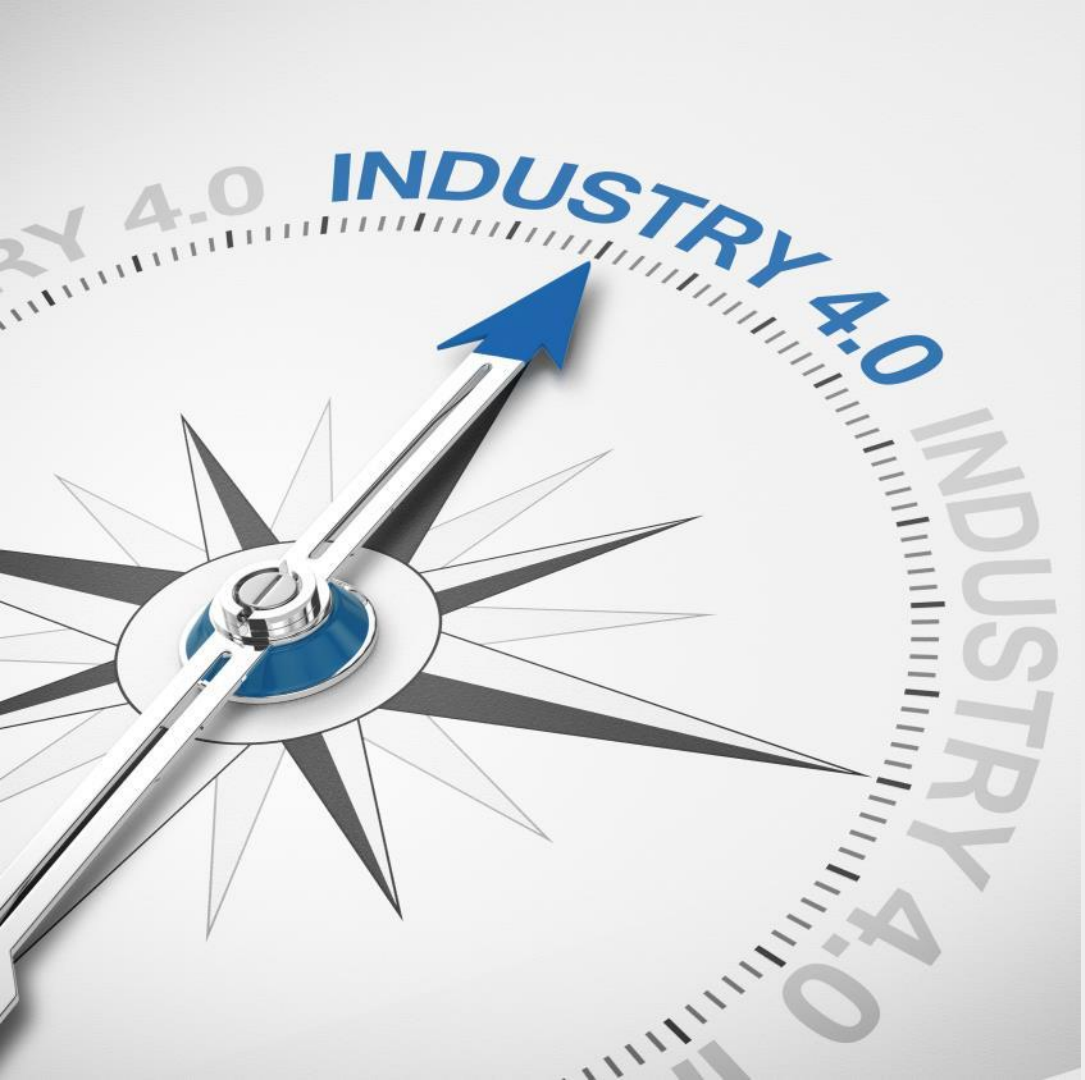


Secure your “things”

Luciana Scognamiglio
HPE Aruba Systems Engineer

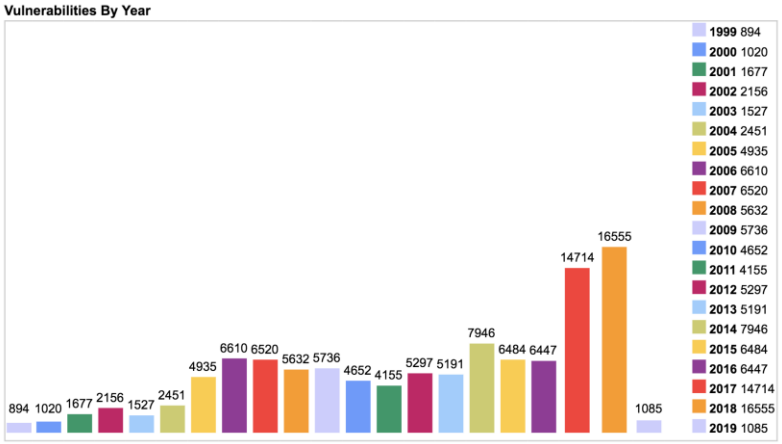
Organizzato da

Security Challenges – IoT & Vulnerabilities

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

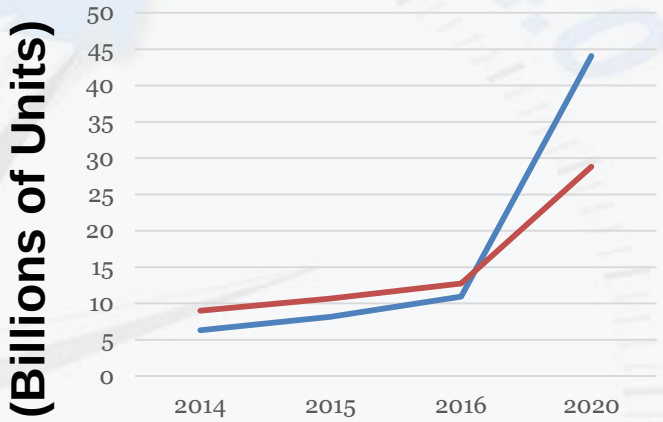
CONFINDUSTRIA

Vulnerabilities Identified per year



Source : MITRE CVE

IoT Units Installed Base by Category



Source : Gartner 2016

The Internet of Things **(IoT)** is the network of physical objects that contain embedded technology to **communicate** and sense or interact with their internal states or the external environment.

-Gartner

Security Challenges – Separate Systems

Today's Security Reality

Traditional security perimeter is broken

Mobility threats now originate from within

How To Take Control

ANIE FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE — CONFINDUSTRIA

Anie Servizi Integrati

VISIBILITY

- Know what's connected, connecting in your wired & wireless multivendor environment

aruba a Hewlett Packard Enterprise company · Hewlett Packard Enterprise · JUNIPER NETWORKS · BROCADE · CISCO · Extreme networks · ARISTA

CONTROL

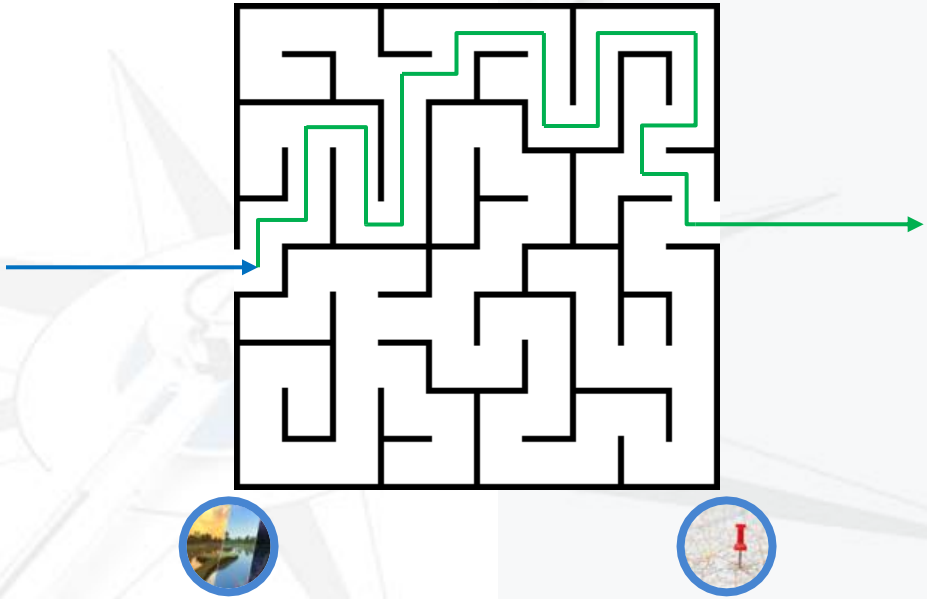
- Reduce risk and workload through Automation
- All devices are Authenticated or Authorized – NO UKNOWN DEVICES

RESPONSE

- Adaptive response brokering best of breed security solutions

paloalto NETWORKS · splunk> · ArcSight · MobileIron · DUO · intel Security · Microsoft · Check Point SOFTWARE TECHNOLOGIES LTD.

Automated Authentication & Authorization



user/role

device type / health

- IoT
- BYOD
- CORP

time / day

location

Visibility – Profile Everything

Contractor

IoT

Headless

Employee BYOD

Infrastructure

Visitor

Administrator

Employee

Servers

Data & Storage

Internal Applications

Cloud Applications

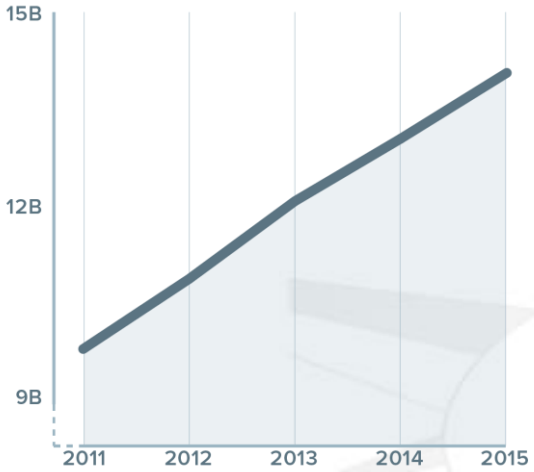
Network Infrastructure

The Security Gap

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

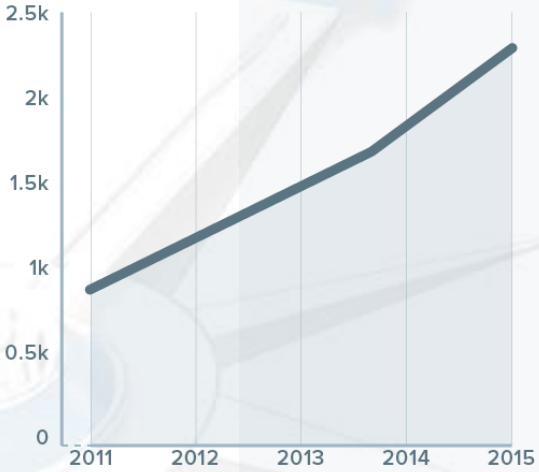
CONFINDUSTRIA

SECURITY SPEND

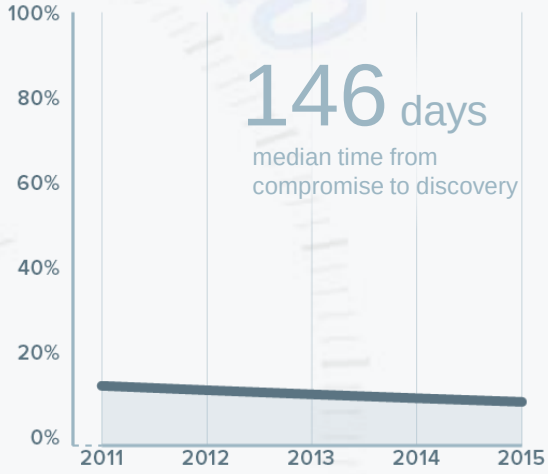


PREVENTION & DETECTION (US $B)

DATA BREACHES



BREACHES



146 days

median time from compromise to discovery

% DISCOVERED INTERNALLY

SOURCES | Mandiant M-Trends 2016, Verizon Data Breach Investigations 2016, IDC 2016

Attacks on the Inside

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENDED TO LEAK INFORMATION

NEGLIGENT

DDoS attack from 10M+ hacked home devices took down major websites

ALL USED THE SAME PASSWORD

Technology

MACHINE LEARNING

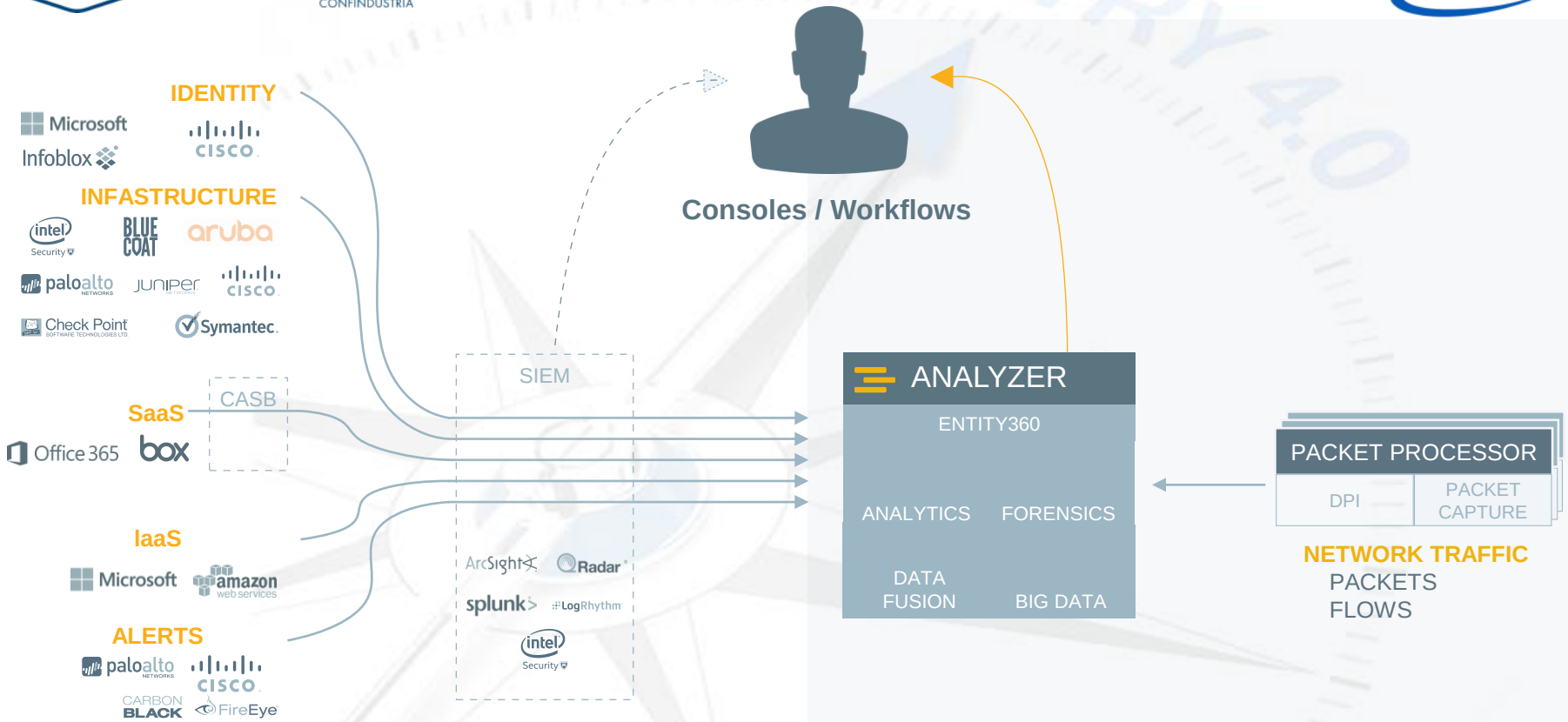
CAN DETECT UNKOWN THREATS

+

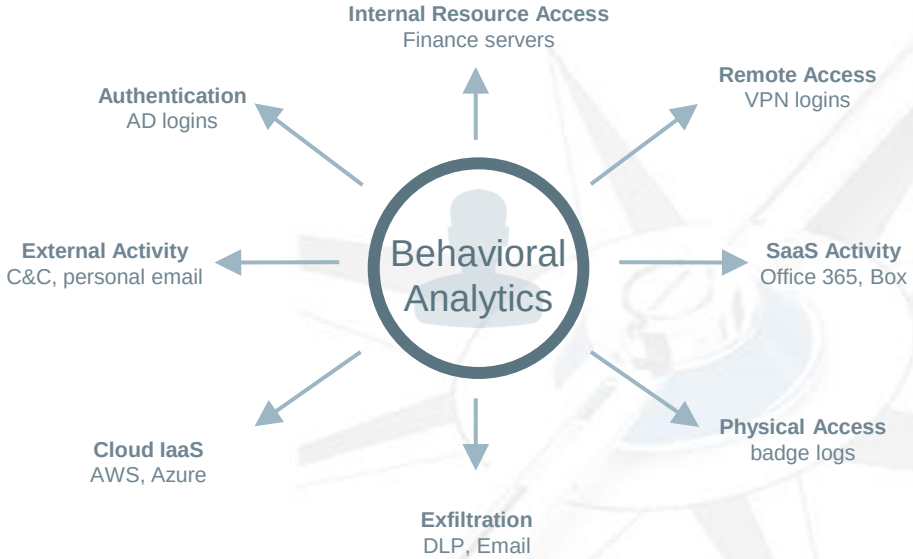
BIG DATA

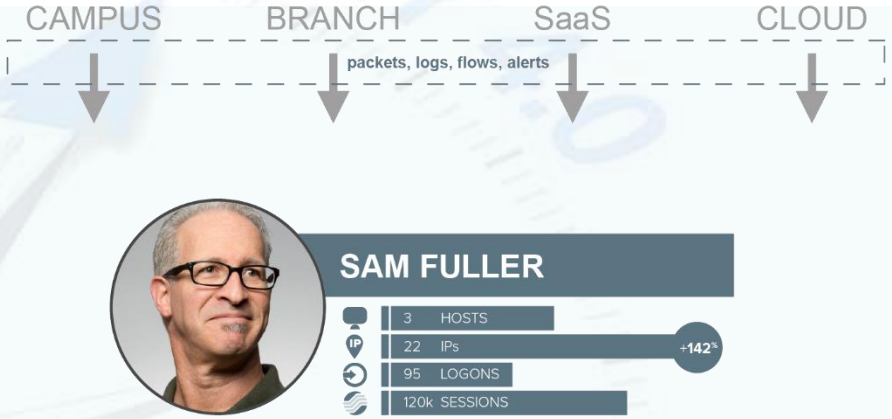
CAN SCALE

Solution – Integrated with Security Ecosystem



Behavior – Many Different Dimensions





Basics of Behavioral Analytics

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

MACHINE LEARNING

UNSUPERVISED

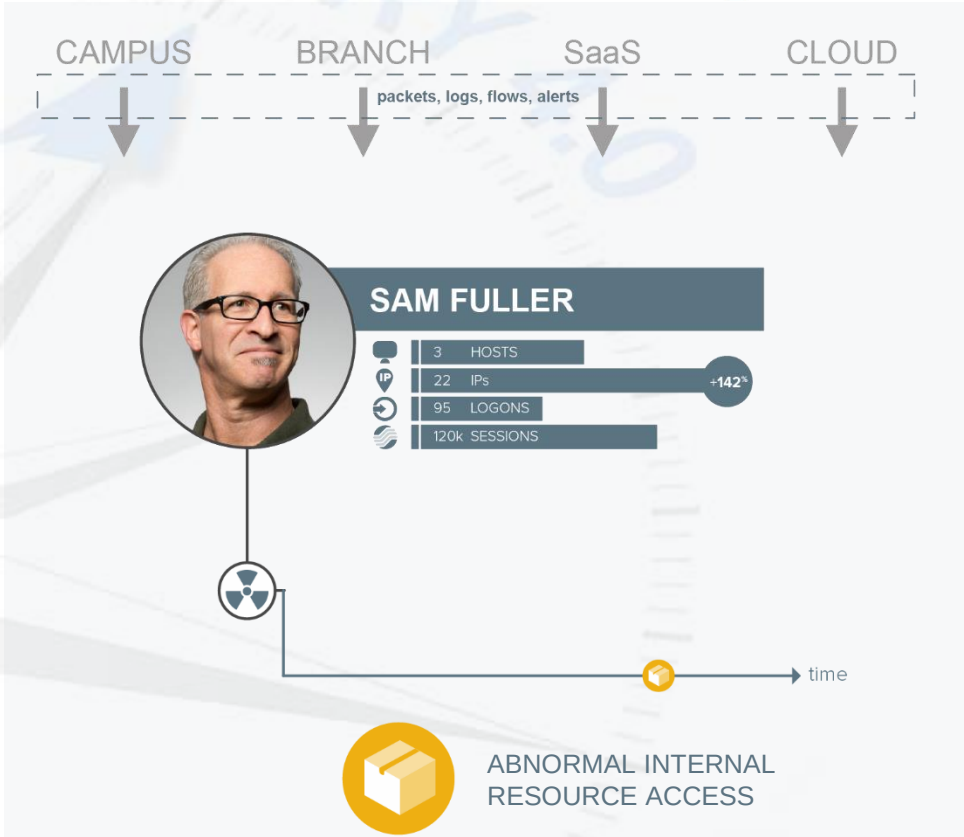
Behavioral Analytics

BASELINES

HISTORICAL

+

PEER GROUP



Finding the Malicious in the Anomalous

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

BUSINESS CONTEXT
High Value Assets
High Value Actors

MACHINE LEARNING
SUPERVISED
UNSUPERVISED

THIRD PARTY ALERTS
DLP
Sandbox
Firewalls
STIX
Rules
Etc.