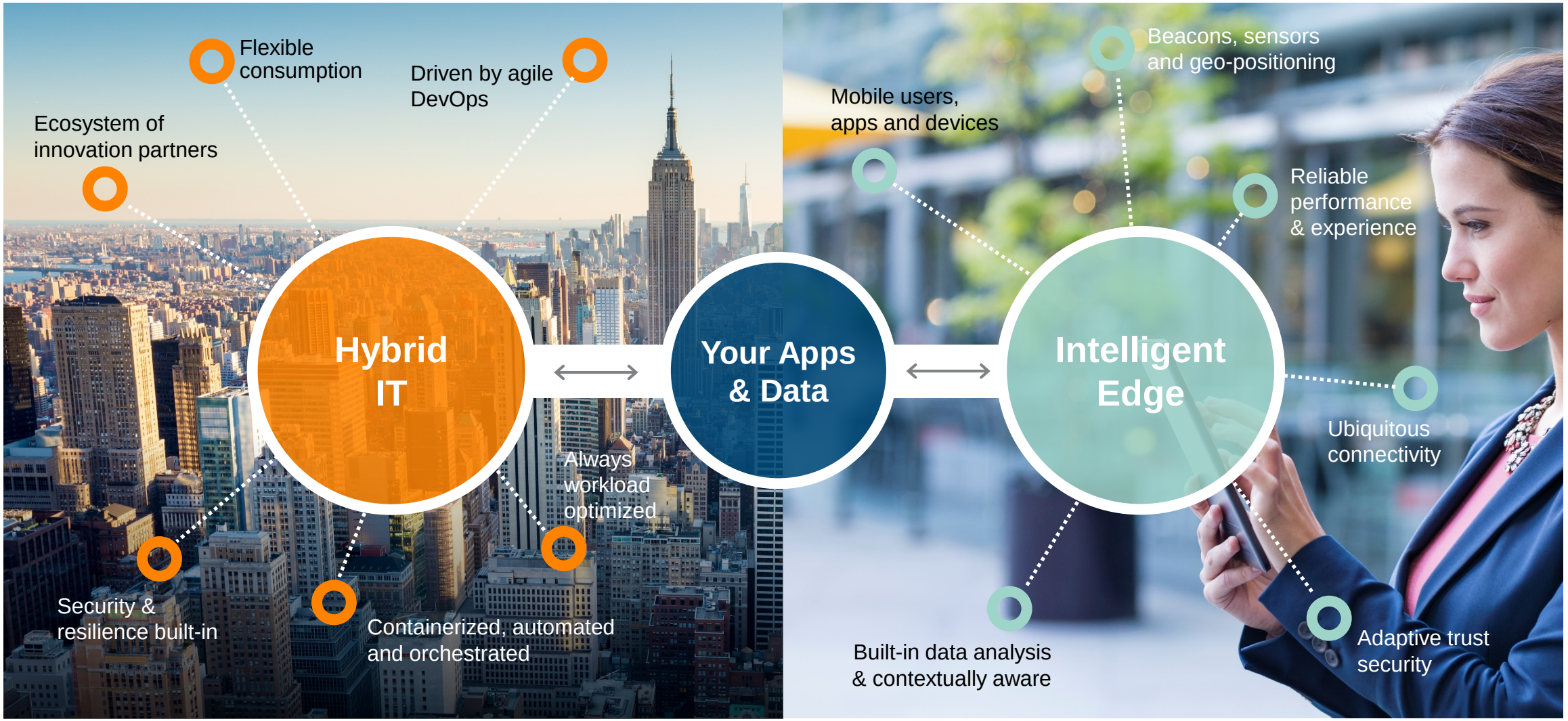
aruba
a Hewlett Packard Enterprise company

Intelligent Edge Protection

Sicherheit im Zeitalter von IoT und Mobility

September 26, 2017



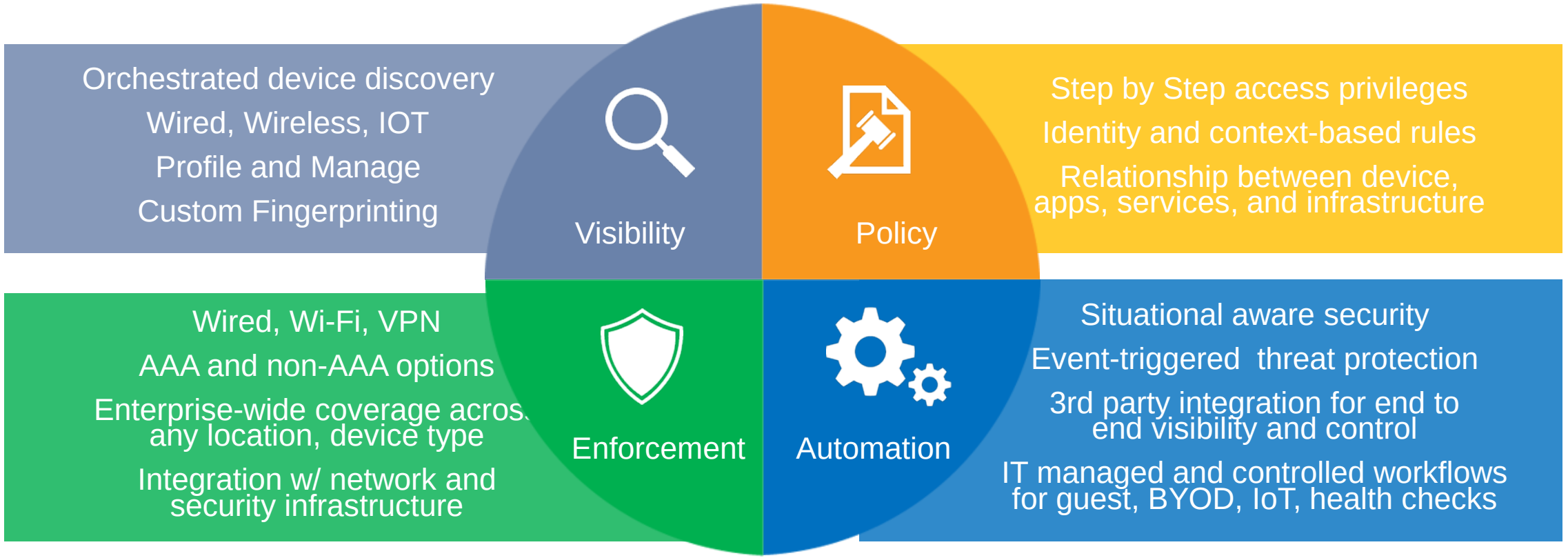
aruba
a Hewlett Packard Enterprise company

“Aruba takes untrusted devices and converts them into sources of trusted and actionable data”

The Fundamentals of Network Access

- **Profile** the Asset
  - Asset, location and basic posture information
  - Passive and active techniques
- **Validate** the Identity
  - Traditional network authentication methods 802.1x, MAC, PSKs
  - Leverage profile data as input to identity
  - Reference an existing asset register or start building one
- **Authorize** its Role
  - Lookup existing databases or trigger approval workflows
  - IT policies about security behavior, risk, access control
  - OT policies regarding SLA, auditing, compliance

The 4 stages of visibility and control



aruba
a Hewlett Packard Enterprise company

ClearPass Policy Manager and NAC Solution

CLEARPASS POLICY MGR

Built-in:

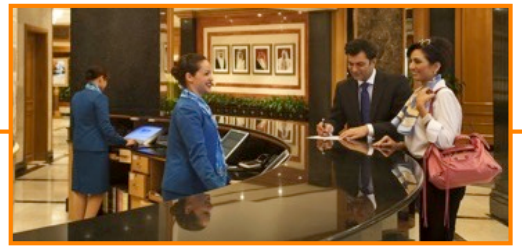
- Policy Engine
- RADIUS/CoA/TACACS
- Profiling
- Accounting/reports
- Identity store

REMOTE LOCATION

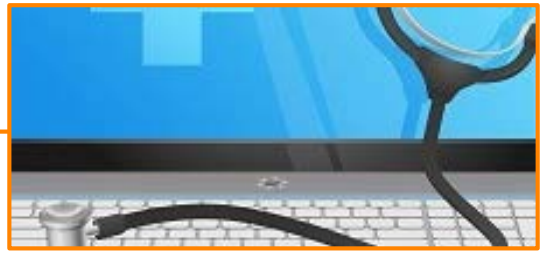
Expandable Applications

- BYOD onboarding
- Simple guest access
- Health assessments

Onboard



Guest



OnGuard

aruba
a Hewlett Packard Enterprise company

Sources of Usable Context

Device Profiling

- Samsung SM-G900
- Android
- “Jons-Galaxy”

EMM/MDM

- Personal owned
- Registered
- OS up-to-date

- Hansen, Jon [Sales]
- MDM enabled = true
- In-compliance = true

Identity Stores

- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive office
- City – London

Active Directory

Office 365

MySQL

Google Apps

SAML

OAUTH 2

Enforcement Points

- Location – Bldg 10
- Floor – 3
- Bandwidth – 10Mbps

Comprehensive Profiler Methods

Helps ensure accurate fingerprints

Passive Profiling

- DHCP Fingerprinting (MAC OUI & Certain Options)
  - DHCP Relay or SPAN
- HTTP User-Agent
  - AOS IF-MAP Interface, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Cisco Device Sensor
- Netflow/IPFIX
  - Identifies open ports

Active Profiling

- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP





aruba
a Hewlett Packard Enterprise company

ClearPass Exchange

Granular traffic control with user and device data

Next-Gen Perimeter Defense

paloalto NETWORKS, ★ Juniper Networks, Check Point Software Technologies Ltd, Fortinet

Visibility and interactive control features

ArcSight An HP Company, splunk>, RSA SecurID, ServiceNow, QRadar, ★ Duo

SIEM, Automation, MFA

Client Devices

IoT Devices

MDM / EMM

airwatch, MobileIron, Google, Citrix, ★ Microsoft, BlackBerry

Network controls using real-time device data

Infrastructure

aruba a Hewlett Packard Enterprise company, Hewlett Packard Enterprise, Brocade, Juniper Networks, Cisco

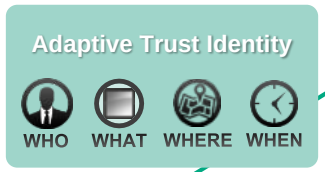
Visibility into location and time with granular controls

aruba a Hewlett Packard Enterprise company

★ NEW

Demo Time

Use Case: IoT Device Security Incident



ClearPass

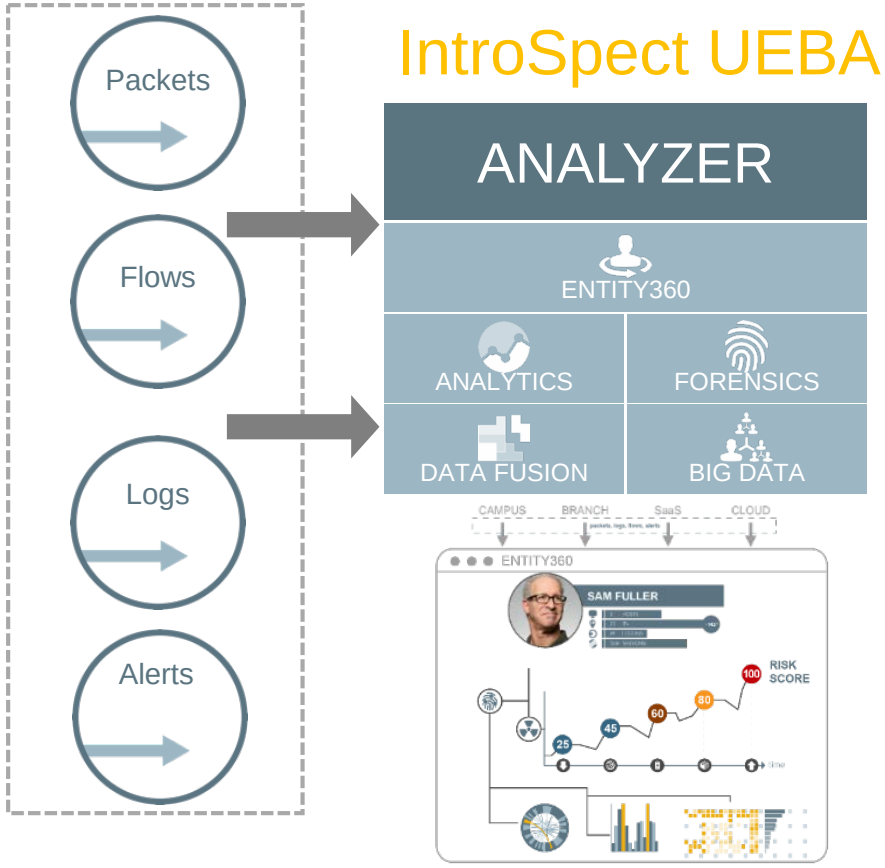
Operator — WHO

Asset DB — WHAT, WHERE, WHEN

- Update switch (sandbox role, shutdown port)
- Update FW policy for store
- Block access to update URL
- Generate notifications to OT and IT
- Update risk profile for other fridges
- Flag inventory application to review data

Vendor: **Selecta**
Class: **Beverage Fridge**
Role: **Store IoT devices**
Location: **Pike Place, Seattle**
Authentication: **MAC, SQL**
Mac Address: **AA:BB:CC:11:22:33**
Firmware Version: **12.35b**
Risk Profile: **High (open ports)**
Polling Frequency: **83 in last 5 mins**
BW Profile: **89% increase**

IntroSpect Overview



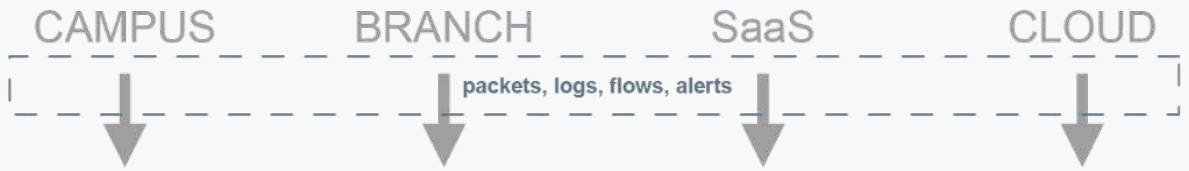
Entity360 Profile with Risk Scoring

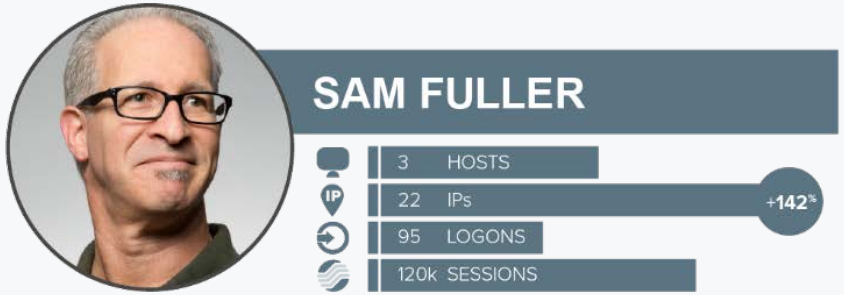
- Most complete visibility
- 100+ supervised and unsupervised machine learning models
- Integrated forensics data
- Scales from small projects to full enterprise deployment
- Open, integrated platform
- Fast-start option

aruba
a Hewlett Packard Enterprise company

The Start: User/Entity View of Events

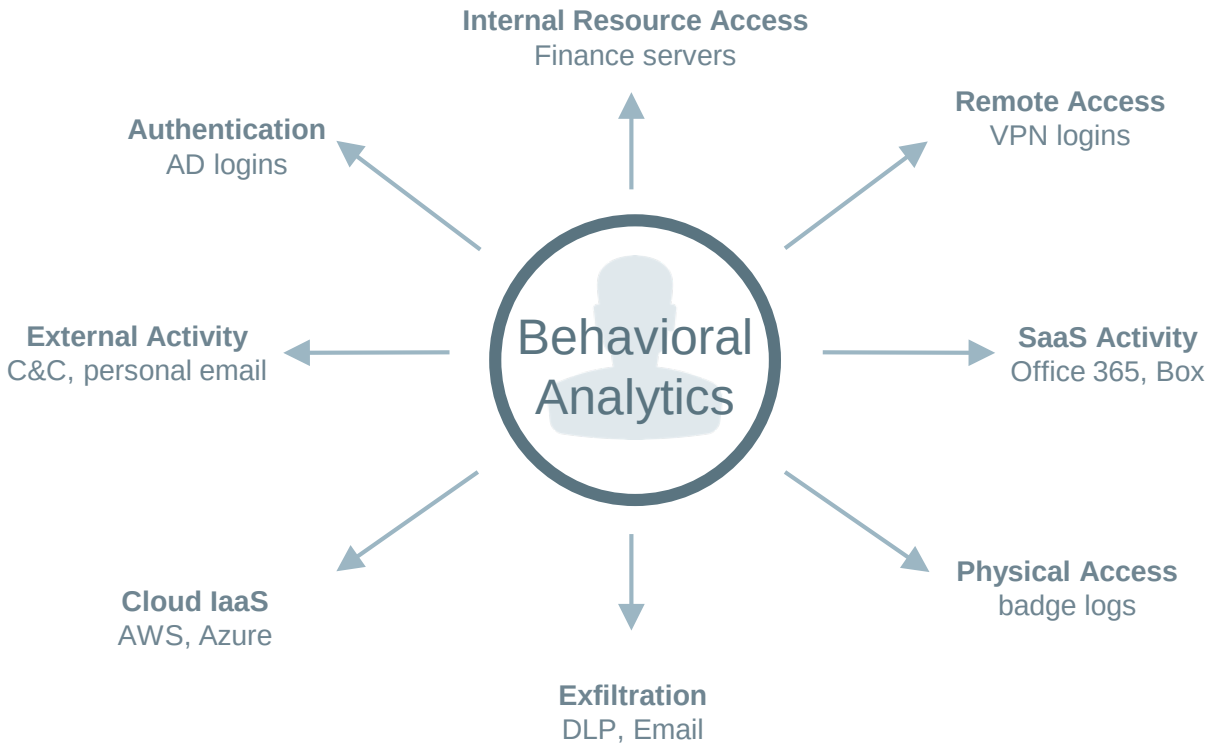
IP Address

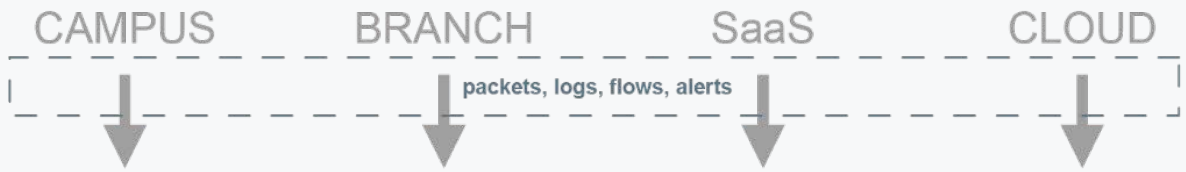


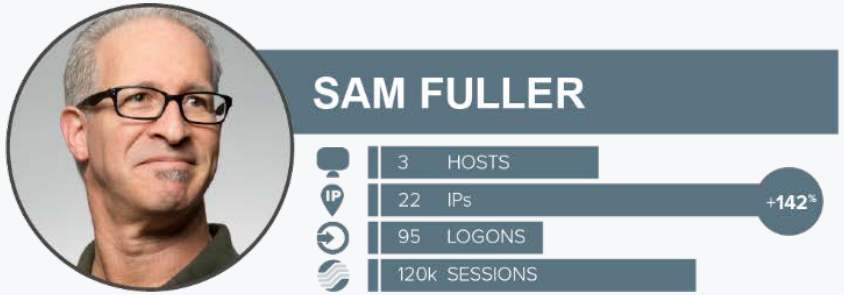


aruba
a Hewlett Packard Enterprise company

Behavior – Many Different Dimensions







aruba
a Hewlett Packard Enterprise company

Basics of Behavioral Analytics

MACHINE LEARNING

UNSUPERVISED

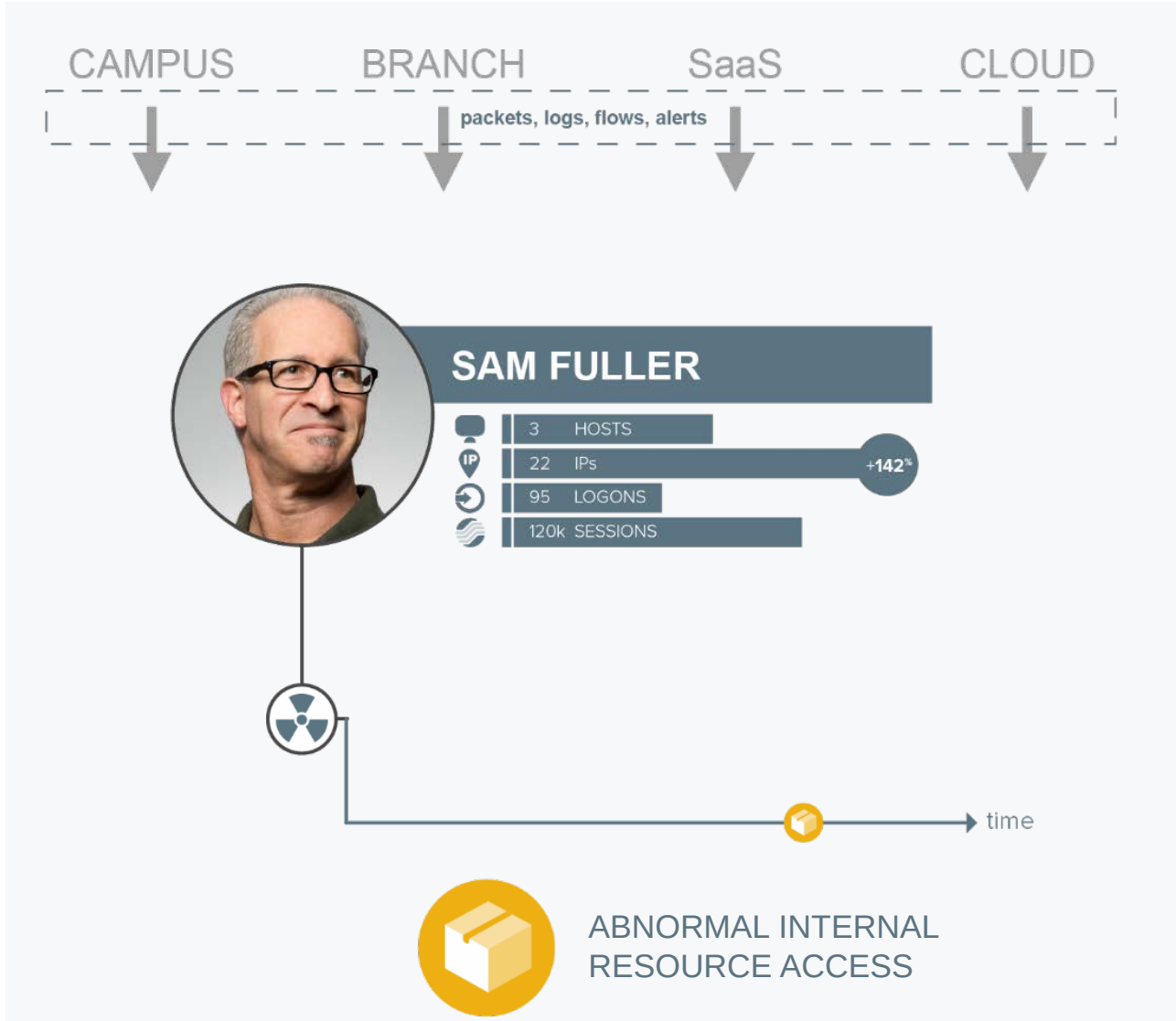
Behavioral Analytics

BASELINES

INDIVIDUAL
HISTORICAL

+

PEER GROUP
(e.g. from AD designation or profiling from ClearPass)



aruba
a Hewlett Packard Enterprise company

Finding the Malicious in the Anomalous

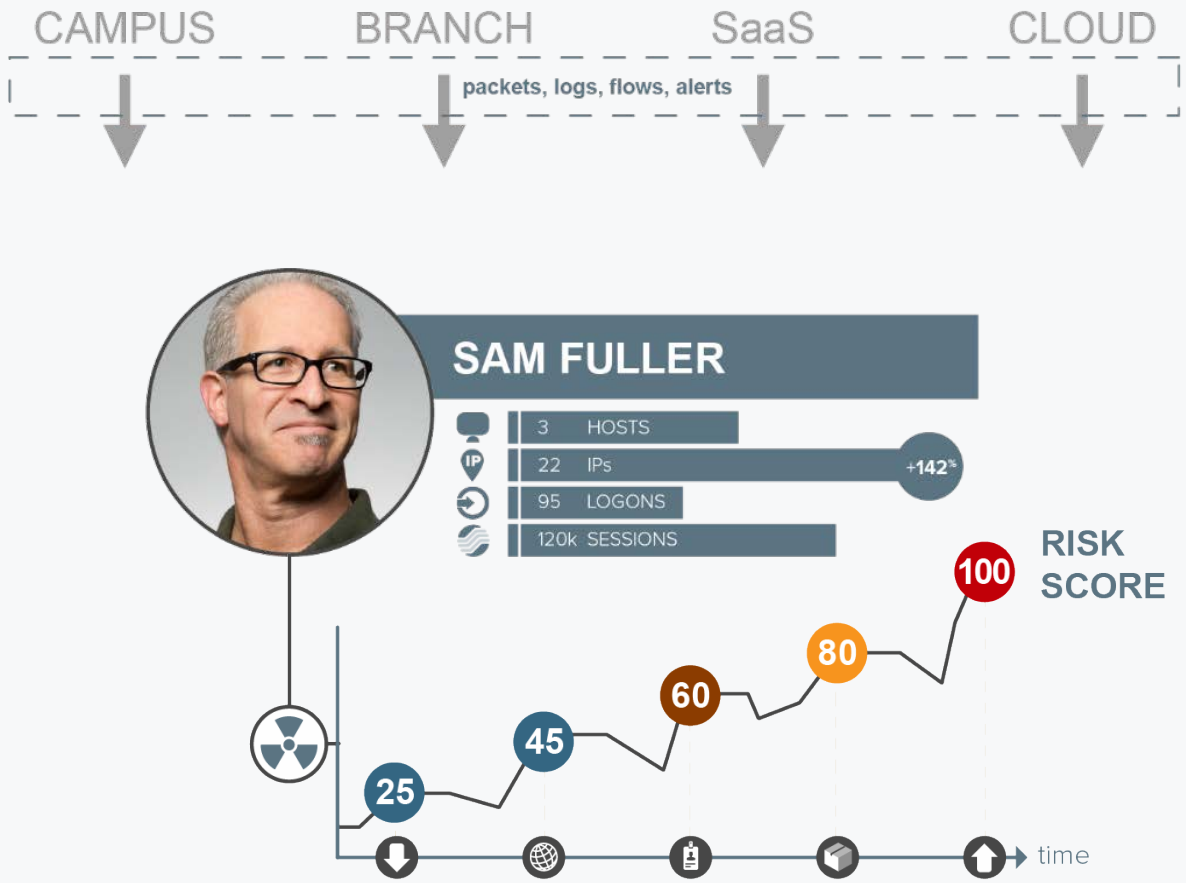
BUSINESS CONTEXT
High Value Assets
High Value Actors

MACHINE LEARNING

SUPERVISED
UNSUPERVISED

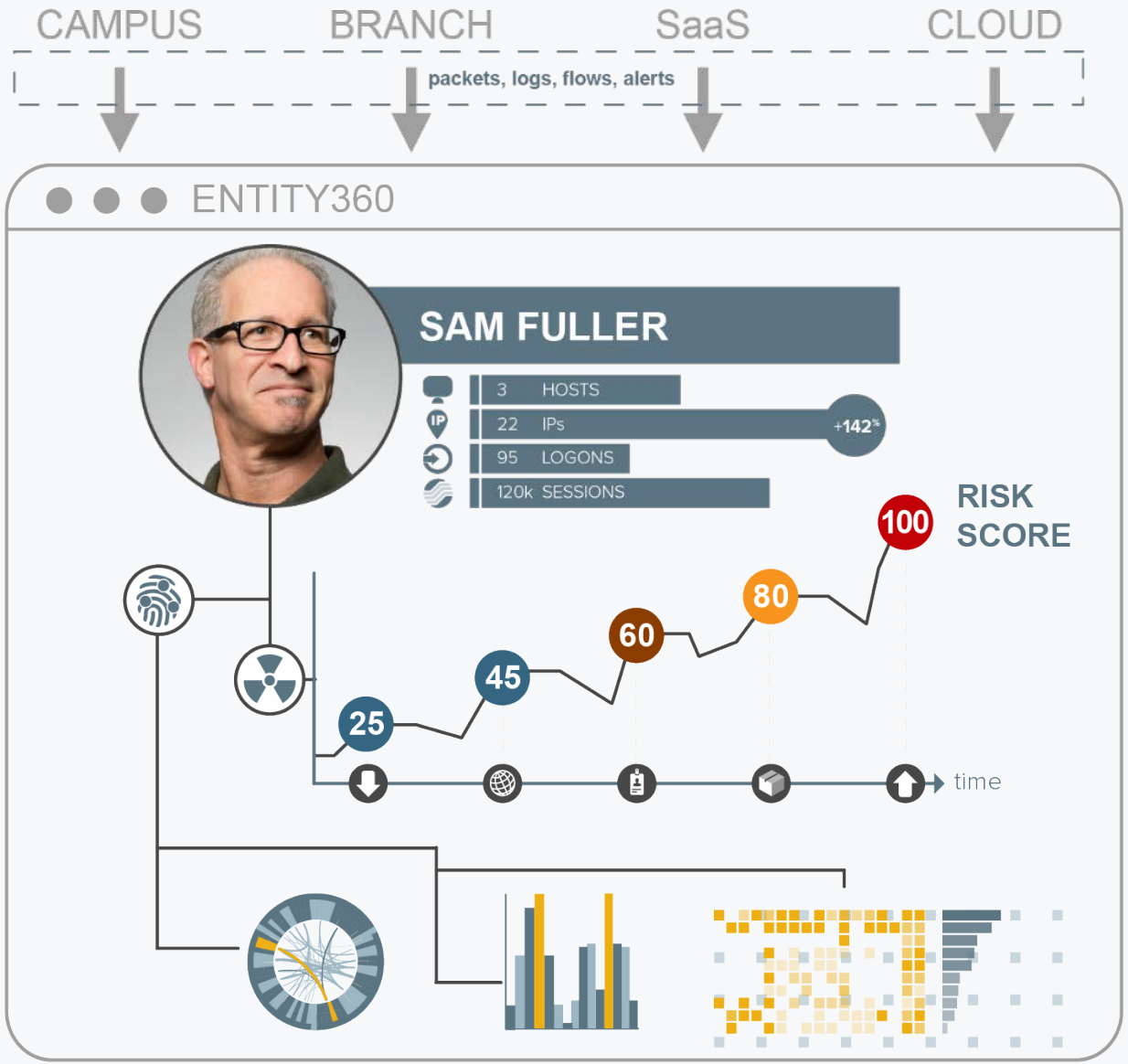
THIRD PARTY ALERTS

DLP
Sandbox
Firewalls
STIX
Rules
Etc.



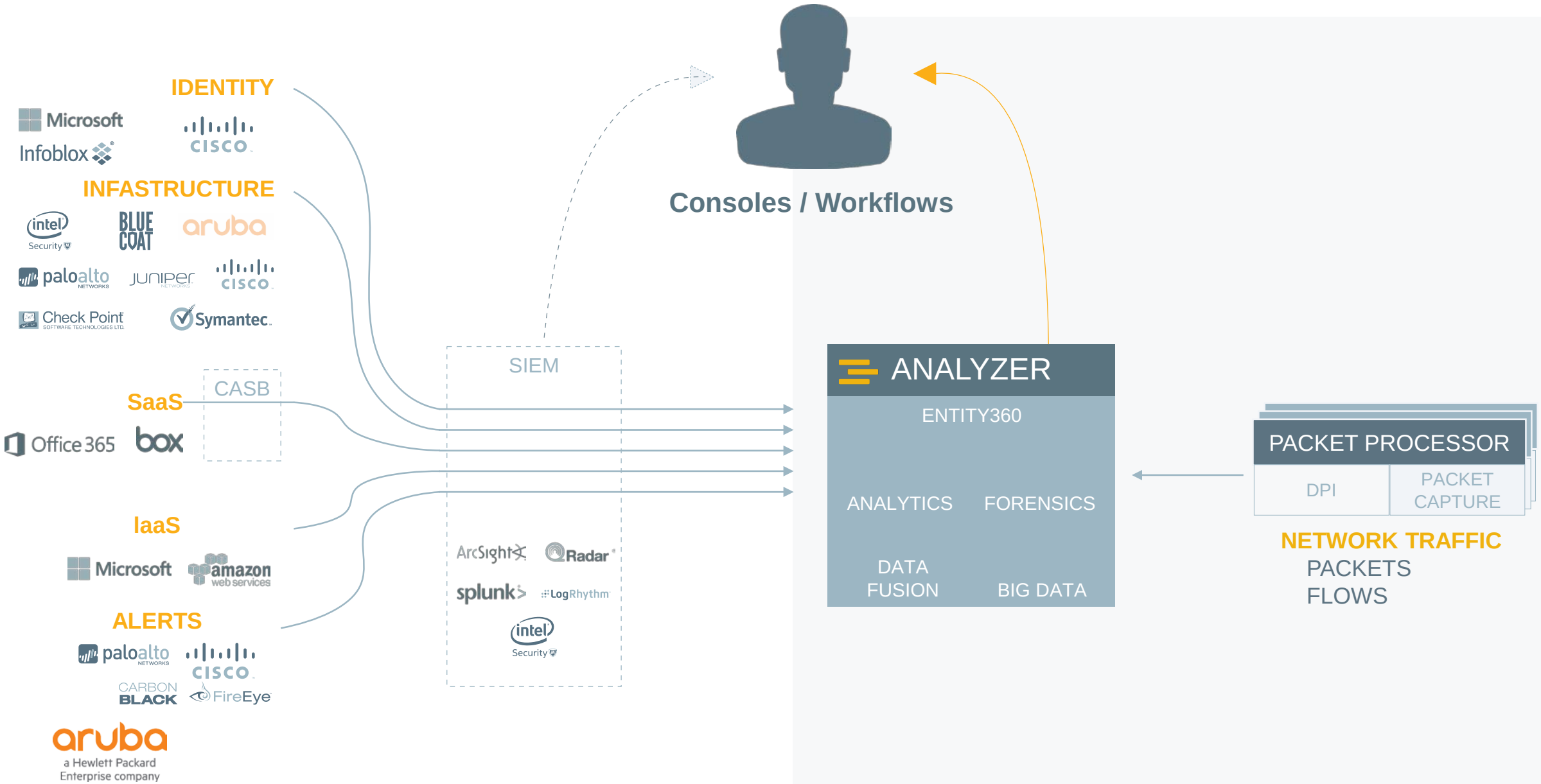
aruba
a Hewlett Packard Enterprise company

Accelerated Investigation and Response



aruba
a Hewlett Packard Enterprise company

SOLUTION – INTEGRATED WITH SECURITY ECOSYSTEM



ClearPass + IntroSpect = 360° Protection!

1. Detect and Authorize

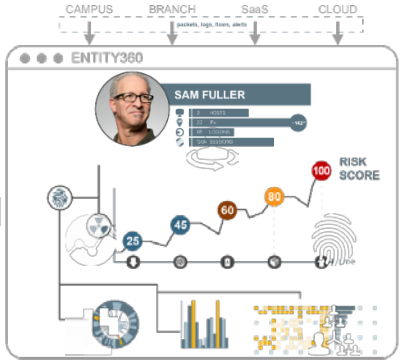
Wired/Wireless
Device Authentication

ClearPass Policy Manager

User/Device Context

Actionable Alerts

IntroSpect UEBA



Entity360 Profile with Risk Scoring

2. Monitor and Alert

3. Decide and Act

ClearPass Real-time Policy-based Actions

- Real-time quarantine,
- Re-authentication
- Bandwidth Control
- Blacklist

aruba
a Hewlett Packard Enterprise company

www.arubanetworks.com/clearpass

www.IntroSpect.com

Demo Time

Why all of this?

- BYOD, NAC, Guest Access, OT, IT
  - Different level of scale…..again
  - Cannot VLAN or MAC whitelist your way out of IoT
  - Automation a requirement, not a nice to have

- Role Based Access Control is key
  - Extend WLAN roles to the LAN and VPN
  - Leverage controllers for low bandwidth LAN devices
  - Firewall at the edge to help with network segmentation

a Hewlett Packard Enterprise company

OLIVER WEHRLI

TECHNOLOGY CONSULTANT | SWITZERLAND
T: +41 58 199 00 55

UEBERLANDSTRASSE 1 | CH-8600
DUEBENDORF | SWITZERLAND

AIRHEADS COMMUNITY | **FOLLOW US** | **Twitter** | **LinkedIn**

Thank You