Mikrosegmentacja w sieciach kampusowych

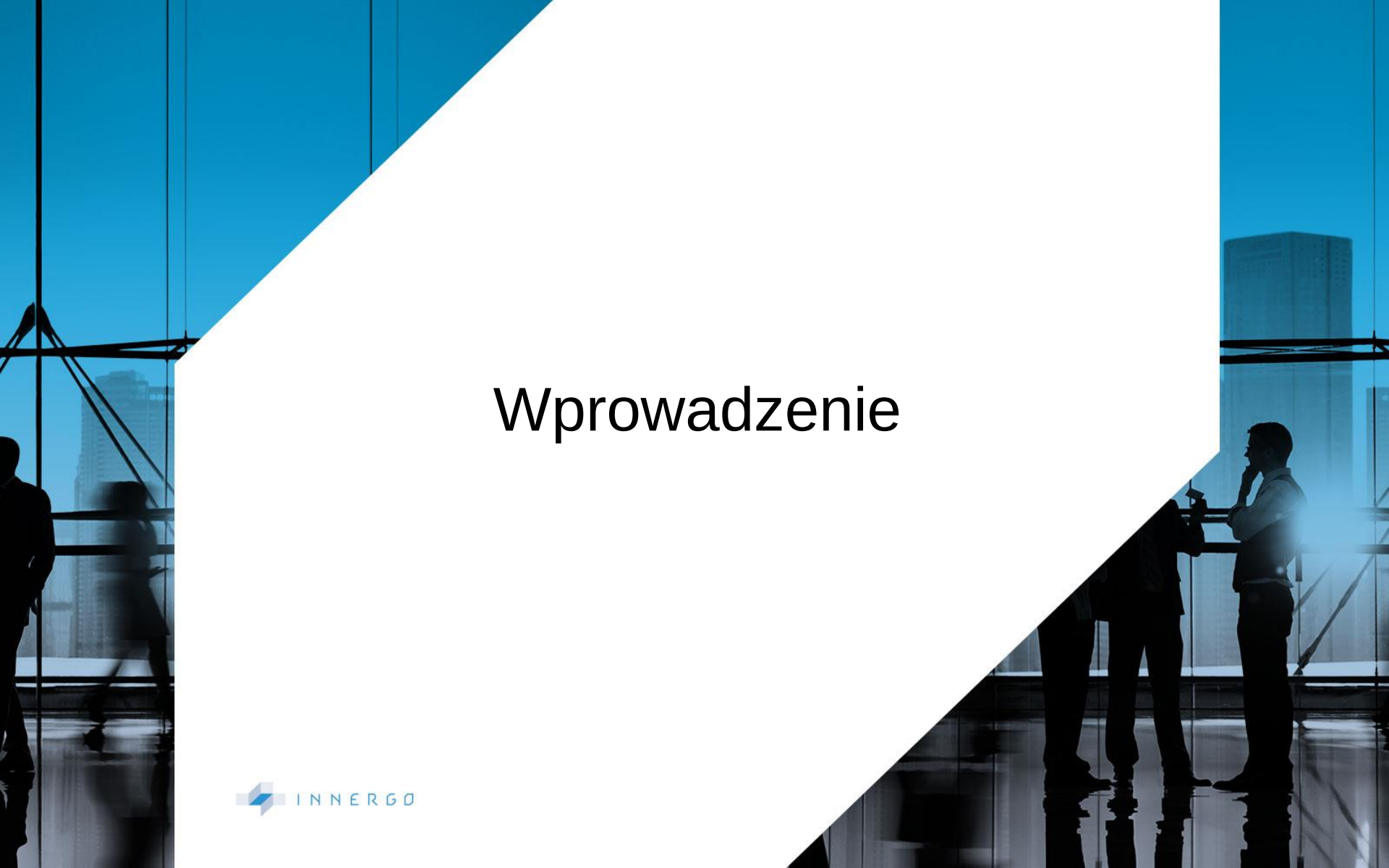
Aruba 360 Security Fabric

Warszawa, 18.04.2018

AGENDA

1. Wprowadzenie
2. Mikrosegmentacja
3. Mikrosegmentacja w produktach Aruba Networks
4. Aruba 360 Secure Fabric

Wprowadzenie



Aruba Networks

a Hewlett Packard Enterprise company

- Założona w 2002 roku
- W 2004 roku domniemane rozmowy na temat przejęcia przez Cisco Systems
- W 2005 roku Cisco kupuje największego konkurenta Aruba - Airespace
- Pierwszy duży, globalny kontrakt – Microsoft w 2005 roku
- W 2015 roku, Aruba zostaje przejęta przez Hewlett Packard Enterprise
- HQ – Santa Clara, Kalifornia

Pojęcie roli

- Identyfikator przypisywany użytkownikowi podłączonemu do systemu
- Definiuje uprawnienia użytkownika takie jak dostęp do systemów, politykę firewall, poziom uprawnień, prawo do odczytu itp.
- Znaczenie lokalne dla systemu gdzie została zastosowana

Zastosowanie roli w systemach IT

- Dostęp w oparciu o rolę stosowany powszechnie w kontroli dostępu administracyjnego
- Wielu producentów wspiera mechanizm roli dla dostępu do sieci
- Rola dostępna na urządzeniach firewall, dynamicznie przypisuje polityki do ruchu użytkownika (Palo Alto, Check Point, Fortinet)

Pojęcie roli w sieci

- Identyfikator przypisywany każdemu użytkownikowi podłączonemu do urządzenia sieciowego
- Definiuje uprawnienia użytkownika takie jak dostęp do systemów i kontrakt QoS, może również zwierać politykę aplikacyjną
- Znaczenie lokalne
- Przeważnie przekazywana z systemu typu NAC (np. ClearPass)
- Rola może ulec zmianie w trakcie trwania sesji

Elementy roli w Aruba Networks

- Polityka firewall, w tym reguły stateful oraz QoS
- VLAN ID
- Czas reautentykacji
- Parametry VPN
- Przekierowanie na stronę WWW
- Maksymalna ilość sesji
- Tryb pracy (tunelowanie)

Downloadable User Roles

Single point of policy management

– Dynamically assigned by ClearPass at the time of authentication

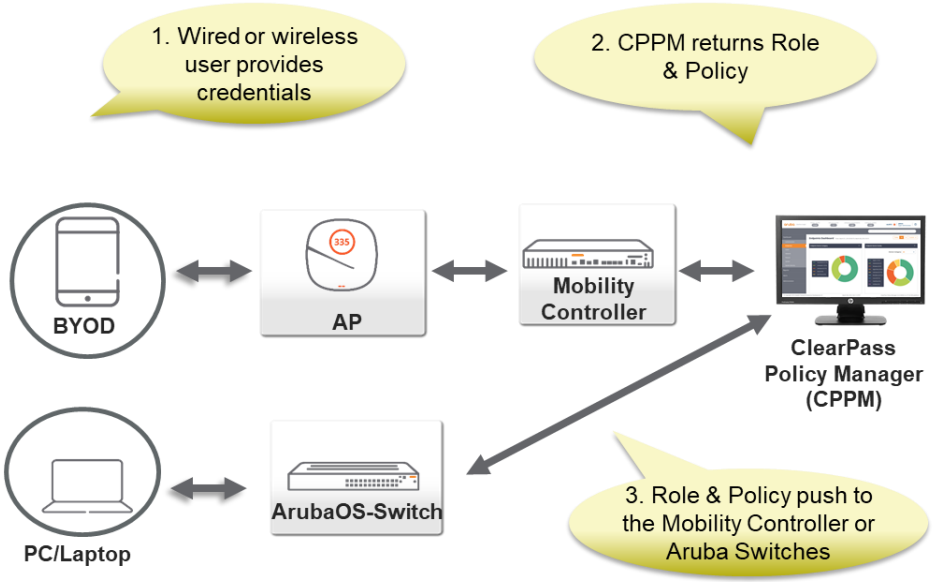
Builds on top of the existing local User Roles

– Every user/device is assigned a User Role

– User Role policies include QoS, VLAN, ACL, Rate Limits

Consistent wired/wireless policy management

– Same as WLAN AP, simplify policy configuration and management



Mikrosegmentacja

INNERGO

Mikrosegmentacja

- Segmentacja - logiczna separacja grup usług/ruchu tego samego typu w sieci, przeważnie realizowana na bazie VLAN
- Mikrosegmentacja – separacja pojedynczych elementów, takich jak serwery czy użytkownicy
- Zwiększa:
  - Kontrolę – więcej ruchu jest poddawane weryfikacji z politykami bezpieczeństwa
  - Widoczność ruchu (analityka)

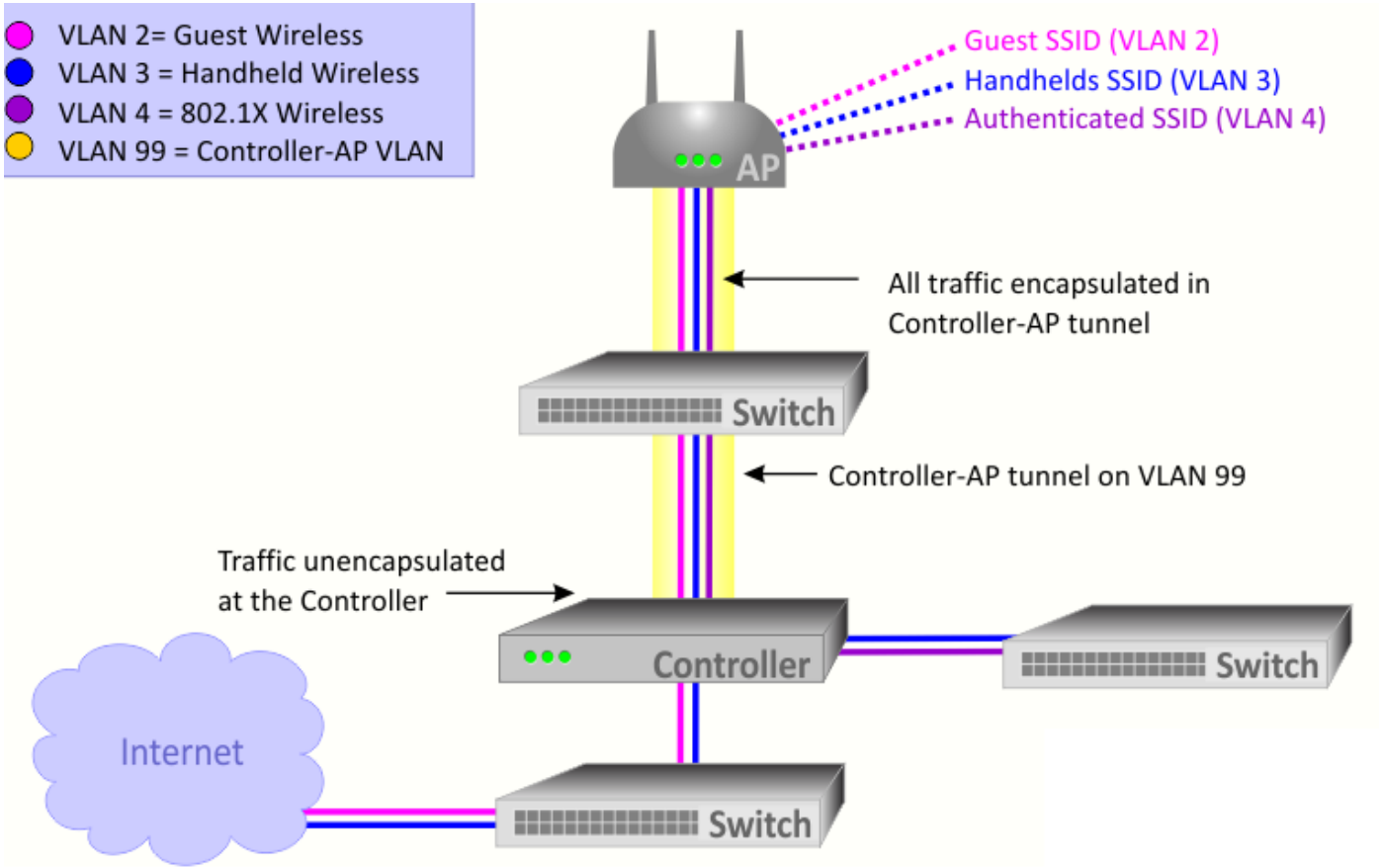
Mikrosegmentacja w Data Center

- Powszechnie stosowana w dużych ośrodkach
- Najczęściej pod nazwą Network Overlay lub Network Virtualization
- Wiele technologii:
  - VXLAN
  - NVGRE
  - STT
  - LISP
  - SDN

Wyzwania związane z mikrosegmentacją

- Infrastruktura
- Zarządzanie
- Integracja z istniejącymi systemami kontroli dostępu do sieci i systemami operacyjnymi

Transport ruchu w sieci bezprzewodowej



Mikrosegmentacja w produktach Aruba Networks

INNERGO

Mikrosegmentacja w kontrolerach Aruba

- Klasyczny model tunelowania ruchu z AP do kontrolera
- Możliwość tworzenia tunelu do więcej niż 1 kontrolera – Multi Zone
- Kontroler jest firewall’em:
  - Pełna inspekcją state-full
  - Kontrola aplikacji
  - Filtrowanie URL’i

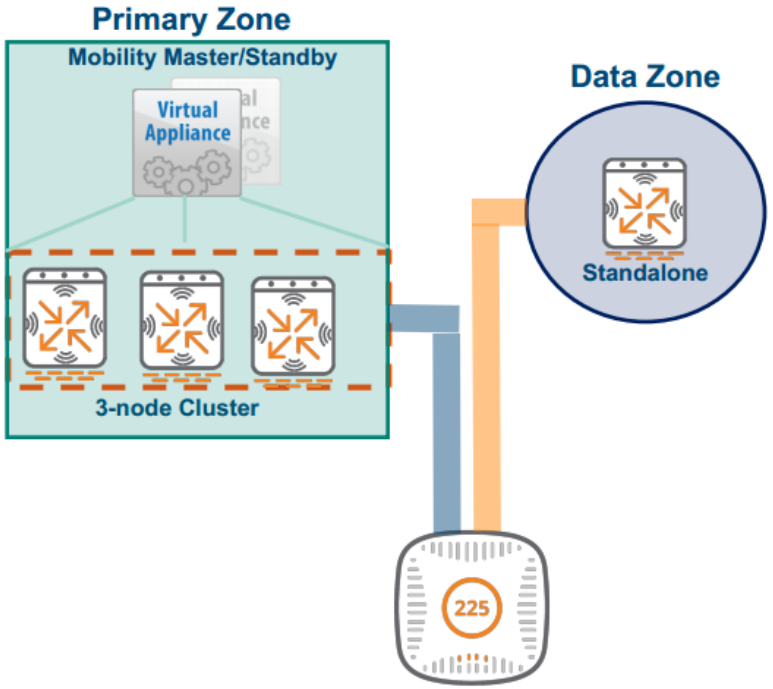
Multi Zone

Zone

1. Collection of controllers under a single administration domain
2. Can be a single controller or a cluster of controllers

Multi-Zone AP

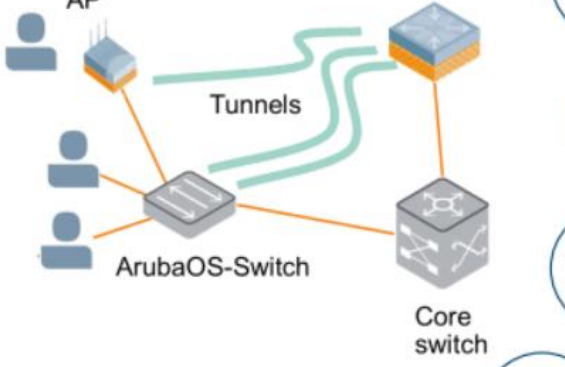
1. AP capable of terminating its tunnels on controllers residing in different zones



Mikrosegmentacja przełącznikach Aruba

- Klasyczny model tunelowania ruchu z AP do kontrolera
- Możliwość tworzenia tunelu do więcej niż 1 kontrolera – Multi Zone
- Kontroler jest firewall’em:
  - Pełna inspekcją state-full
  - Kontrola aplikacji
  - Filtrowanie URL’i

Per Port Tunneled Node

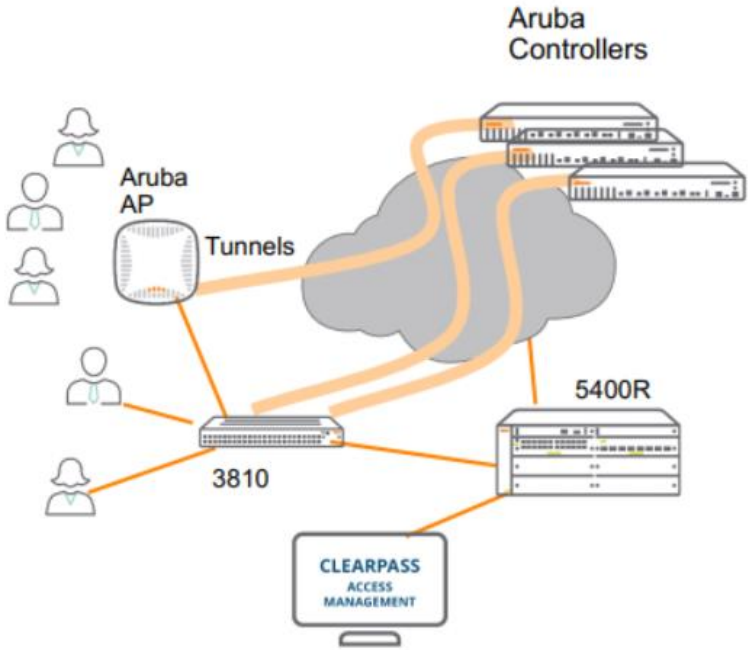


- Consistent wireless-wired network architecture
- Centralized role-based policy enforcement
- Access to Aruba controller's security features such as Firewall, packet inspection and finger printing
- Enhanced security with traffic separated by tunnels
- Redundant controllers supported

* Tunneled Node is supported in 2920/2930/3810/5400R & ArubaOS 6.5, 8.1+

Per User Tunneled Node

- Secured and flexible control of access layer
  - With ClearPass or switch configuration, only traffic from a specific user/device role is sent to the mobility controller
  - Policies (e.g., QoS, ACL, rate-limit) can be enforced at Tunneled Node ports or at the controller
- Access to Controller's applications
  - Users can access Controller's applications such as stateful firewall and AppRF
- Higher availability and scalability
  - Load balance to multiple controllers for high scalability
  - Stateful failover to standby management module for high availability
- Support on 5400R/v3, 3810, and 2930F/M
  Requires AOS 8.1 or later in the controllers

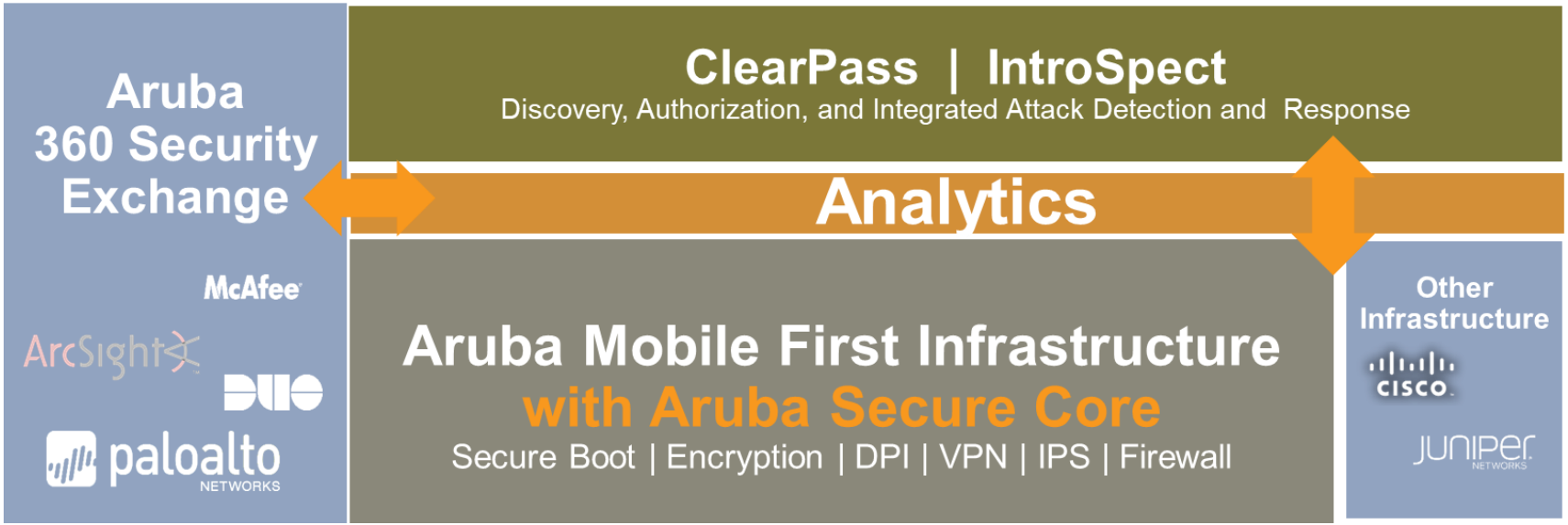


Aruba 360 Secure Fabric

INNERGO

Aruba 360 Secure Fabric

aruba
a Hewlett Packard Enterprise company



INNERGO

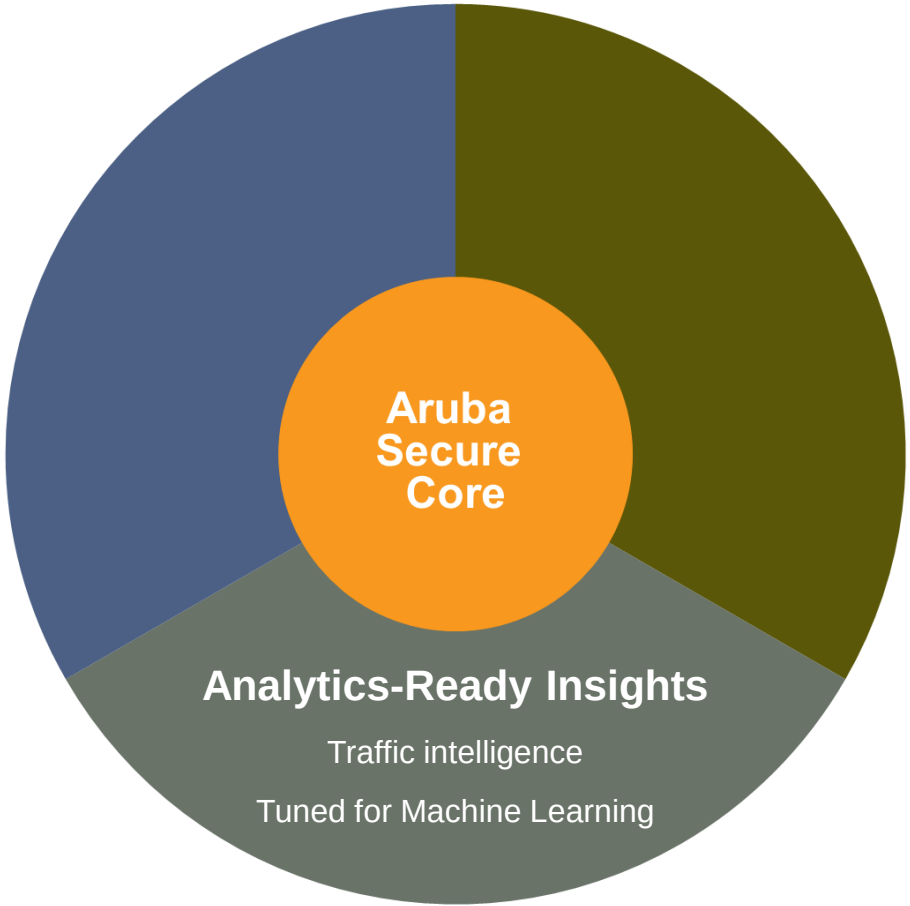
Secure Core

aruba
a Hewlett Packard Enterprise company

Trusted Traffic

Centralized encryption

Per-user virtual connection/FW



Device Assurance

Hardware-enforced protection

Per-user virtual connection/FW

INNERGO

ClearPass Policy Manager

aruba
a Hewlett Packard Enterprise company

Security Exchange

aruba
a Hewlett Packard Enterprise company

aruba a Hewlett Packard Enterprise company | cisco | JUNIPER NETWORKS | BROCADE | Hewlett Packard Enterprise | ARISTA | SIEMENS

ACCESS POINT

CONTROLLER

SWITCH

paloalto NETWORKS | Check Point SOFTWARE TECHNOLOGIES LTD. | TippingPoint | TREND MICRO

Firewall / IPS

INFRASTRUCTURE

PERIMETER

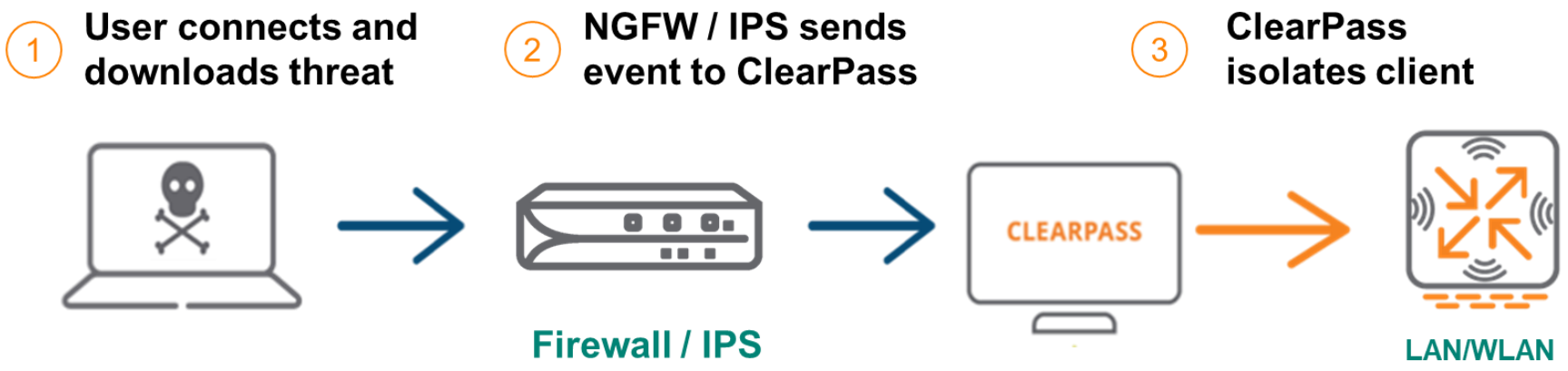
ArcSight An HP Company | DUO | airwatch by vmware | splunk> | MobileIron | intel Security

SECURITY & ENDPOINT MANAGMENT

INNERGO

Przykładowa integracja w ramach Security Exchange

aruba
a Hewlett Packard Enterprise company



INNERGO

Wsparcie dla produktów

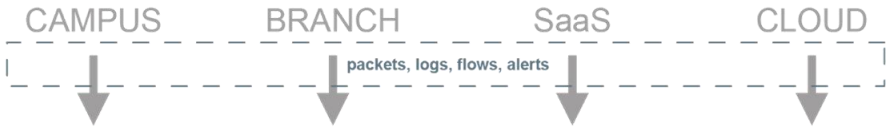
aruba
a Hewlett Packard Enterprise company

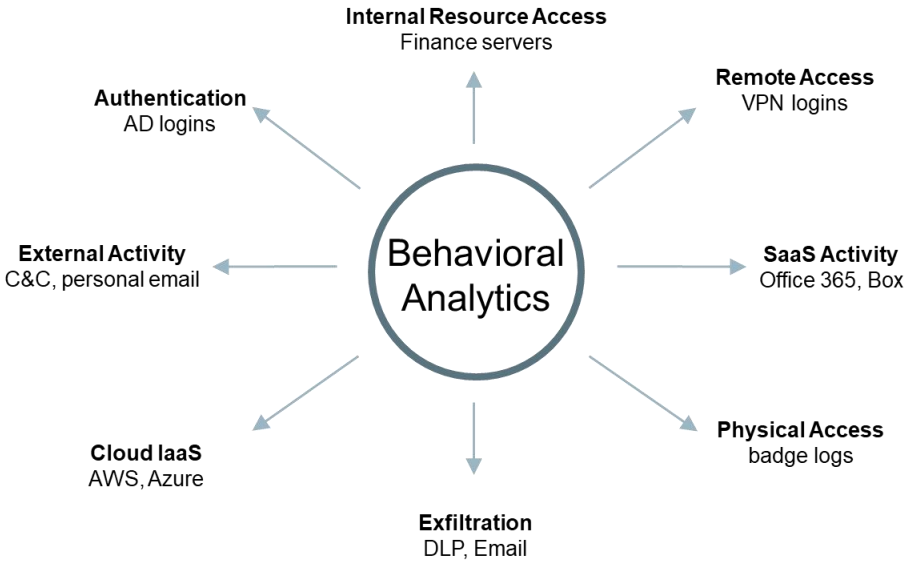
Infrastructure	Security	SIEM	Device Management	MFA	Services
ARISTA	JUNIPER NETWORKS	ArcSight An HP Company	Microsoft	DUO	servicenow
JUNIPER NETWORKS	paloalto NETWORKS	splunk>	MobileIron	IWS ImageWare Systems, Inc.	pagerduty
cisco	Check Point SOFTWARE TECHNOLOGIES LTD.	Radar	Google	kasada	SendGrid
aruba a Hewlett Packard Enterprise company	intel Security	intel Security	airwatch by vmware	okta	Envoy
Hewlett Packard Enterprise	Infoblox CONTROL YOUR NETWORK		SAP Afaria		sine
	Attivo NETWORKS				

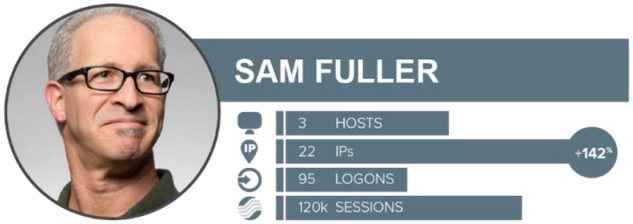
INNERGO

IntroSpect

aruba
a Hewlett Packard Enterprise company







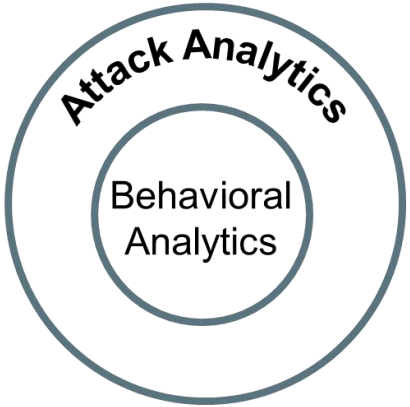
INNERGO

IntroSpect

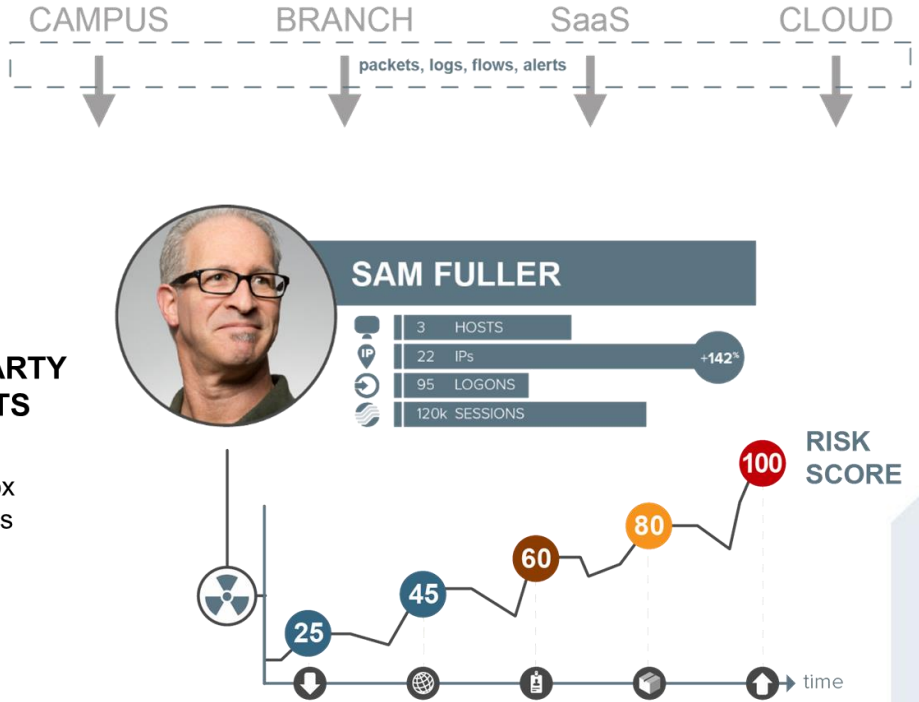
a Hewlett Packard Enterprise company

BUSINESS CONTEXT
High Value Assets
High Value Actors

MACHINE LEARNING
SUPERVISED
UNSUPERVISED



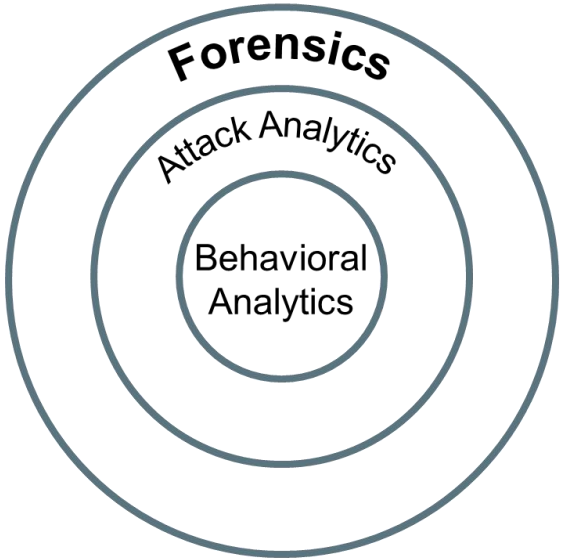
THIRD PARTY ALERTS
DLP
Sandbox
Firewalls
STIX
Rules
Etc.

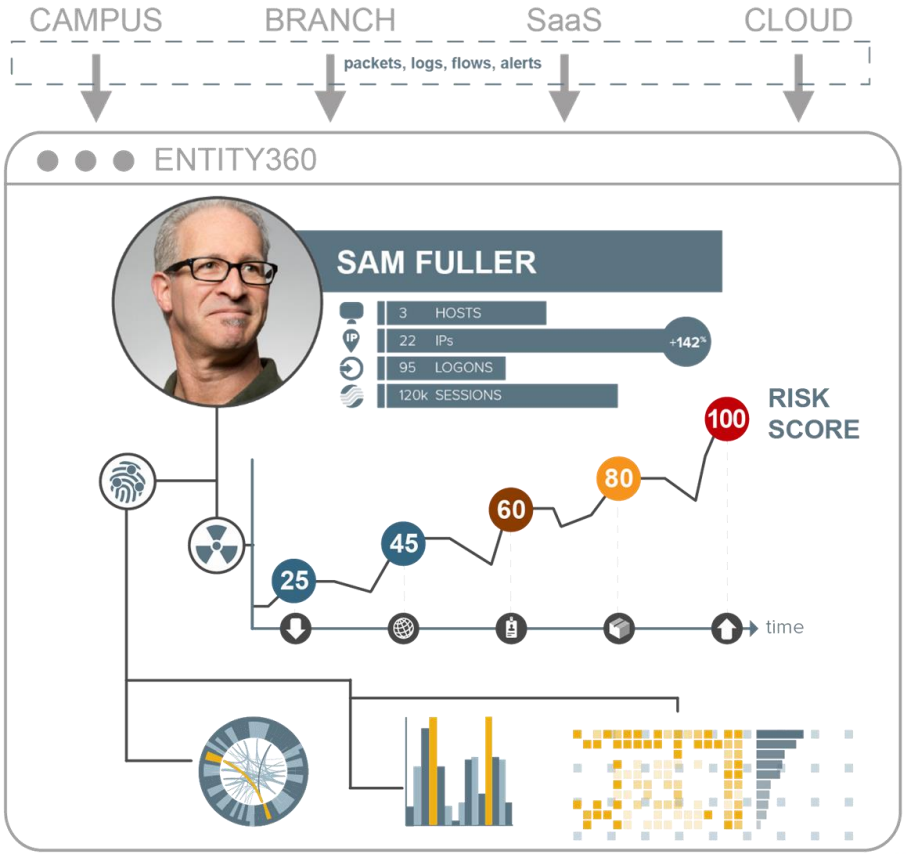


INNERGO

IntroSpect

aruba
a Hewlett Packard Enterprise company





INNERGO

IntroSpect i ClearPass

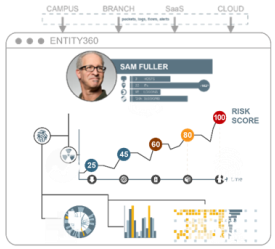
aruba
a Hewlett Packard Enterprise company

1. Discover and Authorize

User/Device Context

ClearPass
Secure Network Access Control

2. Monitor and Alert



Entity360 Profile with Risk Scoring

Actionable Alerts

3. Decide and Act

- Real-time Quarantine
- Re-authentication
- Bandwidth Control
- Blacklist

ClearPass
Adaptive Response

IntroSpect UEBA

INNERGO

INNERGO

Tomasz Mańka

Presales Team Manager

tomasz.manka@innergo.pl

+48 519 351 406