Akamai Guardicore Segmentation

Paolo Andreani – Regional Sales Manager
Fabrizio Pettinau – Senior Solutions Engineer

Giornata Tecnologica - Lumit

19/04/2023

Agenda

01. The Problem

02. AGS – Our Approach

03. Akamai Hunt

04. Use Cases

The Problem

Perimetro di Sicurezza Nazionale

Tassonomia degli Incidenti

- **Decreto legge 105/2019 (perimetro di sicurezza cibernetica) convertito in legge 133/2019.**
- **Determina 3 gennaio 2023, Agenzia per la Cybersicurezza Nazionale**

Categorie incidenti

Accesso iniziale	Esecuzione	Installazione	Movimenti Laterali	Azione sugli obiettivi	Ricognizione

Initial Foothold
(Spear)Phishing or vulnerable exposed applications

Lateral Movement
Spread across the network for maximum coverage

Exfiltration
Find and steal valuable data

Encryption
PKI with encryption to prevent cracking

Ransom Note
Wallpaper and ransom txt file

Profit

Akamai

Raccomandazioni CSIRT - ACN

RANSOMWARE - Misure di protezione e organizzazione dei dati per un ripristino efficace.

ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	L'identificazione dei flussi dei dati (da quali e verso quali dispositivi e reti transitano) consente l'individuazione delle informazioni e processi a rischio in caso di attacco e di prevedere i possibili percorsi degli attaccanti in caso di movimenti laterali.	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013 A**.13.2.1,A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1
PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Applicare il principio del privilegio minimo anche all'accesso ai dati risulta di fondamentale importanza per limitare l'impatto di eventuali attacchi.	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5

Primary Blockers

Limited Visibility

Missing an **accurate single source of truth**.

Known and unknown endpoints connecting from **many locations.**

Complexity

Frequent change windows and downtime are untenable.

Competing priorities lead to friction and delays.

Infrastructure Changes

Most organizations are now **Hybrid cloud.**

Microservices and containers **communicate differently.**

*"The only constant is the **change**"*

Akamai Guardicore Segmentation

Our Approach

Zero Trust Principles

Zero Trust is a network security **strategy** based on the philosophy that no person or device inside or outside of an organization's network should be granted access to connect to IT systems or workloads unless it is explicitly deemed necessary. In short, it means zero implicit trust.

- All entities are **untrusted** by default;
- **Least-privilege** access is enforced;
- Constant security **monitoring** is implemented.

> *"Preventing good people from doing bad things"*

Our Approach to Segmentation

Discover

See everything, everywhere in high definition

Divide

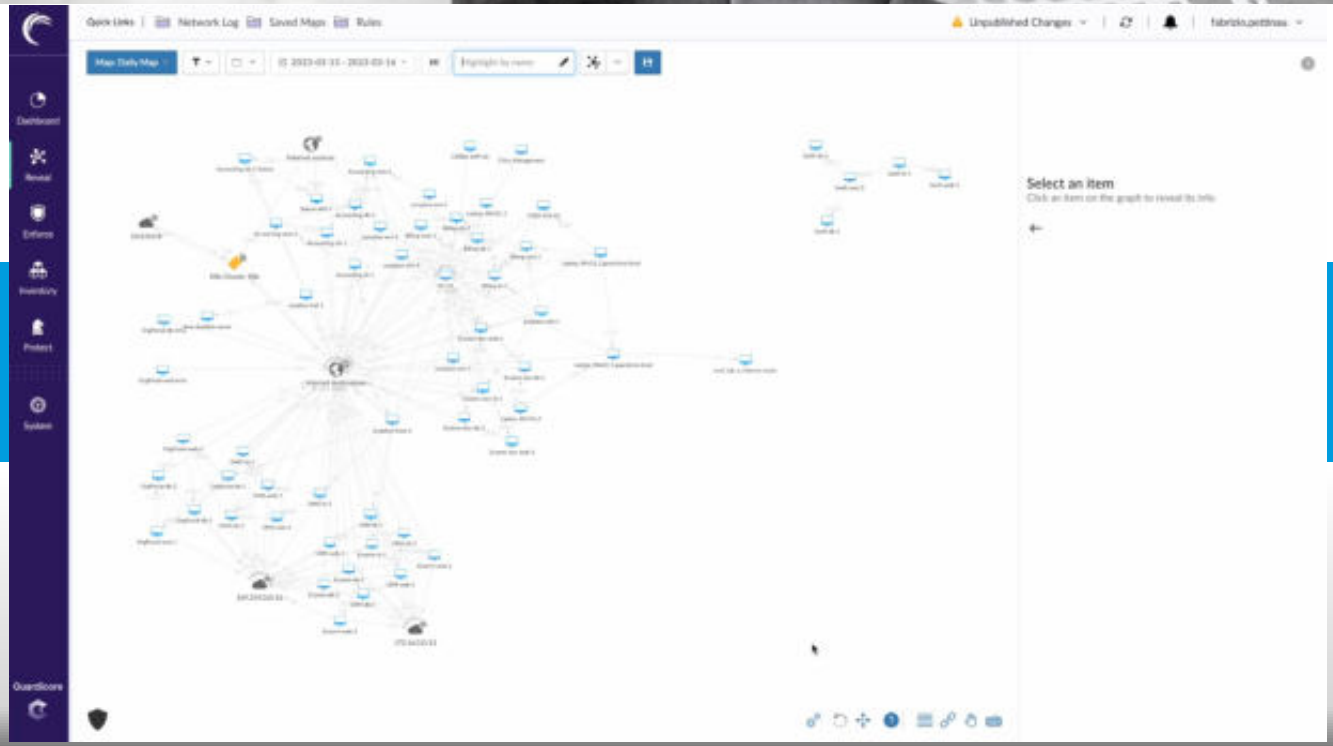
Create Software-Defined Zero Trust (micro)perimeters

Conquer

Detect threats and respond with speed and precision

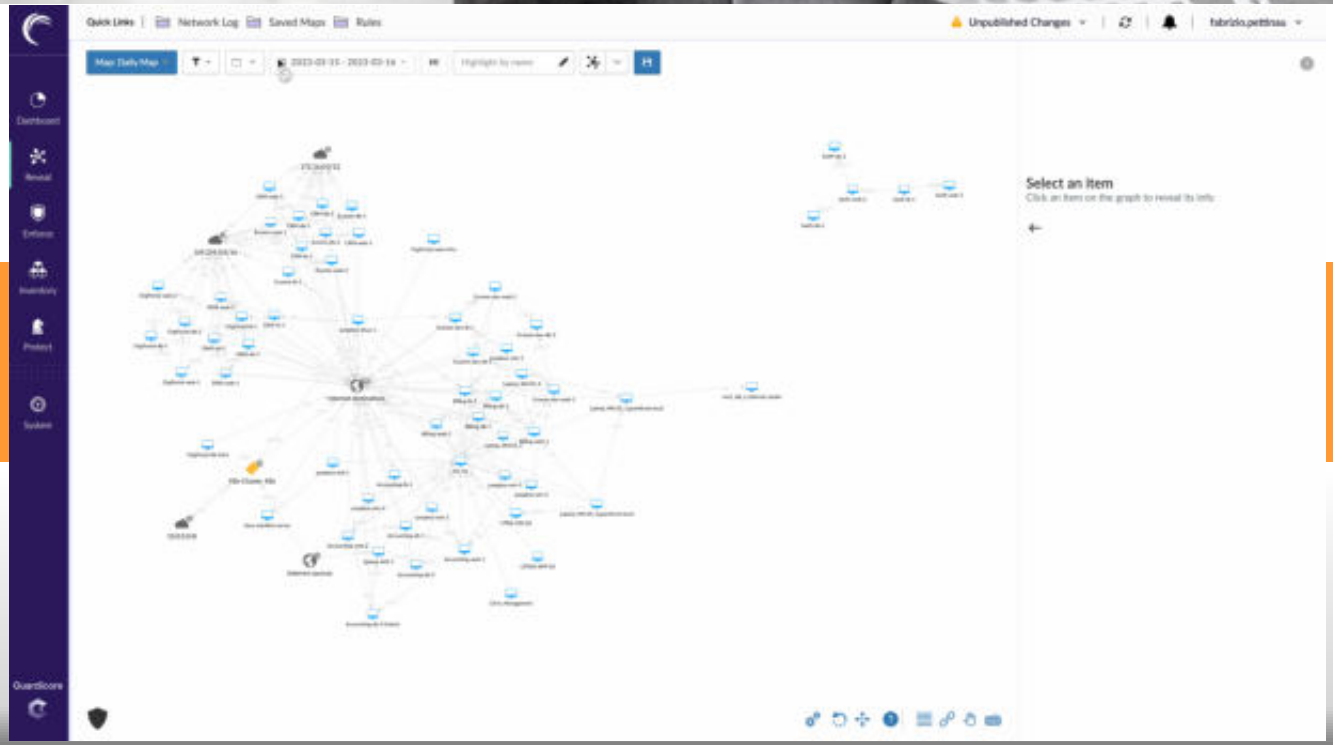
Our Approach - Visibility

Visualization



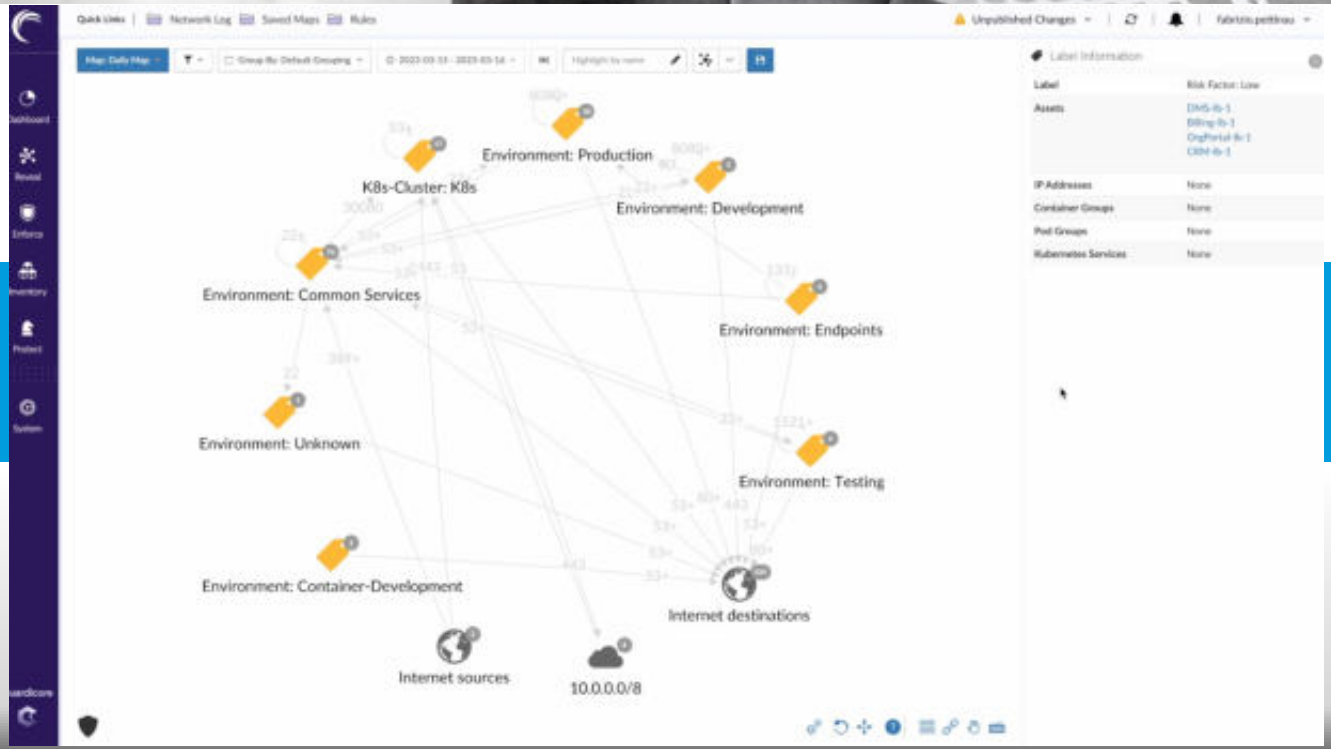
Our Approach - Mapping

Mapping



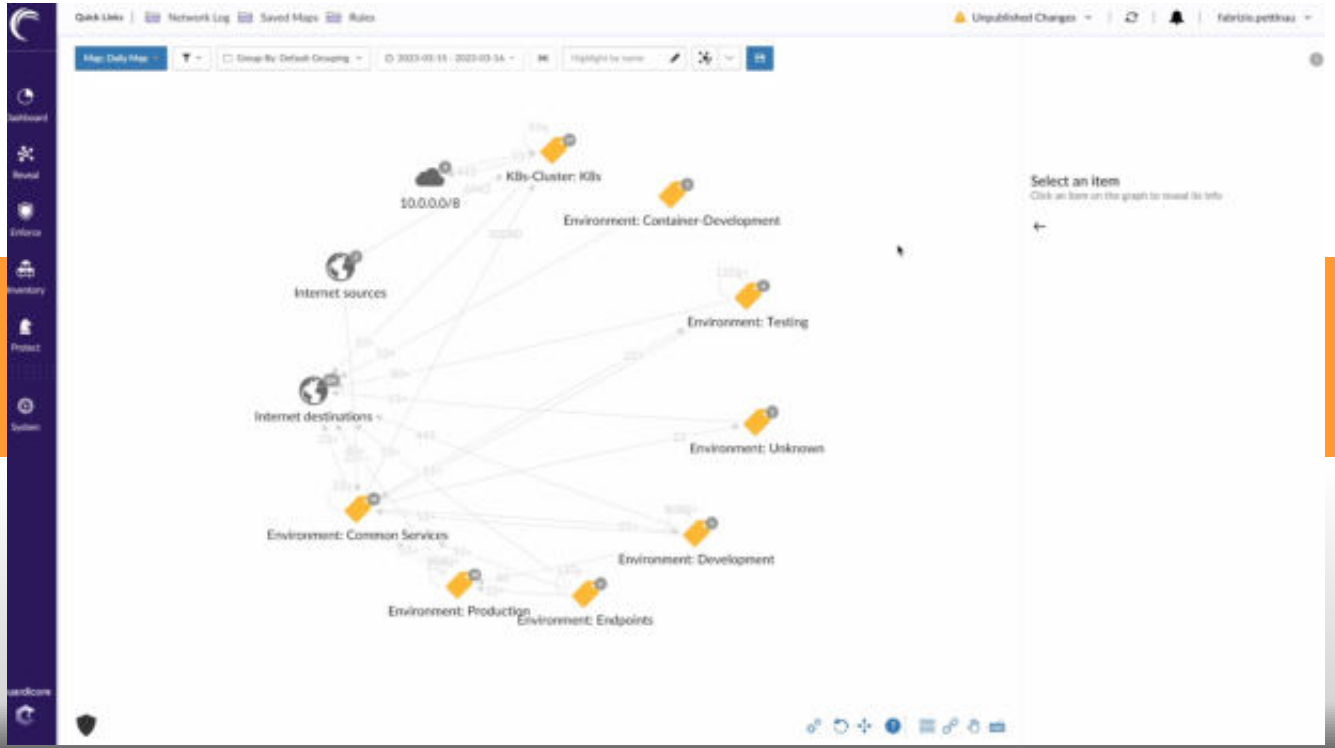
Our Approach- Enforcement

Enforcement



Our Approach – Detect

Detect



Our Approach – Benefits

Software-Based Segmentation Approach VS Infrastructure Approach.

- **No infrastructure Changes** required and no Application downtime;
- **Faster** Time-to-Value;
- **Less resources required** to deploy and Manage;
- Significantly **lower costs**;
- **Process-Level** Visibility and Enforcement.

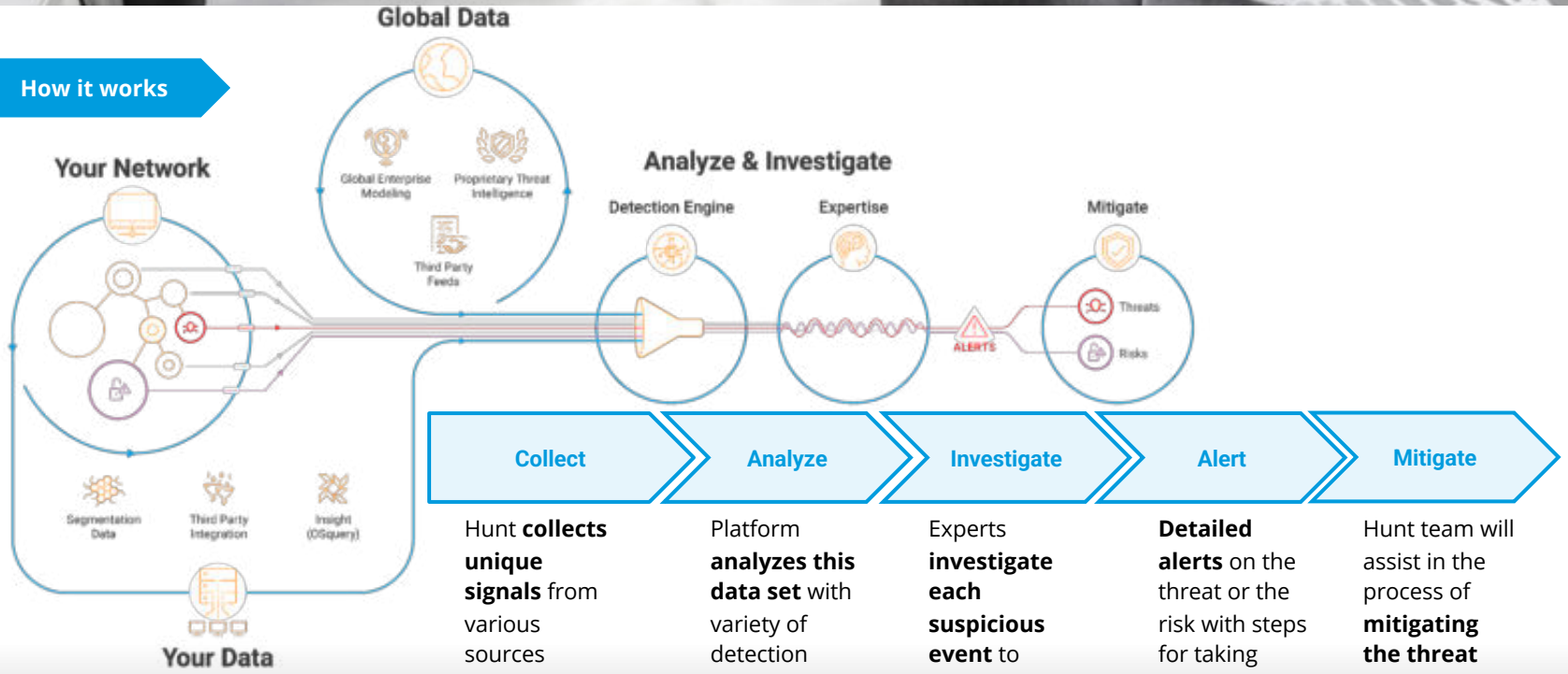
Infrastructure Agnostic and Broad OS Coverage.
Past, Present and Future…

Bare Metal | VM | Cloud | Container | Endpoint

Akamai Hunt
Threat Hunting

Akamai Hunt - Detect

How it works



Collect	Analyze	Investigate	Alert	Mitigate
Hunt **collects unique signals** from various sources	Platform **analyzes this data set** with variety of detection algorithms	Experts **investigate each suspicious event** to minimize false positives	**Detailed alerts** on the threat or the risk with steps for taking action	Hunt team will assist in the process of **mitigating the threat**

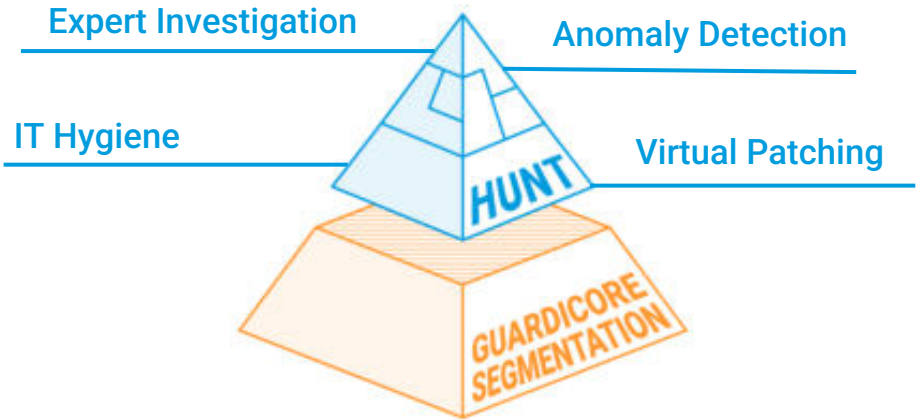
Akamai Hunt - Benefits

A service to detect and remediate threats and risks.

Secure
- Reduce attack surface

Immediate
- Leverage segmentation infrastructure

Seamless
- No additional software, agent rollouts or upgrades



Akamai Guardicore Segmentation

Use Cases

Common Uses of Zero Trust Network segmentation

- Mapping of hybrid Data Centers and Cloud Migration
- Critical Application / Environment Isolation
- Lateral movement Visibility and Control (Least Privilege approach)
- Legacy Application Protection
- Single policy (and Single Pane of glass) across on-prem / cloud / containers
- Identity-based Access Control Supply-chain Control
- Ransomware\Malware containment and protection
- Zero Trust Initiative
- Compliance visibility, Segmentation and reporting (PCI, SWIFT, etc.)
- Context Aware segmentation (Insight), Isolation and Virtual Patching

Simplify and Secure with ONE ZERO TRUST

Real Project

April - 2022

Project Kickoff

April - 2022

Initial Agent rollout

May – 2022

Labeling strategy formalized & Phase 1 of policy creation; 190 Agents targeted

June – 2022

3 Months

~60 Applications in block !

July - 2022

Significant Legacy Agent Issues Encountered. Escalated internally.

Ray Zhao brought in to help push progress on agent issues

10 Months

February - 2023

Planning to segment FURTHER

260 Total Applications in block !

August - 2022

After pushing from PS, JCI hired on two dedicated Network Engineers to the Guardicore project.

Agent count doubles !

January - 2023

EXPANSION ORDER ($1m) submitted & progressing internally. JCI begins to rollout additional agents, up to ~1,400 currently.

December - 2022

Phase 1 - policy clean-up begins

September - 2022

Phase 2 of Policy creation starts; Oct - **90 apps**, Nov - **80 apps**, and Dec **95 apps** to be moved to Block

6 Months

Agent installation issues behind us

250 Applications now in block !

Breaches will happen, but they don’t have to be catastrophic.

Thank you!
Grazie!

Paolo Andreani - Regional Sales Manager
pandrean@akamai.com

Fabrizio Pettinau – Senior Solutions Engineer
fpettina@akamai.com