

The Service Mesh

Turning Multiple Managed Security Services Into One

Context-Aware System



CYBERSEC
EUROPE

Cybersec Europe 2026
May 20th, 2026

The logo for ACEN, featuring the letters 'A', 'C', 'E', and 'N' in a bold, white, sans-serif font. An orange ring is positioned around the letter 'A', suggesting a globe or a network mesh.

Chapter 1

Siloed teams close tickets.

Context finds attacks.

The Case That Started This Framework



Organization's Context

- Healthcare
- +500 Users
- Multiple locations



Tech & Service Stack

- 24/7 MDR
- M365 Managed Security
- AD Security (Silverfort)
- EDR
- Imprivata



The Compromise

- AD related alerts
- Extended Threat Hunts
- Fully contained in 90 mins.

**Even with all the logs,
context is hard.**

You need the experts.

What if there's more...
**Like a physical
security attack?**

Finding The Missing Piece



- Used to authenticate in different systems with a badge.
- SOC had the SecOps knowledge, but the Imprivata Team knew the specifics
- **Strong correlation with physical locations within an organization.**

Knowledge + Timestamps + Physical devices = ?



Chapter 2

Understanding The Problem

Our Context

MDR & CSIRT

Identity Security

Infra & Cloud Security

Advisory

40+

Active 24/7 SOC
Organizations

350+

Customers across
domains

20+

Vendors

12

Teams

Integration: The Marketing Bluff

89% of MSPs struggle with tool integration

20% MSPs have consolidated their stack

And we are not even touching the service and team layers

Tech, backoffice, sales, service management...

Systemic Problems



Human Layer

Silos aren't laziness. They are a rational response to how teams are measured.

- Every team is optimized for their own KPIs
- Immediate success: MDR handles alerts, identity management implements, etc.
- Nobody's KPI "Did you share context today"



Operational Layer

Interconnections create **systemic problem** with exponential impact and difficulty.

- Every new tool and team adds friction
- Every new process creates resistance
- The harder you push, the more frustrations you create
- Lack of ownership everywhere

Chapter 3

The Framework In Motion

The Three Pillars



Aligned Incentives

- Shared KPIs
- Cross-Team Metrics
- Structured Touchpoints



Context Aware Architecture

- Inject context into workflows across teams
- **Focus on systems, not people.**



Multiplier Effect

- Each service compounds the value to others
- Generates hype across teams

Compliance Fluency

Common understanding between teams and customers

Context Aware Architecture

Service Management Layer

The human In the loop. Same service manager across multiple services. Every team starts from the same picture. Reinforced in weekly cross-service meetings.

Customer Intelligence Profile

A persistent record per customer (*Projects, Org structure, asset, open findings, services*).
Updated continuously by other services, ideally automatically by the tools themselves.

New Identity Project

Inject relevant info from last advisory roadmap session + Relevant true positives from SOC.

Context Injection






Leverage On-Prem LLMs to summarize context and inject it across different teams and workflows.
Relevant history, related alerts, and open findings from other services, etc.

New Service Meeting

Inject relevant info from advisory, and latest tracks within that customer.

Context Aware Architecture

Services

-  Cato Networks
-  Imprivata
-  Managed Detection & Response
-  Network support
-  Silverfort


***** CONTEXT *****

[M365 Security]

4 new alerting rules were added on March 18th, 2026. This alert was generated by one of the newly introduced detections.

[Advisory]

Last customer roadmap session was conducted 2 weeks ago. No known business risks or critical asset concerns currently associated with the entities involved in this alert.
Shadow IT Inventory activities are currently in progress. Alert activity may be related to ongoing asset discovery or validation efforts.

 Internal

Never start from
scratch

Inspirations of the Multiplier Effect

Armor sets in games: Each piece provides its own benefits, but together they create new ones.



Multiplier Effect: 1 + 1=3

Each service is useful alone

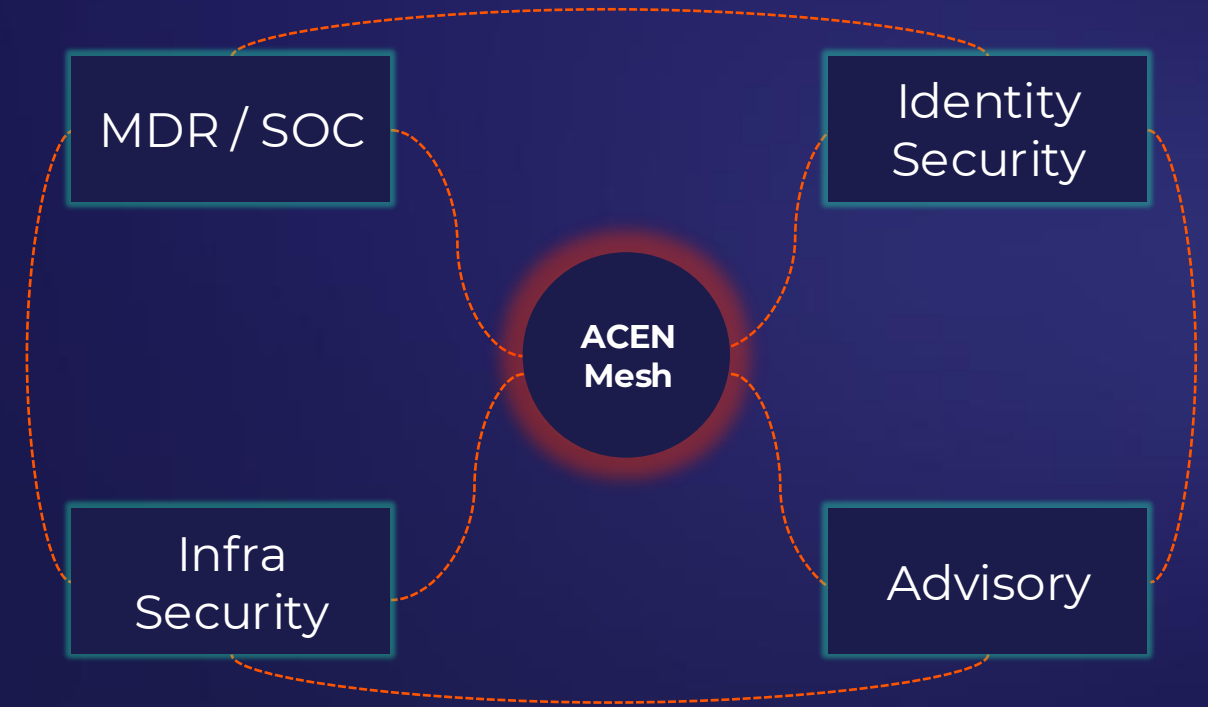
Each service is useful alone. Combined, they can produce value none of them could generate individually.

Not everything can be integrated

Services are evaluated for their synergy and integration capabilities.

Not everything gives value

Value must be perceived by the customers. Many integrations lead nowhere.



The Synergy Matrix

	MDR / SOC	ITDR	M365 Security	Advisory
MDR / SOC			M365 team continuously implements new features that feed the SOC, expanding monitoring capabilities across email, collaboration and cloud activity	Advisory findings added to SOC context. Critical assets, risk priorities and compliance scope inform alert triage and response decisions
ITDR				
M365 Security				
Advisory				

Come to the booth to know more :-)

Is It Working?

Increased Technology Adoption

Cross-Team awareness pushed the implementation of unused features

3/5

Technology Investments Justification

Customers reported an easier time during budget rounds.

60%

Faster Containment and Investigation Times

Imprivata case. Easier to have the full picture and trigger required actions.

Thanks!

Want to know more?

www.acen.eu

info@acen.eu

Contact me:

