• USE CASE

MICROSEGMENTATION: SECURE YOUR NETWORK, ELIMINATE DISRUPTION

MUGATO®

Organizations implementing Zero Trust architecture face a critical challenge: deploying network segmentation that limits lateral threat movement without breaking applications. Whether driven by compliance, breach containment or to protect critical assets, incomplete traffic visibility and manual policies create security gaps and costly disruptions.

THE CHALLENGE

- Segmentation attempts relying on estimates and outdated documentation create policies that either break legitimate applications or fail to provide adequate security protection
- Self-inflicted denial of service when incomplete dependency mapping leads to overly restrictive rules
- Policy decay as rules become outdated while environments evolve, leaving security gaps
- Missing intermittent traffic patterns from one-time testing block critical functions after enforcement

WHY TRADITIONAL APPROACHES FALL SHORT

Most organizations implementing microsegmentation face one or more of these common pitfalls:

MANUAL TRAFFIC ANALYSIS & DOCUMENTATION

Interviews and network diagrams to map communication patterns

Why it fails:

- Manual discovery typically captures 60-70% of traffic flows
- Static documentation becomes outdated as applications change and new services deploy
- Tribal knowledge is incomplete and often contradictory
- Misses intermittent, scheduled, and rare communication

POINT-IN-TIME NETWORK MONITORING

One-time packet captures or flow analysis to identify dependencies

Why it fails:

- Snapshots miss scheduled processes & periodic activities
- Cannot identify seasonal or infrequent communications
- Provides data without behavioral context or frequency patterns
- No continuous updates as environment evolves

SPREADSHEET-BASED POLICY MANAGEMENT

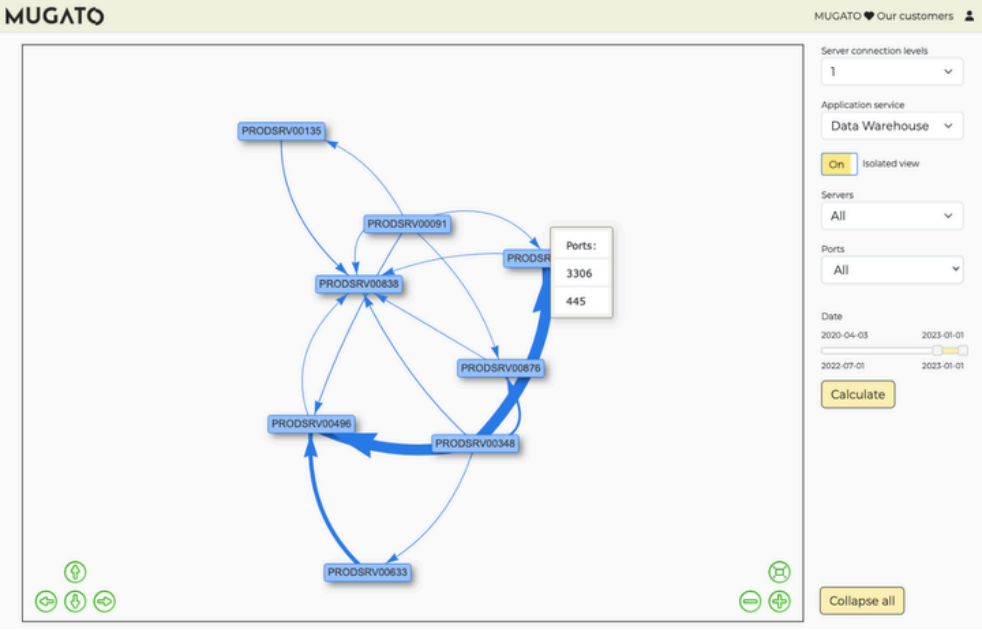
Manual tracking of segmentation rules in static documents

Why it fails:

- Policies decay immediately as infrastructure changes but spreadsheets don't update
- Human errors create security gaps and overly permissive rules
- Extended validation cycles with owners delay deployment
- Cannot prove compliance or policy effectiveness to auditors

THE MUGATO DIFFERENCE

Mugato delivers **agentless, continuous monitoring combined with behavioral analytics** to enable data-driven segmentation that secures your network without breaking applications.



AUTOMATED TRAFFIC FLOW DISCOVERY

Mugato continuously monitors all network and application communications without agents, capturing actual traffic patterns, protocols, frequency and data volume. You see intermittent processes, scheduled activities and rare, but critical comms, that point-in-time tools miss.
Why it matters: Complete visibility into actual behavior prevents both under-segmentation that leaves security gaps and over-segmentation that blocks legitimate business functions.

BEHAVIORAL POLICY GENERATION

Generate precise Zero Trust segmentation rules based on observed traffic patterns. Mugato analyzes minute-granularity communication data to create policies that permit legitimate application flows while blocking unauthorized lateral movement.
Why it matters: Policies grounded in actual behavior prevent application breaks during enforcement, maintaining business continuity while dramatically reducing security risk.

CONTINUOUS POLICY LIFECYCLE MANAGEMENT

Mugato automatically tracks infrastructure changes as new assets deploy, applications evolve and old communications cease. Generate templates and scripts to create new rules and decommission dormant policies, ensuring rules never decay.
Why it matters: Dynamic policy management eliminates the security gaps created by static rules that become outdated as environments change over months and years.

OPTIMAL SEGMENTATION GRANULARITY

Asset-by-asset behavioral analysis determines appropriate segmentation levels based on actual dependencies and business functions. Mugato ensures granular protection where needed while avoiding excessive complexity.
Why it matters: Right-sized segmentation achieves security objectives without creating unmanageable policy sprawl or requiring excessive operational overhead to maintain.

ACCELERATED STAKEHOLDER VALIDATION

Provide application owners with concrete, observed traffic data showing actual communication patterns, frequency and dependencies. Factual evidence replaces manual discovery interviews, shortening validation cycles from months to weeks.
Why it matters: Data-driven validation eliminates debate, accelerating deployment timelines while ensuring policies protect without disrupting operations.

PAIN POINTS	MUGATO PAINKILLERS
"We can't implement segmentation because we don't know which applications talk to each other"	**Agentless continuous monitoring reveals actual network and application traffic flows across your entire infrastructure, eliminating guesswork**
"Our last segmentation attempt caused a three-day outage when overly restrictive rules blocked critical integrations we didn't know existed"	**Observed traffic patterns permit legitimate application flows while blocking unauthorized movement, preventing self-inflicted denial of service**
"Validating segmentation policies takes months because we lack concrete data about traffic patterns"	**Traffic data showing communication frequency and dependencies shortens validation cycles**
"We're stuck between inadequate protectionand unmanageable complexity"	**Asset-by-asset behavioral analysis determines optimal levels based on dependencies**
"One-time traffic captures missed our monthly batch processes, causing them to fail at enforcing policies"	**Continuous observation identifies intermittent, scheduled and rare traffic flows that point-in-time assessments miss**
"When segmentation causes problems, we can't identify which rules are blocking legitimate traffic"	**Clear visualization of communications and dependency maps enable rapid root-and-affected cause analysis**

KEY OUTCOMES

By using Mugato for microsegmentation, organizations reduce risk, accelerate deployment and maintain availability:

Drastically reduce security risk: Limit lateral threat movement and contain breaches through Zero Trust architecture, reducing the blast radius of successful attacks

Accelerate deployment timelines: Shorten microsegmentation projects from months to weeks by automating dependency mapping and policy creation

Prevent service disruptions: Validate segmentation policy impact before enforcement using observed traffic patterns, eliminating self-inflicted denial of service

Accelerate incident response: Visibility into traffic patterns and dependencies enables faster troubleshooting and analysis during security incidents

MUGATO®

Mugato provides enterprises a real-time blueprint of their entire IT landscape used to map, plan, execute and monitor IT transformation projects. The platform reveals company-wide IT architecture through automatic mapping of applications, infrastructure and dependencies so organizations avoid making critical decisions based on outdated and inaccurate information. Delivering project and cost predictability with no setbacks, no rollbacks and no guesswork.

IT'S NOT MAGIC, IT'S SCIENCE