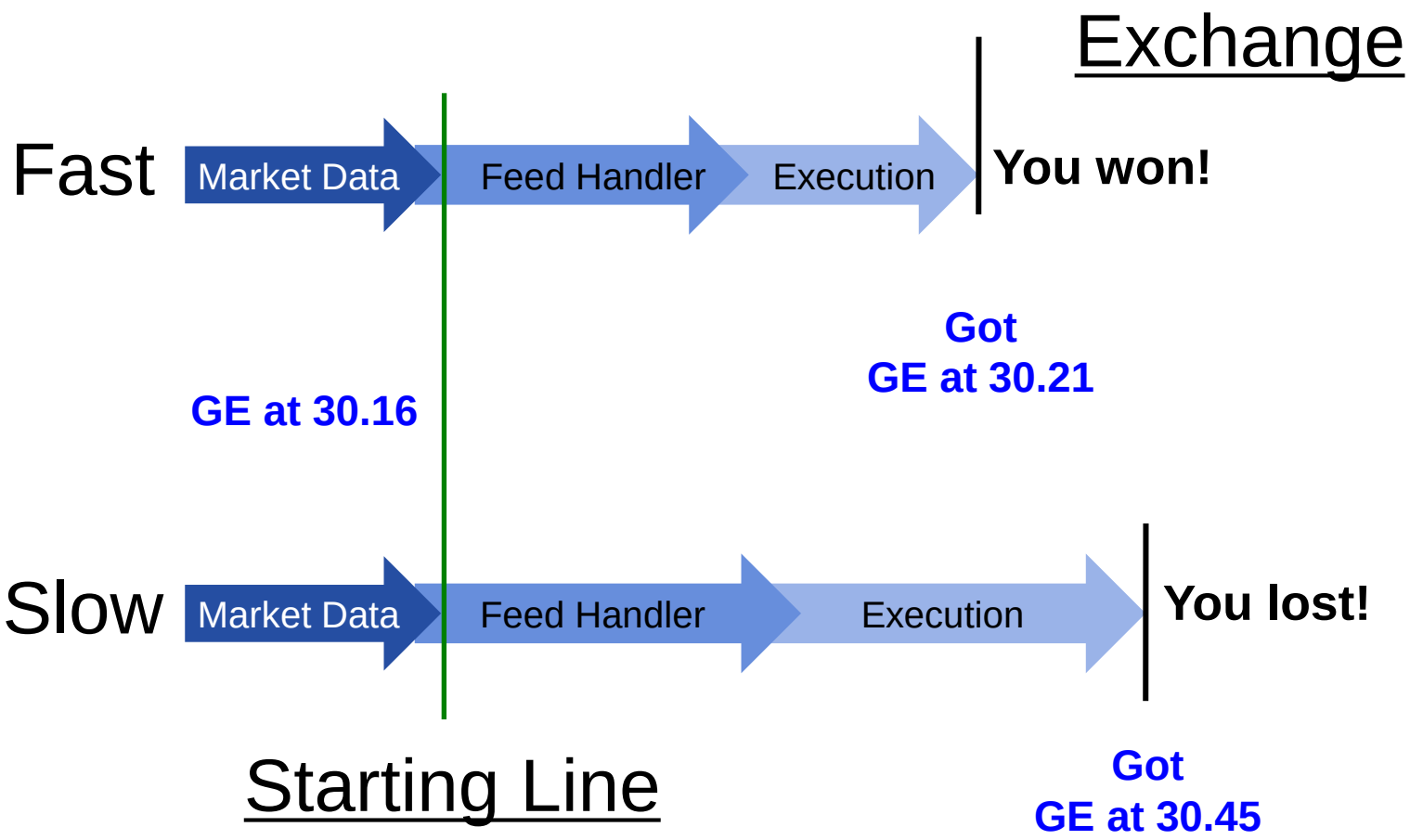
Message Fabric for Cyber Defense

IACD / SCRE Focus Group
JHU/APL

Feb 16, 2016

The Race to the Exchange

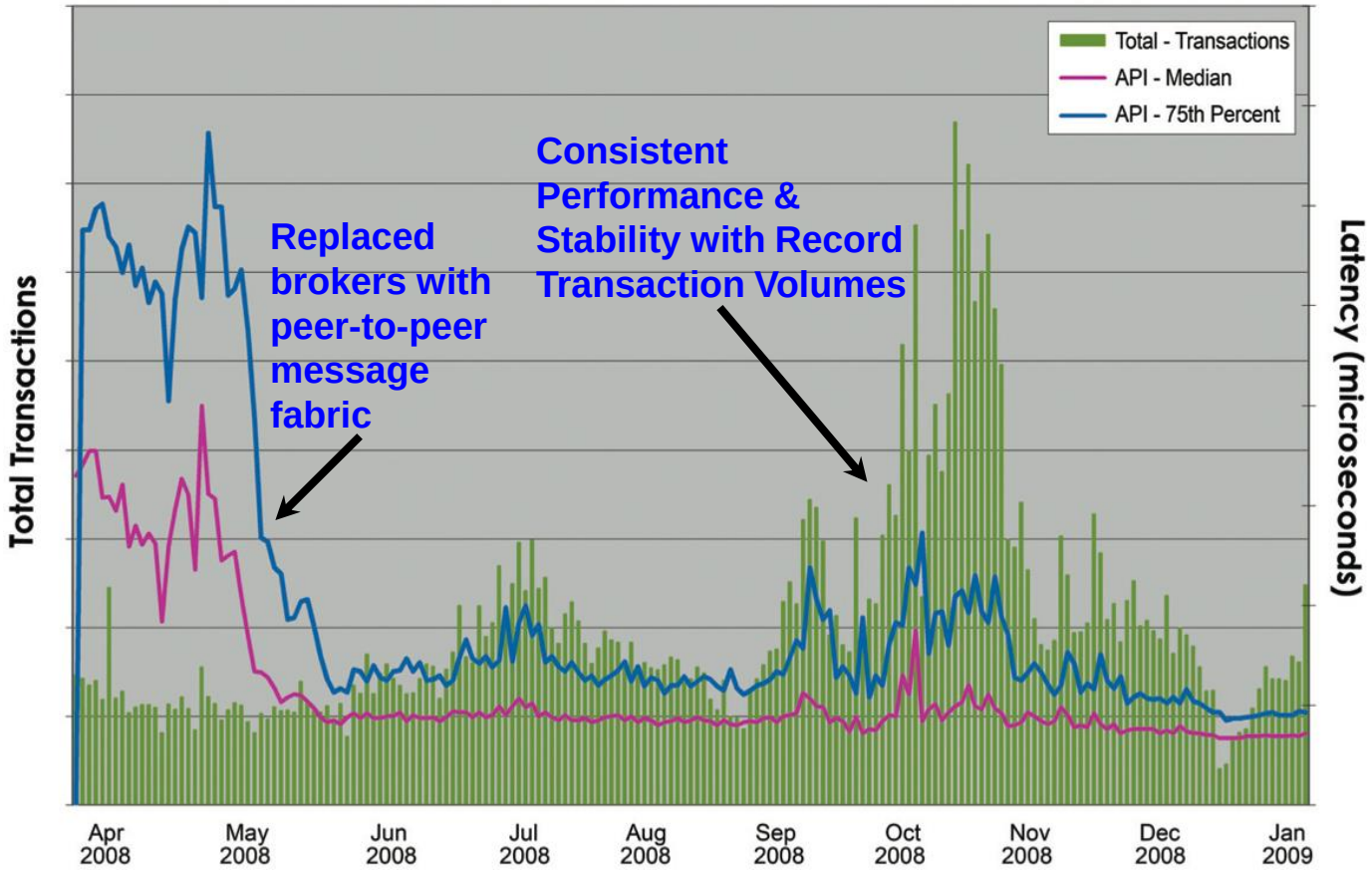
why speed is critical for Capital Markets



informatica

Case Study: Direct Edge

3rd Largest US Stock Exchange in 2008 (after NYSE and NASDAQ)



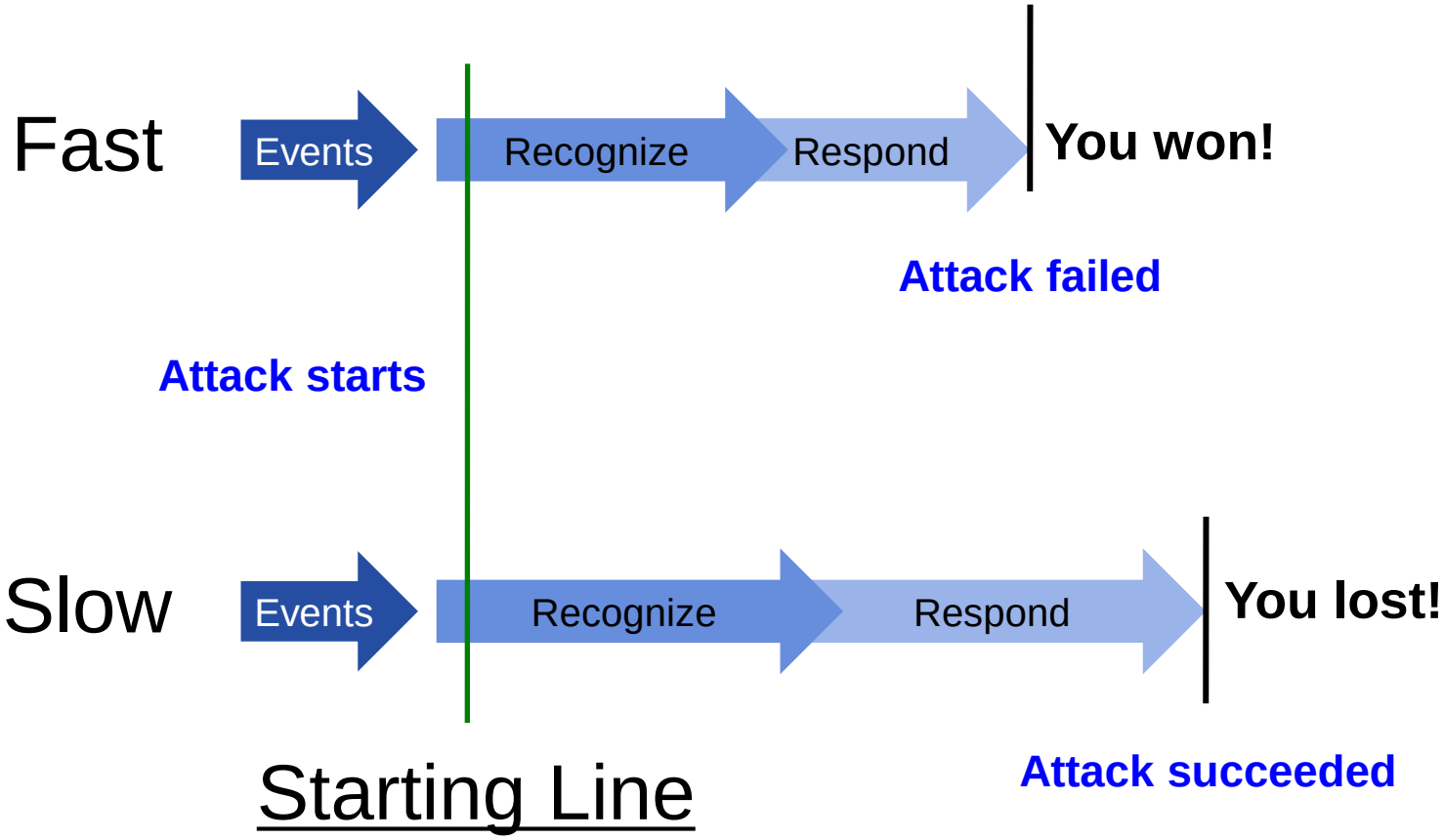
Source: Direct Edge 2008-2009

- ✓75% lower latency
- ✓50% reduction in hardware cost
- ✓Increased resiliency
- ✓Predictable performance

informatica

The Race to Respond

why speed is critical for Cyber Defense

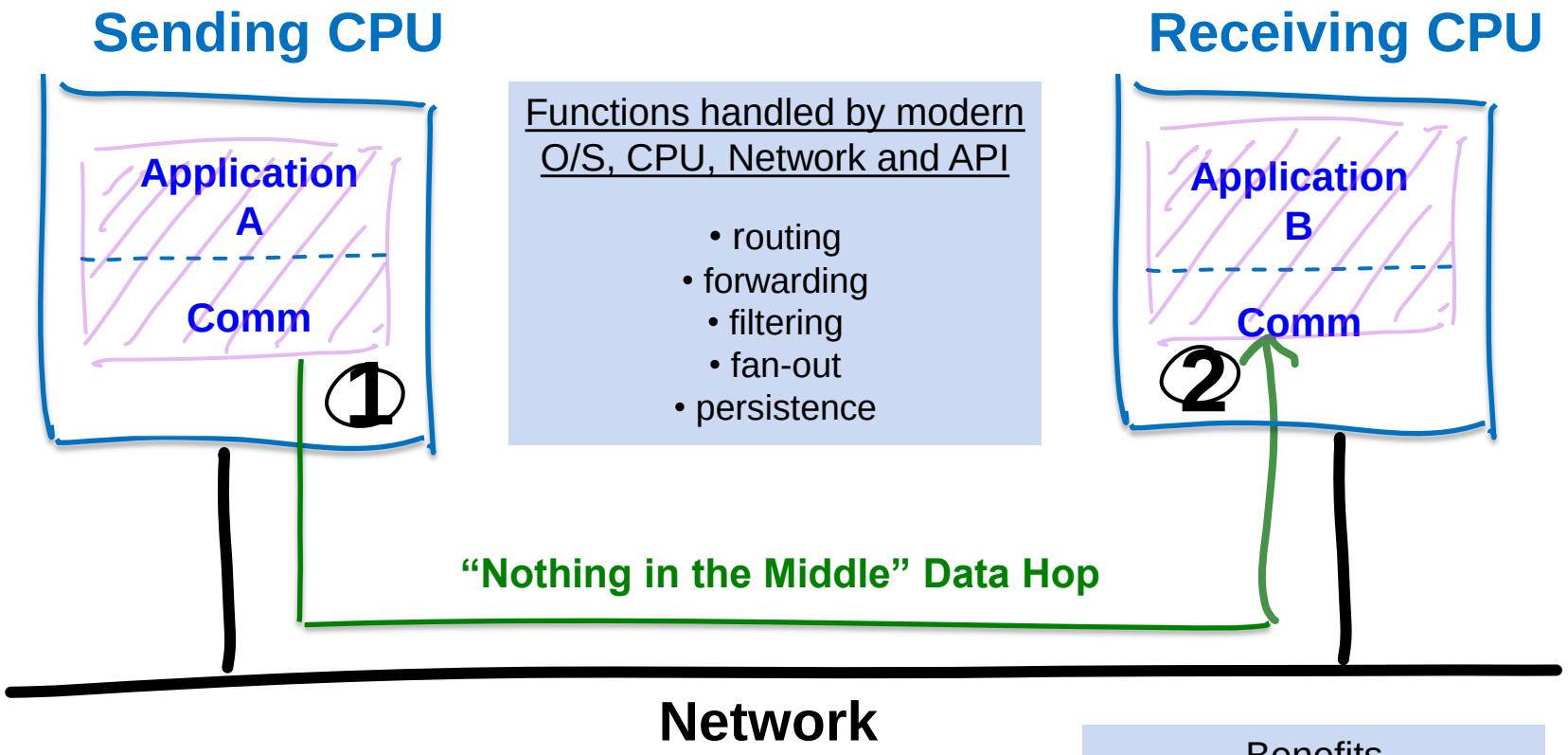


informatica

Why a Message Fabric?

- Agility, Adaptability, Reliability, Scalability, Modularity, Maintainability
- Different data, different requirements = **Use right tool for *each* job**
- "Get Left of Boom" = Detect and Respond faster = **Latency matters!**
- Better late than never or better never than late = **Choice of *quality of service***
  - e.g., only-latest-matters (no recovery), reliable (only recovery between active participants), guaranteed (keep data for offline participants too)
- Some data matters to one component; some data matters to all = **Choice of *patterns***
  - e.g., publish/subscribe, request/response, load-balanced, queuing
- Modularity
  - **Easily integrate new technologies and algorithms into existing system**
- Maintainability
  - Software on commodity hardware = **future proof and lowest O&M**
  - **Centralized control, distributed components (avoid bottlenecks)**
- Build vs. buy
  - **Focus on core competencies!**

Peer-to-Peer Message Fabric



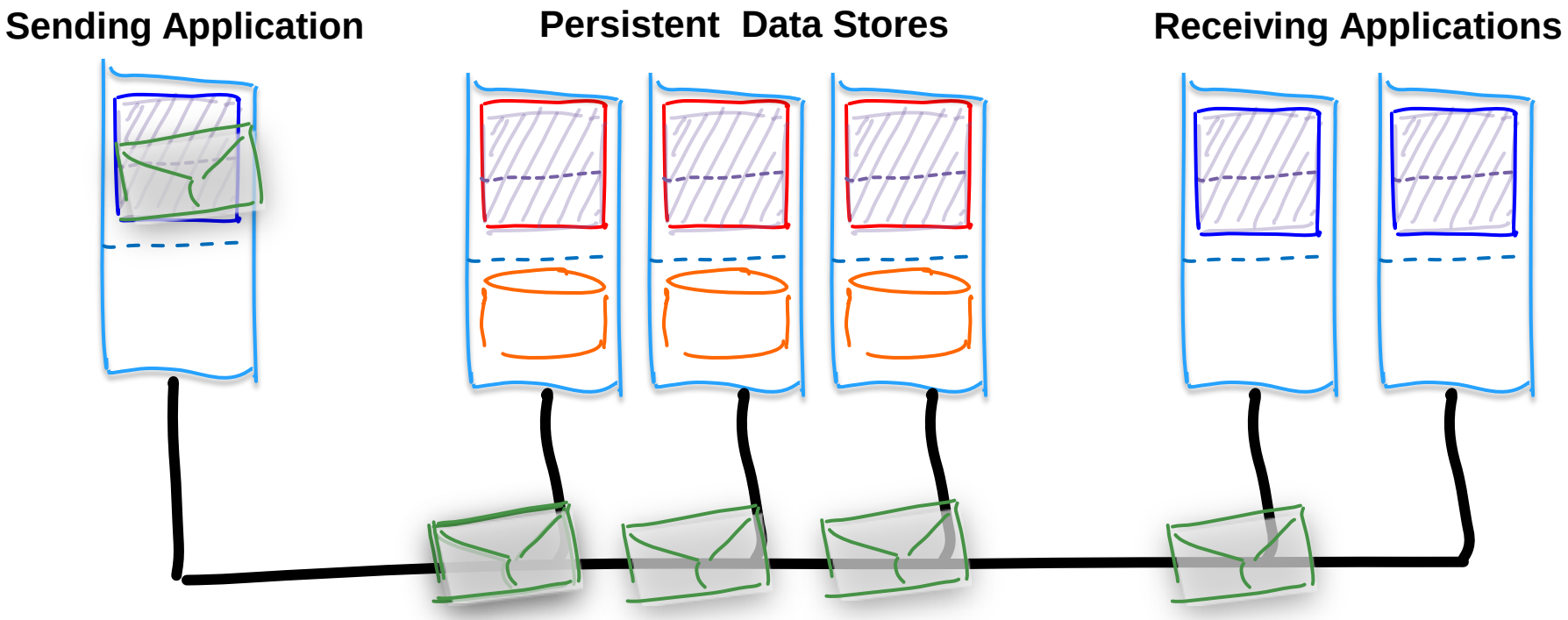
Just 2 steps to move from A to B!!!
Less is more!!

Benefits

- efficient (single data hop)
- maximizes performance
- no single points of failure
- scalable and flexible
- easier to administer

informatica

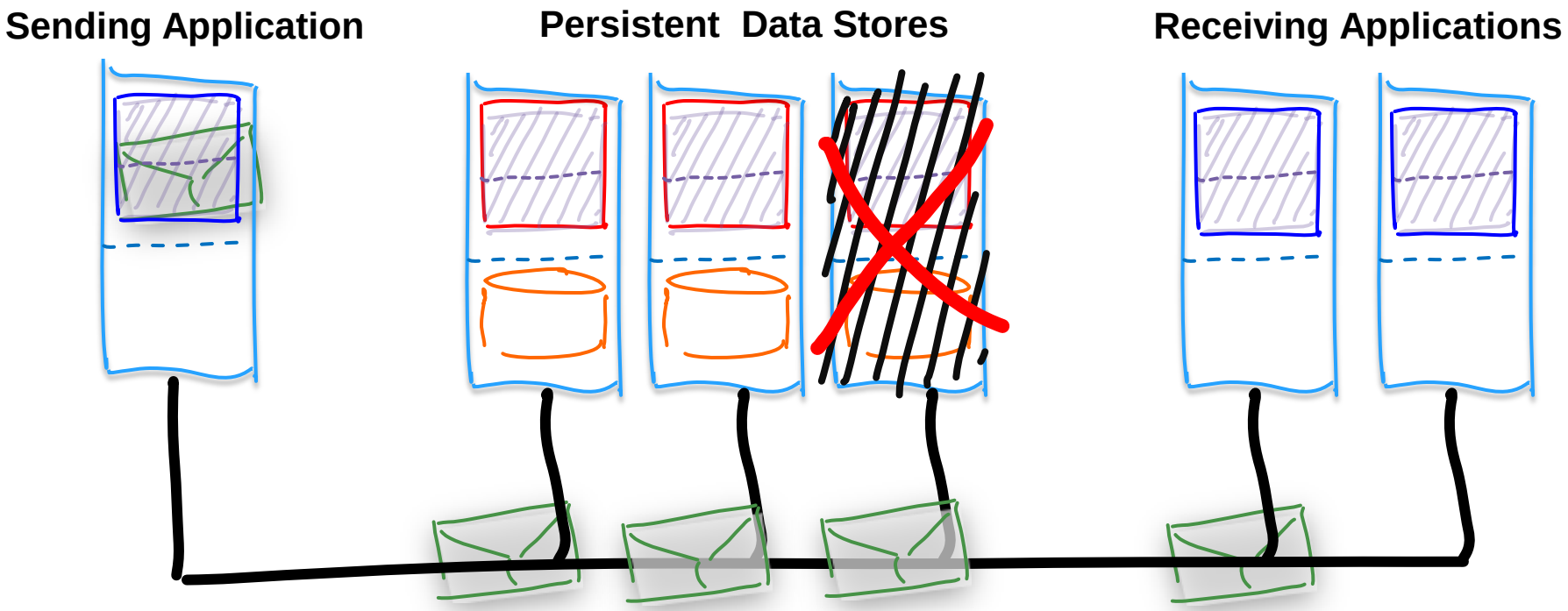
Parallel Persistence®



informatica

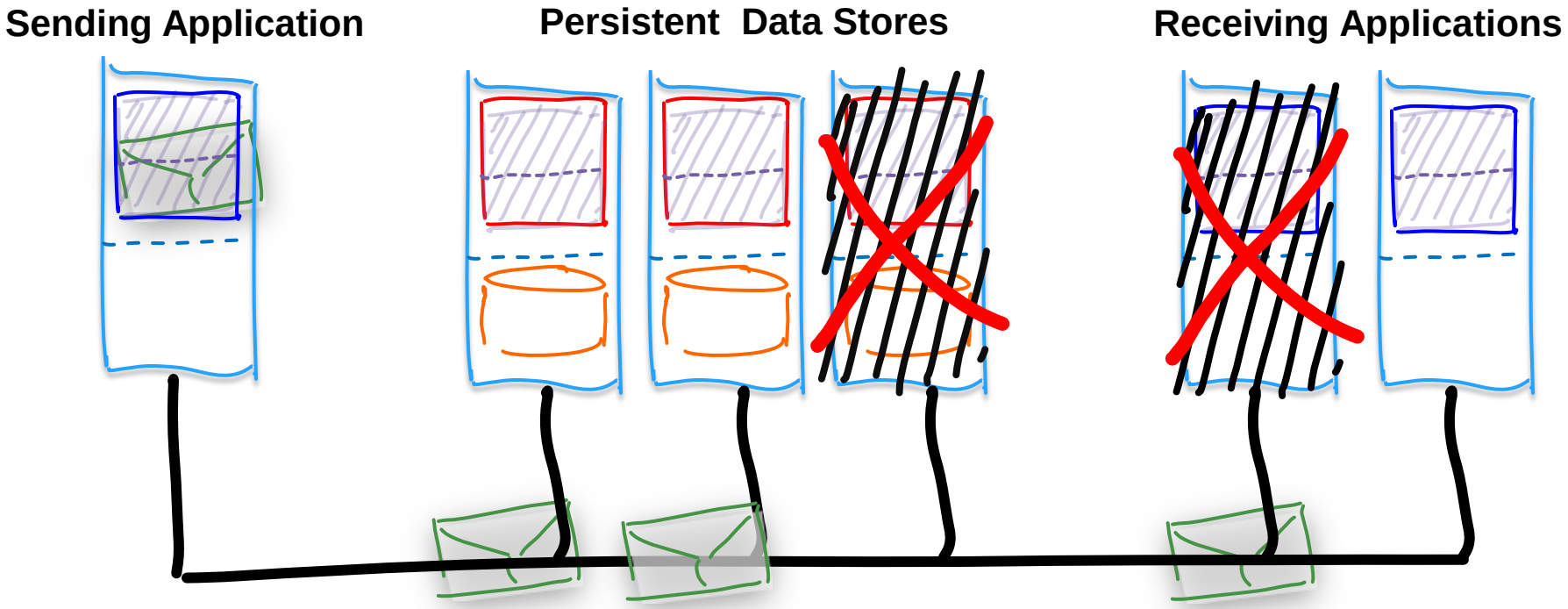
Parallel Persistence®

Zero System Downtime!
Zero Latency Failover!



informatica

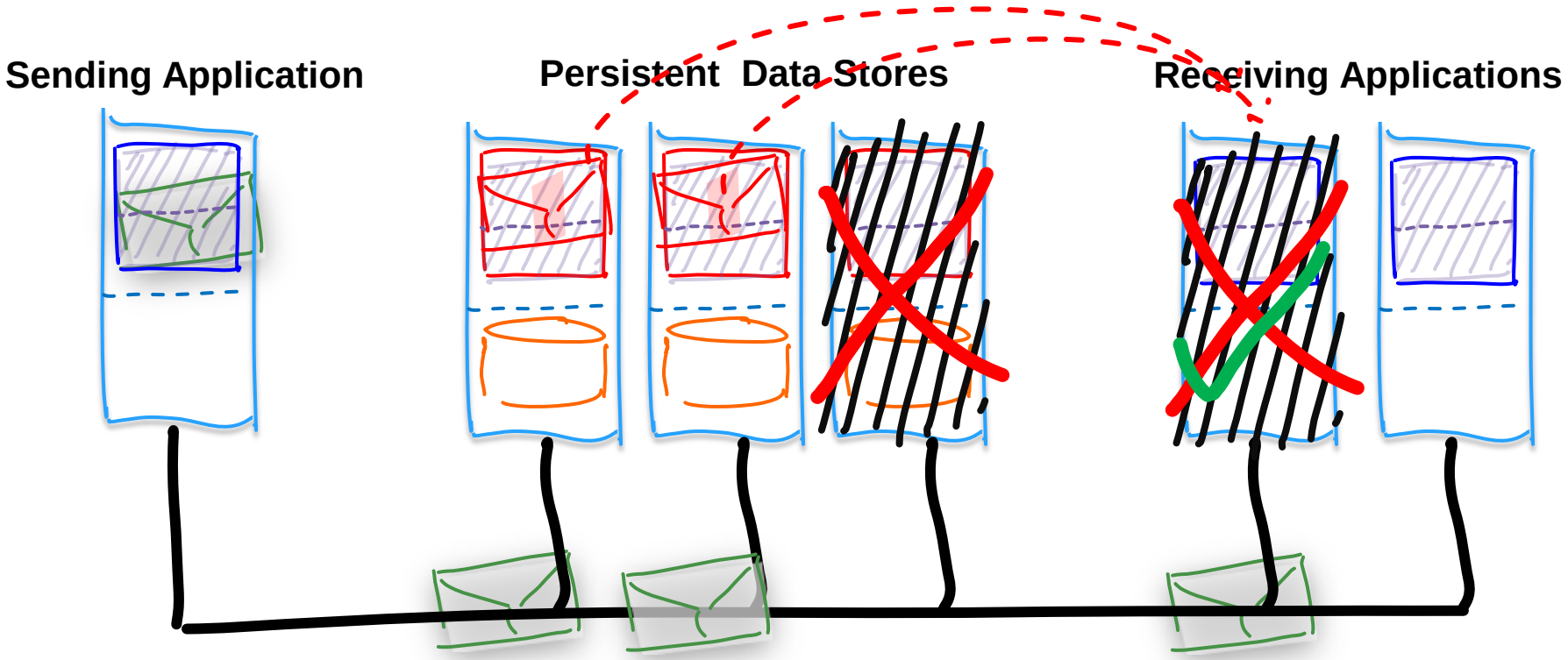
Parallel Persistence®



informatica

Parallel Persistence®

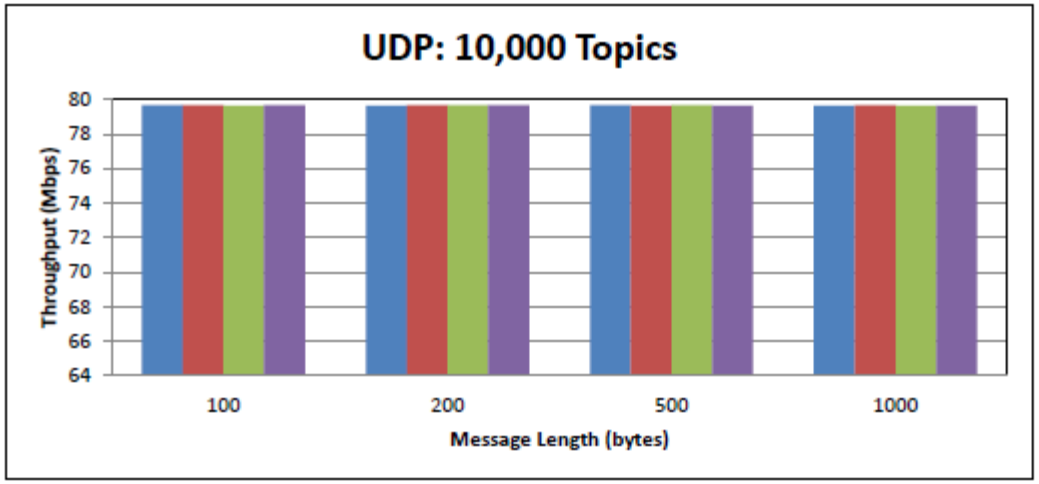
Receiver recovers with no impact to live message stream, then rejoins the live stream!

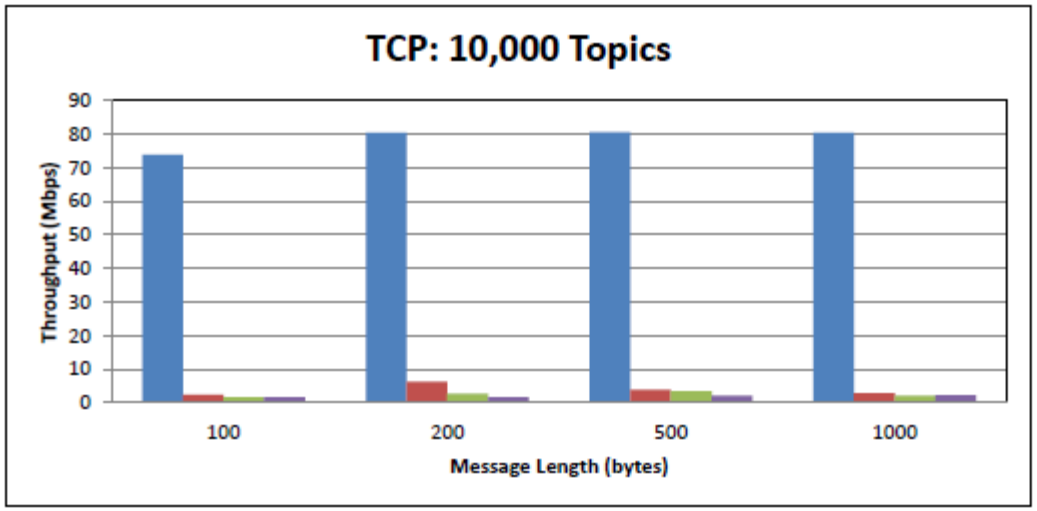


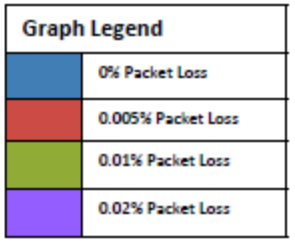
informatica

Why reliable UDP? Packet loss kills TCP

WAN Messaging Throughput: UDP vs. TCP (100 Mbps Link Speed)



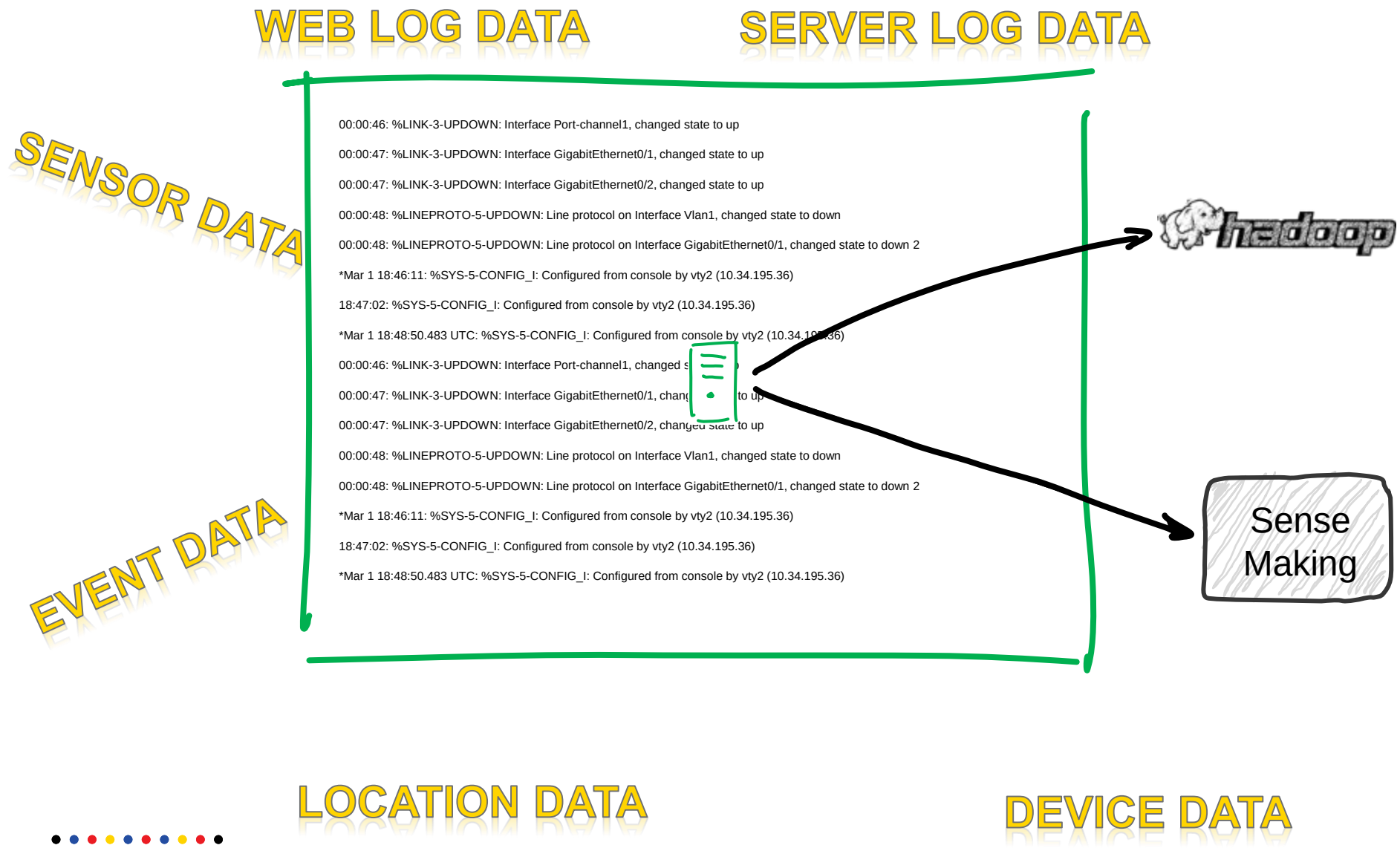




informatica

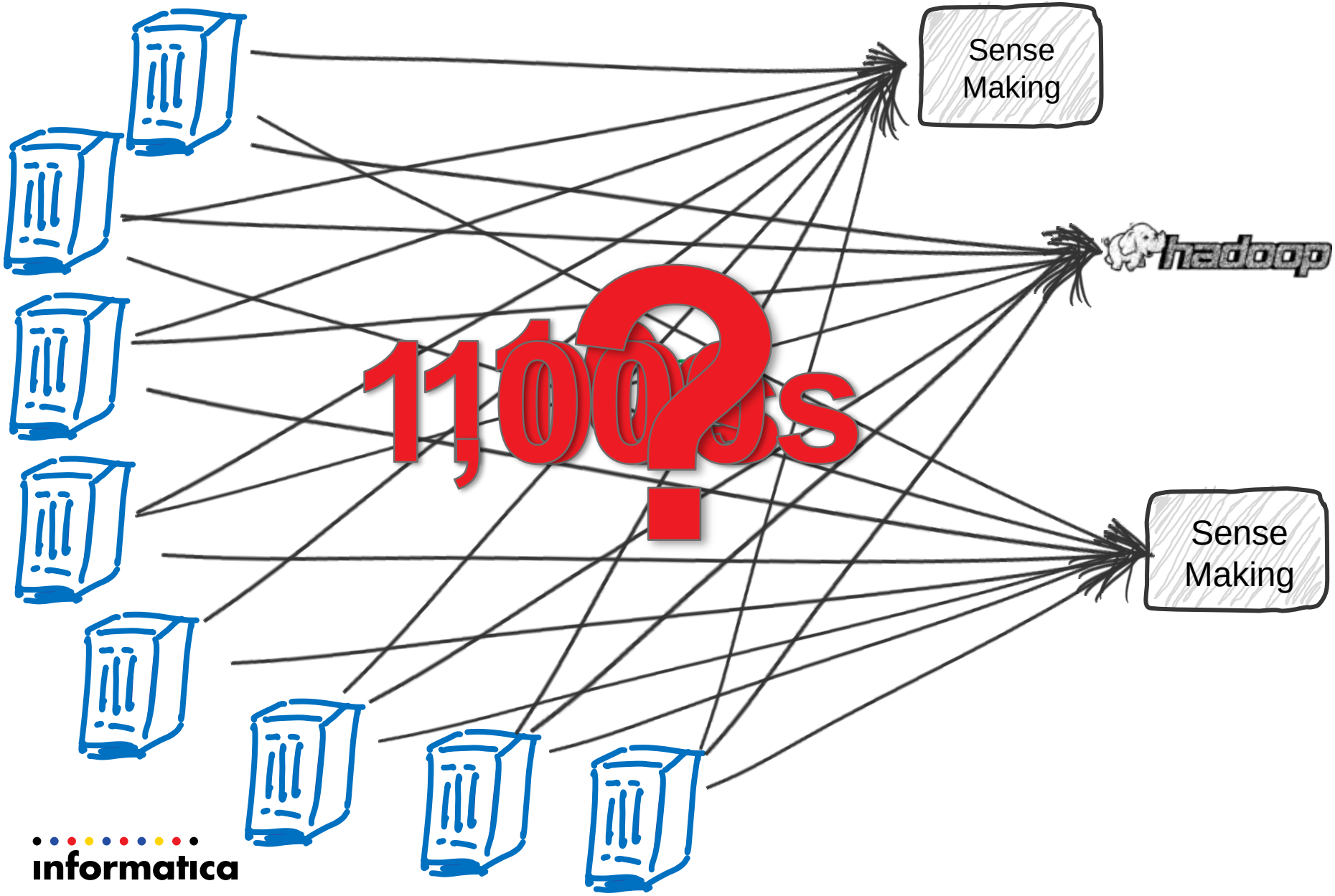
How can you combine a peer to peer message fabric with standardized interfaces and centralized management?

Streaming data collection…



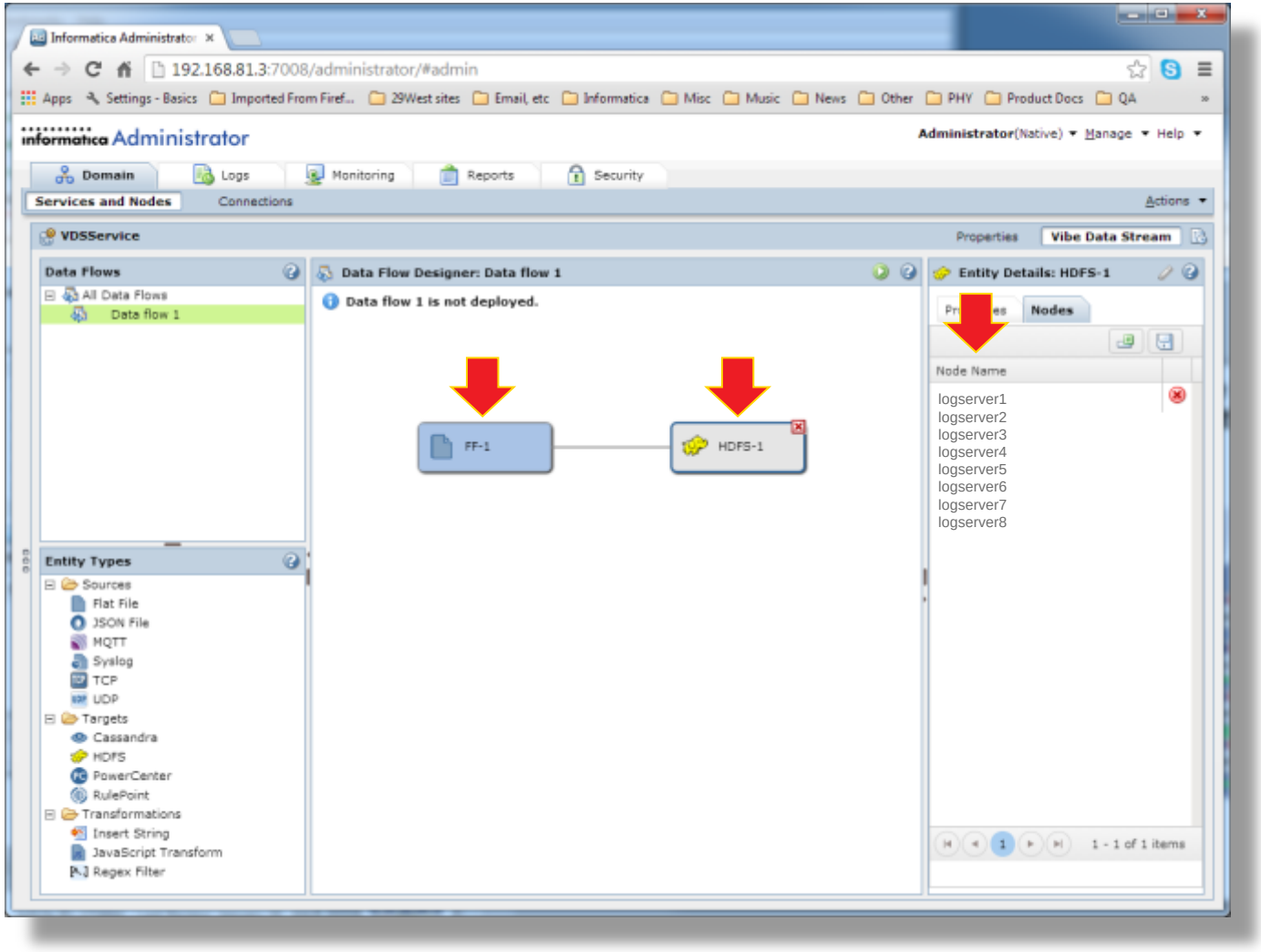
informatica

Collection at Scale and Processing at the Edge



informatica

Logical data flows mapped to physical nodes



informatica

Summary

- No daemons or servers in delivery path
  - Maximize speed and scalability
  - No single points of failure
- Choice of protocols (data “payload” agnostic)
  - TCP, UDP, AMQP, unicast, multicast, shared memory, etc.
- Secure transports, handshakes and storage
  - Integrity, with or without confidentiality
- Secure message routing for extended enterprise
  - Intelligently bridge segmented networks and applications
- Centralized monitoring (with API)
  - Integrated insight from every endpoint (other layers too!)

Summary (cont'd)

- Dynamic service and peer discovery
  - Move applications without changing configuration or code
  - Establish data flows out-of-band to minimize overhead
- Full range of qualities of service
  - From reliable (best-effort) to durable (guaranteed)
- Standards-based interfaces
  - Easily plug in third-party products and services
- Centralized management (with API)
  - Configure top-down; implement locally
- No custom hardware or storage required
  - Pure software to always run on best infrastructure

Thoughts

- Message fabric as a sensor – self awareness
- Encryption hides bad data from the good guys
- Latency, throughput, reliability trade-offs
  - Send more data at once = more throughput, less speed
  - If data is lost or delayed, how long to wait before giving up?
  - Better never than late or better late than never?
  - Reliability doesn't have to slow you down
- Processing at the edge (when can you afford XML?)

Thank You!

Gay Adams

gadams@informatica.com

cell: 301-980-9148

informatica