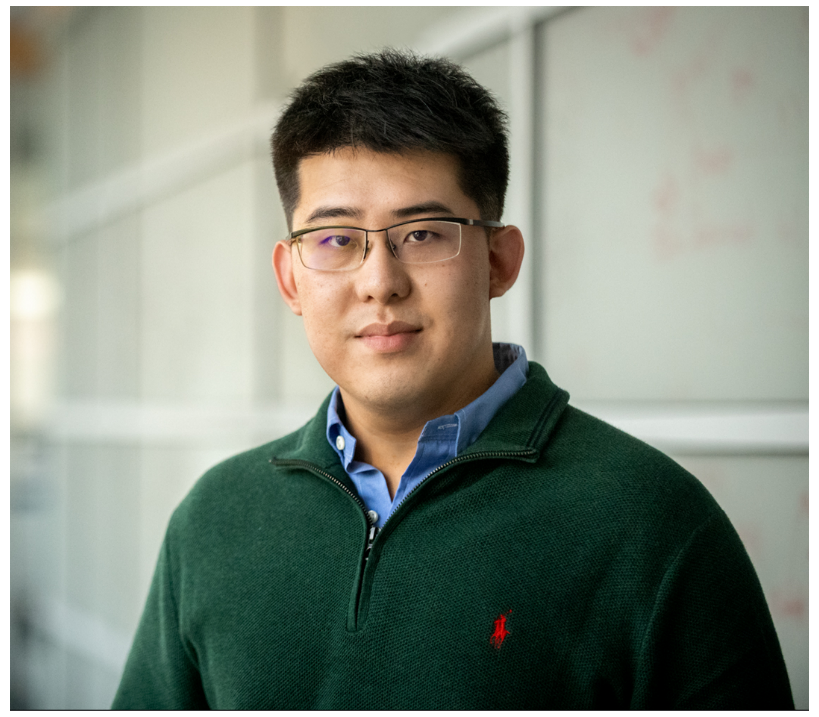
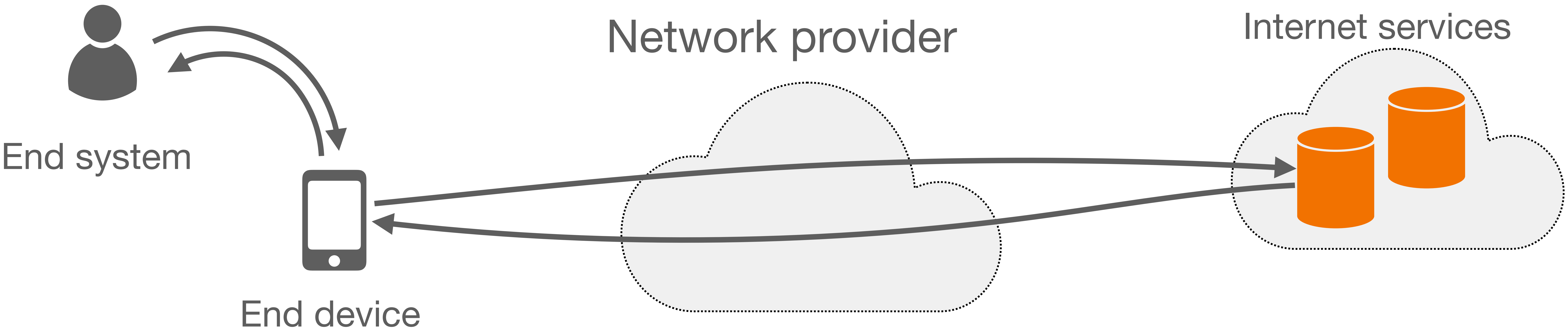
Toward Flexible Auditing for In-Network Functionality

Shuwen Sun, *Northeastern University*
David Choffnes, *Northeastern University*



CoNEXT Student Workshop (CoNEXT SW ’22), Dec. 09, 2022

In-network functionality to assist End devices



Network Function

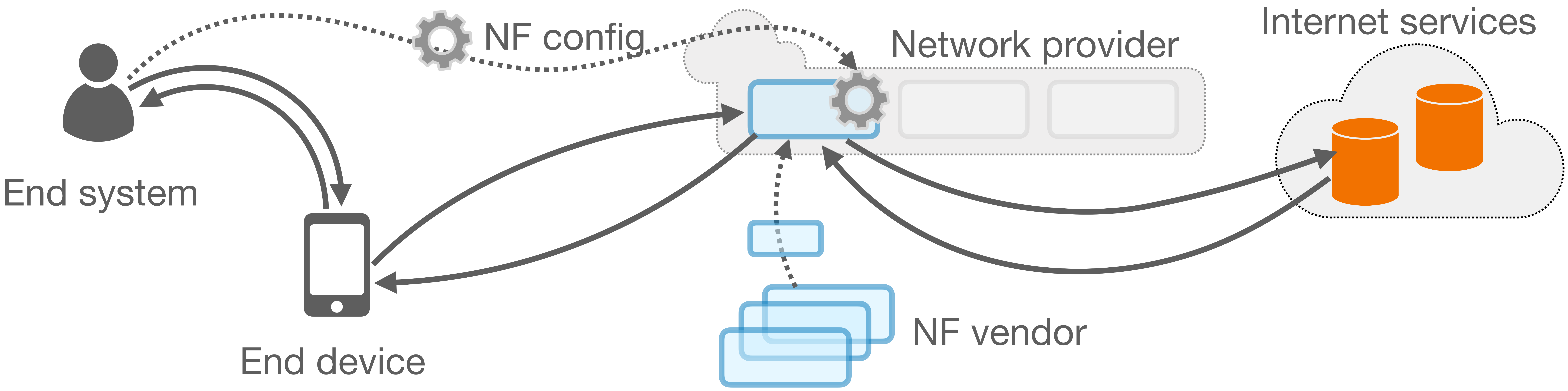
Mobile browser proxy

- Prophecy [NSDI '19]

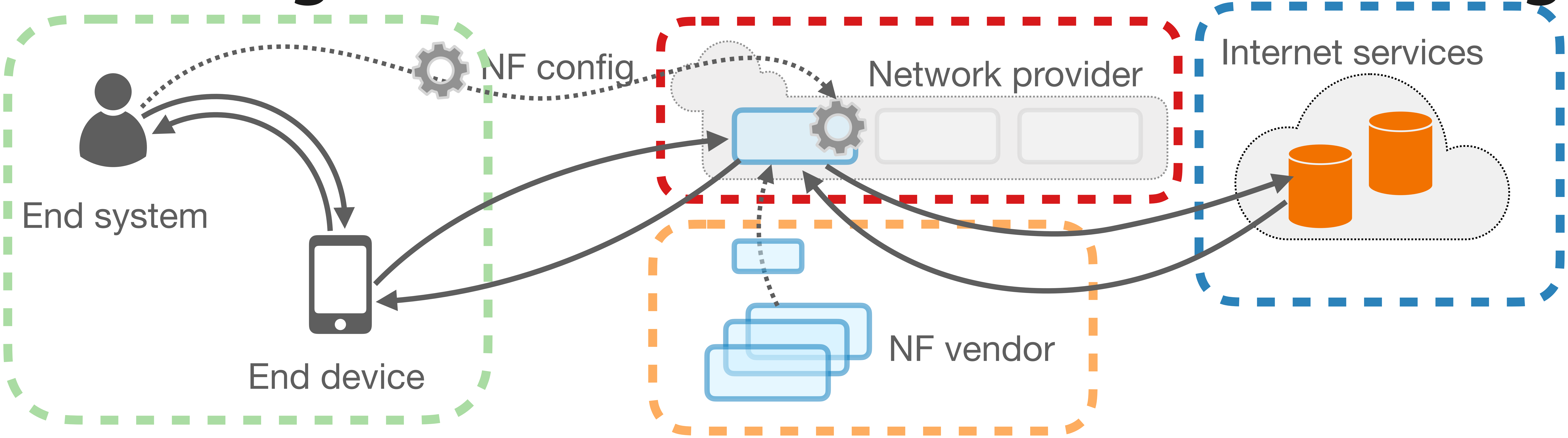
Security and privacy

- ZKMB [USENIX Sec '22]
- Bento [SIGCOMM '21]

In-network functionality to assist End devices

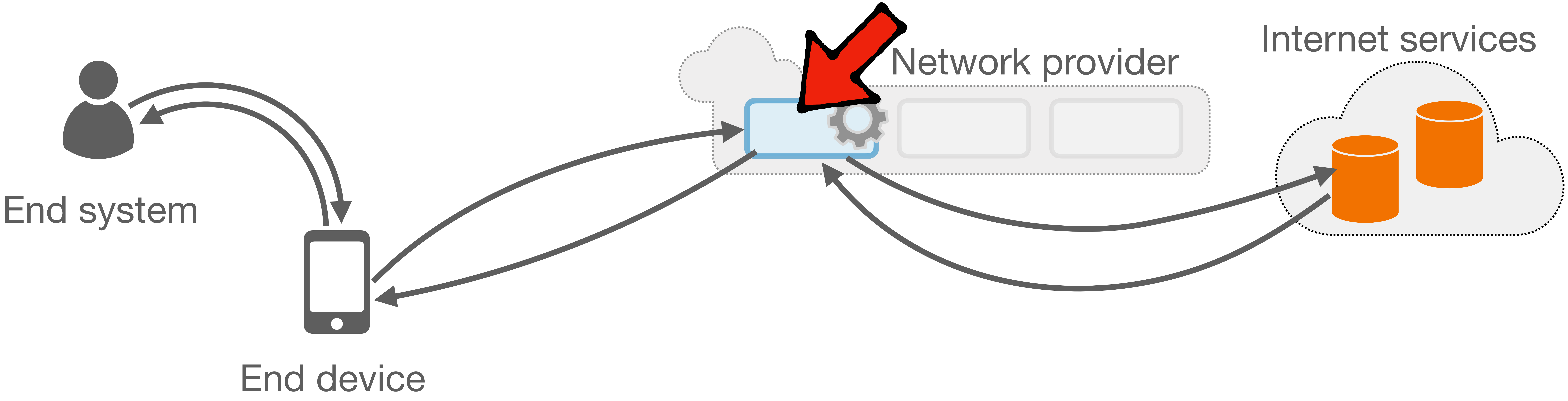


Challenges: Lack of trust and need for auditing



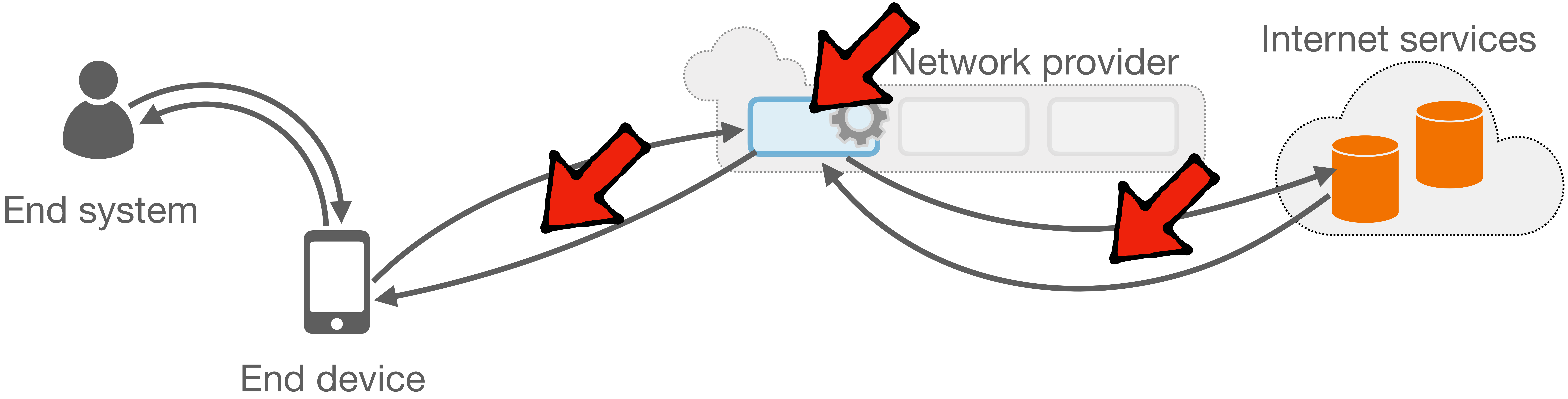
End devices, NF vendor, Network provider and Internet service
do not mutually trust each other.

Challenges: Lack of trust and need for auditing



Need to audit whether functionality is
- faithfully deployed

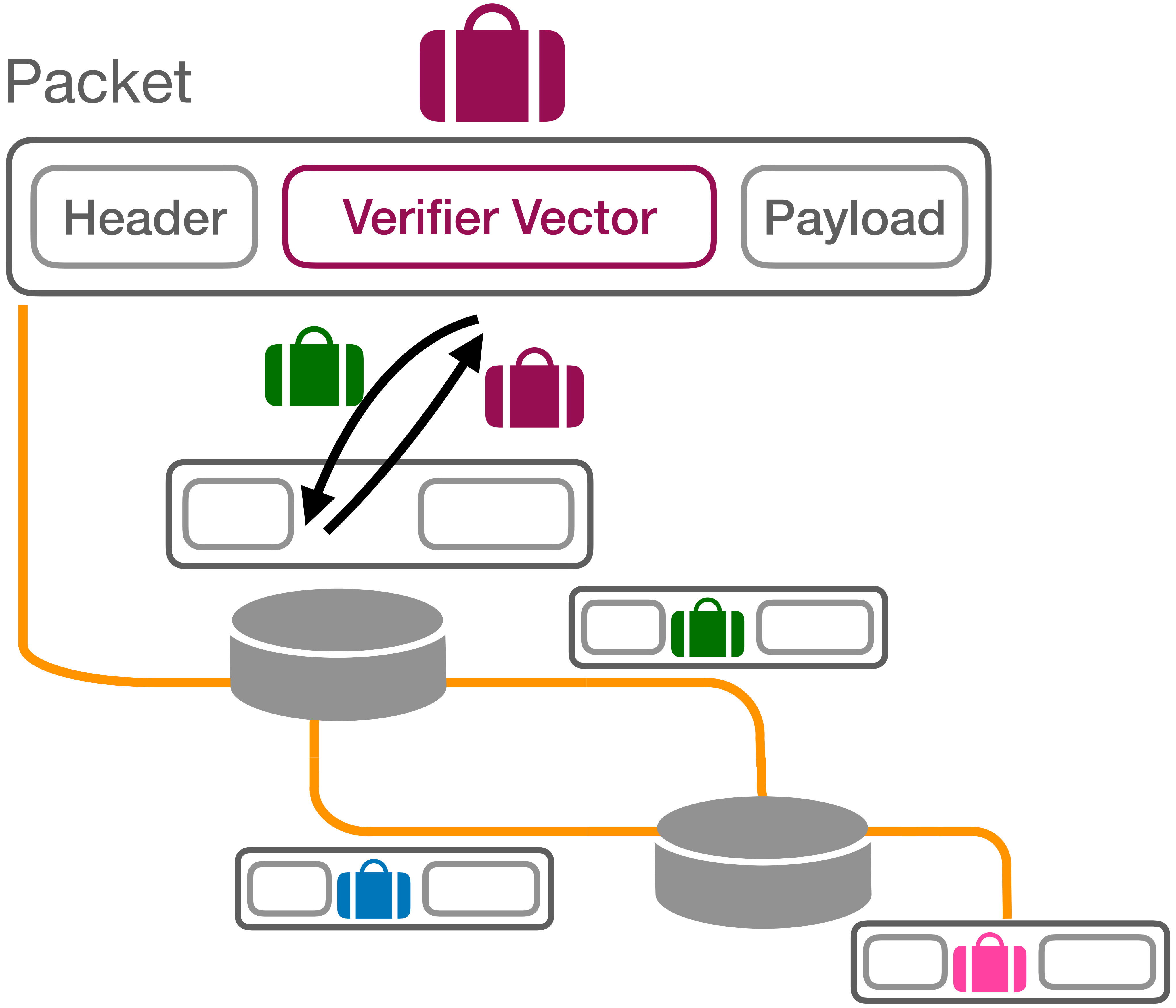
Challenges: Lack of trust and need for auditing



Need to audit whether functionality is

- running as intended

Prior work: Verifiable Routing Protocol (VRP)



VRP: Icing [CoNEXT ’11], OPT [SIGCOMM ’19]

What does VRP achieves:

- Routing is verified and enforced
- No need to trust routers/switches

Limitations:

- Not general
  - Only verify and enforce network path
- Inflexible
  - All or nothing guarantees
- Infeasible to deploy
  - High cost
  - Special operation on pkts

Goal of NFAudit

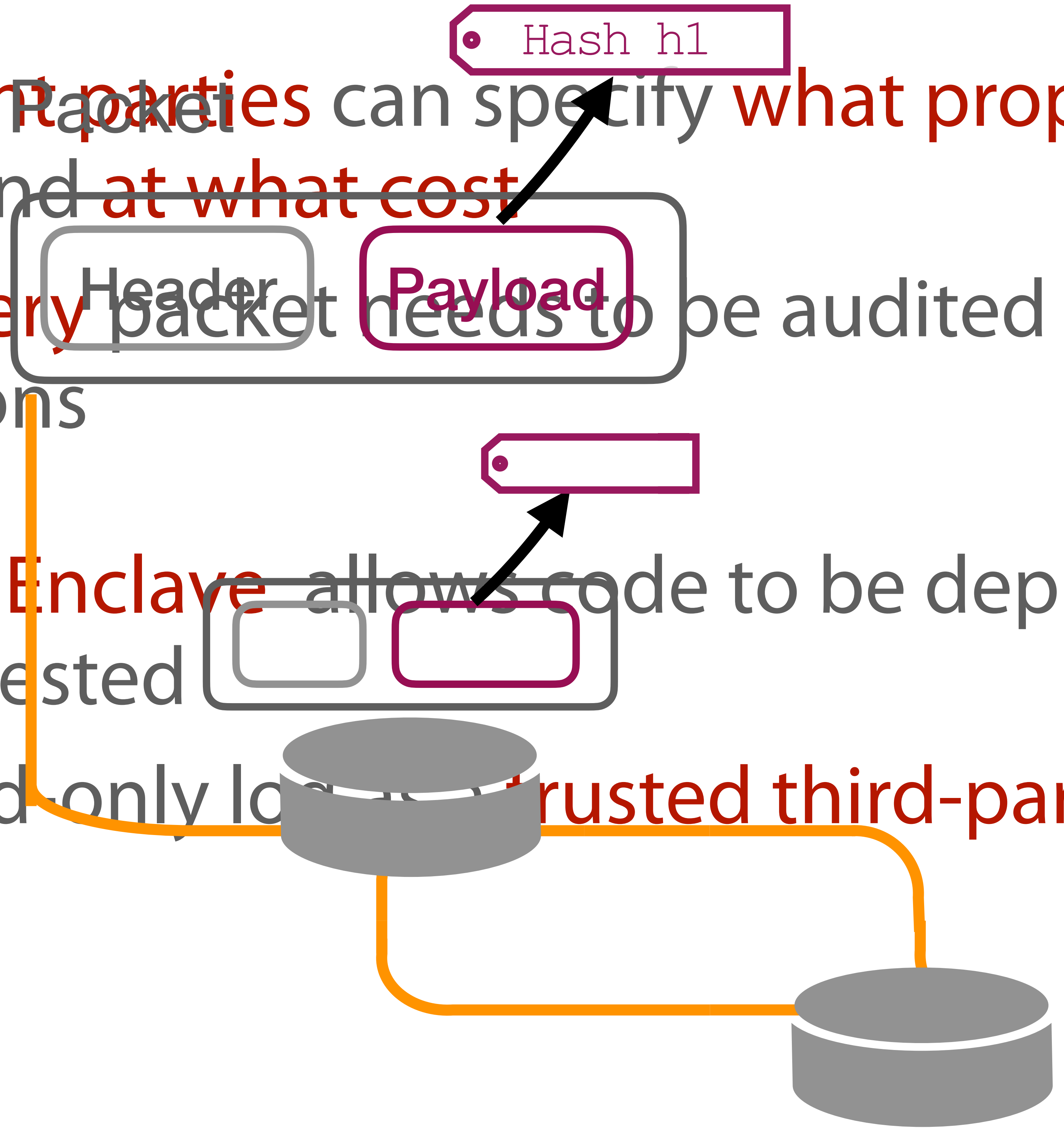
- **General:**
  - A wide range of auditable properties
- **Flexible:**
  - Trade-offs between auditing fidelity and overhead
- **Deployable:**
  - Minimal support from hardware

Key insights:

- **General:** → Use auditing building blocks (primitives) to support wider range of auditing properties

- **Flexible:** →
  - Different parties can specify what property to audit and at what cost
  - Not every packet needs to be audited to detect violations

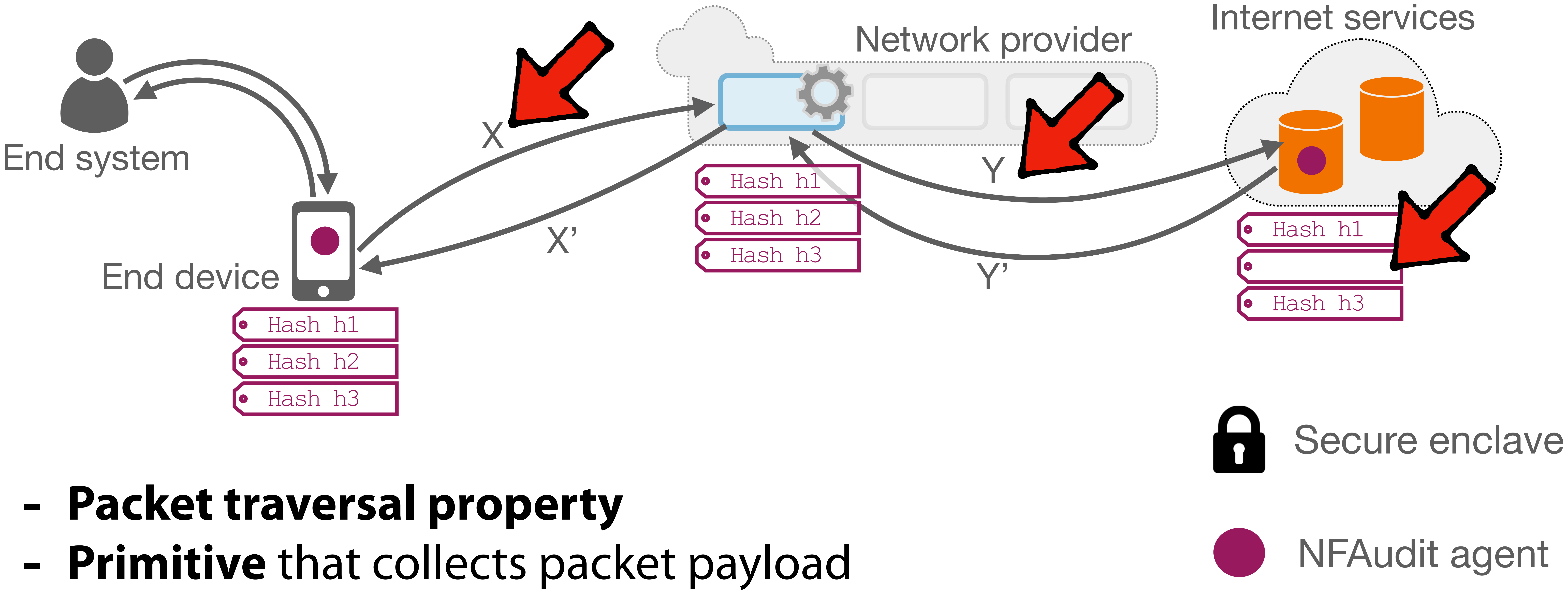
- **Deployable:** →
  - Secure Enclave allows code to be deployed and attested
  - Append-only log as trusted third-party



Key insights:

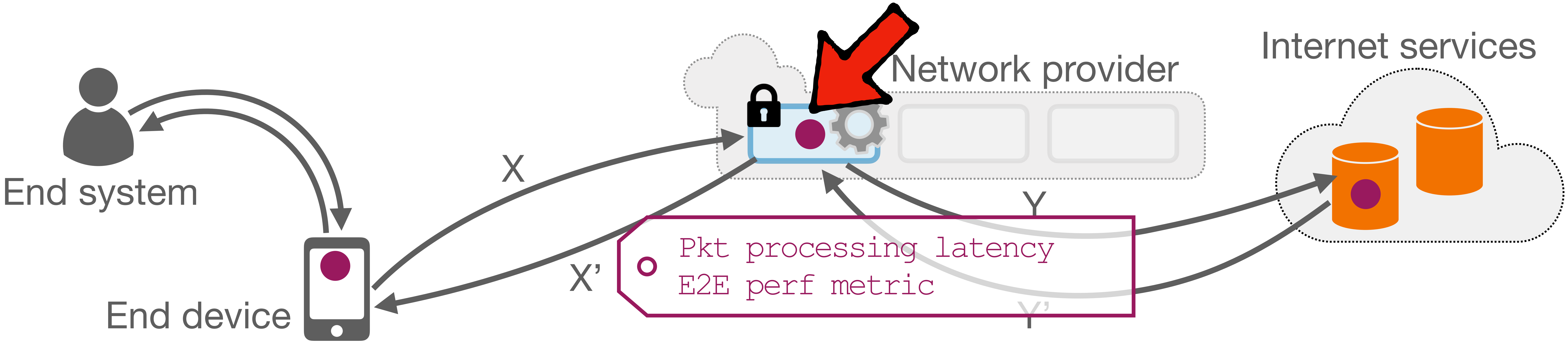
- **General:** → Use auditing building blocks (primitives) to support wider range of auditing properties
- **Flexible:** →
  - Different parties can specify what property to audit and at what cost
  - Not every packet needs to be audited to detect violations
- **Deployable:** →
  - Secure Enclave allows code to be deployed and attested
  - Append-only log as a trusted third-party

Auditing properties with primitives



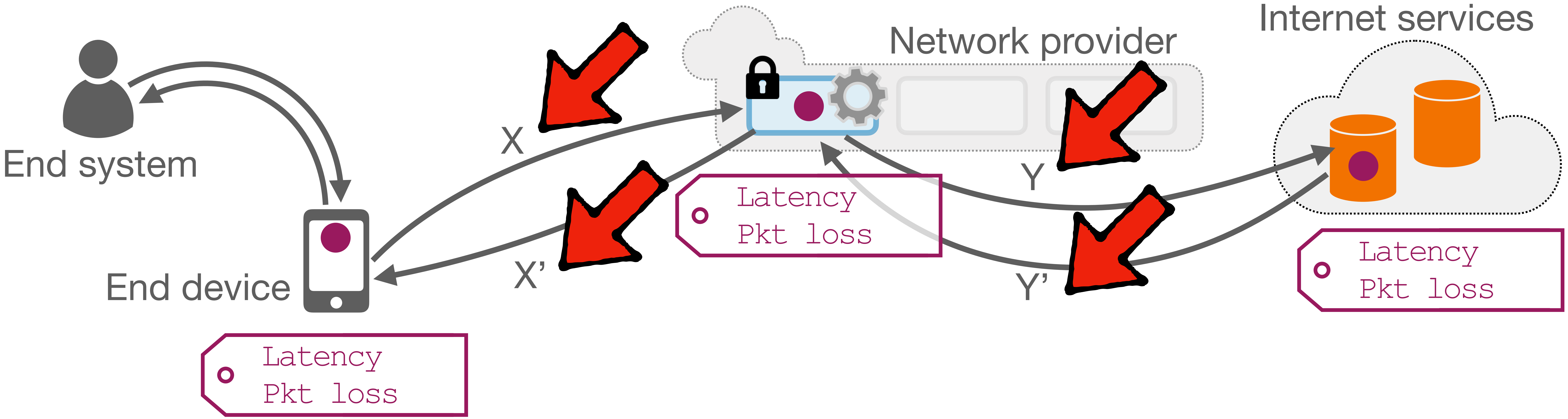
- **Packet traversal property**
- **Primitive** that collects packet payload hash

Auditing properties with primitives



- **NF performance property**
- **Primitive** that monitors NF perf metrics (packet processing time)

Auditing properties with primitives



- **Network performance property**
- **Primitive** that measures network perf along path

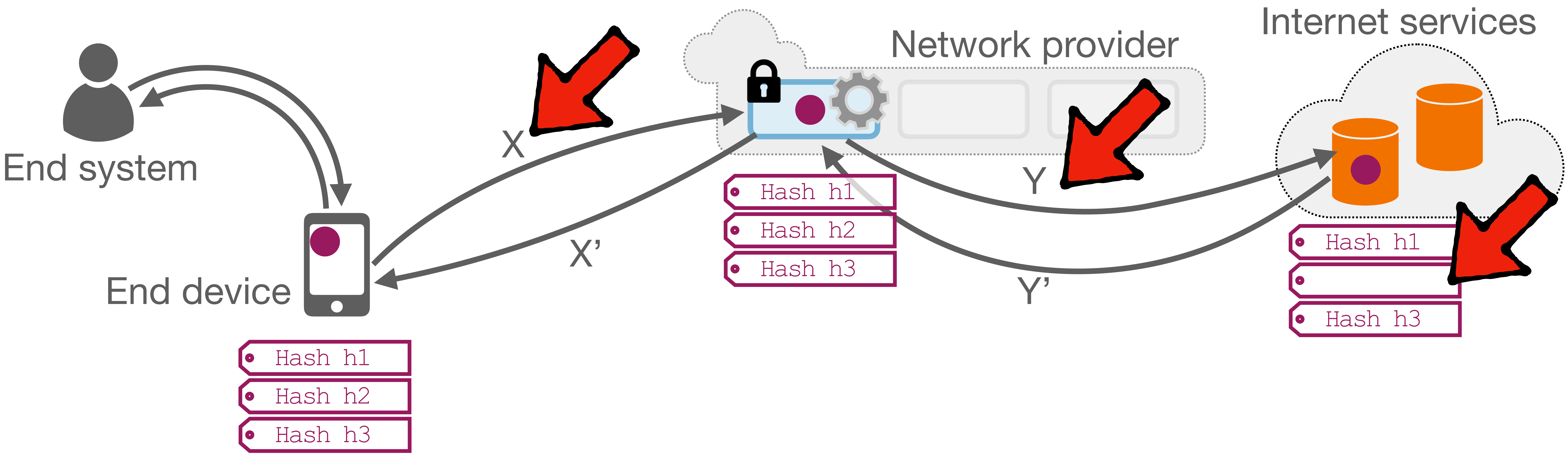
Key insights:

- **General:** → Use auditing building blocks (primitives) to support wider range of auditing properties

- **Flexible:** →
  - Different parties can specify what property to audit and at what cost
  - Not every packet needs to be audited to detect violations

- **Deployable:** →
  - Secure Enclave allows code to be deployed and attested
  - Append-only log as a trusted third-party

Traversal Auditing in more details



Trade off between auditing coverage and fidelity

Traversal Auditing in more details

Key idea: NFAudit only needs to detect one violation

Fraction of manipulated pkts: ***p***

Auditing sampling rate: ***r***

Number of packets in time window: ***m***

Probability of Evasion:

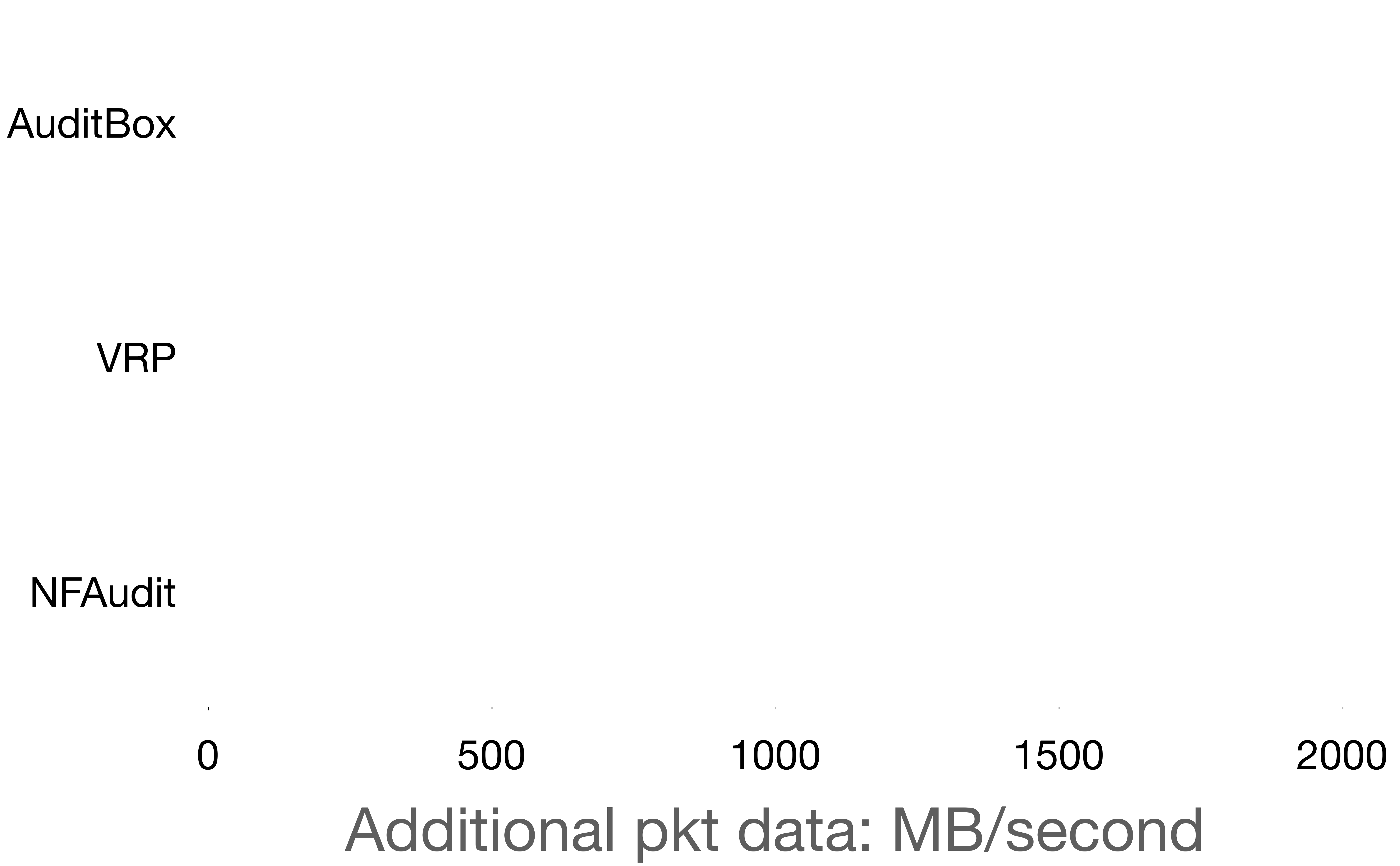
$$(1-p)^{r*m}$$

NFAudit provides high coverage with low overhead

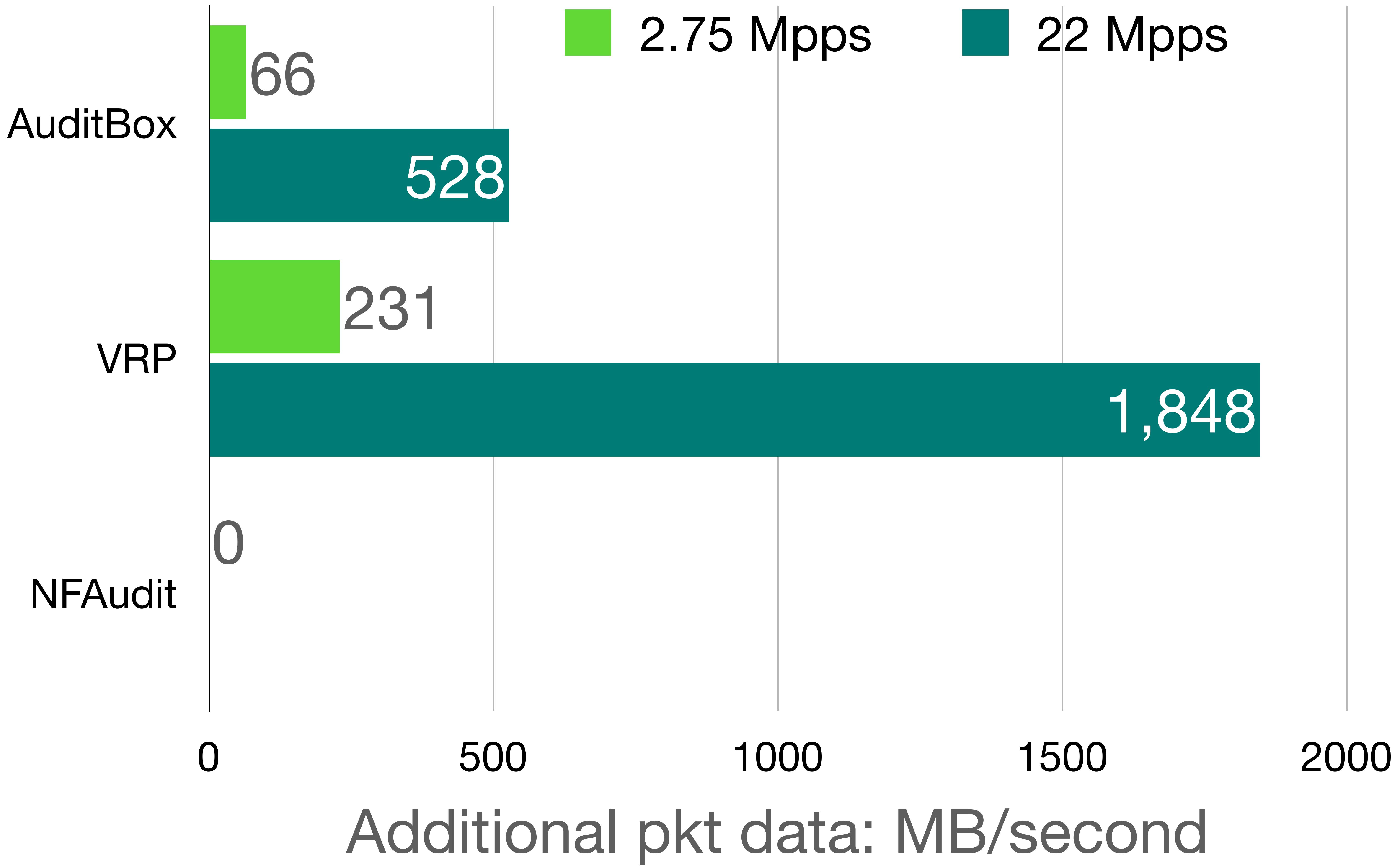
- **For NFAudit**
  - Fraction of manipulation: ***0.01%***
  - Auditing sampling: ***1%***
  - Probability of an evasion **in one second** (for 40 Gb/s traffic)**:**
    - Pkt size = 500 B: 6.39%
    - Pkt size = 64 B: 0.0000000279%
- **VRP** (AuditBox and Icing)
  - **Probability of an evasion is 0**
    - As every packet on every hop is processed

- AuditBox [NSDI '21], Icing [CoNEXT '11]

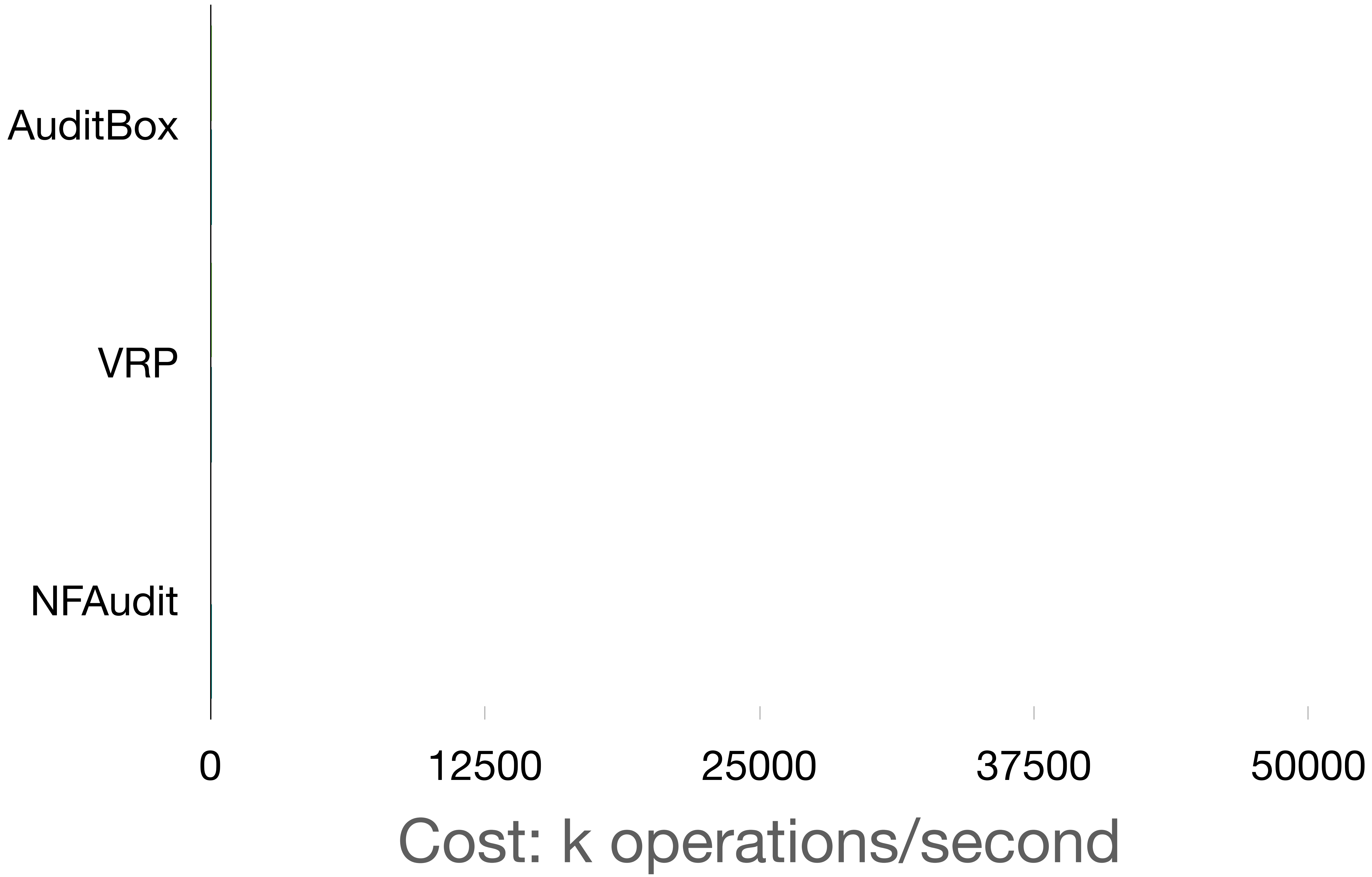
NFAudit provides high coverage with low overhead



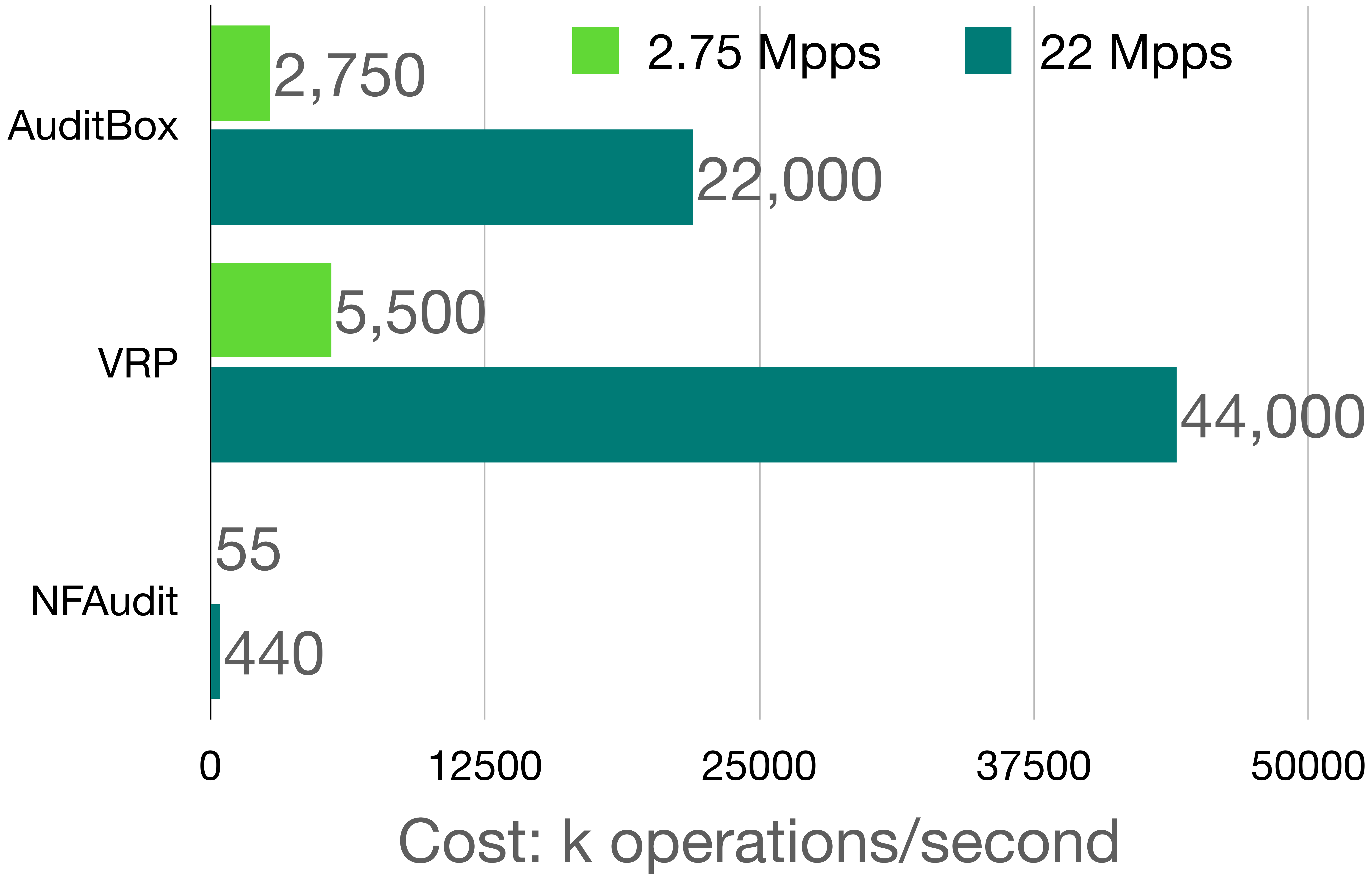
NFAudit provides high coverage with low overhead



NFAudit provides high coverage with low overhead



NFAudit provides high coverage with low overhead



Takeaways / Ongoing Work

- **NFAudit**
  - **Flexible auditing with configurable cost for diverse in-network functionality**
- **Open research questions:**
  - Are all properties auditable?
  - What are perf. trade-offs for other primitives?
  - How accurate is NFAudit for different properties?
- **Questions?**