RSSD: Defend against Ransomware with Hardware-Isolated Network-Storage Codesign and Post-Attack Analysis

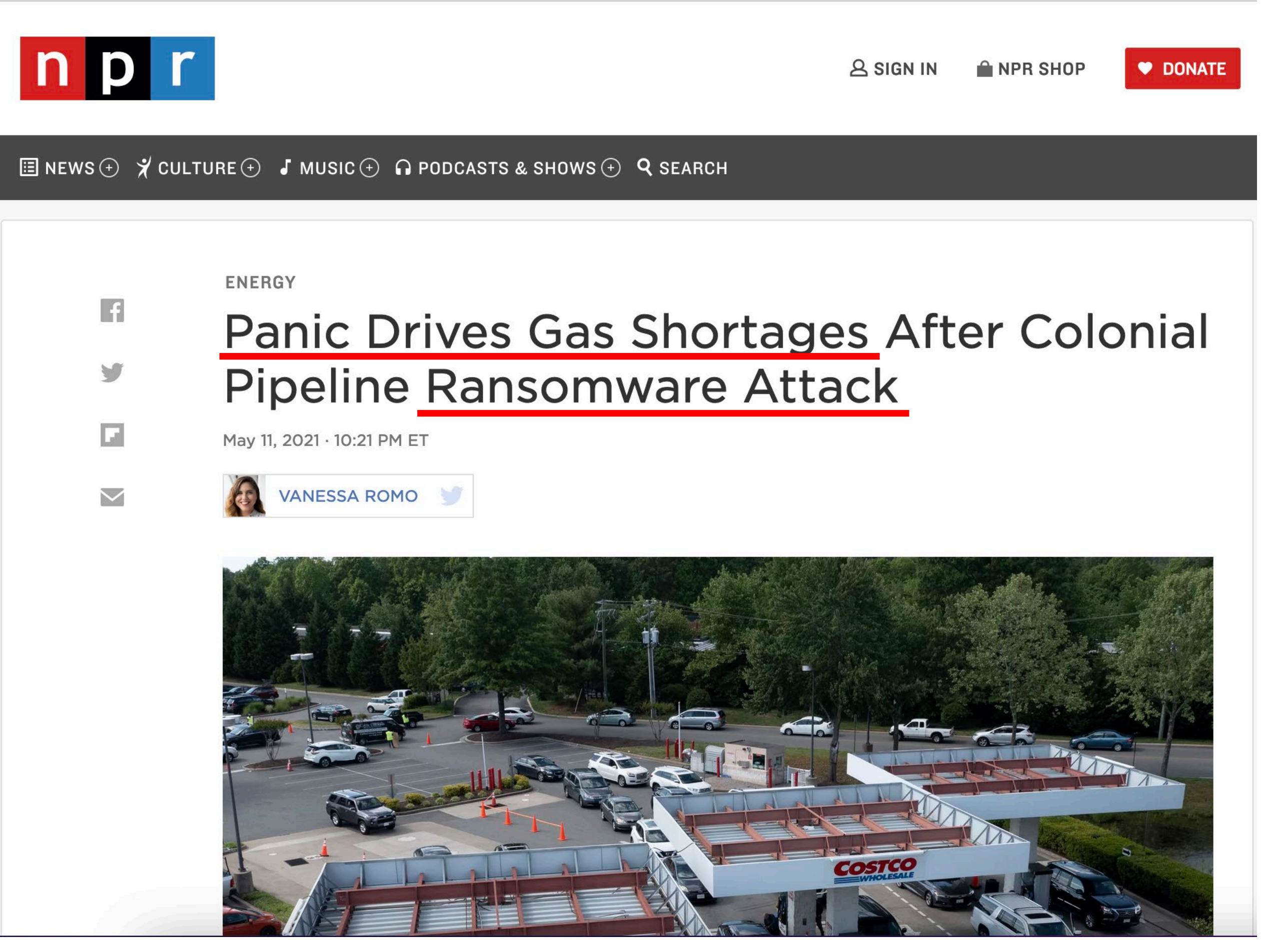
Benjamin Reidys

Peng Liu* Jian Huang

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

* PennState

Ransomware Attacks are a Major Threat



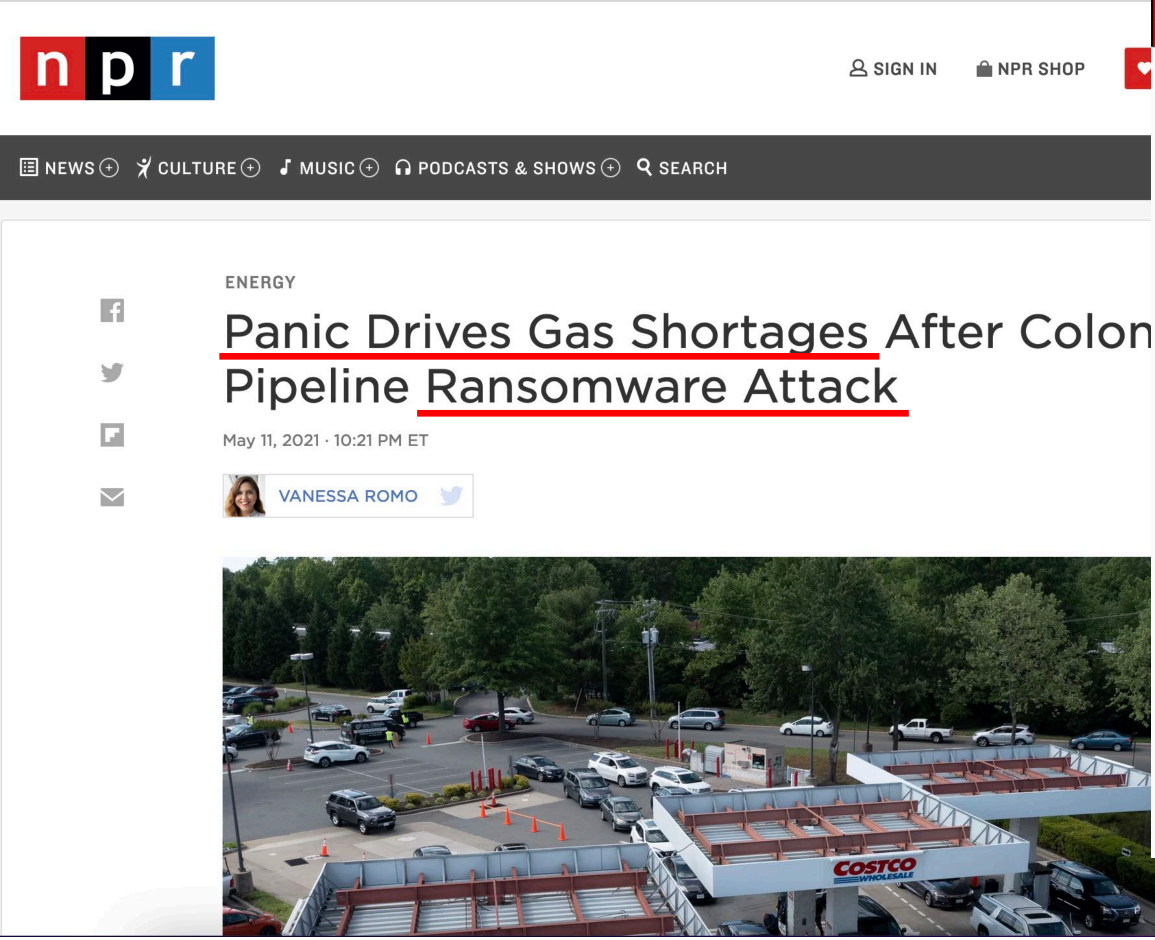
ENERGY

Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack

May 11, 2021 · 10:21 PM ET

VANESSA ROMO

Ransomware Attacks are a Major Threat

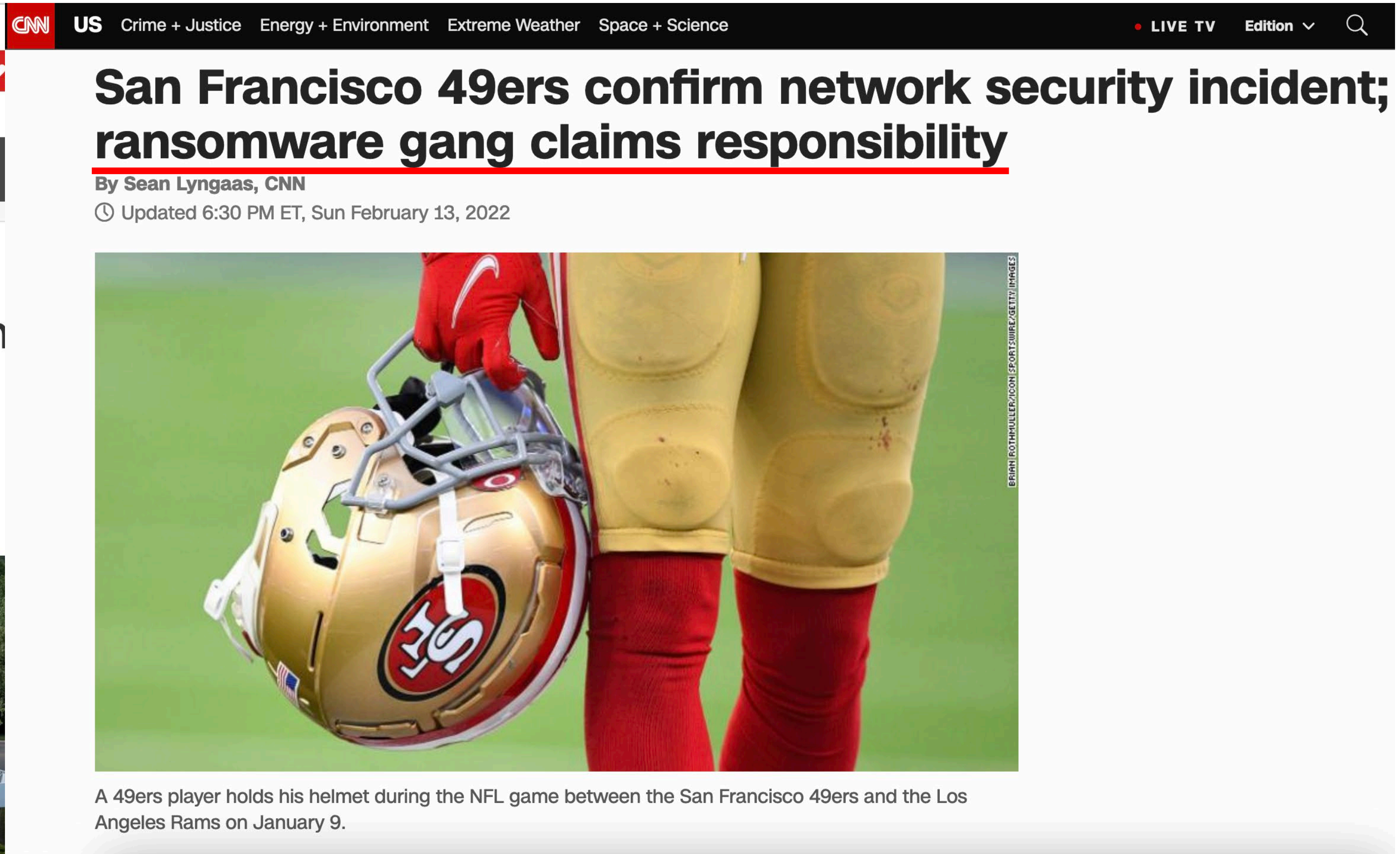


ENERGY

Panic Drives Gas Shortages After Colon Pipeline Ransomware Attack

May 11, 2021 · 10:21 PM ET

VANESSA ROMO



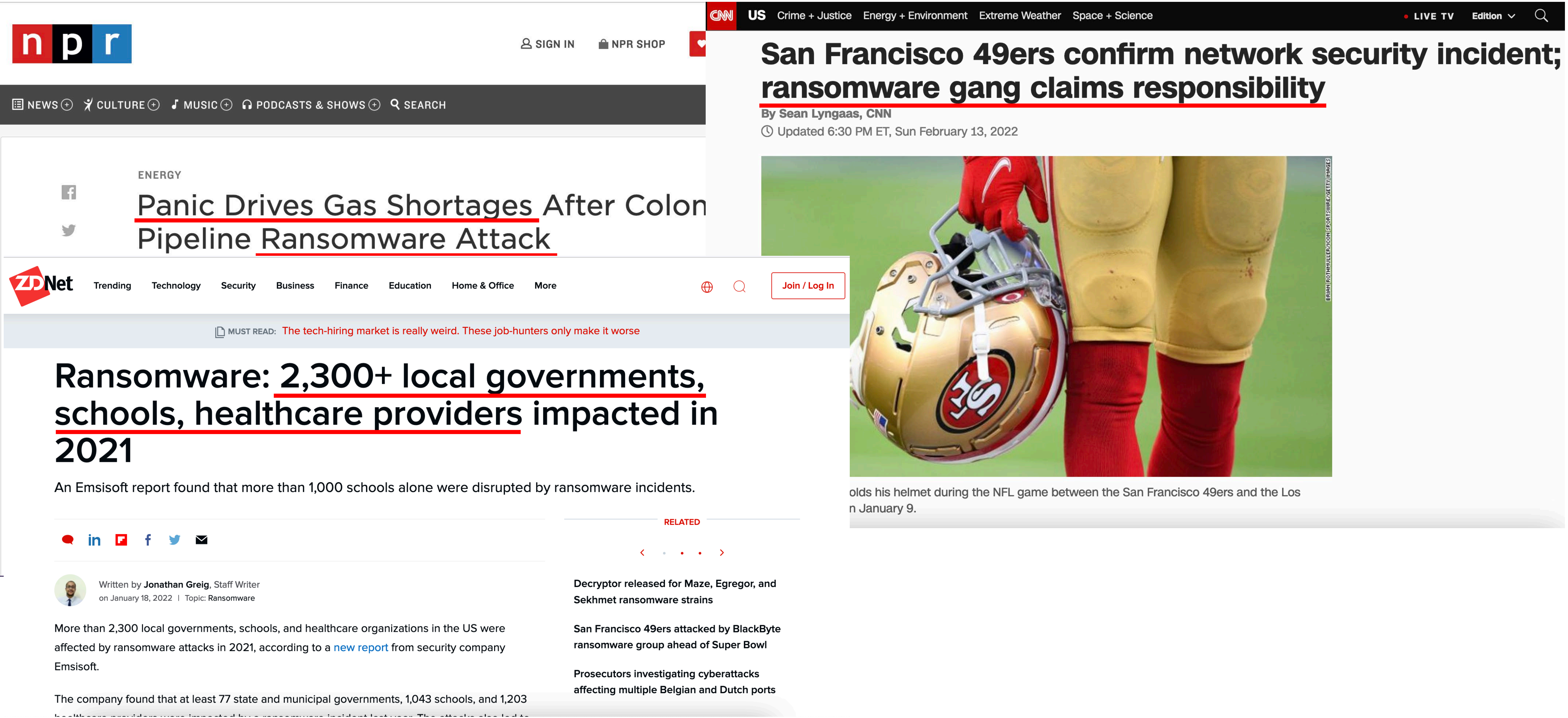
San Francisco 49ers confirm network security incident; ransomware gang claims responsibility

By Sean Lyngaas, CNN

Updated 6:30 PM ET, Sun February 13, 2022

A 49ers player holds his helmet during the NFL game between the San Francisco 49ers and the Los Angeles Rams on January 9.

Ransomware Attacks are a Major Threat



ENERGY

Panic Drives Gas Shortages After Colon Pipeline Ransomware Attack

San Francisco 49ers confirm network security incident; ransomware gang claims responsibility

By Sean Lyngaas, CNN

Updated 6:30 PM ET, Sun February 13, 2022

olds his helmet during the NFL game between the San Francisco 49ers and the Los n January 9.

MUST READ: The tech-hiring market is really weird. These job-hunters only make it worse

Ransomware: 2,300+ local governments, schools, healthcare providers impacted in 2021

An Emsisoft report found that more than 1,000 schools alone were disrupted by ransomware incidents.

Written by **Jonathan Greig**, Staff Writer
on January 18, 2022 | Topic: Ransomware

More than 2,300 local governments, schools, and healthcare organizations in the US were affected by ransomware attacks in 2021, according to a new report from security company Emsisoft.

The company found that at least 77 state and municipal governments, 1,043 schools, and 1,203

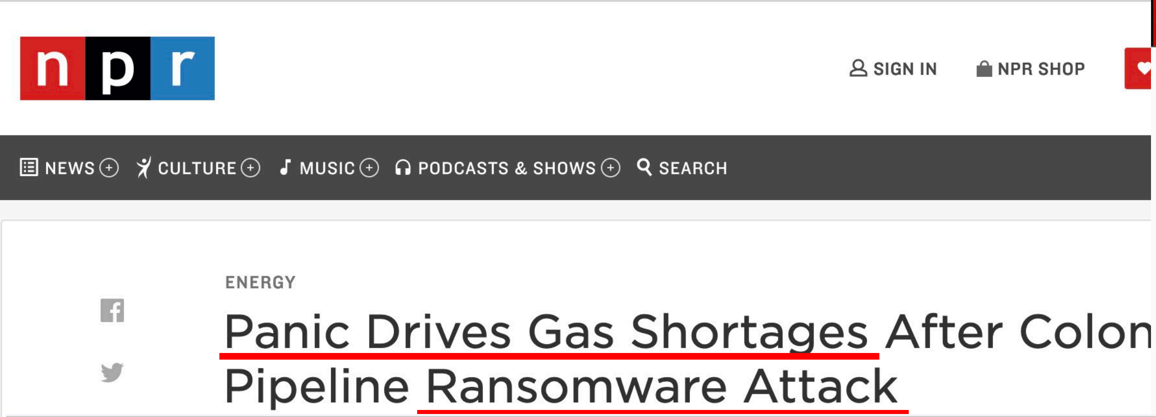
RELATED

Decryptor released for Maze, Egregor, and Sekhmet ransomware strains

San Francisco 49ers attacked by BlackByte ransomware group ahead of Super Bowl

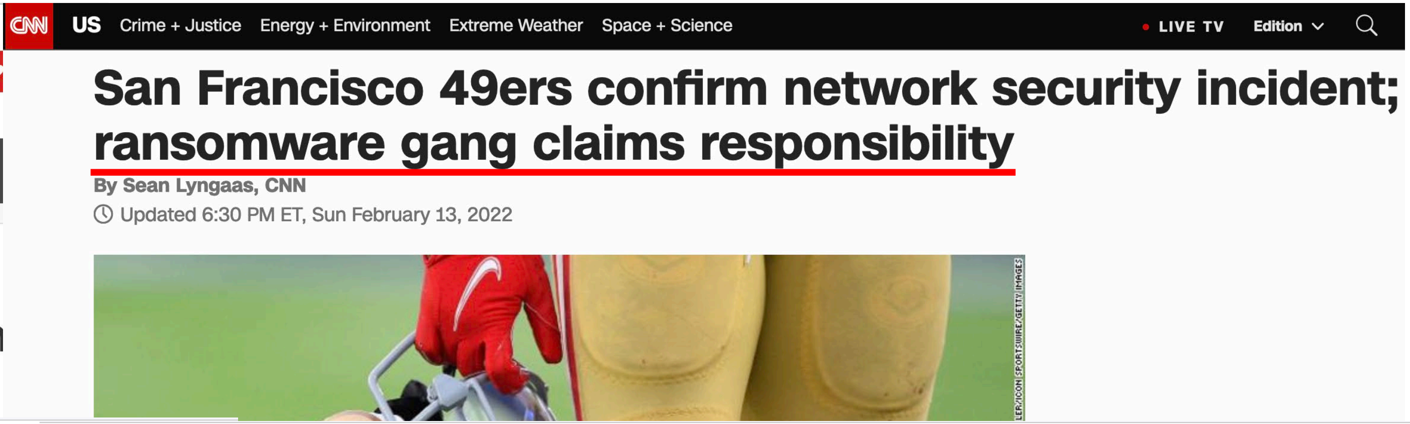
Prosecutors investigating cyberattacks affecting multiple Belgian and Dutch ports

Ransomware Attacks are a Major Threat



ENERGY

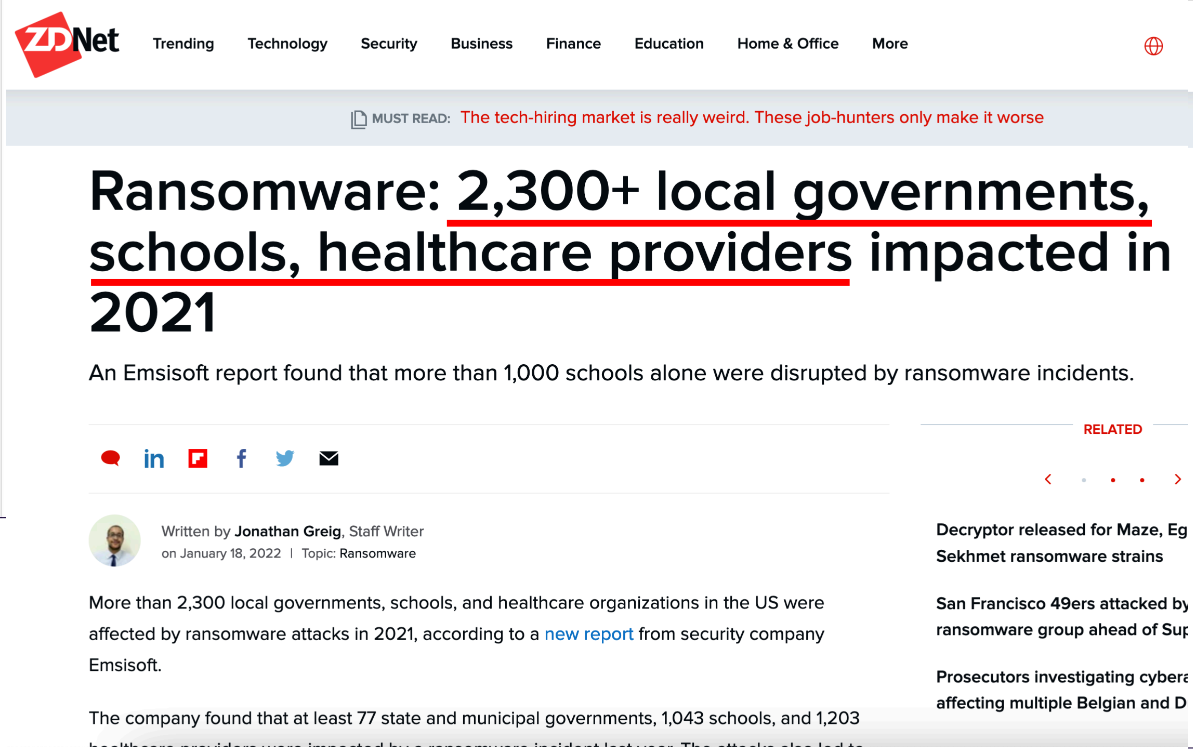
Panic Drives Gas Shortages After Colon
Pipeline Ransomware Attack



San Francisco 49ers confirm network security incident; ransomware gang claims responsibility

By Sean Lyngaas, CNN

Updated 6:30 PM ET, Sun February 13, 2022



MUST READ: The tech-hiring market is really weird. These job-hunters only make it worse

Ransomware: 2,300+ local governments, schools, healthcare providers impacted in 2021

An Emsisoft report found that more than 1,000 schools alone were disrupted by ransomware incidents.

Written by Jonathan Greig, Staff Writer
on January 18, 2022 | Topic: Ransomware

More than 2,300 local governments, schools, and healthcare organizations in the US were affected by ransomware attacks in 2021, according to a new report from security company Emsisoft.

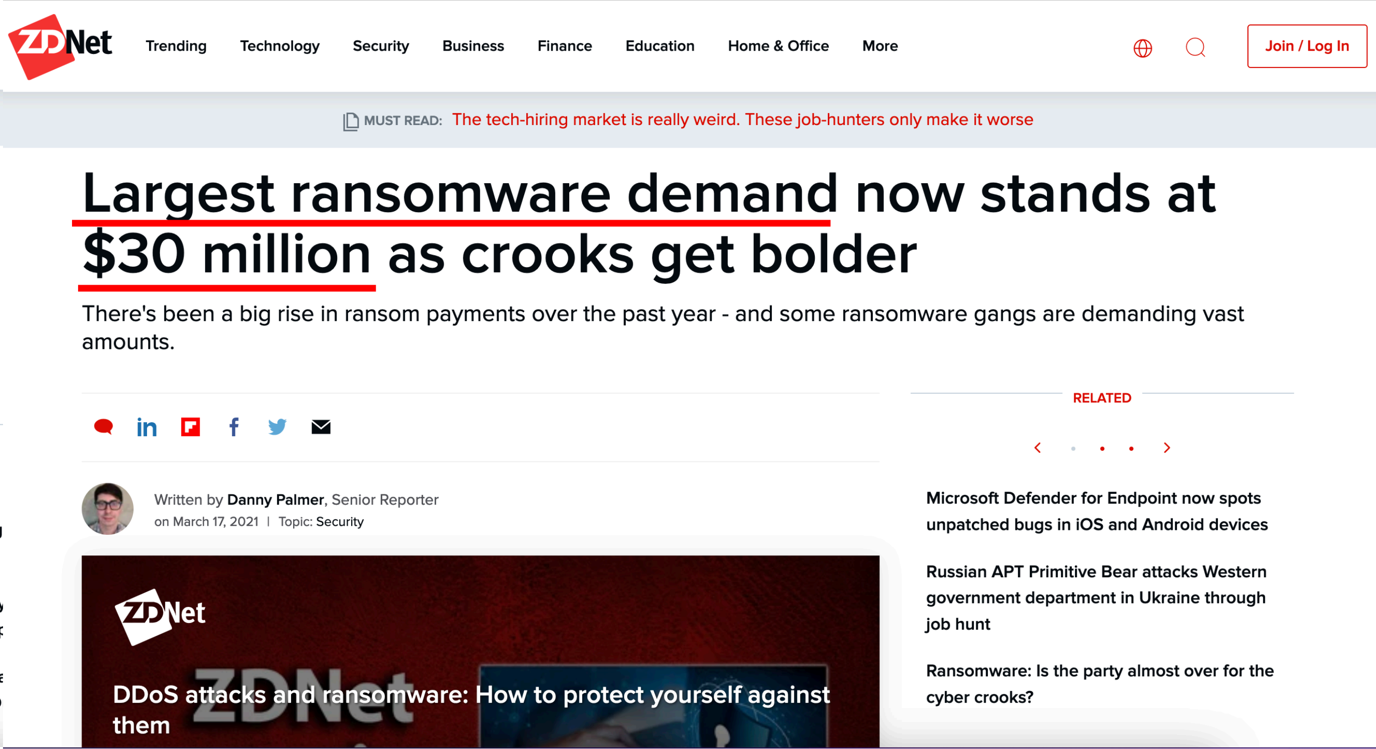
The company found that at least 77 state and municipal governments, 1,043 schools, and 1,203 healthcare providers were impacted by a ransomware incident last year. The attacks also led to

RELATED

Decryptor released for Maze, Eg
Sekhmet ransomware strains

San Francisco 49ers attacked by
ransomware group ahead of Sup

Prosecutors investigating cybera
affecting multiple Belgian and D



MUST READ: The tech-hiring market is really weird. These job-hunters only make it worse

Largest ransomware demand now stands at $30 million as crooks get bolder

There's been a big rise in ransom payments over the past year - and some ransomware gangs are demanding vast amounts.

Written by Danny Palmer, Senior Reporter
on March 17, 2021 | Topic: Security

ZDNet

DDoS attacks and ransomware: How to protect yourself against them

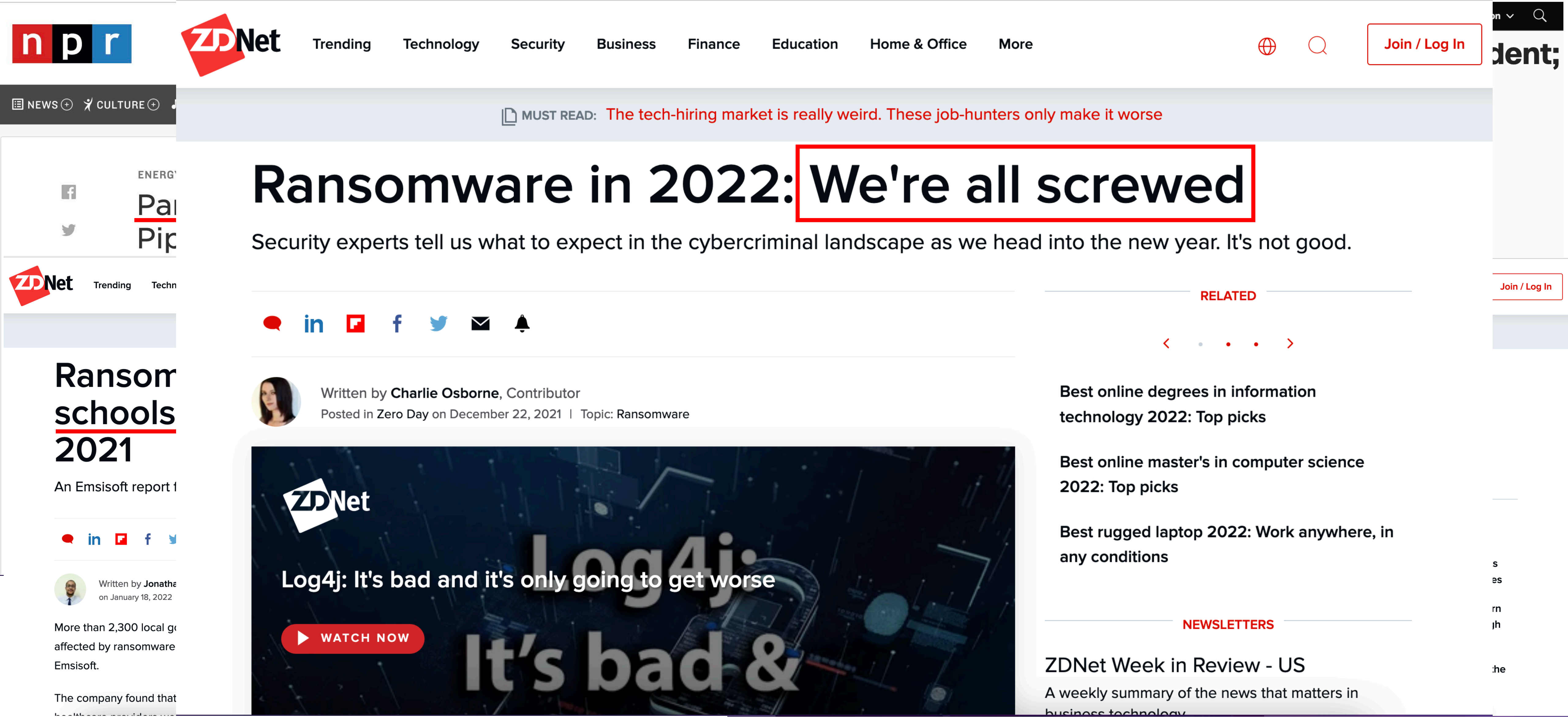
RELATED

Microsoft Defender for Endpoint now spots unpatched bugs in iOS and Android devices

Russian APT Primitive Bear attacks Western government department in Ukraine through job hunt

Ransomware: Is the party almost over for the cyber crooks?

Ransomware Attacks are a Major Threat



MUST READ: The tech-hiring market is really weird. These job-hunters only make it worse

Ransomware in 2022: We're all screwed

Security experts tell us what to expect in the cybercriminal landscape as we head into the new year. It's not good.

Written by **Charlie Osborne**, Contributor
Posted in Zero Day on December 22, 2021 | Topic: Ransomware

RELATED

Best online degrees in information technology 2022: Top picks

Best online master's in computer science 2022: Top picks

Best rugged laptop 2022: Work anywhere, in any conditions

NEWSLETTERS

ZDNet Week in Review - US

A weekly summary of the news that matters in business technology

Ransom schools 2021

An Emsisoft report

Written by Jonatha
on January 18, 2022

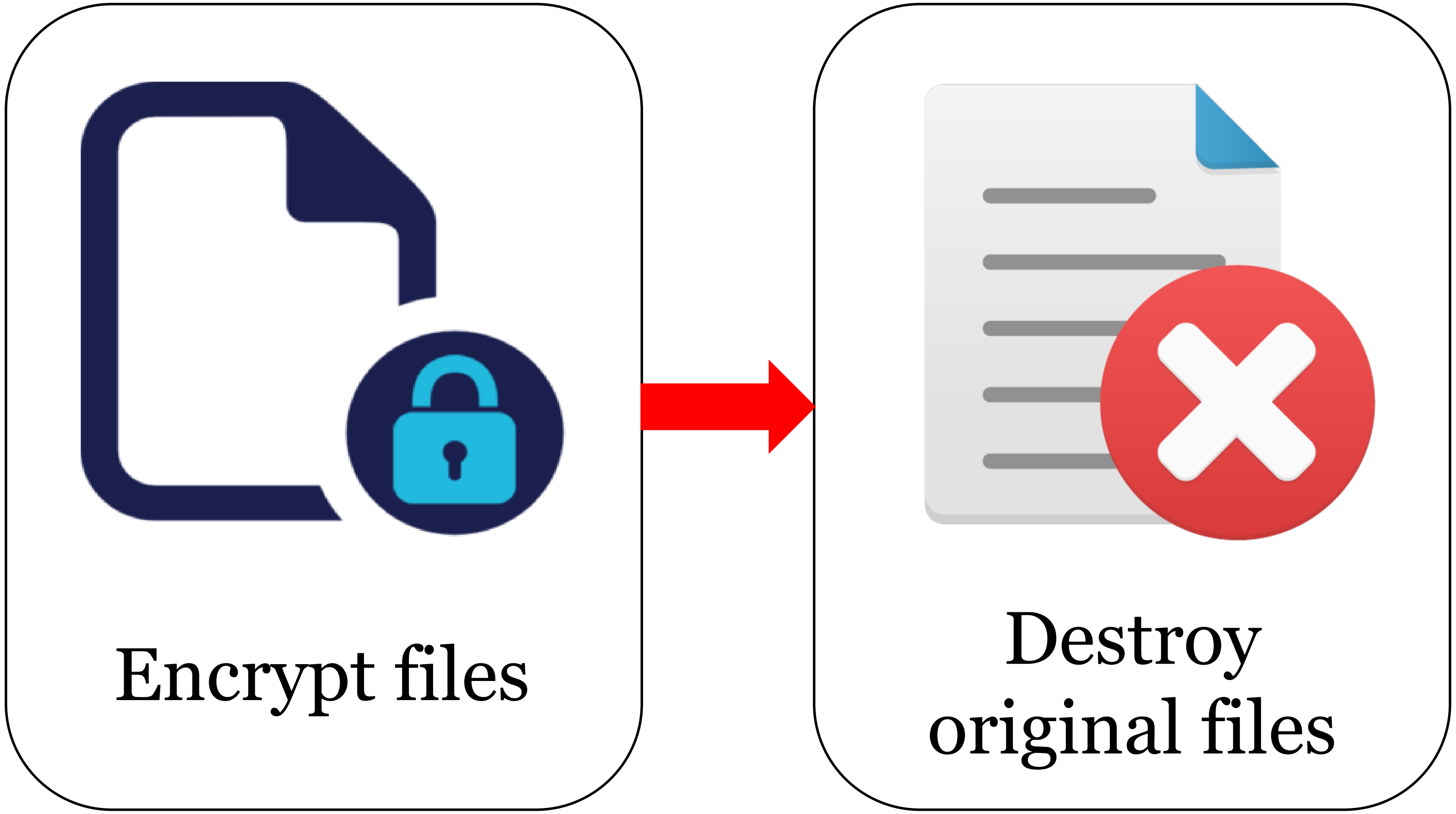
More than 2,300 local go affected by ransomware Emsisoft.

The company found that

What is Encryption Ransomware?

Encrypt files

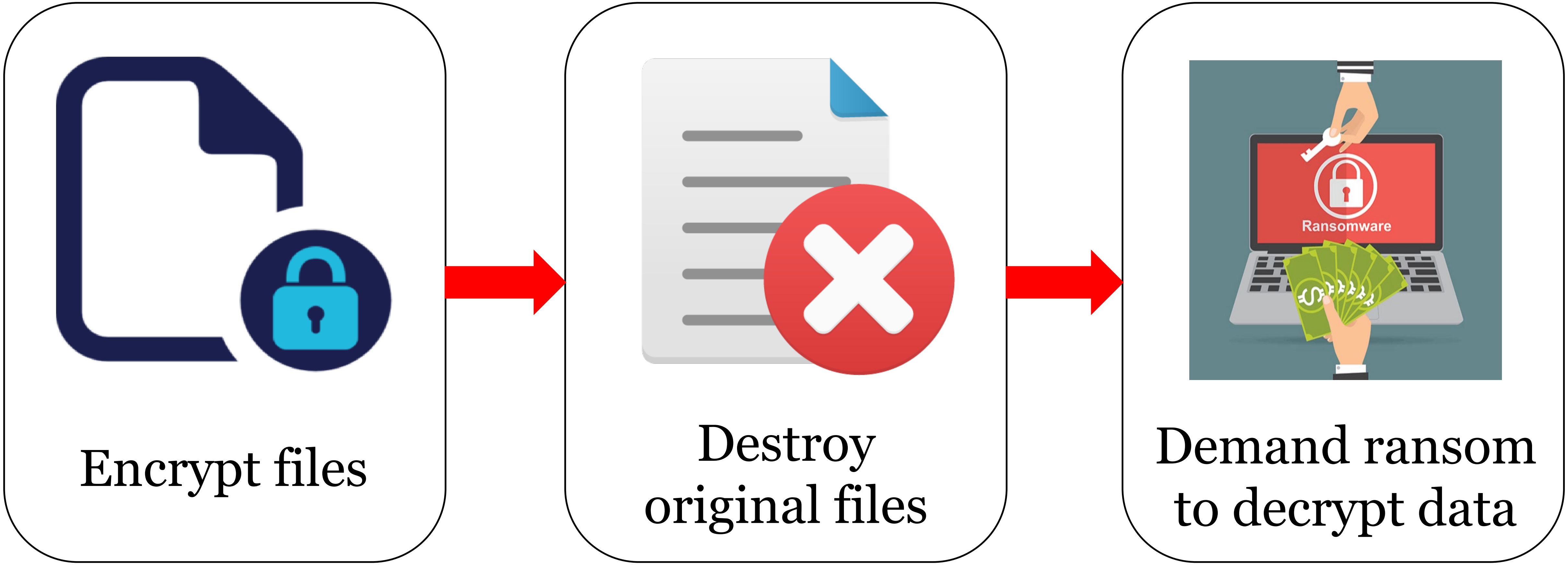
What is Encryption Ransomware?



Encrypt files

Destroy original files

What is Encryption Ransomware?



Encrypt files

Destroy original files

Demand ransom to decrypt data

State-of-the-Art Defenses: Software-Based Approaches

Malware Detection

Cannot recover files encrypted before detection!

State-of-the-Art Defenses: Software-Based Approaches

Malware Detection

Data Backups

Backups could be targeted by ransomware!

State-of-the-Art Defenses: Hardware-Based Solutions

State-of-the-Art Defenses: Hardware-Based Solutions

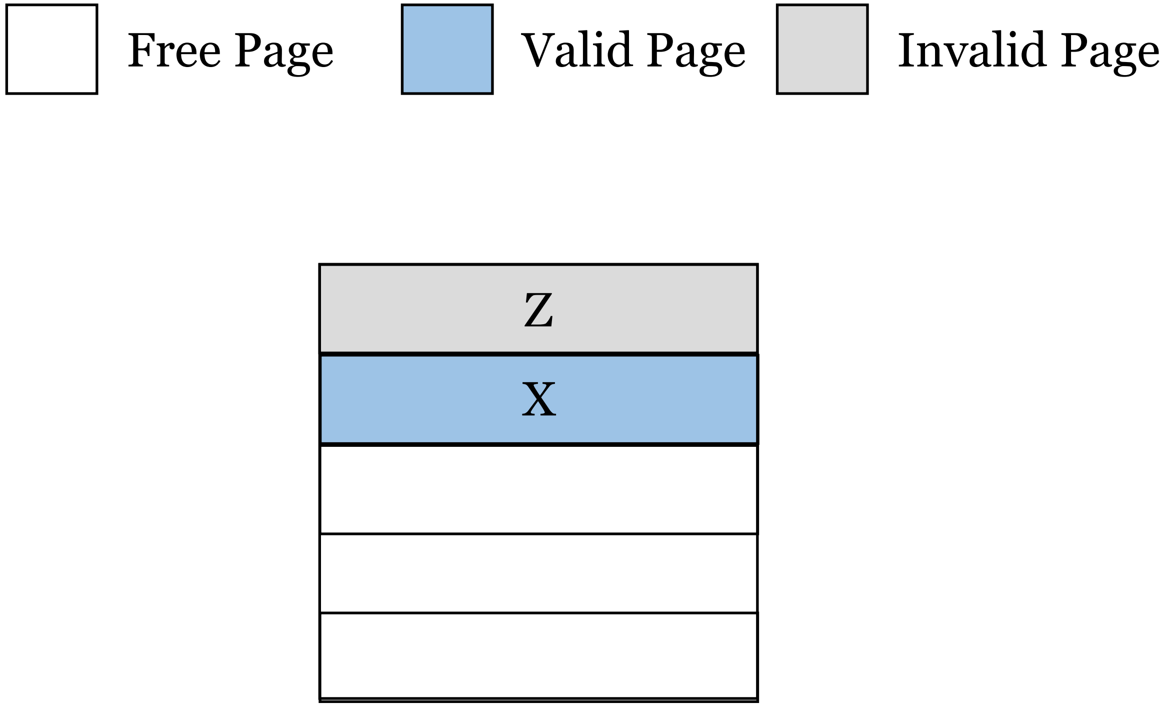
FlashGuard (CCS ‘17)

SSD-Insider (ICDCS’18)

TimeSSD (EuroSys’19)

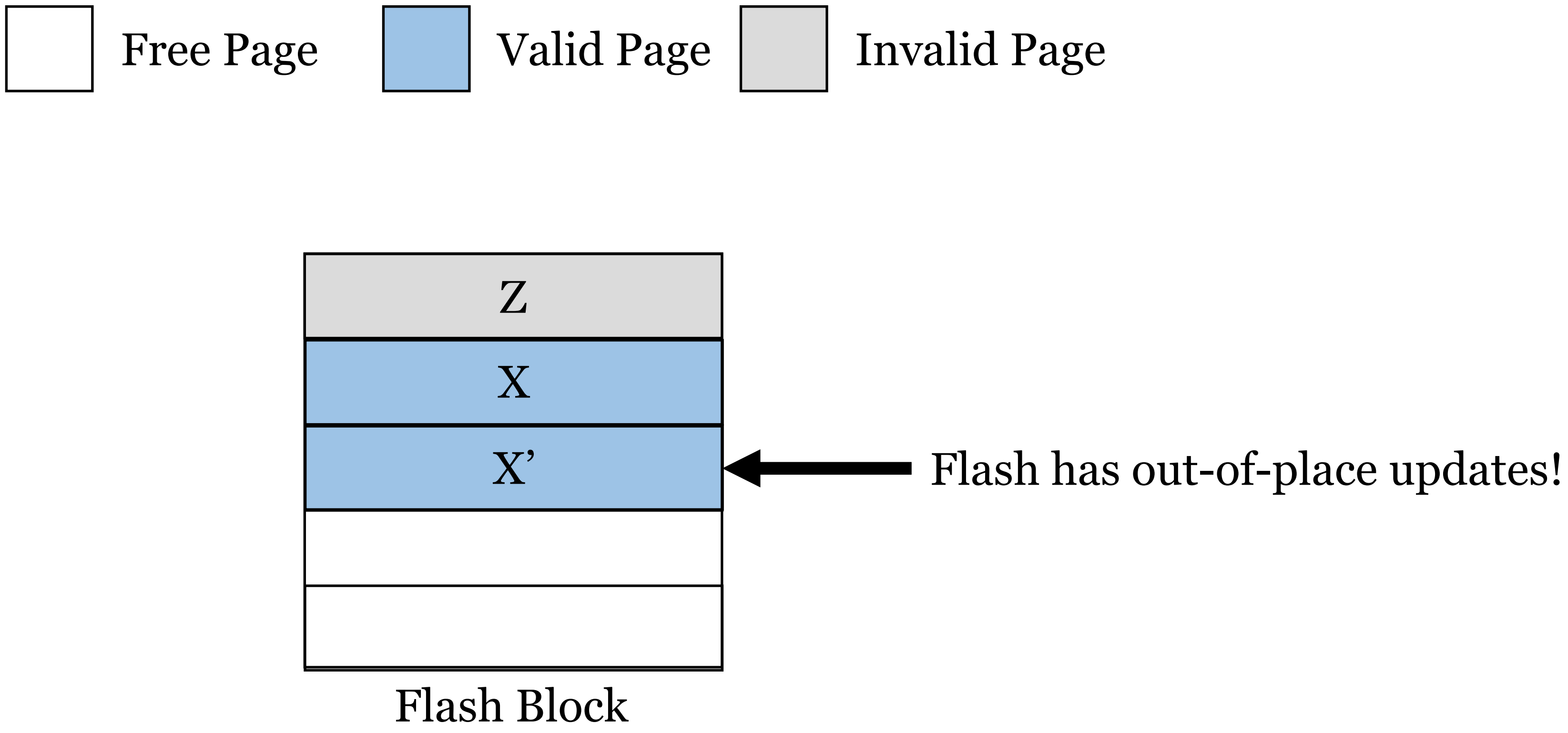
Exploit out-of-place updates in SSD to retain victim data!

SSD 101



Flash Block

SSD 101



□ Free Page

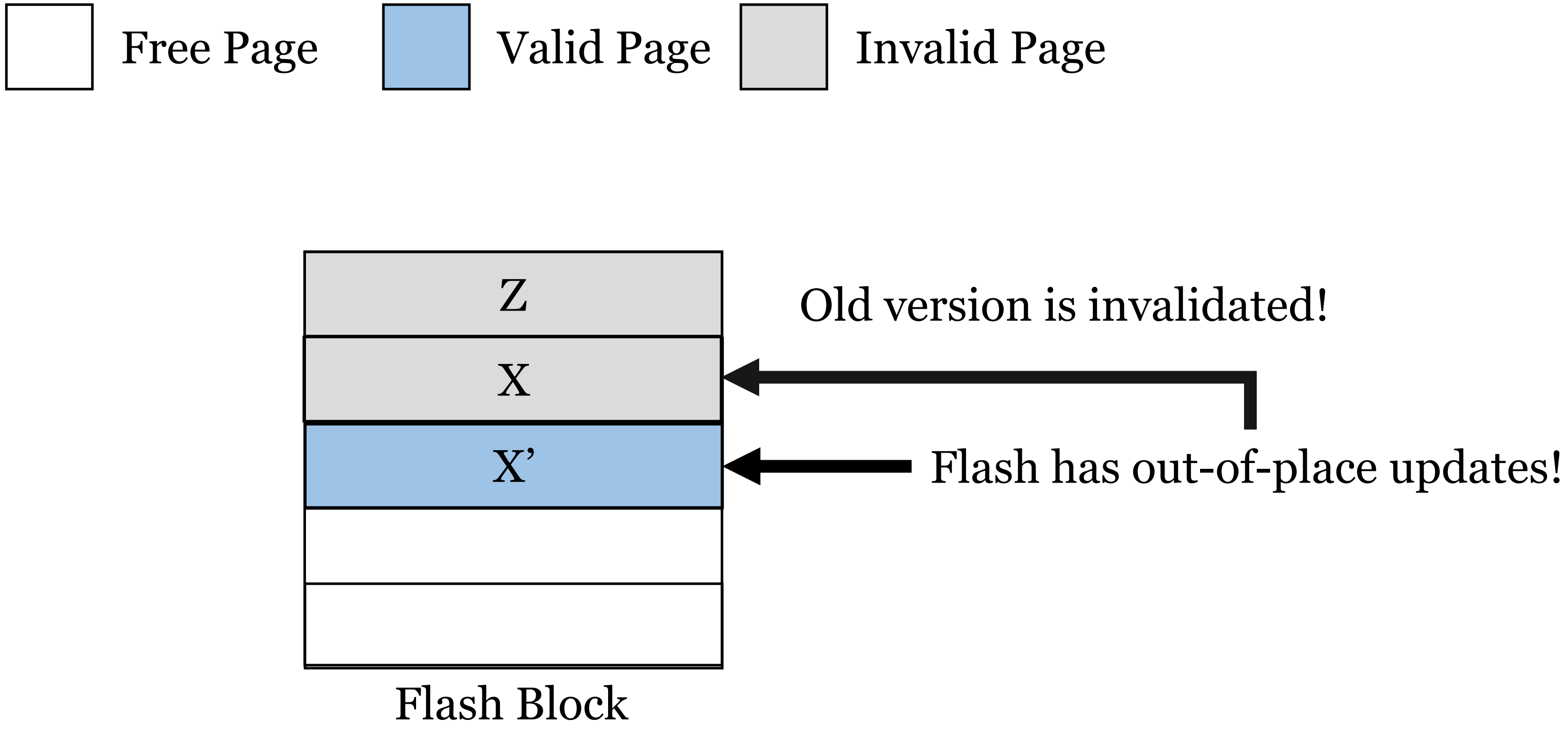
🟦 Valid Page

▨ Invalid Page

Flash has out-of-place updates!

Flash Block

SSD 101



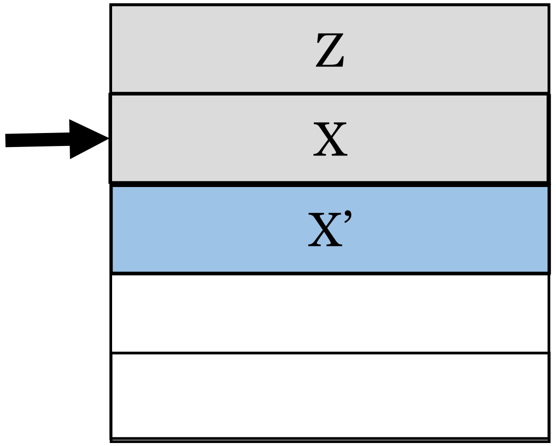
Old version is invalidated!

Flash has out-of-place updates!

SSD 101

□ Free Page 🟦 Valid Page ▨ Invalid Page

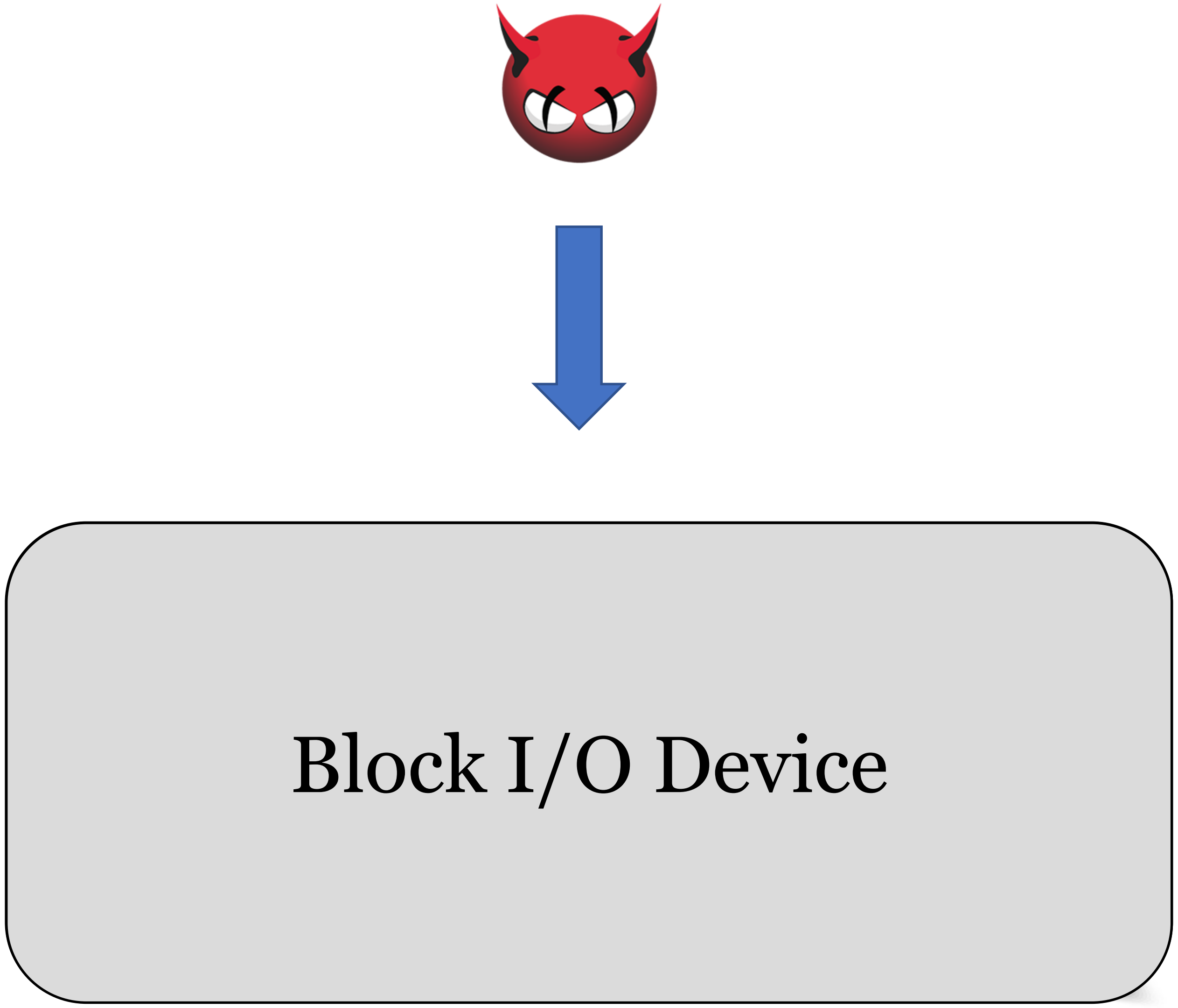
Old version is retained!



Flash Block

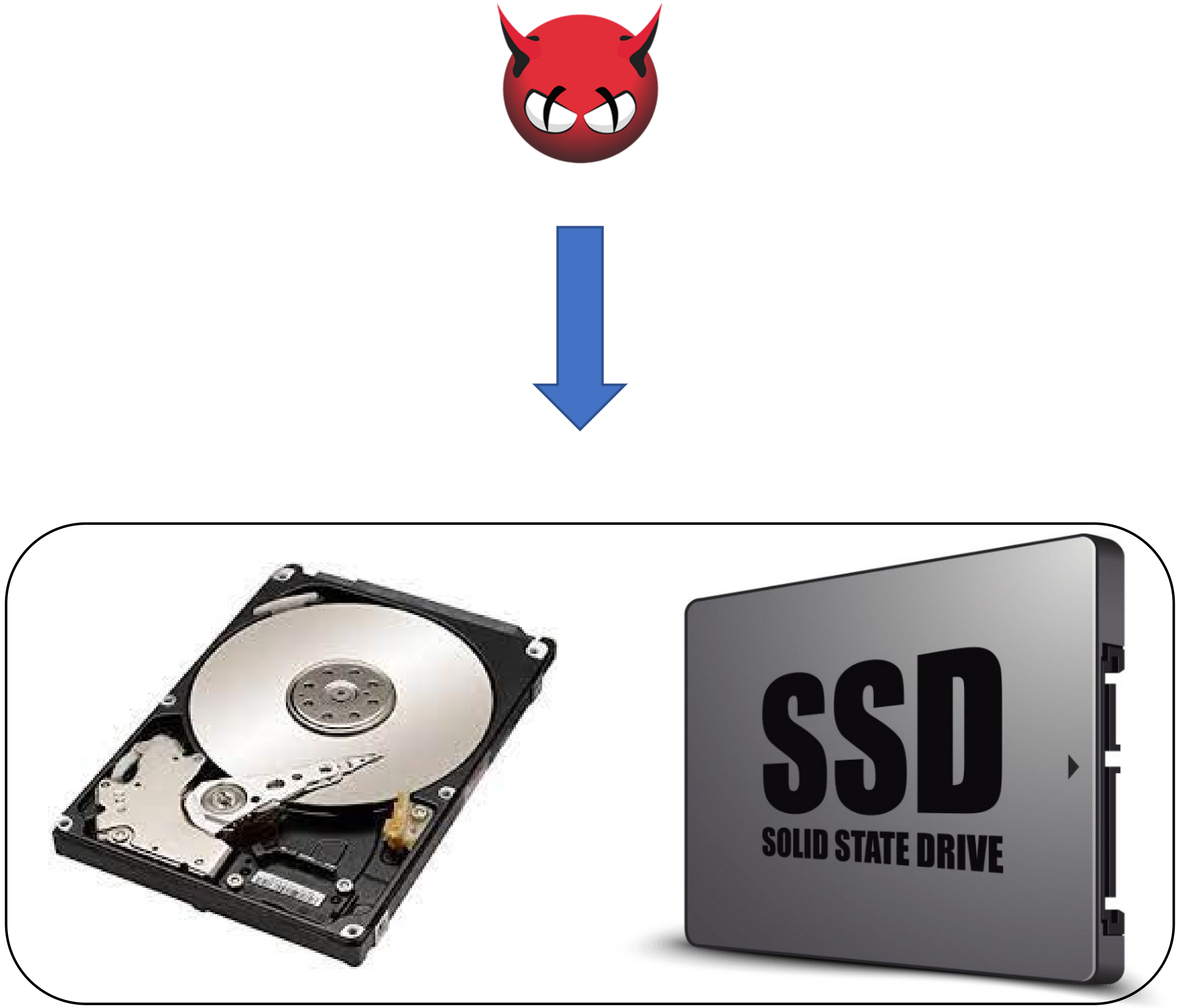
Past storage states can be retained for recovery!

Ransomware will Evolve

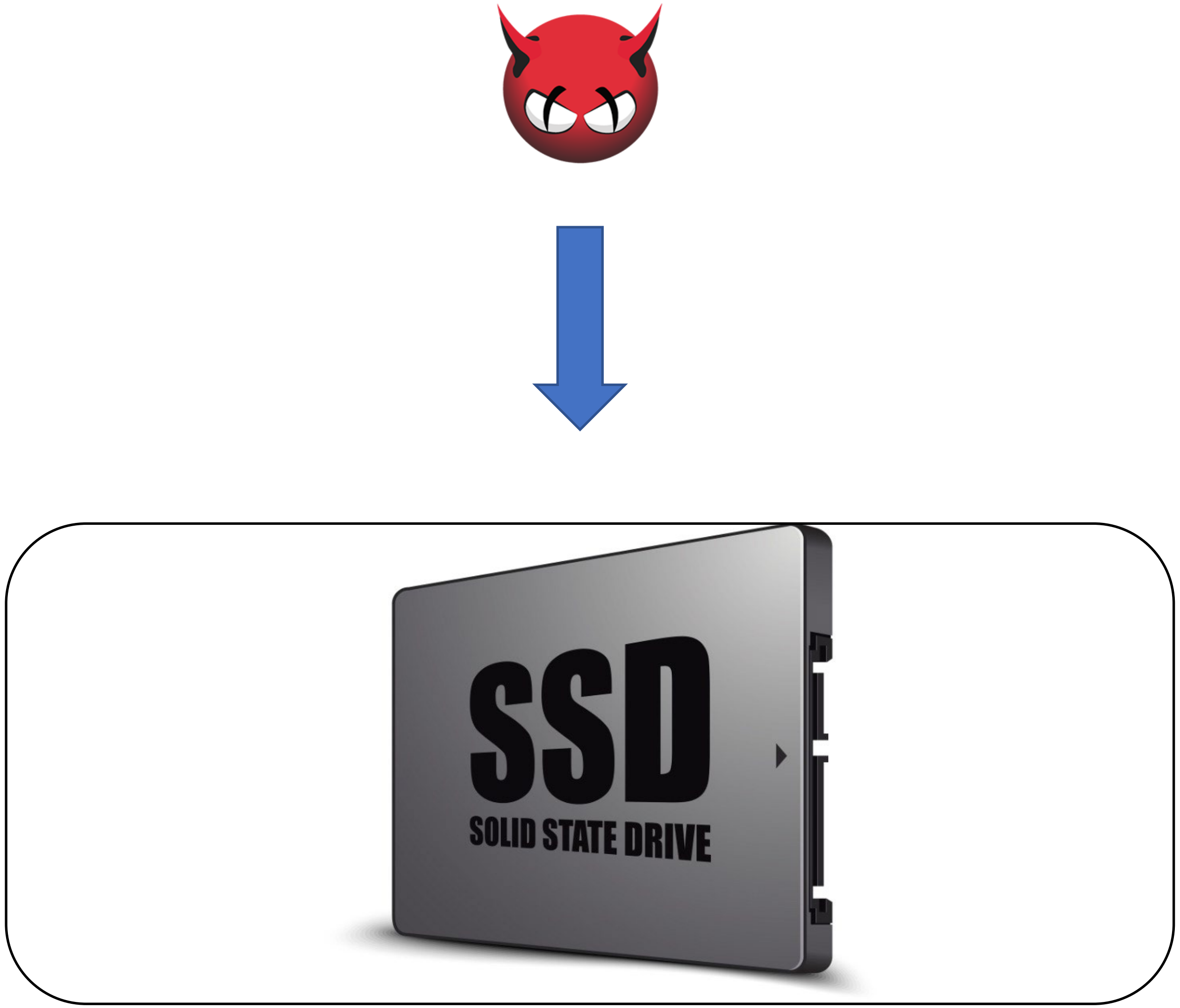


Block I/O Device

Ransomware will Evolve

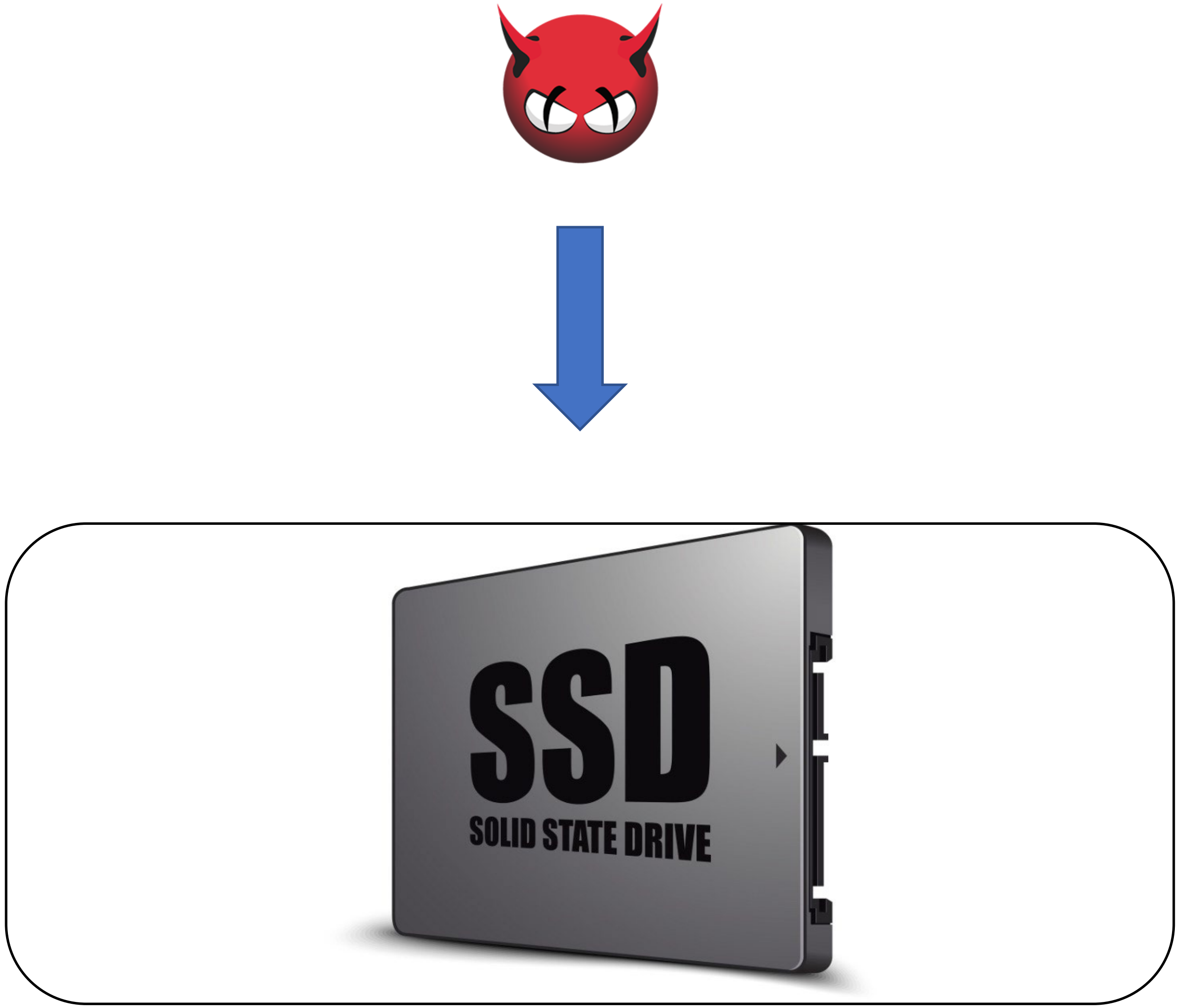


Ransomware will Evolve



SSDs are becoming increasingly popular

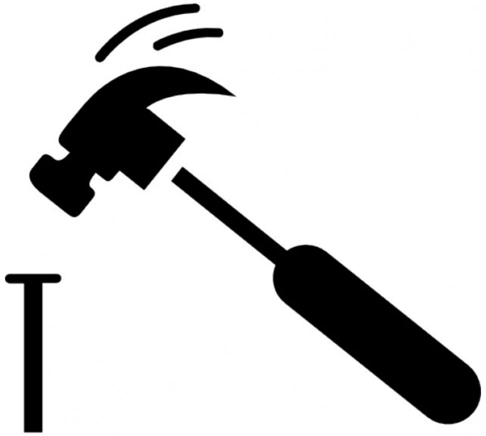
Ransomware will Evolve



SSDs are becoming increasingly popular

Adapting to SSDs requires few changes

Ransomware Evolution: Ransomware 2.0



GC Attack

Dump large amounts of data to SSD to trigger GC!

Ransomware Evolution: Ransomware 2.0

GC Attack

Timing Attack

Waits until data is removed by default GC!

Ransomware Evolution: Ransomware 2.0

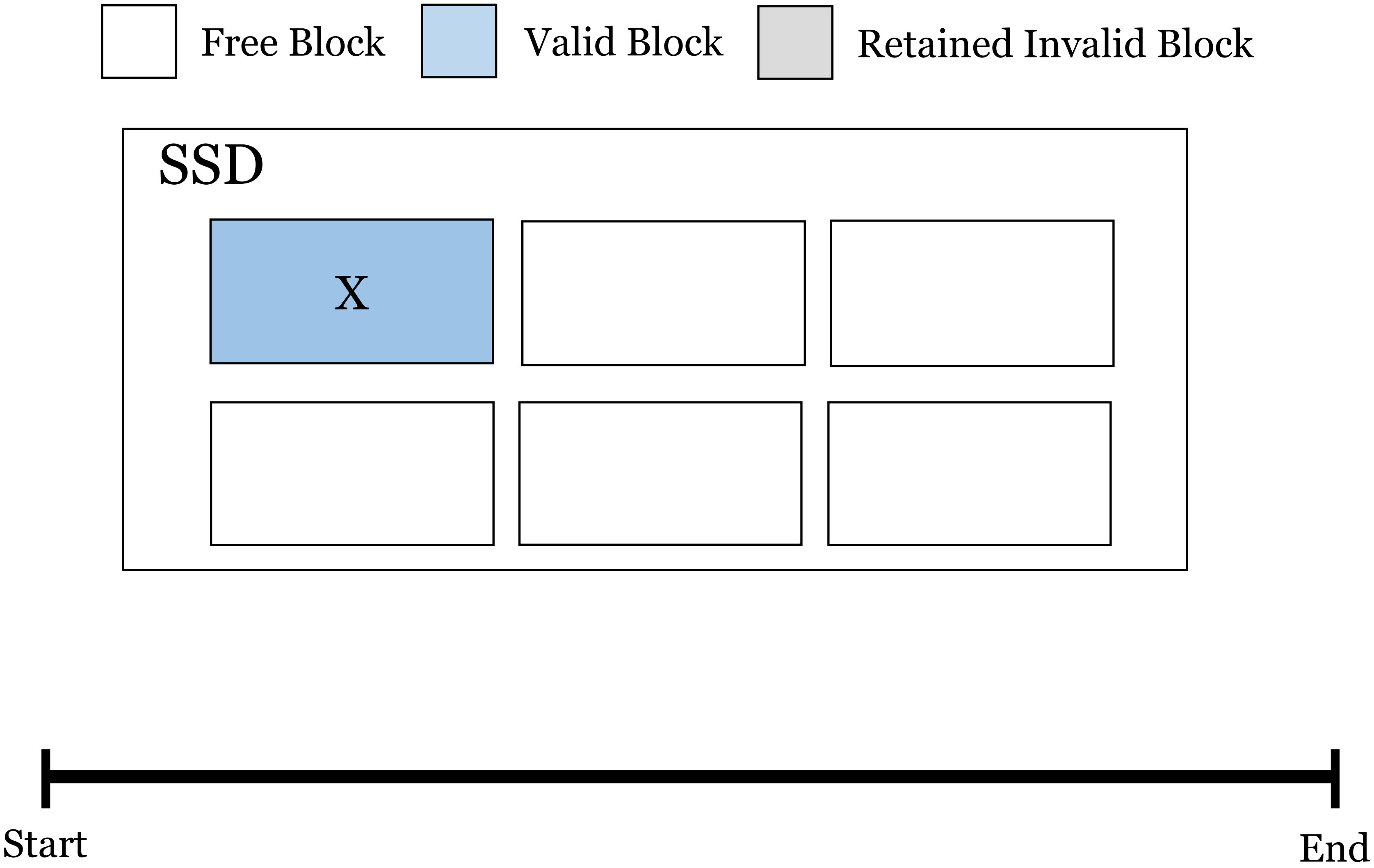
GC Attack

Timing Attack

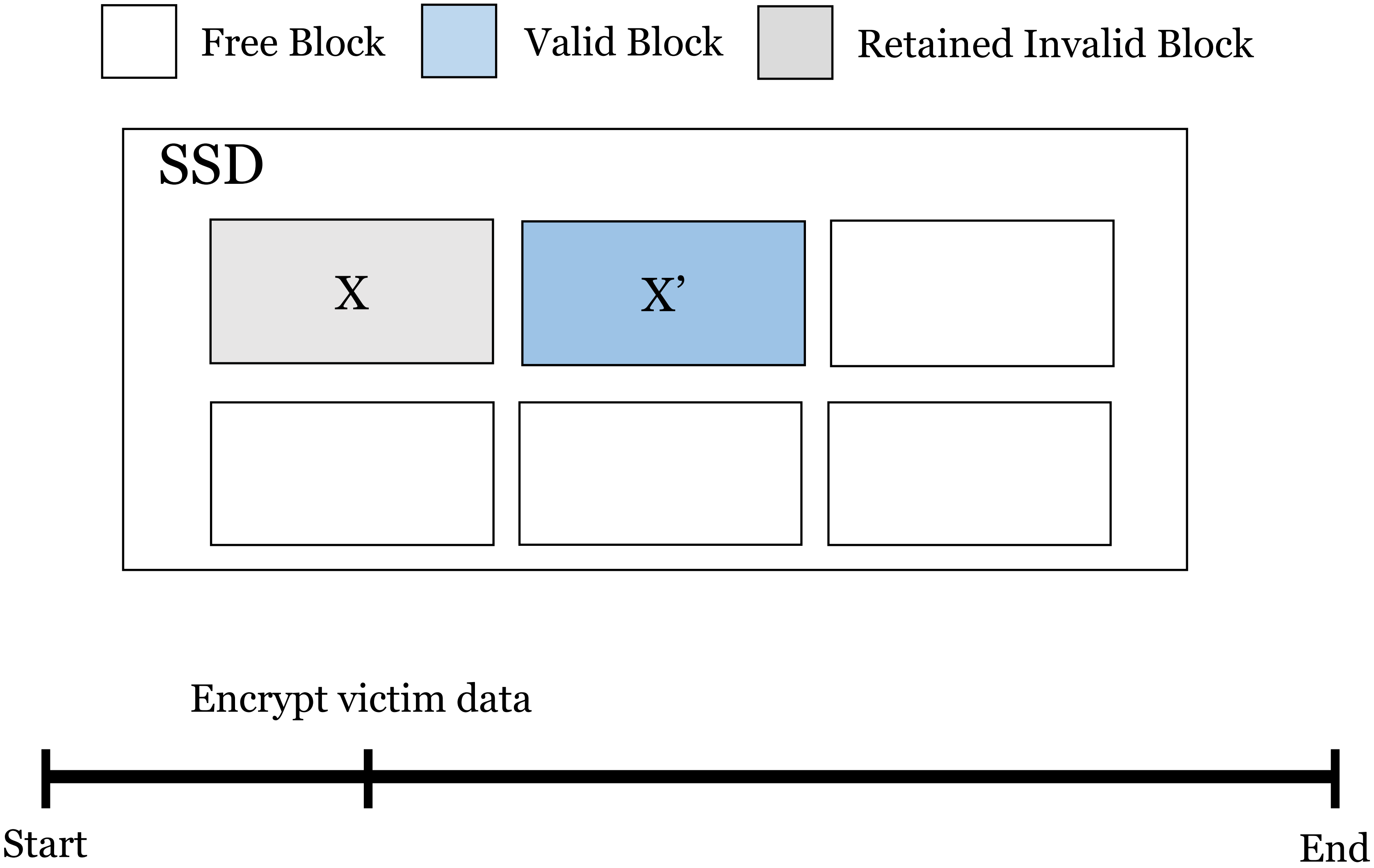
Trim Attack

Use trim command to directly remove data!

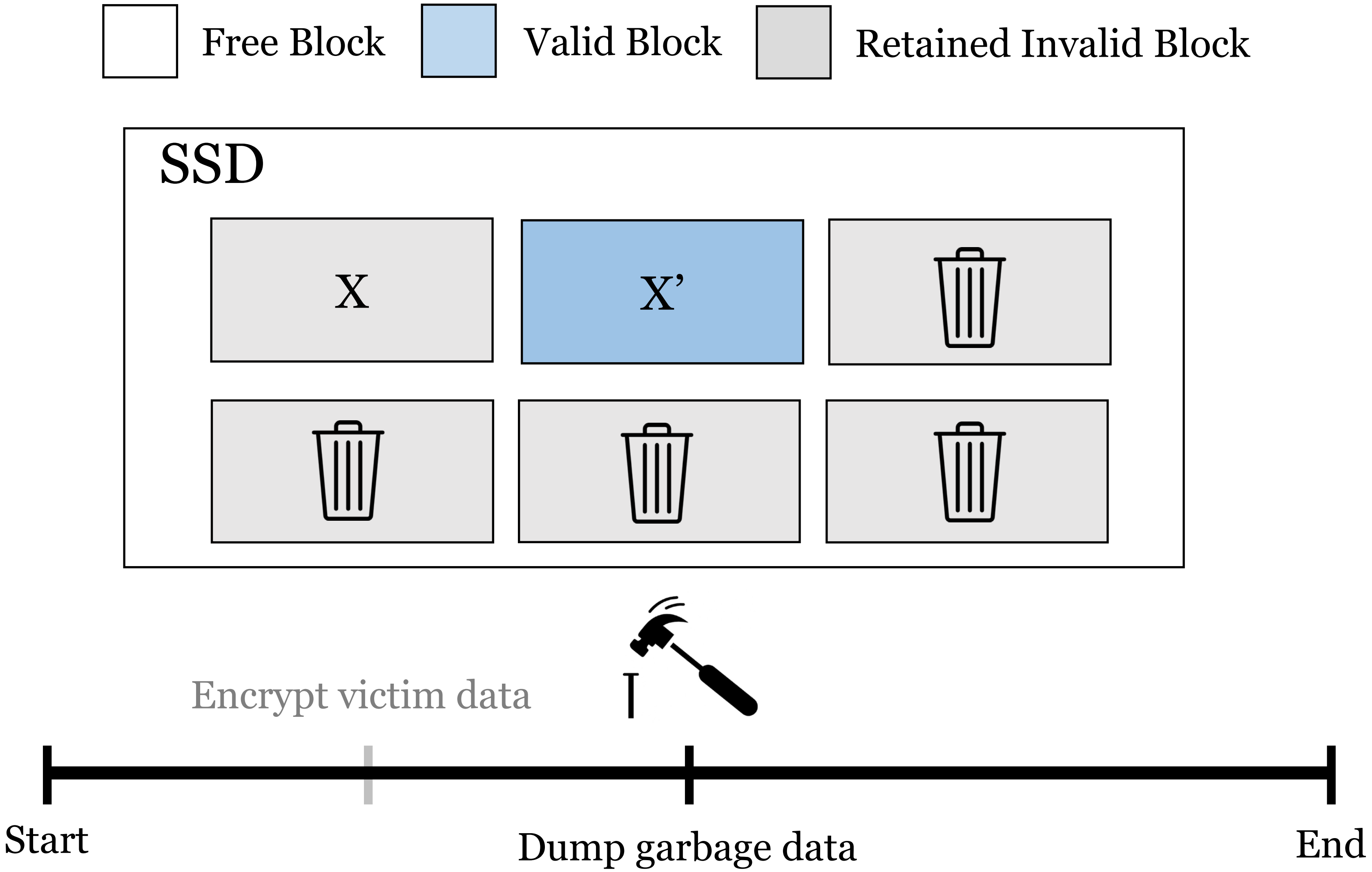
Ransomware 2.0: GC Attack



Ransomware 2.0: GC Attack



Ransomware 2.0: GC Attack



□ Free Block

▨ Valid Block

▨ Retained Invalid Block

SSD

X

X’

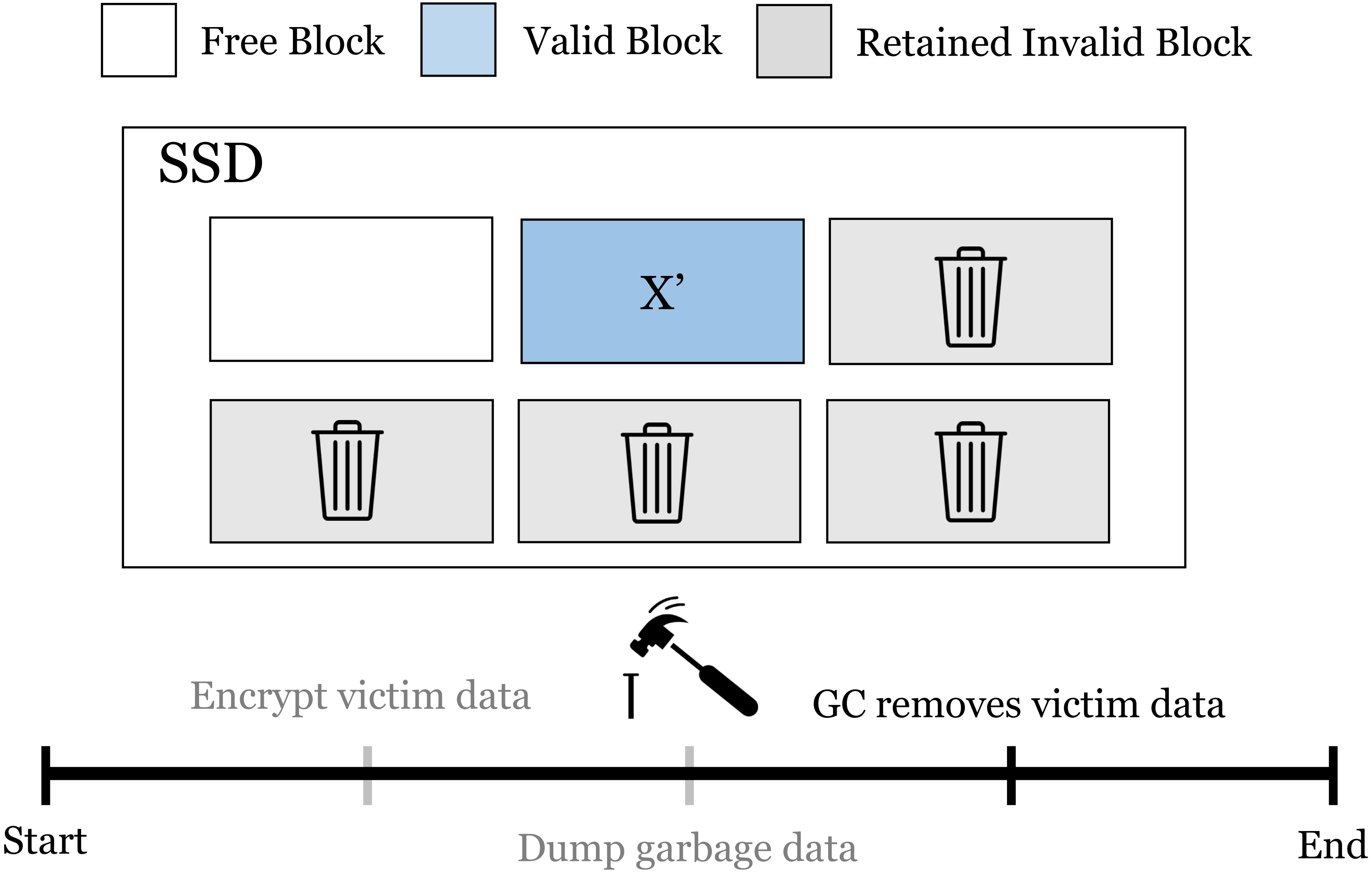
Encrypt victim data

Start

Dump garbage data

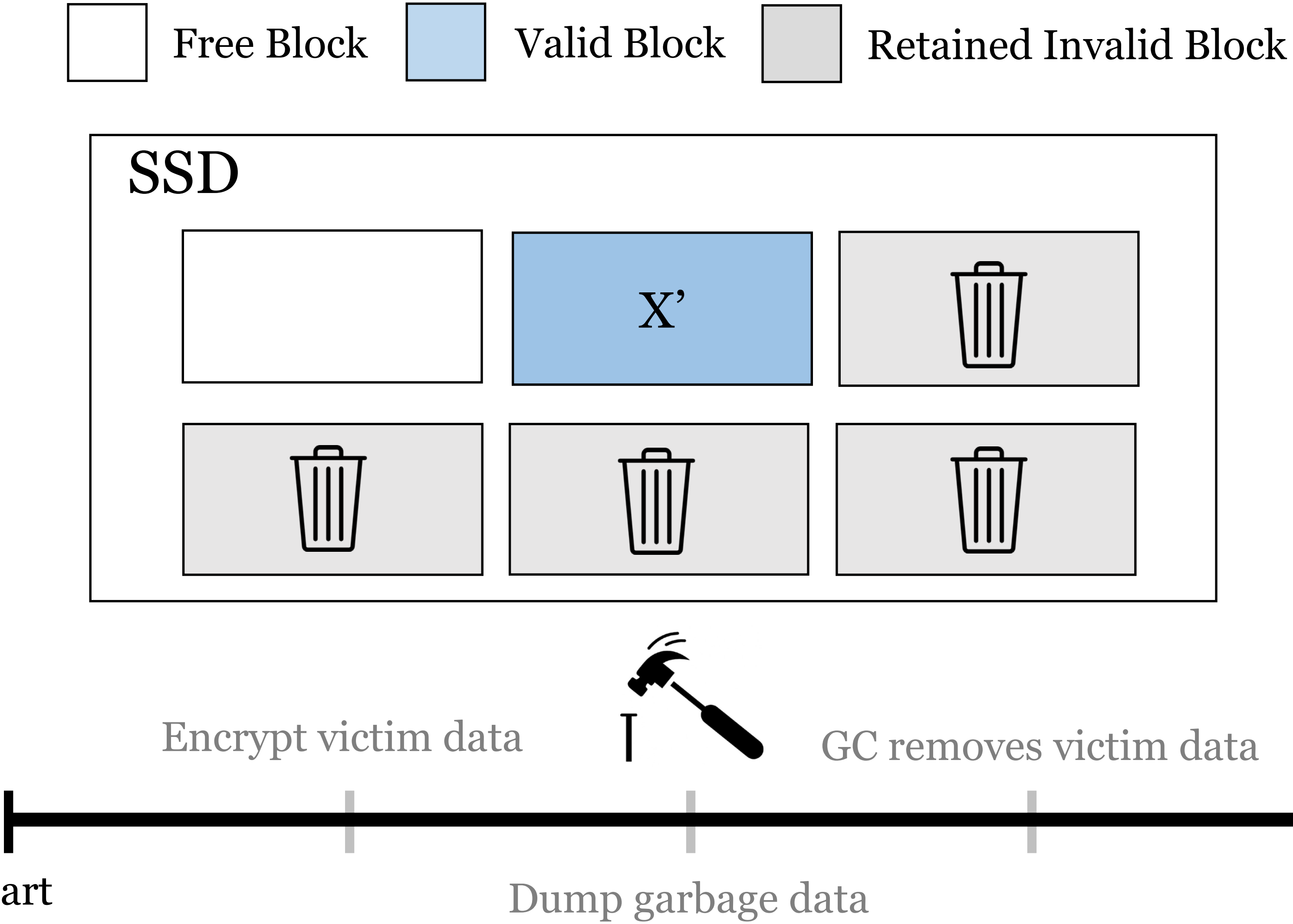
End

Ransomware 2.0: GC Attack



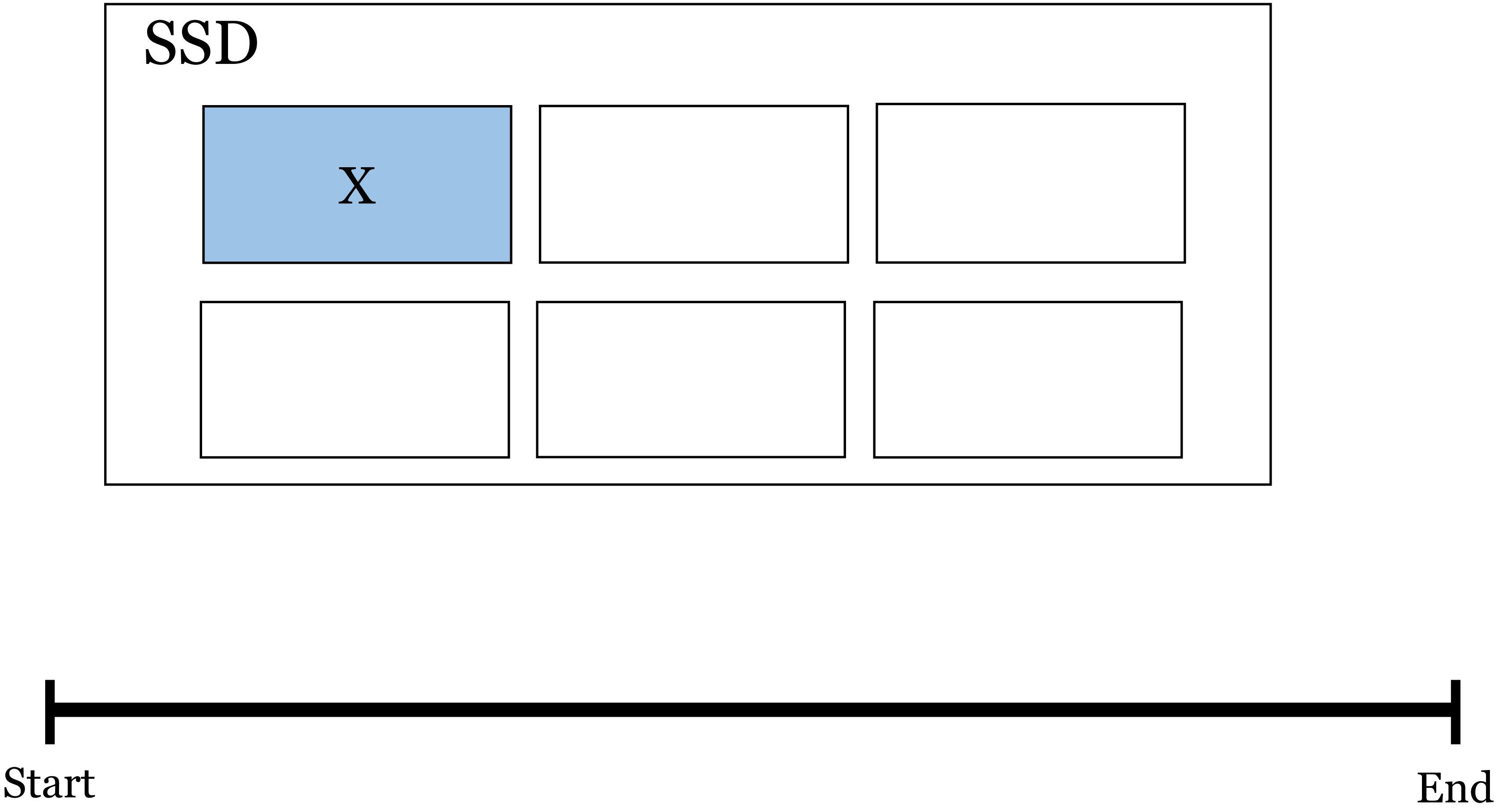
Ransomware 2.0: GC Attack

□ Free Block ▨ Valid Block ▨ Retained Invalid Block

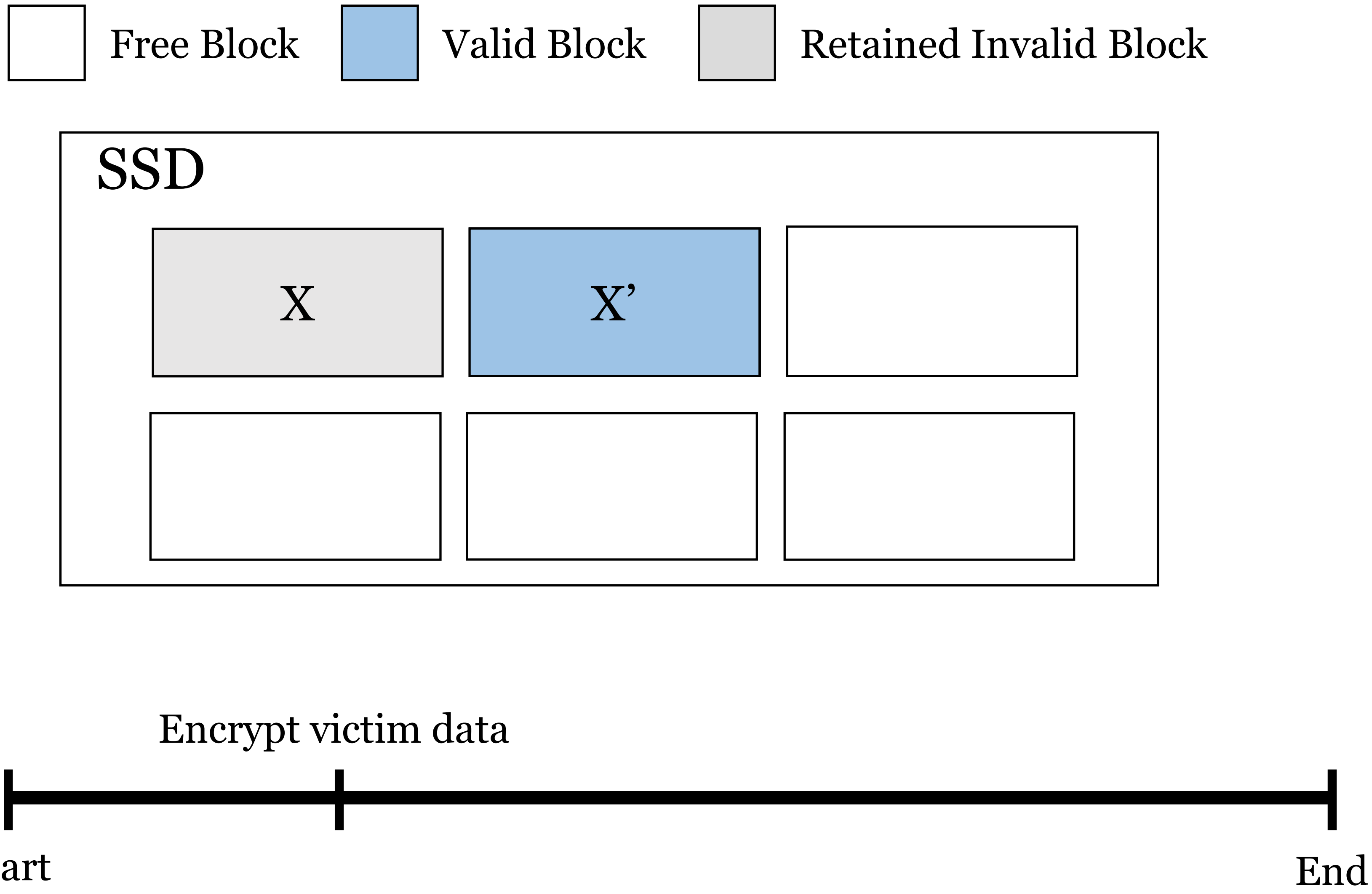


Ransomware 2.0: Timing Attack

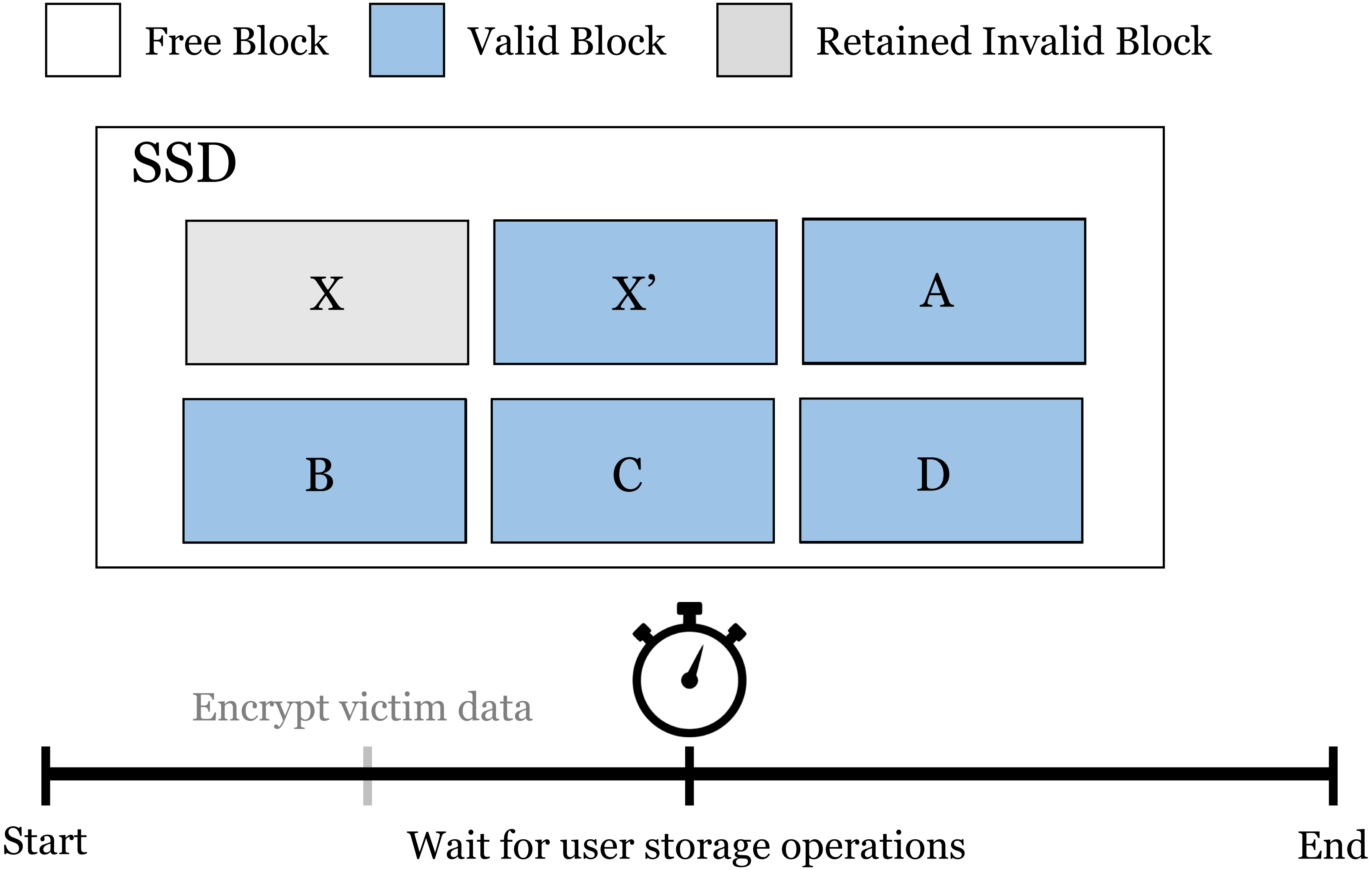
□ Free Block 🟦 Valid Block ▨ Retained Invalid Block



Ransomware 2.0: Timing Attack



Ransomware 2.0: Timing Attack



□ Free Block

🟦 Valid Block

▨ Retained Invalid Block

SSD

X

X’

A

B

C

D

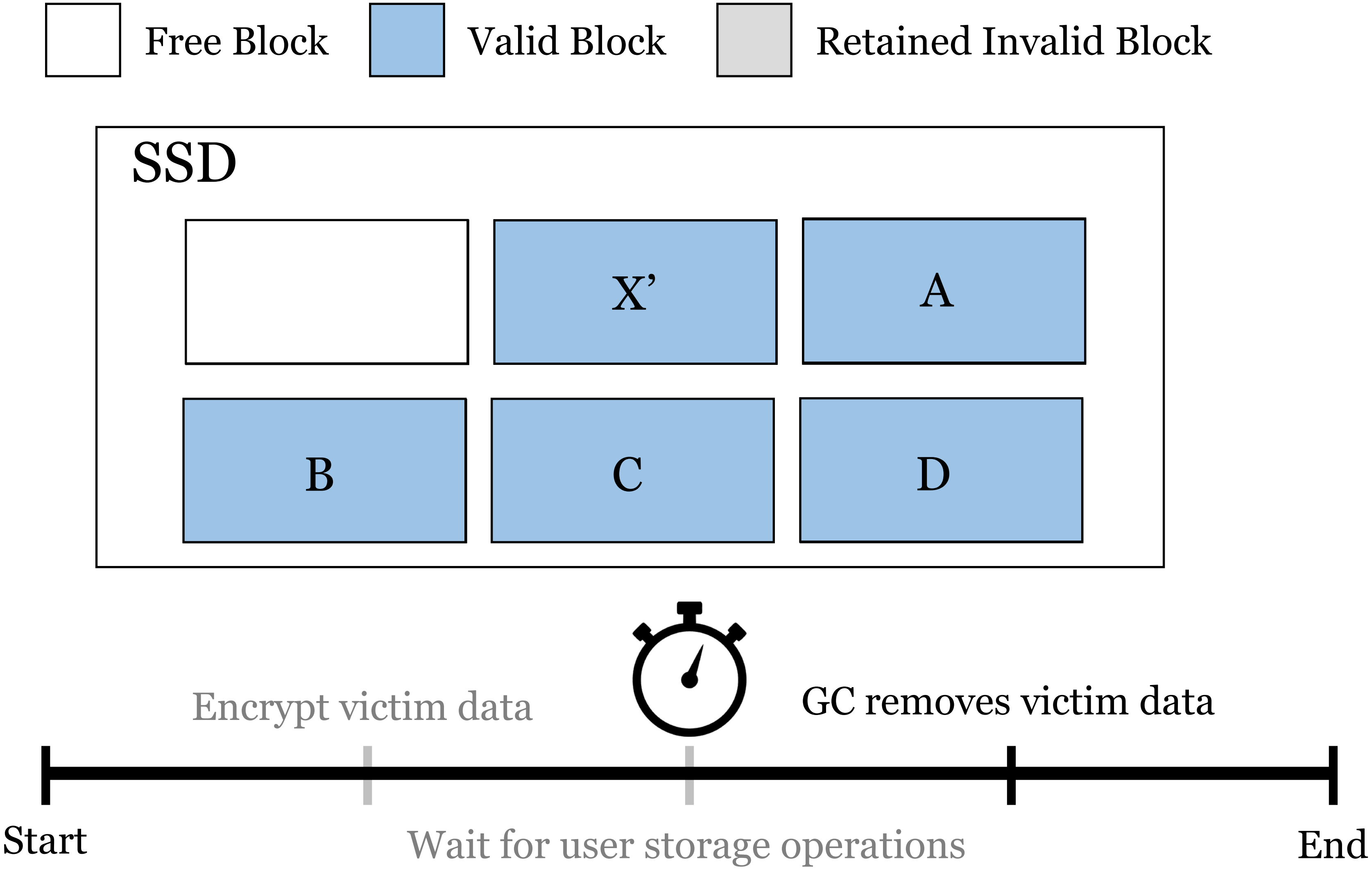
Encrypt victim data

Start

Wait for user storage operations

End

Ransomware 2.0: Timing Attack



□ Free Block

🟦 Valid Block

⬜ Retained Invalid Block

SSD

X’

A

B

C

D

Encrypt victim data

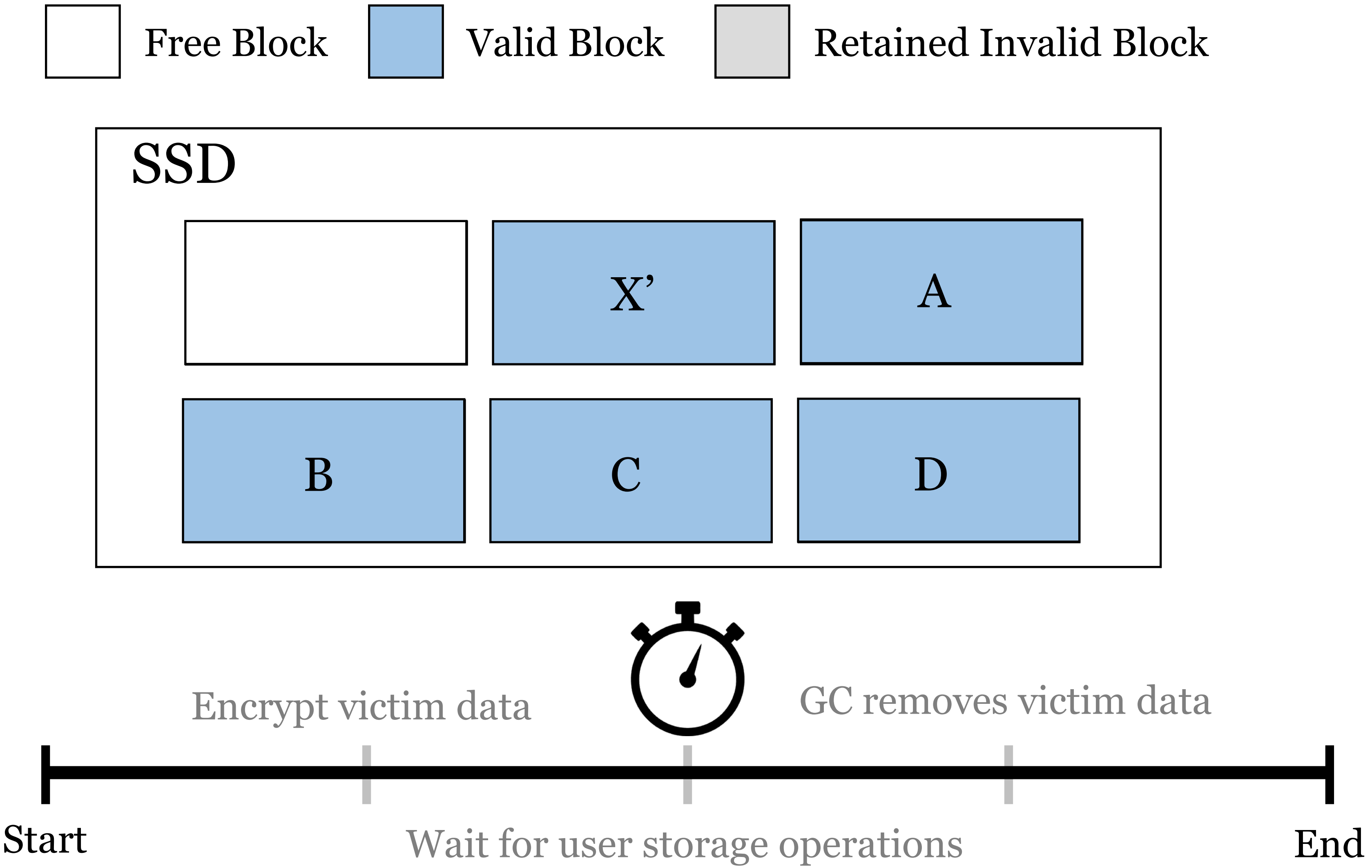
GC removes victim data

Start

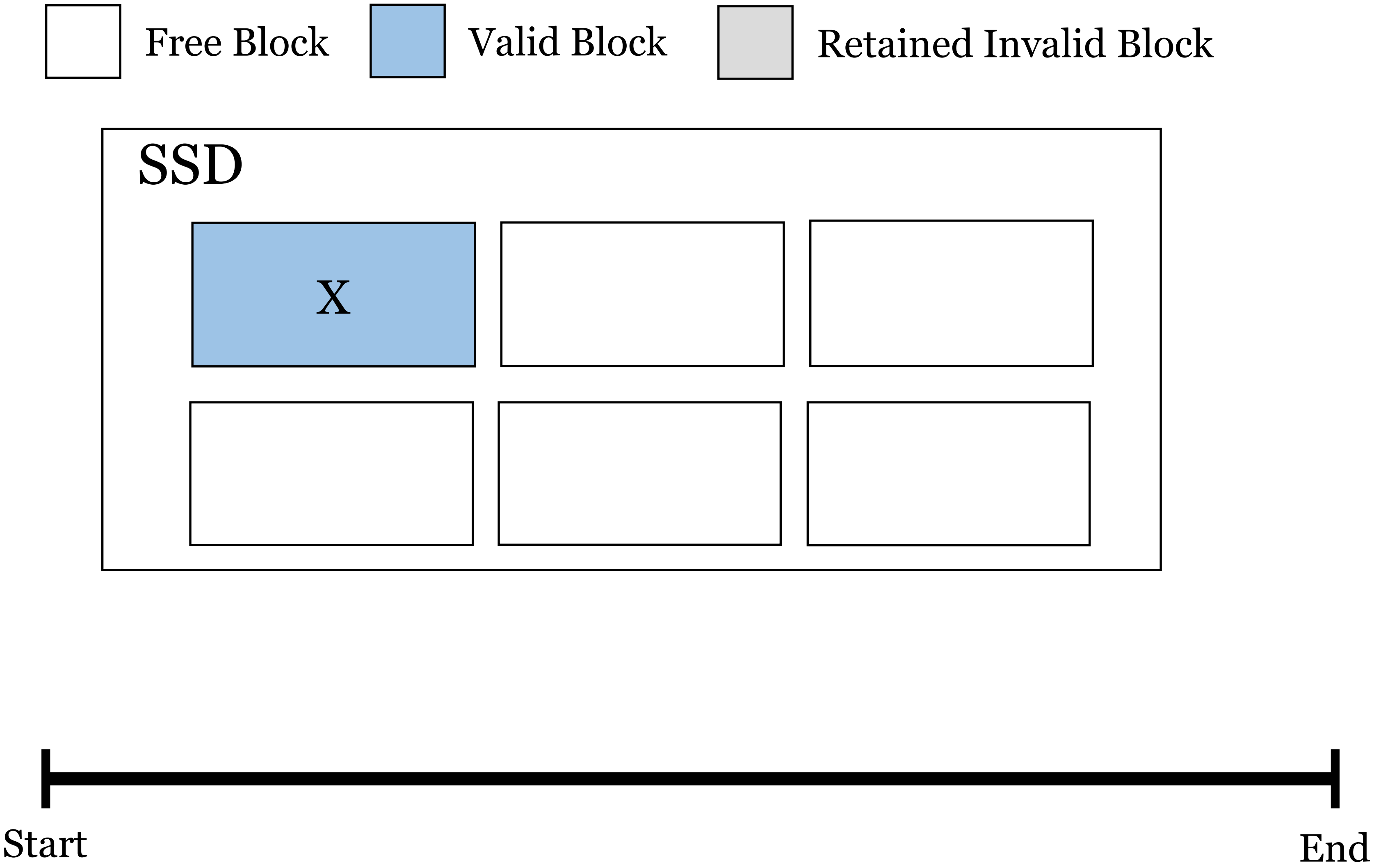
Wait for user storage operations

End

Ransomware 2.0: Timing Attack



Ransomware 2.0: Trim Attack

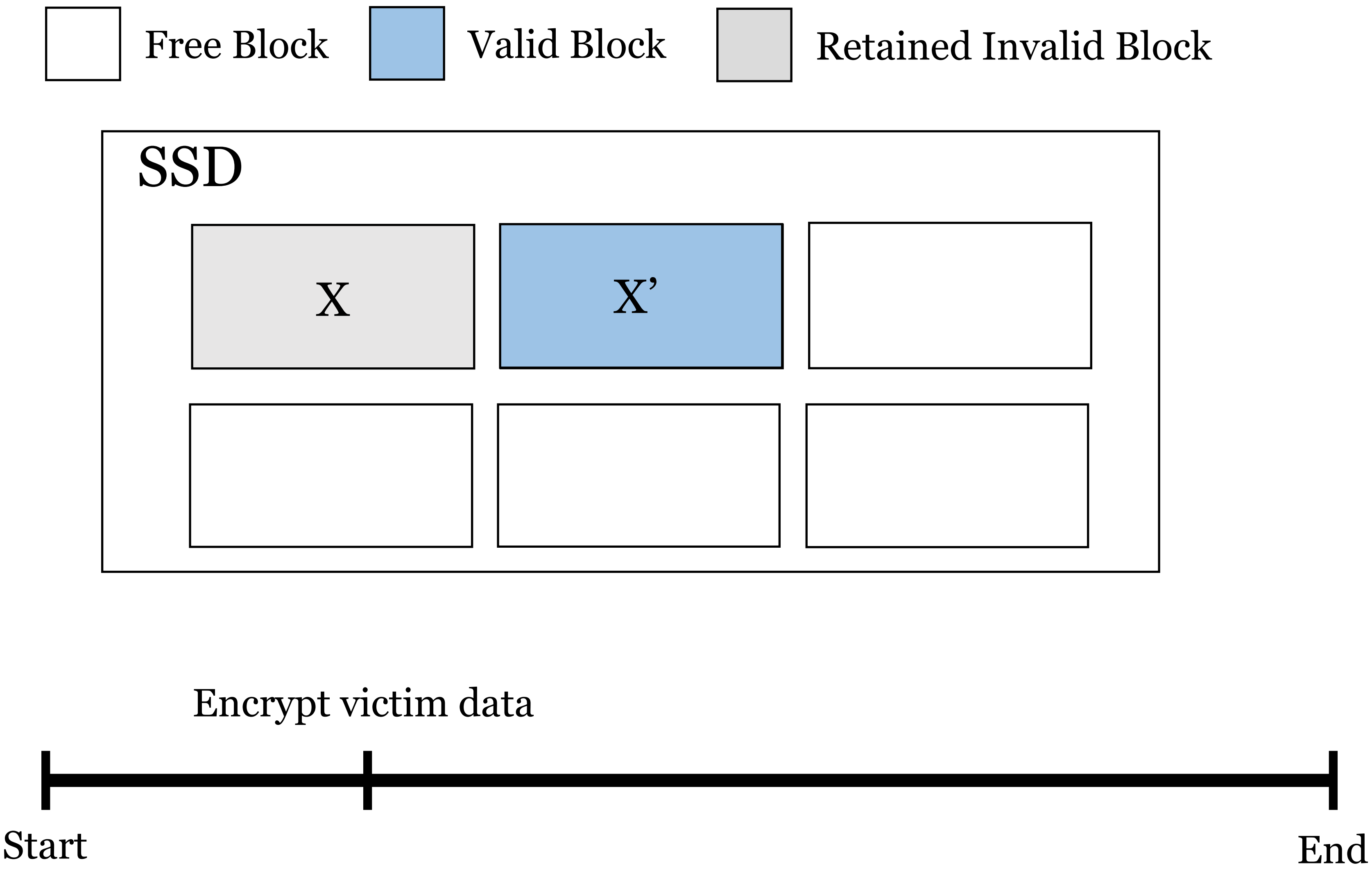


□ Free Block

▨ Valid Block

▨ Retained Invalid Block

Ransomware 2.0: Trim Attack



□ Free Block

🟦 Valid Block

▨ Retained Invalid Block

SSD

X

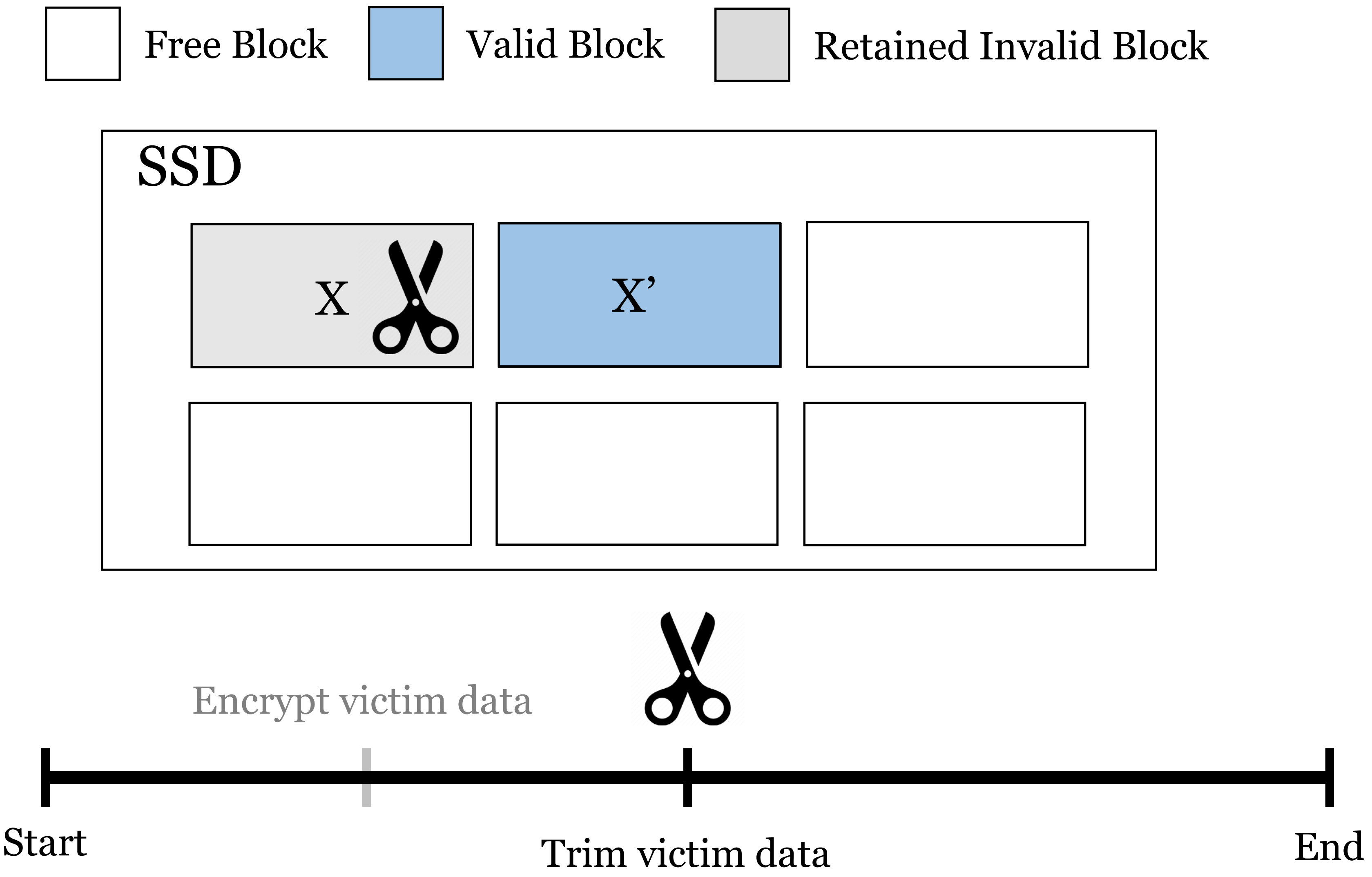
X’

Encrypt victim data

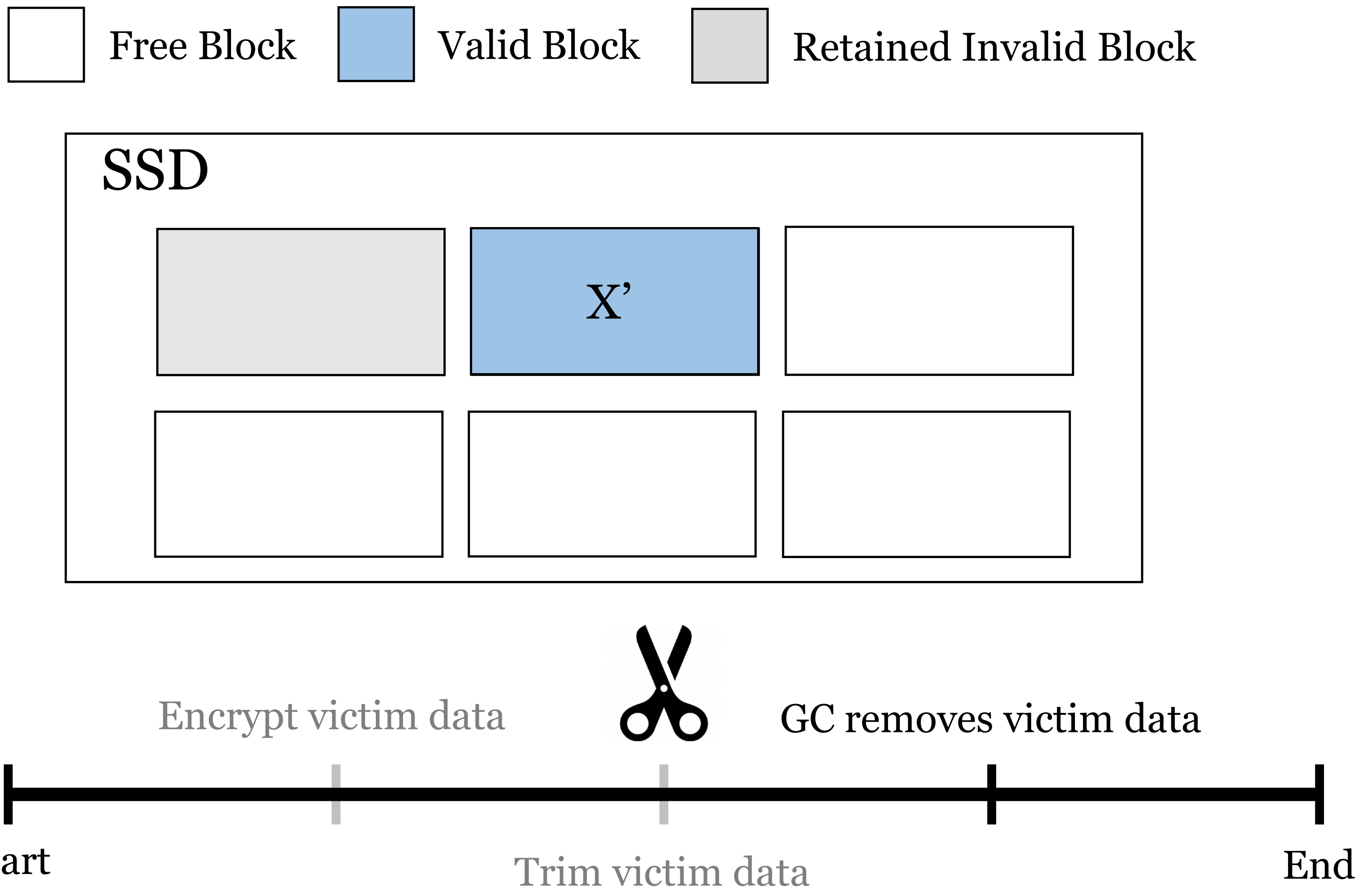
Start

End

Ransomware 2.0: Trim Attack



Ransomware 2.0: Trim Attack



☐ Free Block 🟦 Valid Block ⬜ Retained Invalid Block

SSD

X’

Encrypt victim data

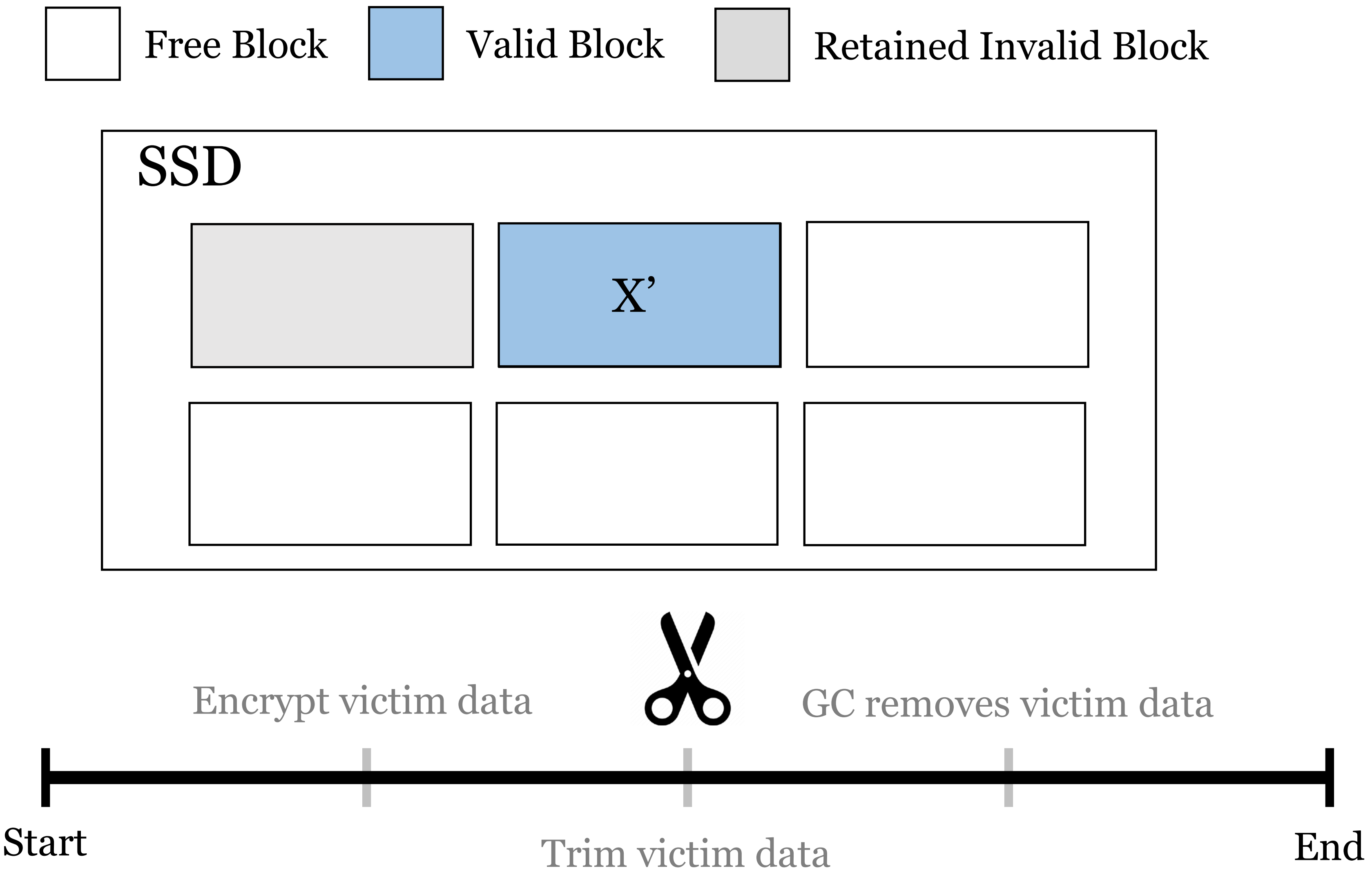
GC removes victim data

Start

Trim victim data

End

Ransomware 2.0: Trim Attack



□ Free Block

🟦 Valid Block

⬜ Retained Invalid Block

SSD

X’

Encrypt victim data

GC removes victim data

Start

Trim victim data

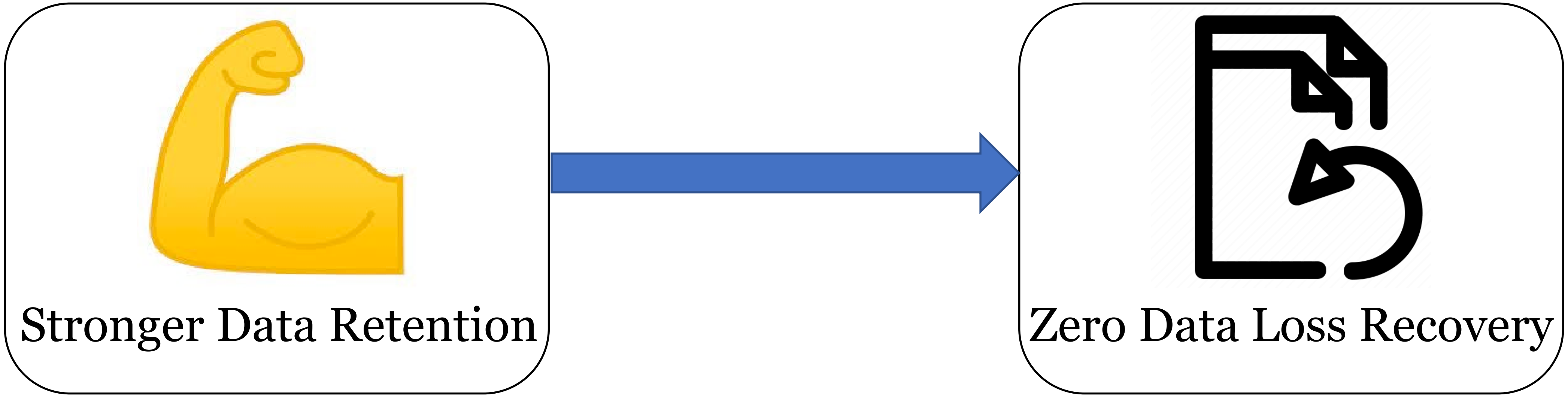
End

Ransomware 2.0 Requires a Fundamental Solution

💪

Stronger Data Retention

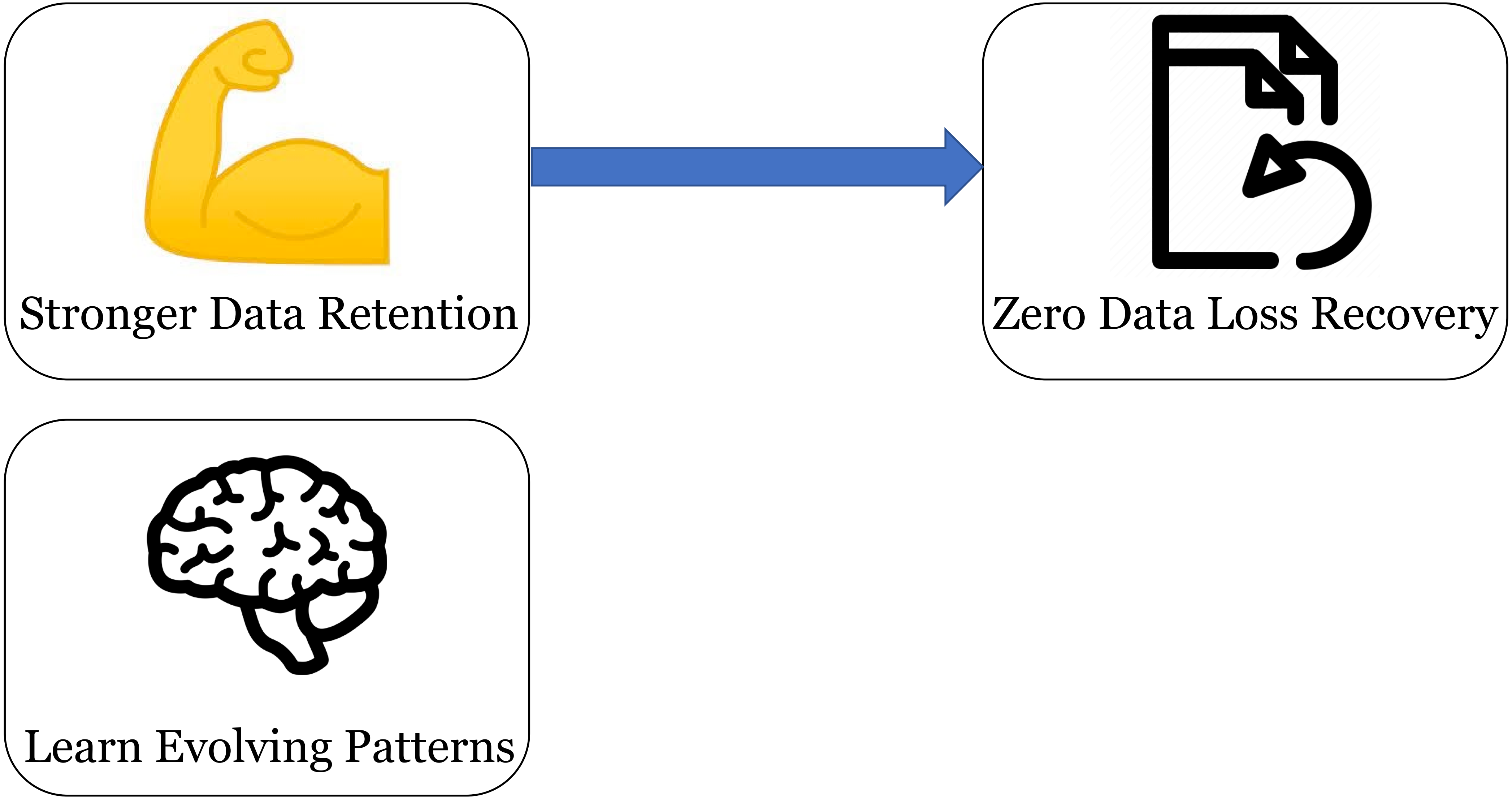
Ransomware 2.0 Requires a Fundamental Solution



Stronger Data Retention

Zero Data Loss Recovery

Ransomware 2.0 Requires a Fundamental Solution

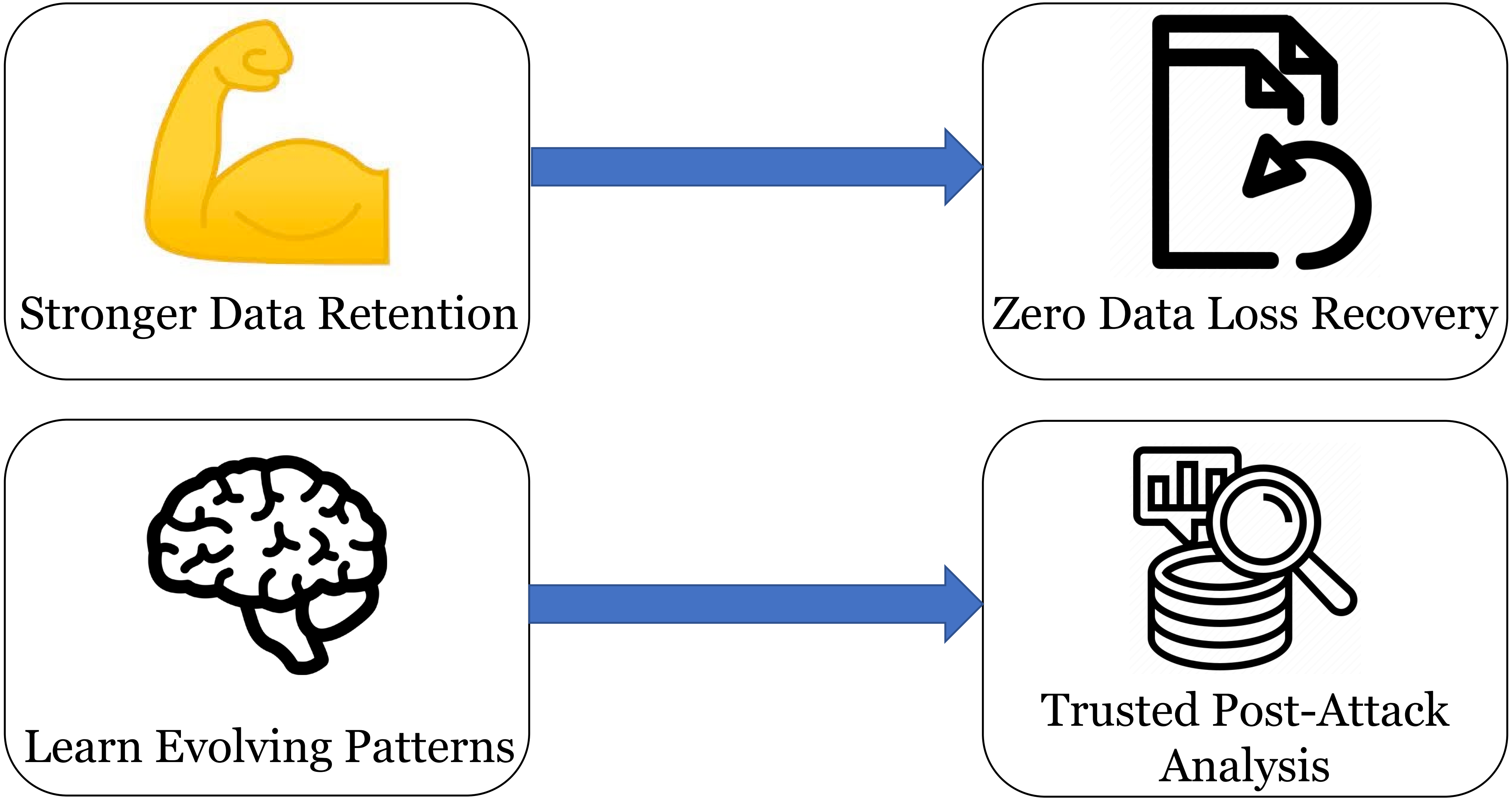


Stronger Data Retention

Zero Data Loss Recovery

Learn Evolving Patterns

Ransomware 2.0 Requires a Fundamental Solution



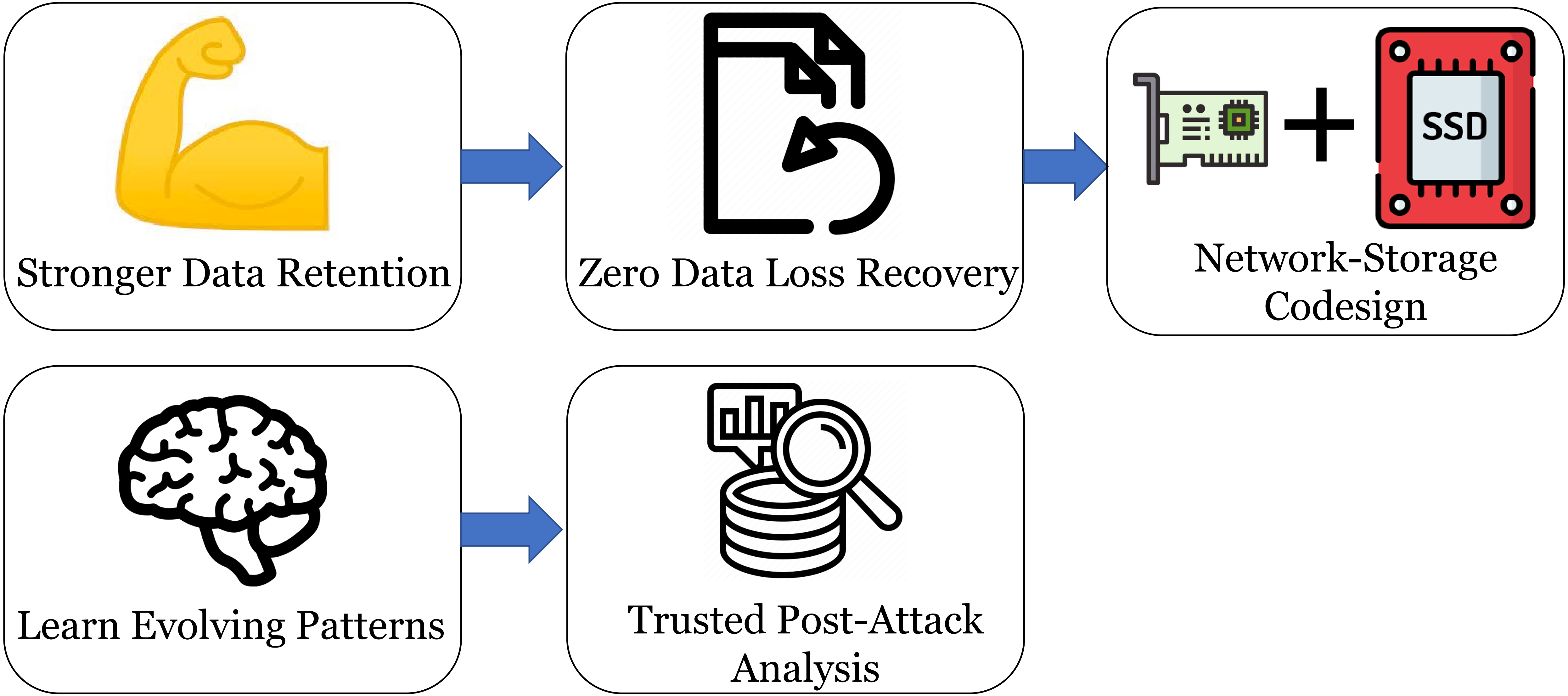
Stronger Data Retention

Zero Data Loss Recovery

Learn Evolving Patterns

Trusted Post-Attack Analysis

RSSD: Hardware-Isolated Network-Storage Codesign



Stronger Data Retention

Zero Data Loss Recovery

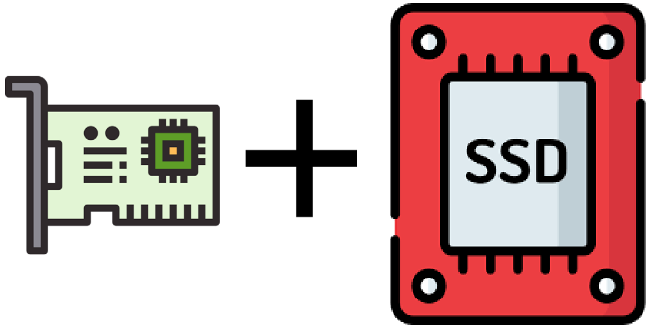
Network-Storage Codesign

Learn Evolving Patterns

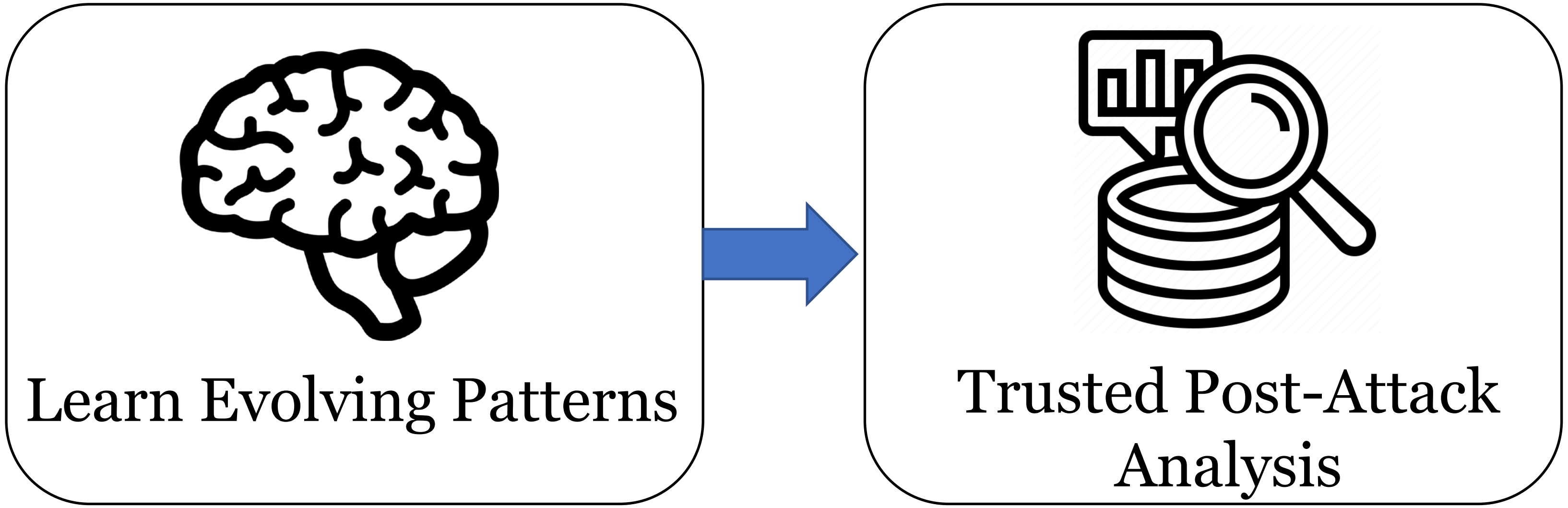
Trusted Post-Attack Analysis

RSSD: Hardware-Isolated Network-Storage Codesign

Transparently offload retained data to remote servers!



Network-Storage Codesign

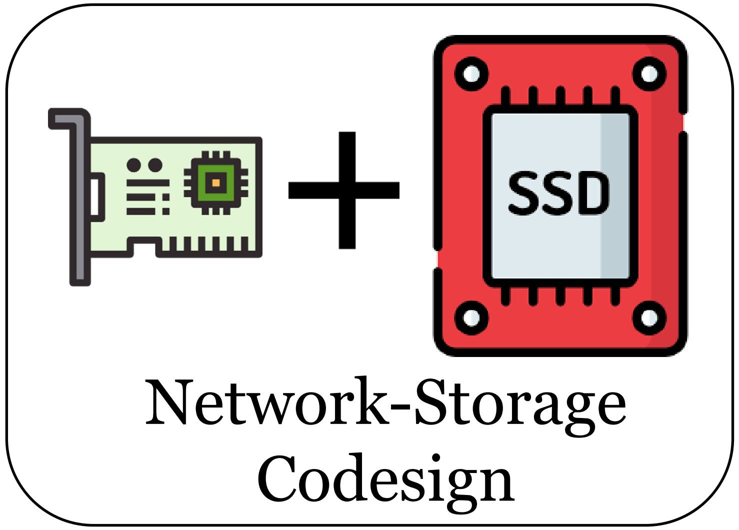


Learn Evolving Patterns

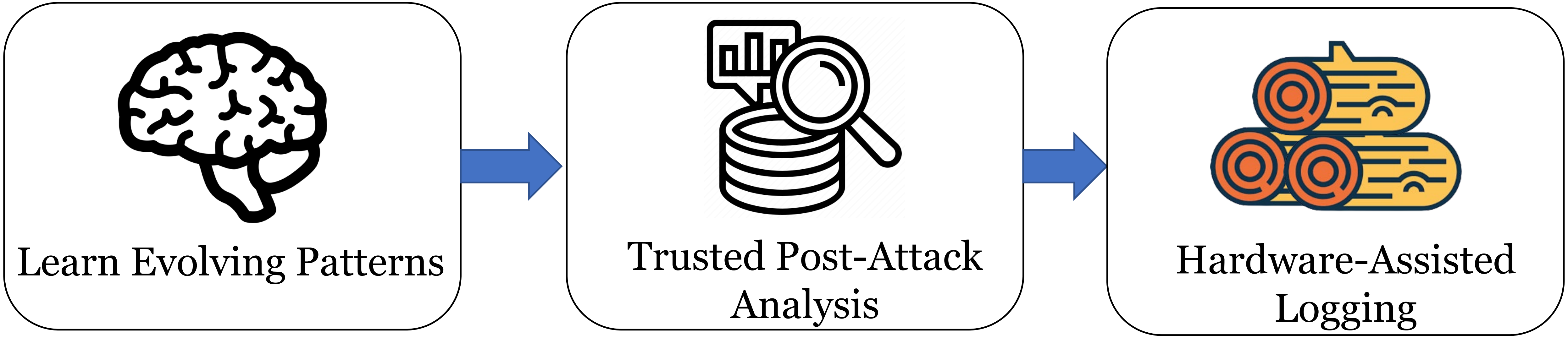
Trusted Post-Attack Analysis

RSSD: Hardware-Isolated Network-Storage Codesign

Transparently offload retained data to remote servers!



Network-Storage Codesign



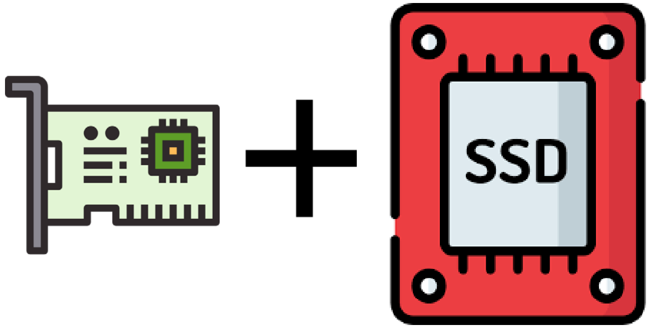
Learn Evolving Patterns

Trusted Post-Attack Analysis

Hardware-Assisted Logging

RSSD: Hardware-Isolated Network-Storage Codesign

Transparently offload retained data to remote servers!

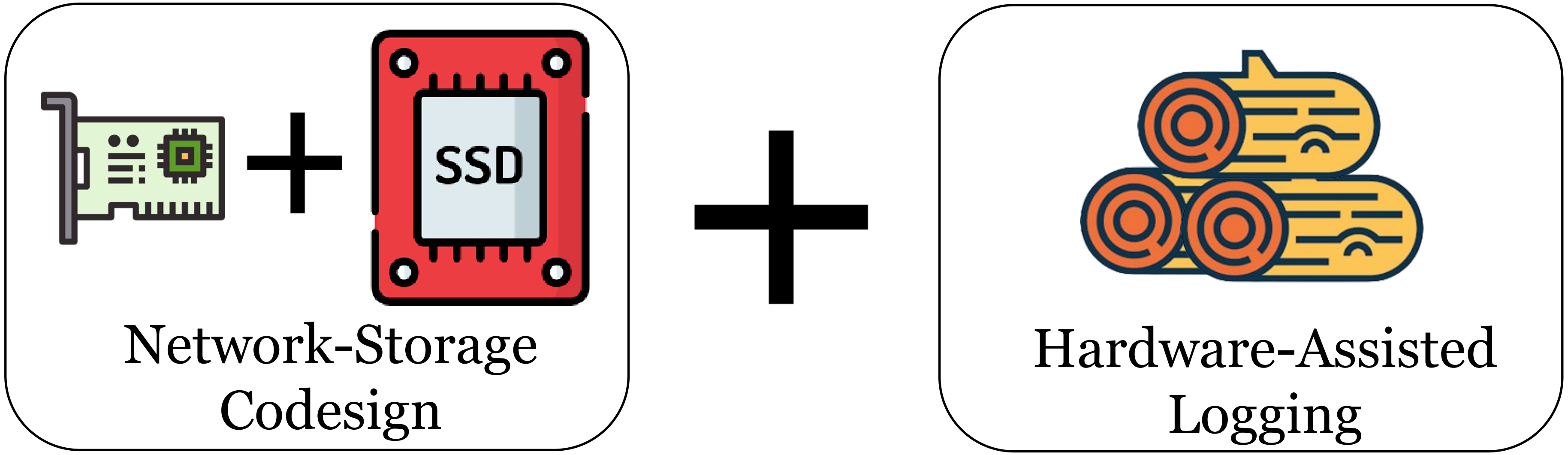


Network-Storage Codesign

Track all operations within the SSD in time order!

Hardware-Assisted Logging

RSSD: Hardware-Isolated Network-Storage Codesign



Network-Storage Codesign

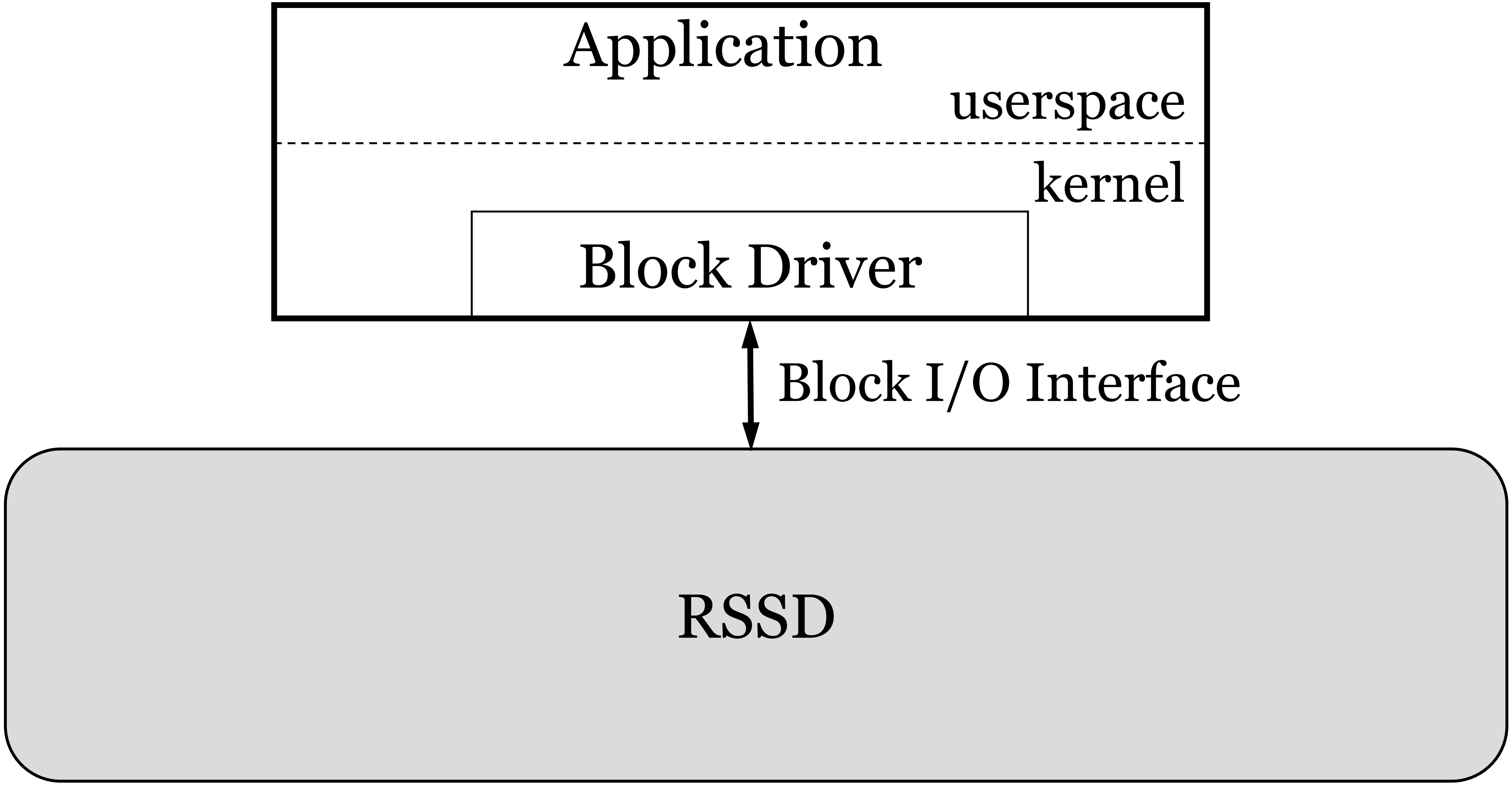
+

Hardware-Assisted Logging

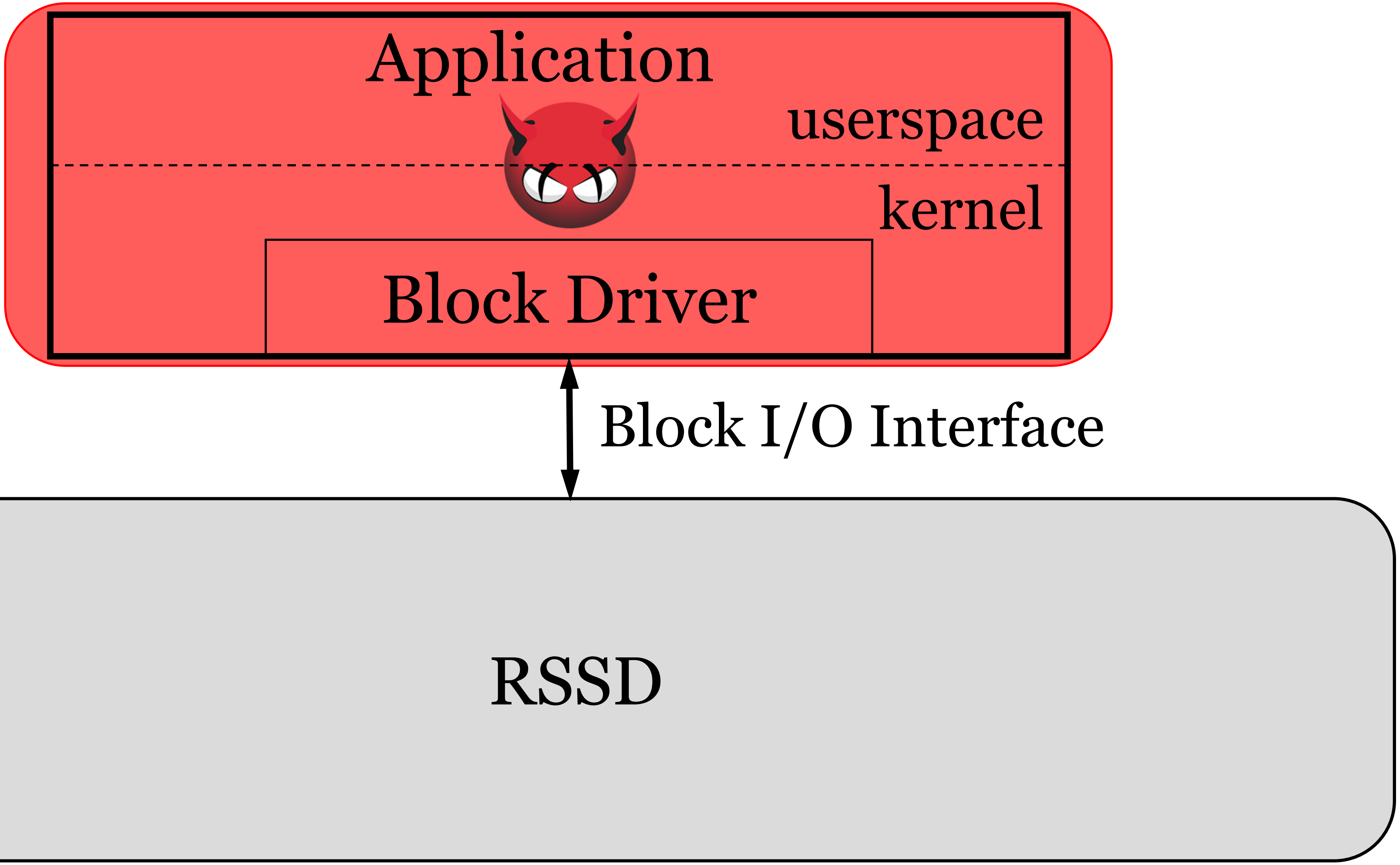
RSSD: Hardware-Isolated Network-Storage Codesign

RSSD

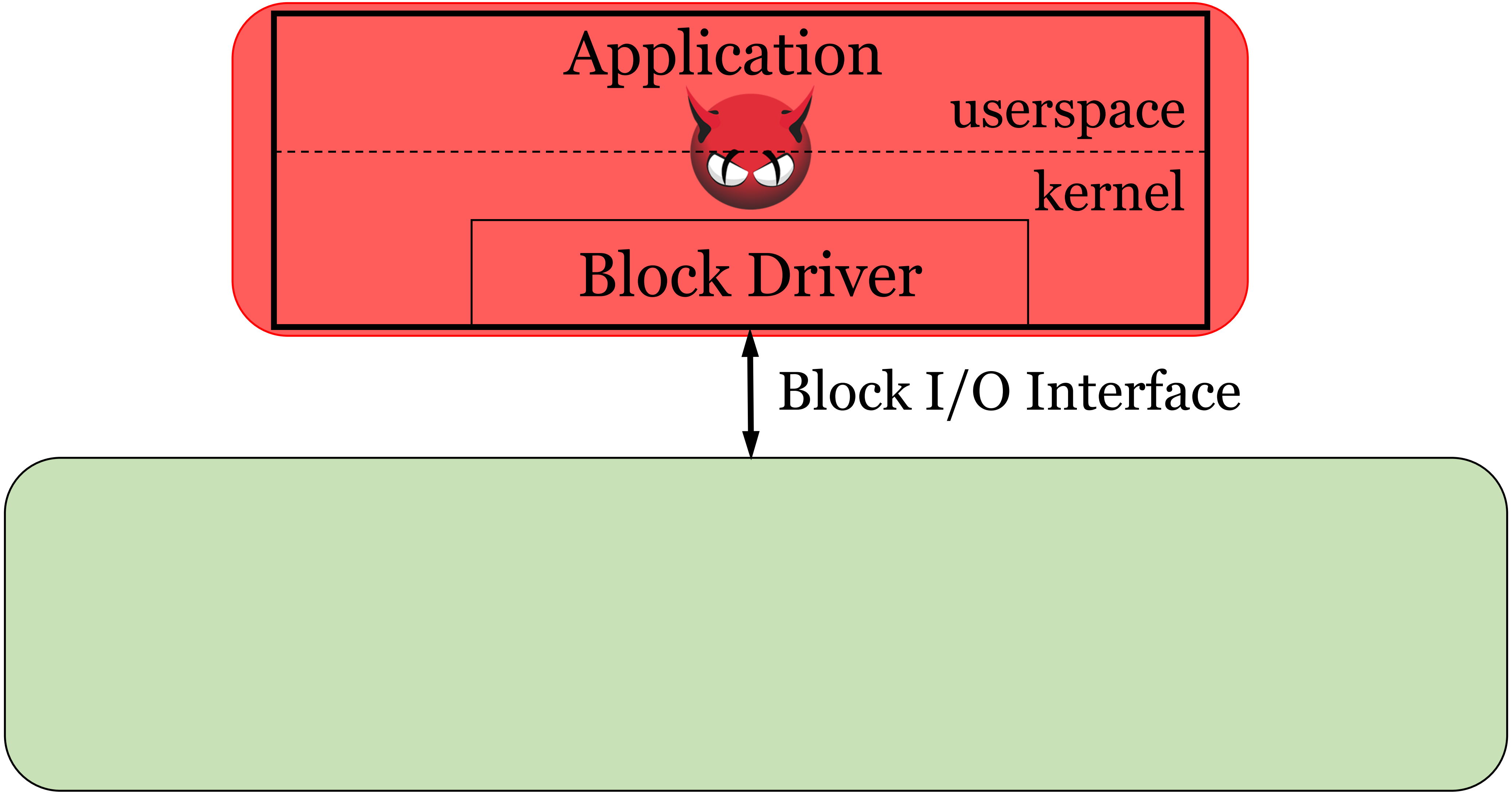
Threat Model for Encryption Ransomware



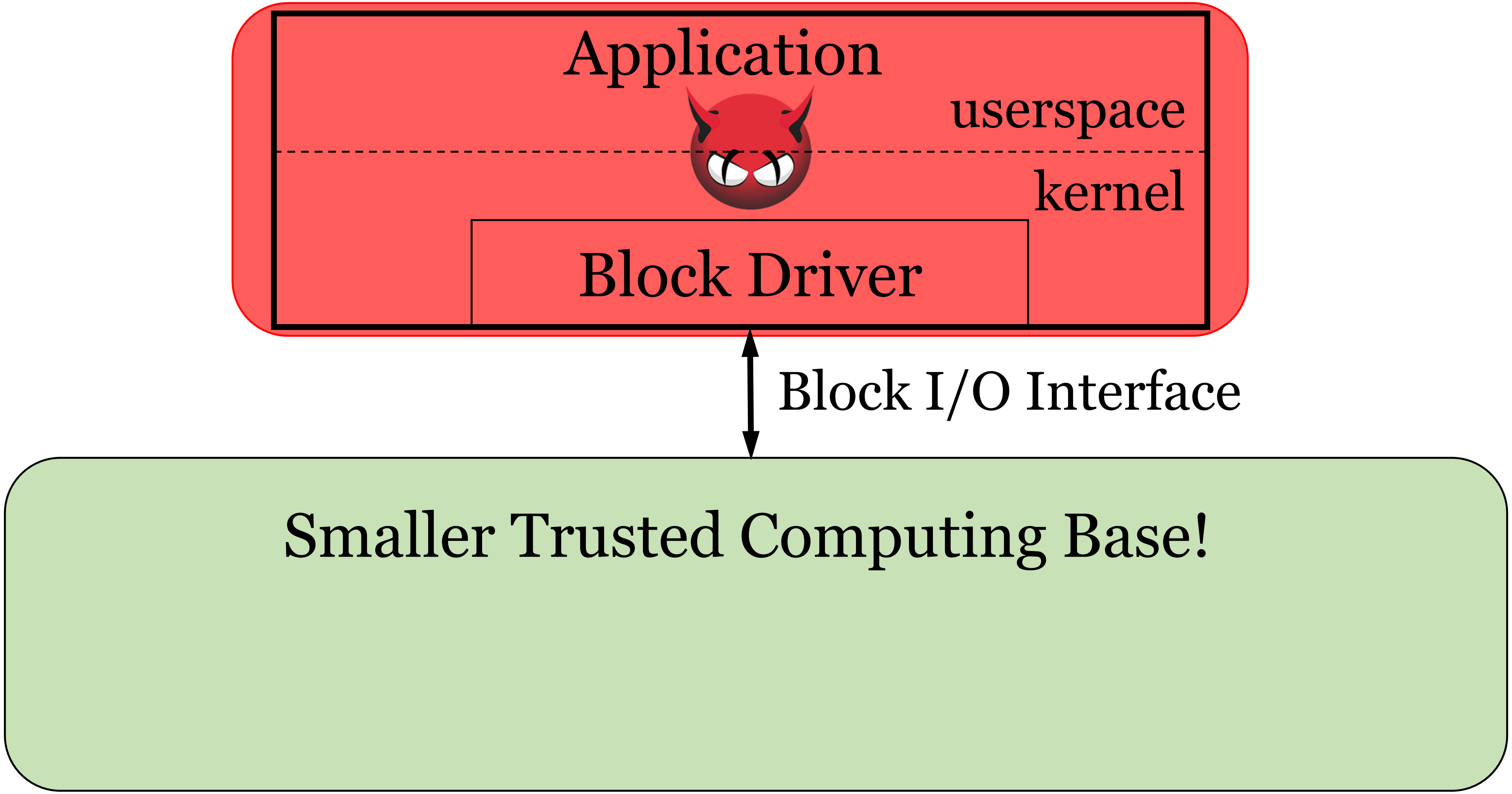
Threat Model for Encryption Ransomware



Threat Model for Encryption Ransomware



Threat Model for Encryption Ransomware



Application

userspace

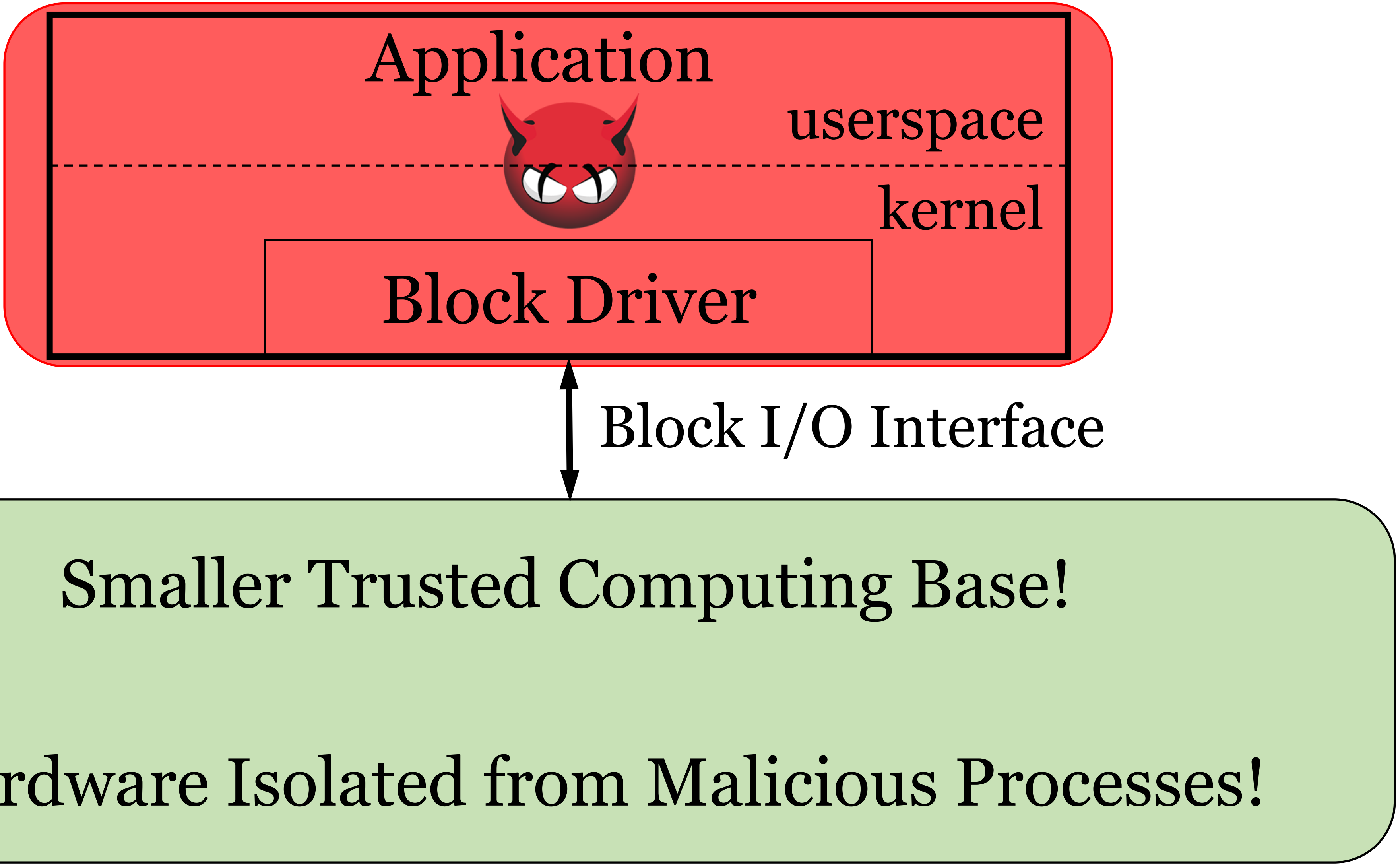
kernel

Block Driver

Block I/O Interface

Smaller Trusted Computing Base!

Threat Model for Encryption Ransomware



Smaller Trusted Computing Base!

Hardware Isolated from Malicious Processes!

RSSD: Design Challenges

Limited Local Storage Capacity

RSSD: Design Challenges

Limited Local Storage Capacity

Compress retained data + Hardware isolated data transfer

RSSD: Design Challenges

Limited Local Storage Capacity

Impact on Storage Performance

RSSD: Design Challenges

Limited Local Storage Capacity

Impact on Storage Performance

Keep valid data locally + Transfer data during idle cycles

RSSD: Design Challenges

Limited Local Storage Capacity

Impact on Storage Performance

Trusted Post-Attack Analysis

RSSD: Design Challenges

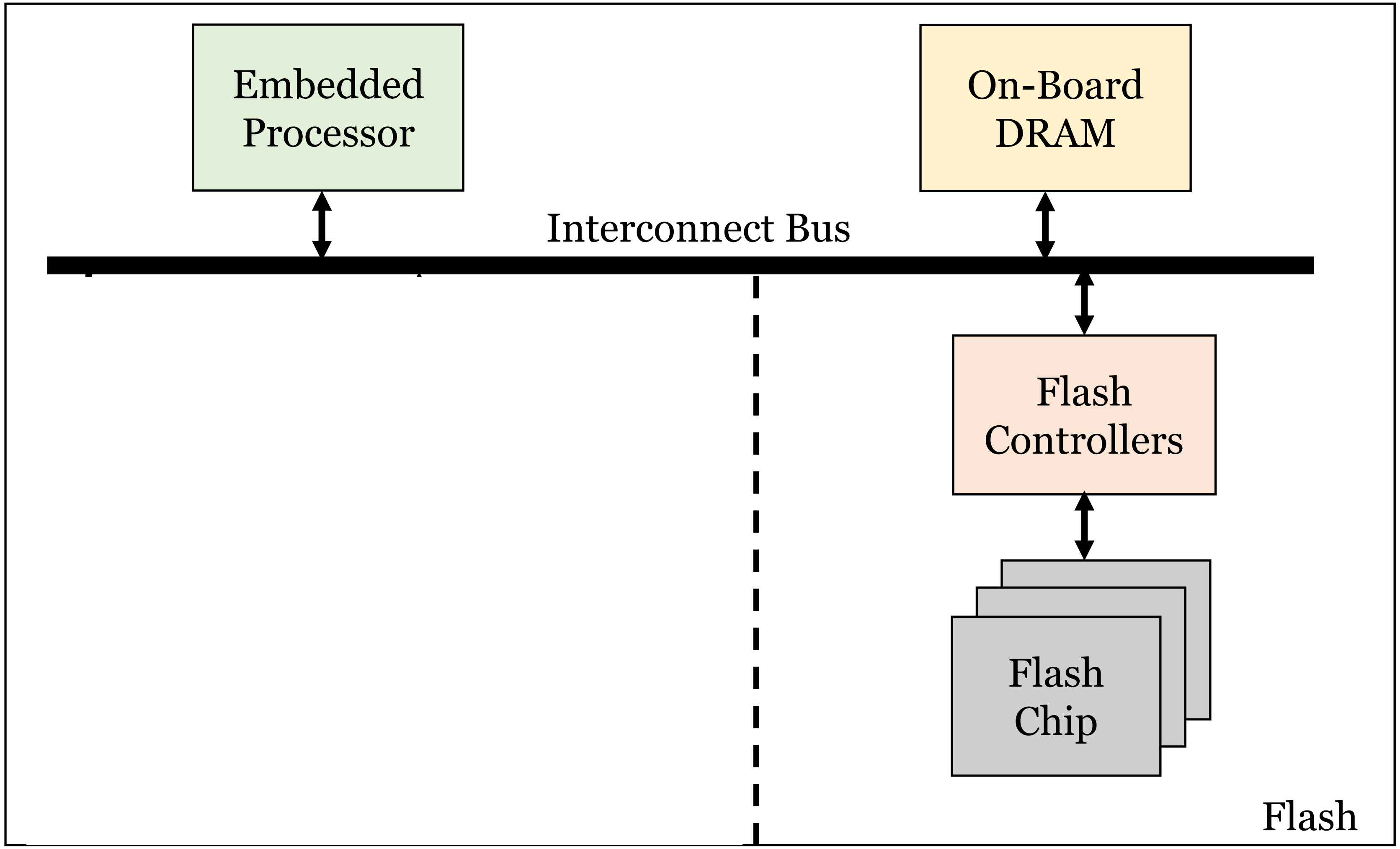
Limited Local Storage Capacity

Impact on Storage Performance

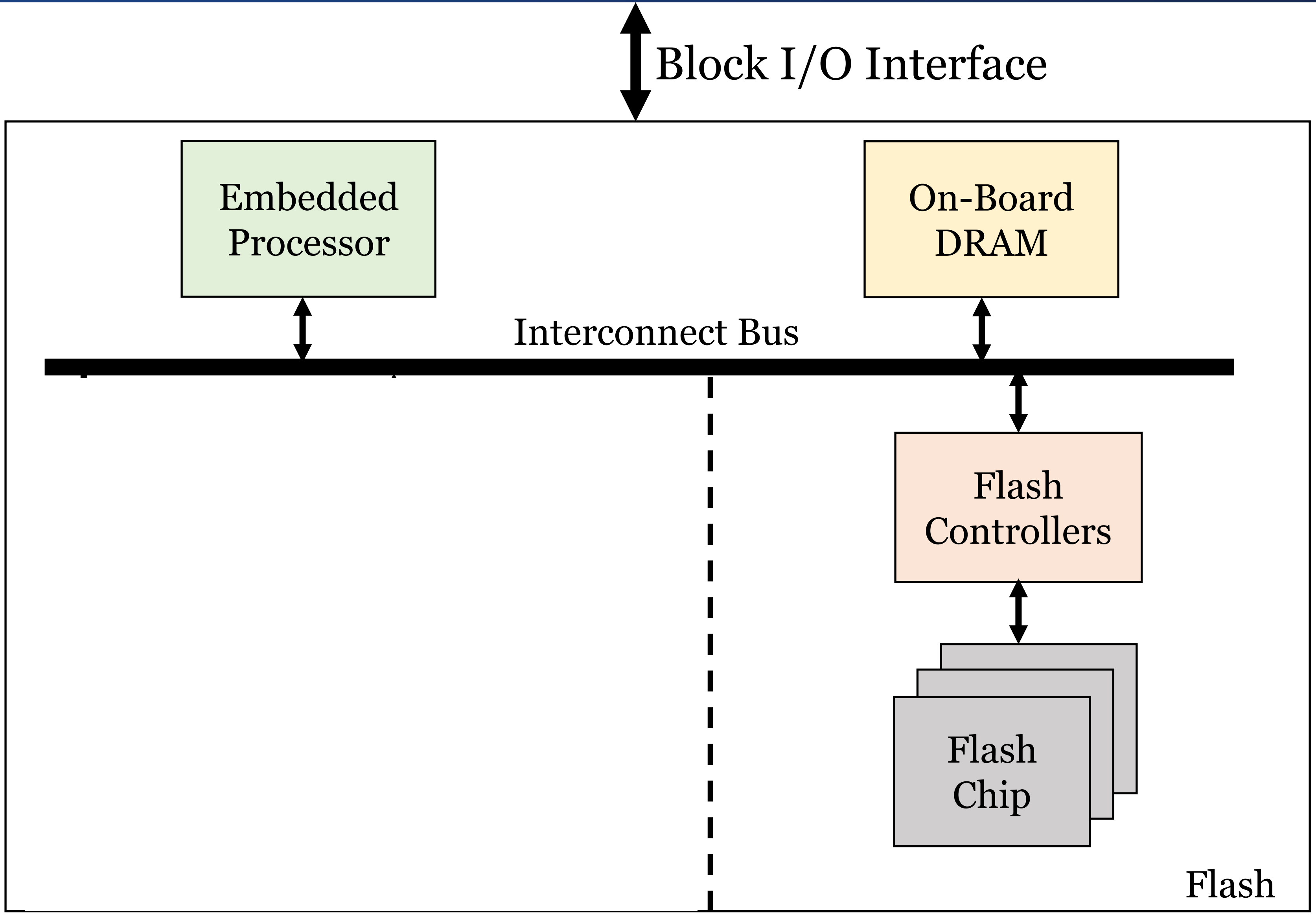
Trusted Post-Attack Analysis

Hardware-isolated logging + Log operations in time order

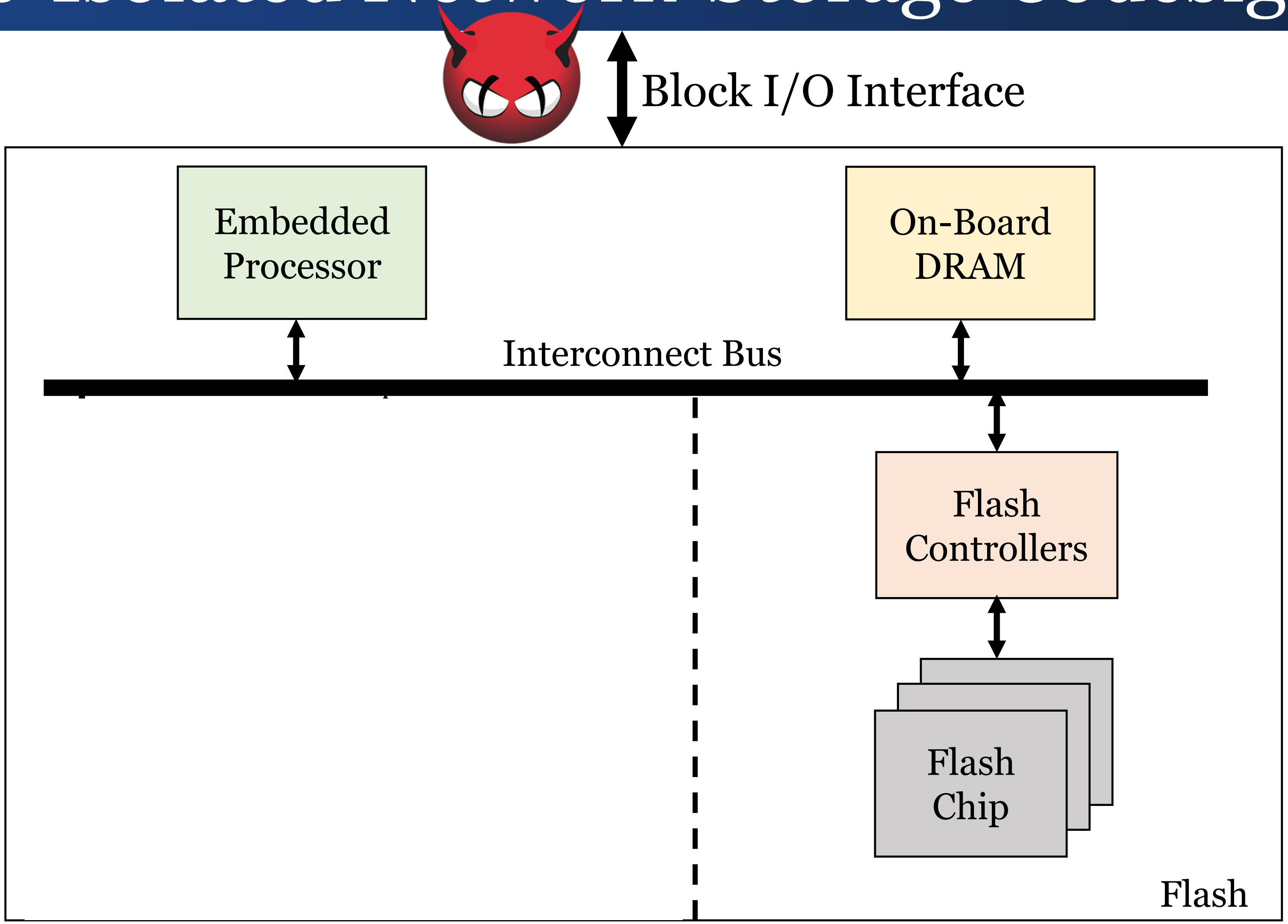
Hardware-Isolated Network-Storage Codesign



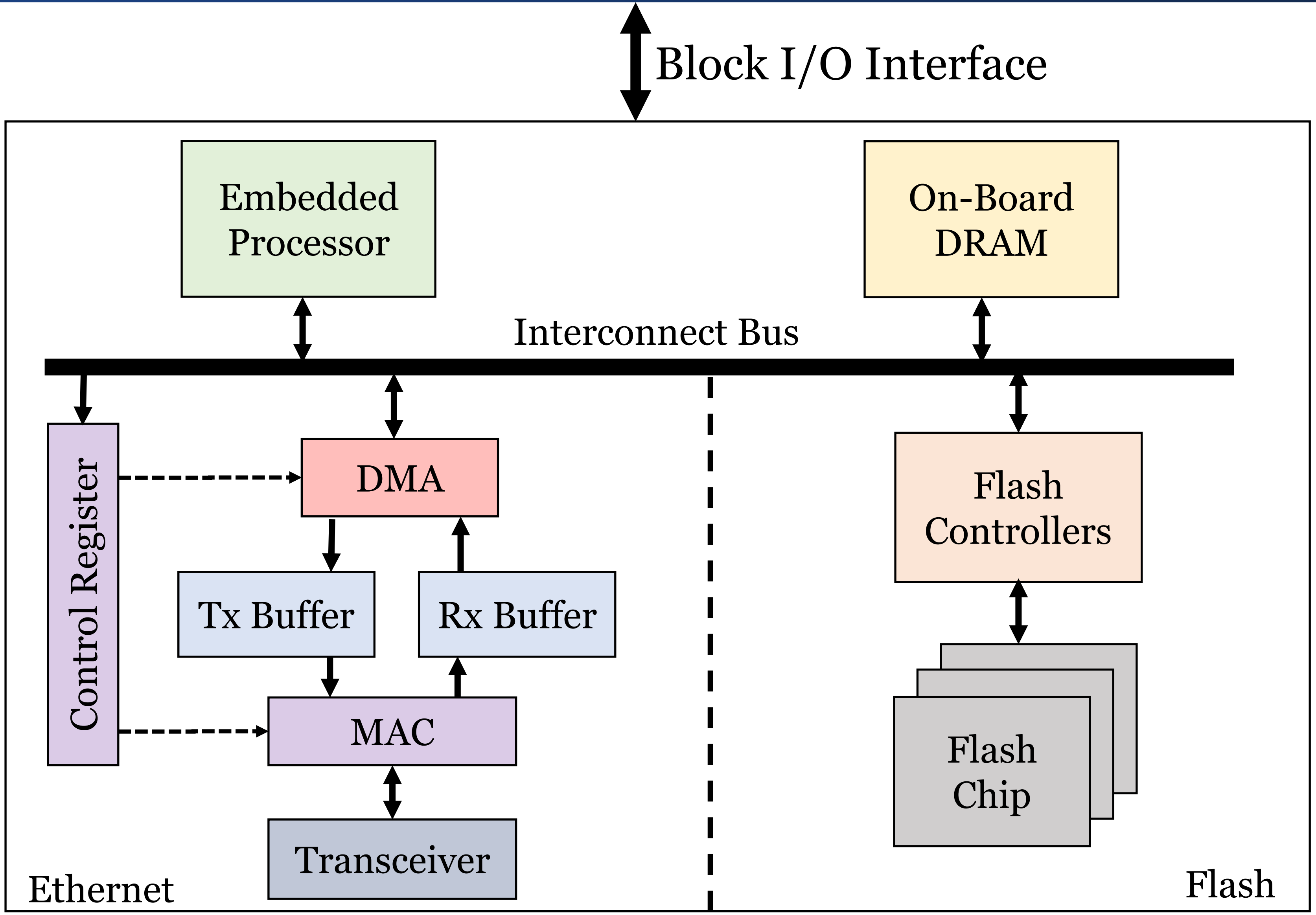
Hardware-Isolated Network-Storage Codesign



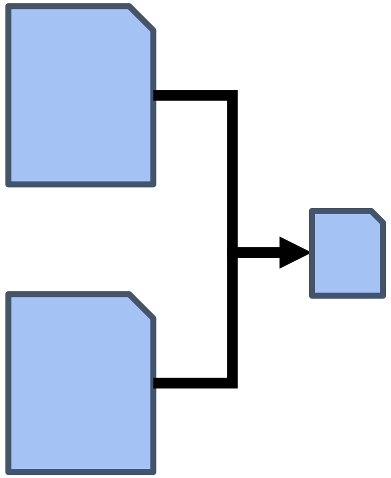
Hardware-Isolated Network-Storage Codesign



Hardware-Isolated Network-Storage Codesign

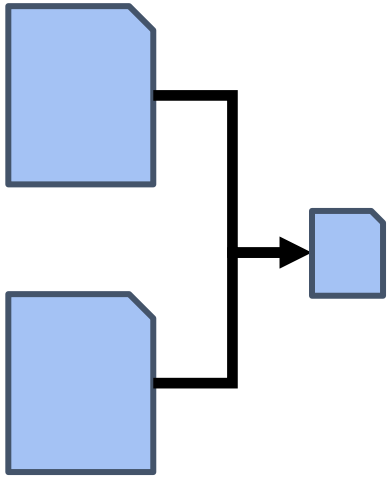


Performance Optimizations in RSSD



Delta compression

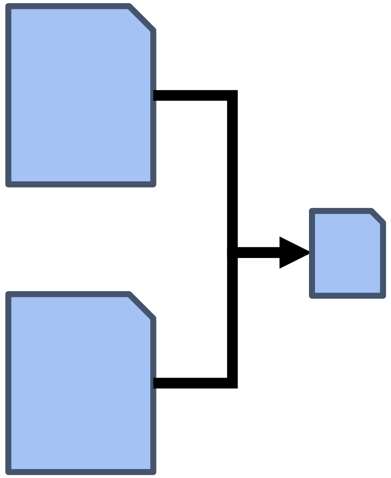
Performance Optimizations in RSSD



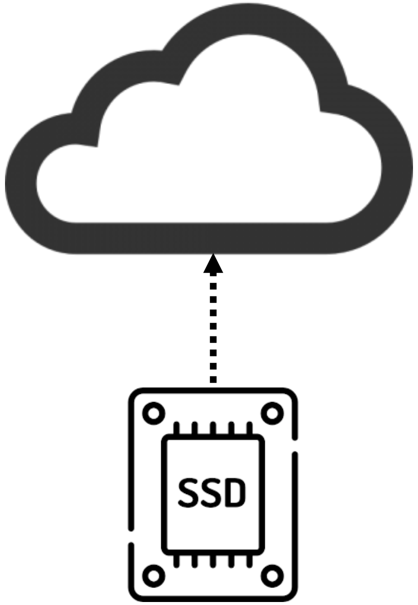
Delta compression

Reduce storage overhead and data transferred!

Performance Optimizations in RSSD

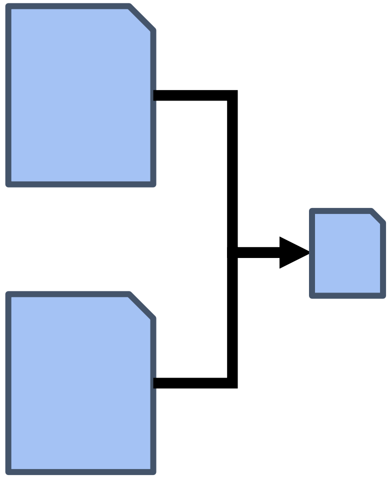


Delta compression

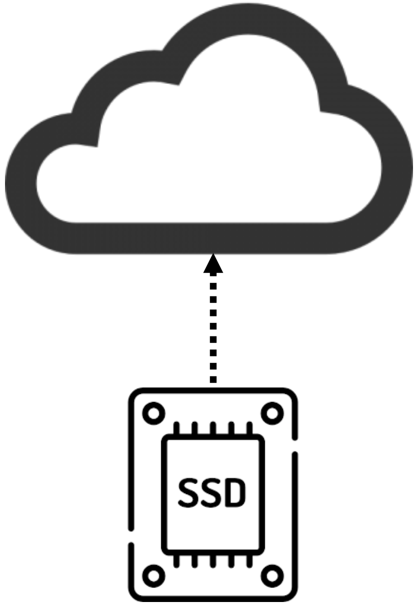


Transfer only retained data

Performance Optimizations in RSSD



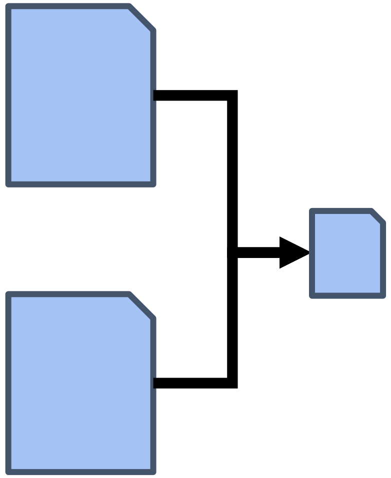
Delta compression



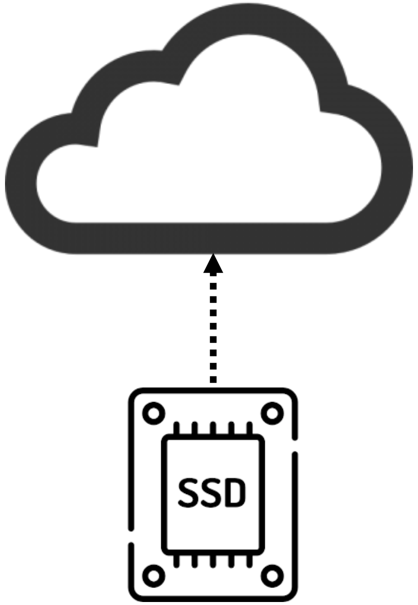
Transfer only retained data

Stale data is rarely accessed!

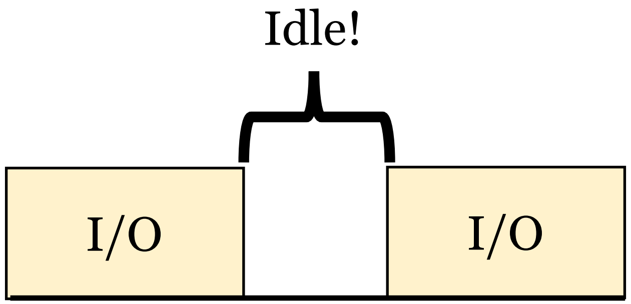
Performance Optimizations in RSSD



Delta compression

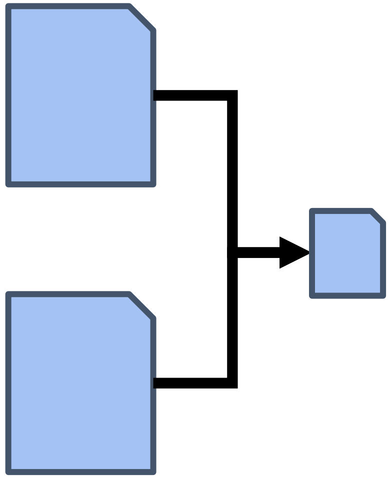


Transfer only retained data

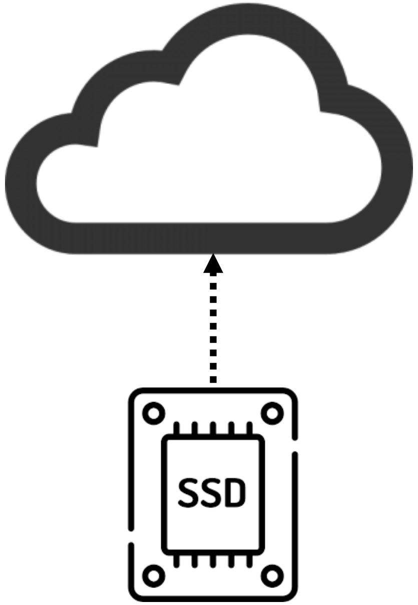


Use idle cycles to transfer data

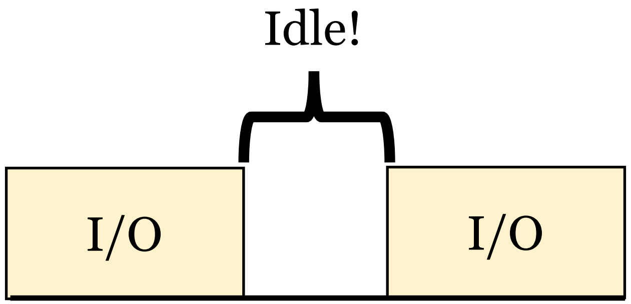
Performance Optimizations in RSSD



Delta compression



Transfer only retained data



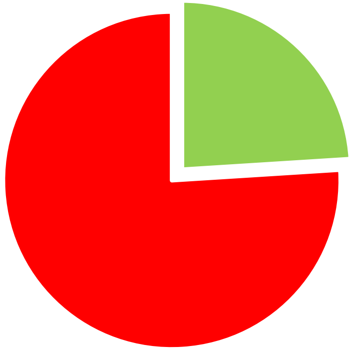
Use idle cycles to transfer data

Transfer data during predicted idle cycles!

Enabling Trusted Post-Attack Analysis

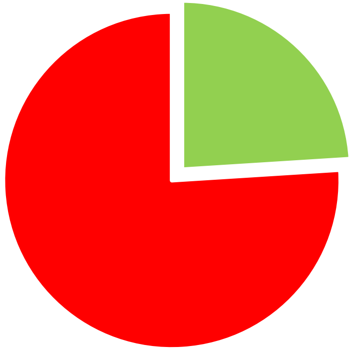
Source: Rocky Mountain

Enabling Trusted Post-Attack Analysis



Only 24% report post-attack analysis!

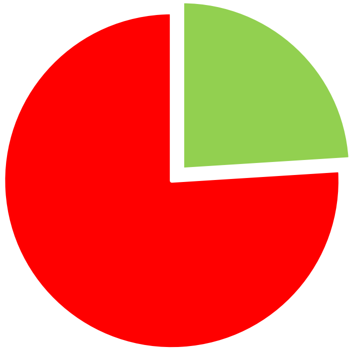
Enabling Trusted Post-Attack Analysis



Only 24% report post-attack analysis!

Analysis took 6 weeks on average!

Enabling Trusted Post-Attack Analysis

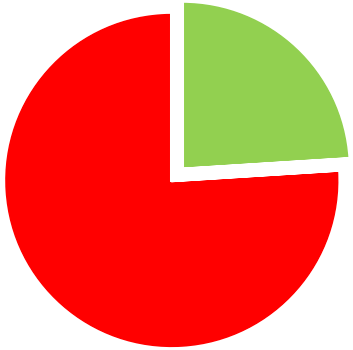


Only 24% report post-attack analysis!

Analysis took 6 weeks on average!

Software-based logging cannot be trusted!

Enabling Trusted Post-Attack Analysis



Only 24% report post-attack analysis!

Analysis took 6 weeks on average!

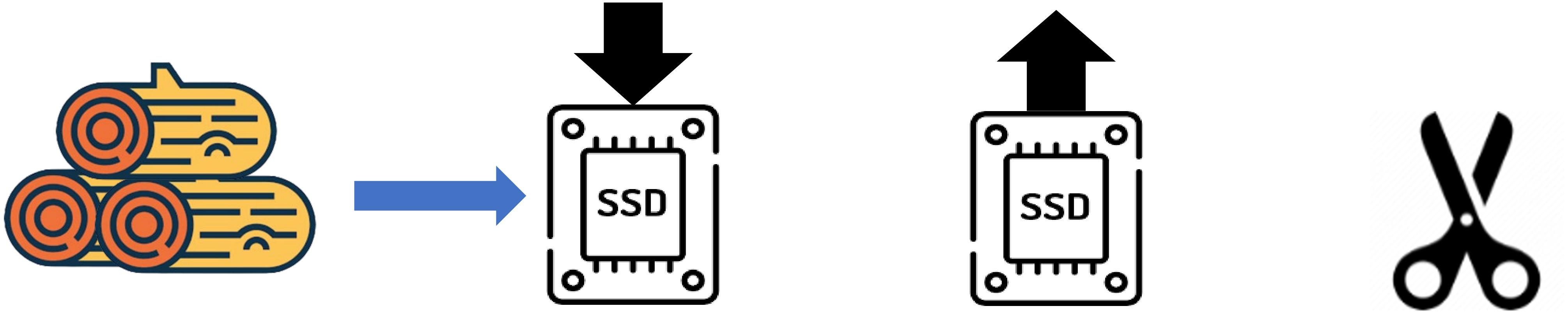
Software-based logging cannot be trusted!

Trusted post-attack analysis is highly desirable!

Enabling Trusted Post-Attack Analysis

Hardware-Assisted Logging

Enabling Trusted Post-Attack Analysis



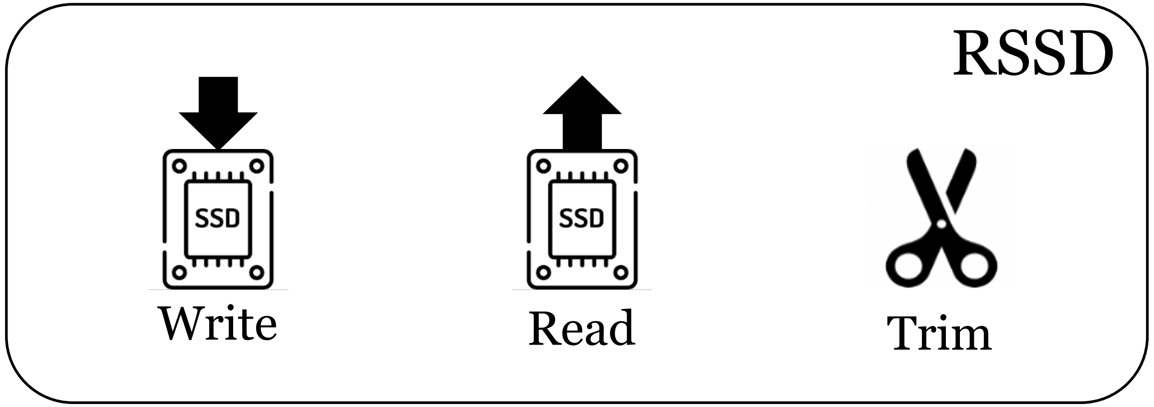
Hardware-Assisted Logging

Write

Read

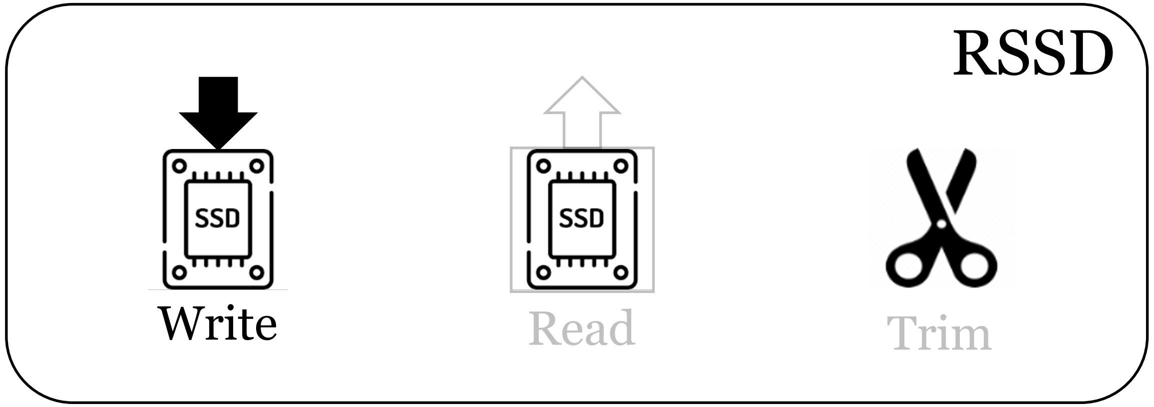
Trim

Enabling Trusted Post-Attack Analysis



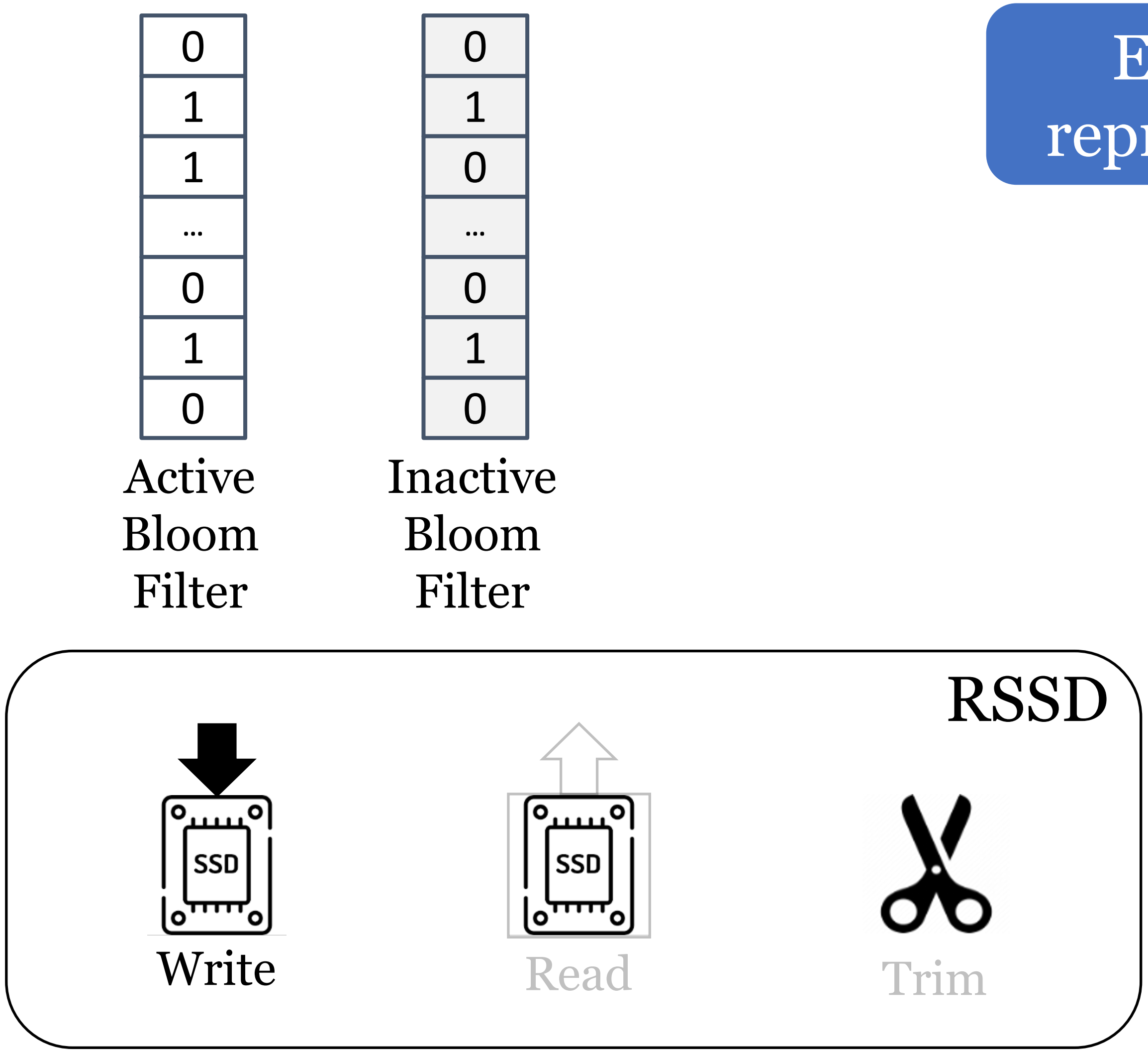
Tracking Invalid Data in Time Order

Active Bloom Filter	Inactive Bloom Filter
0	0
1	1
1	0
…	…
0	0
1	1
0	0



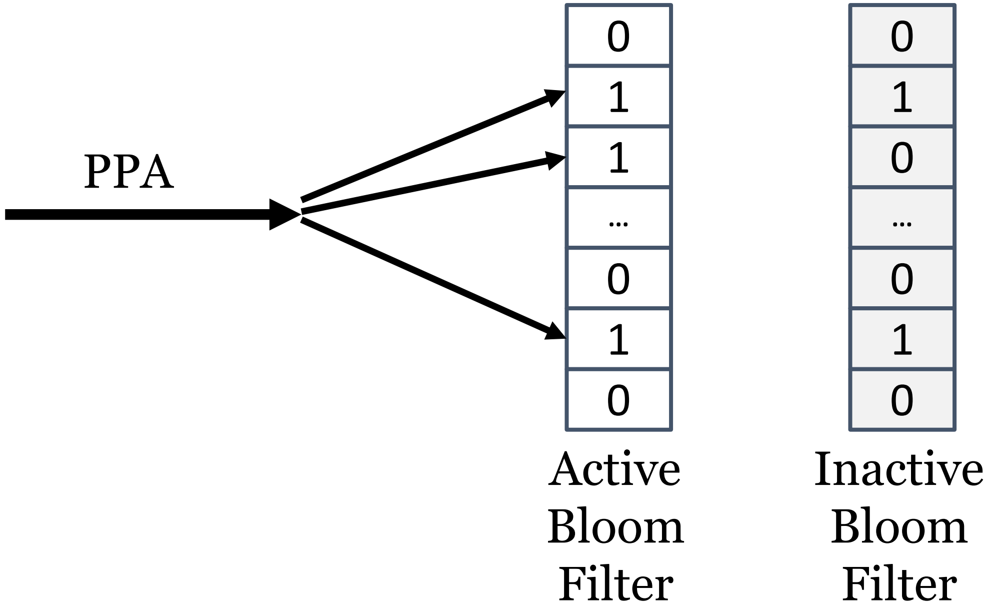
Tracking Invalid Data in Time Order

Each bloom filter represents one epoch!

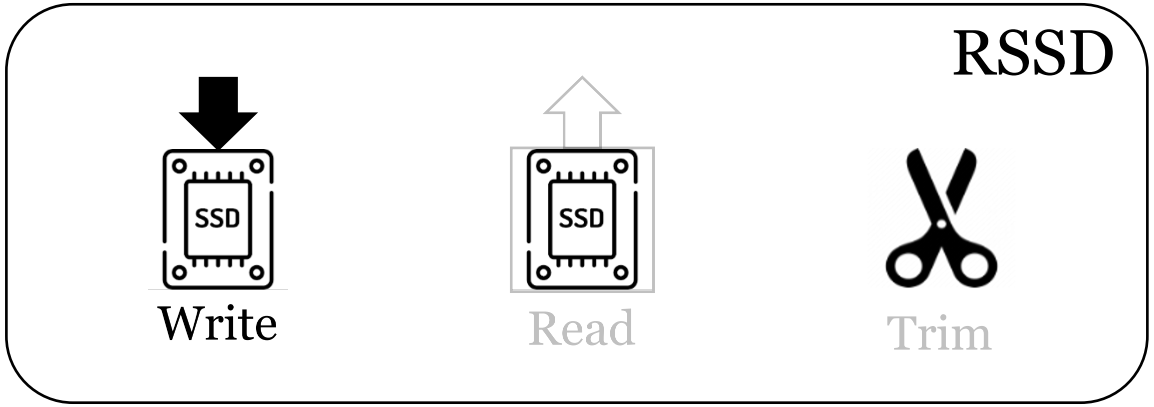


Active Bloom Filter	Inactive Bloom Filter
0	0
1	1
1	0
…	…
0	0
1	1
0	0

Tracking Invalid Data in Time Order

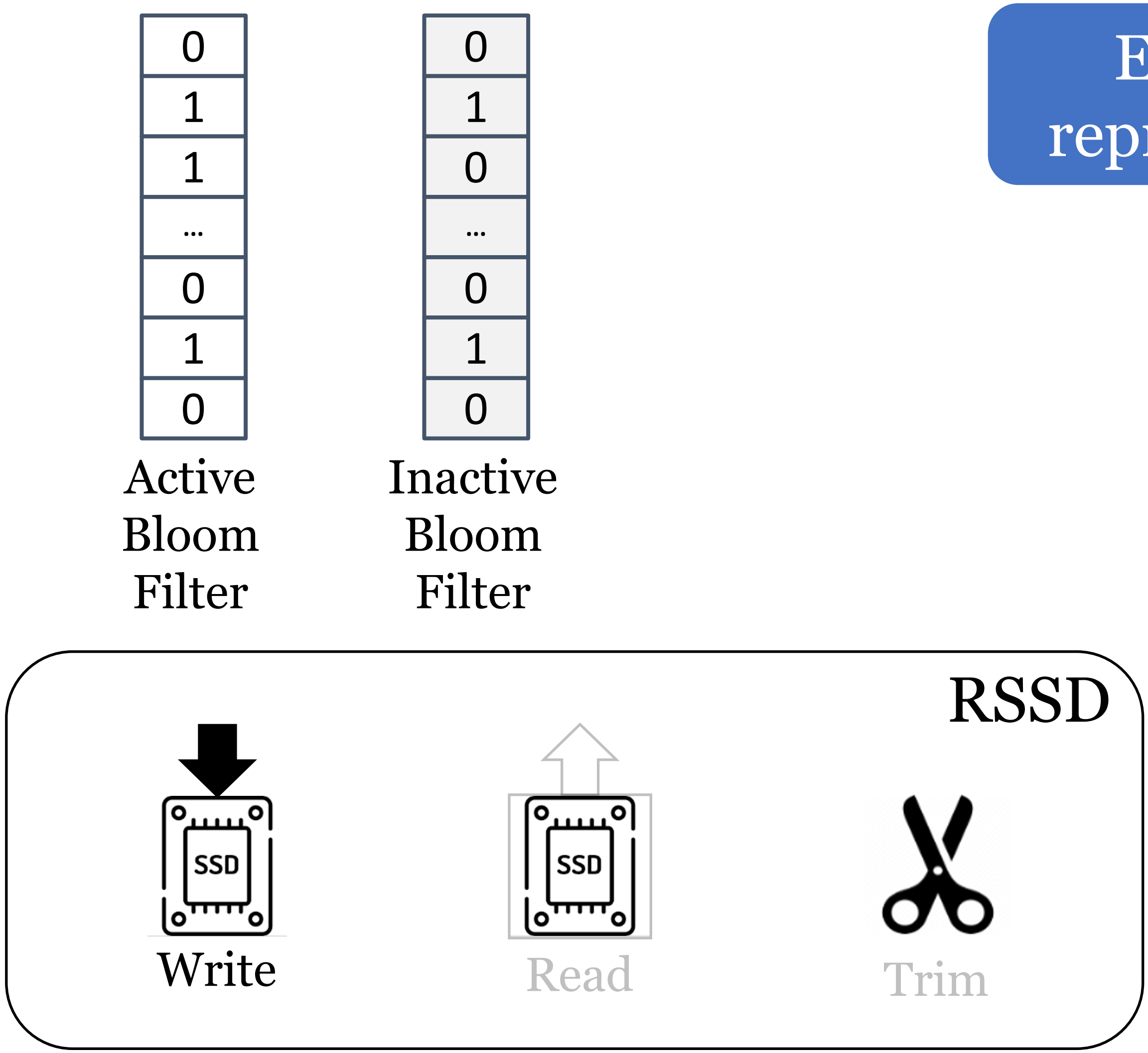


Each bloom filter represents one epoch!



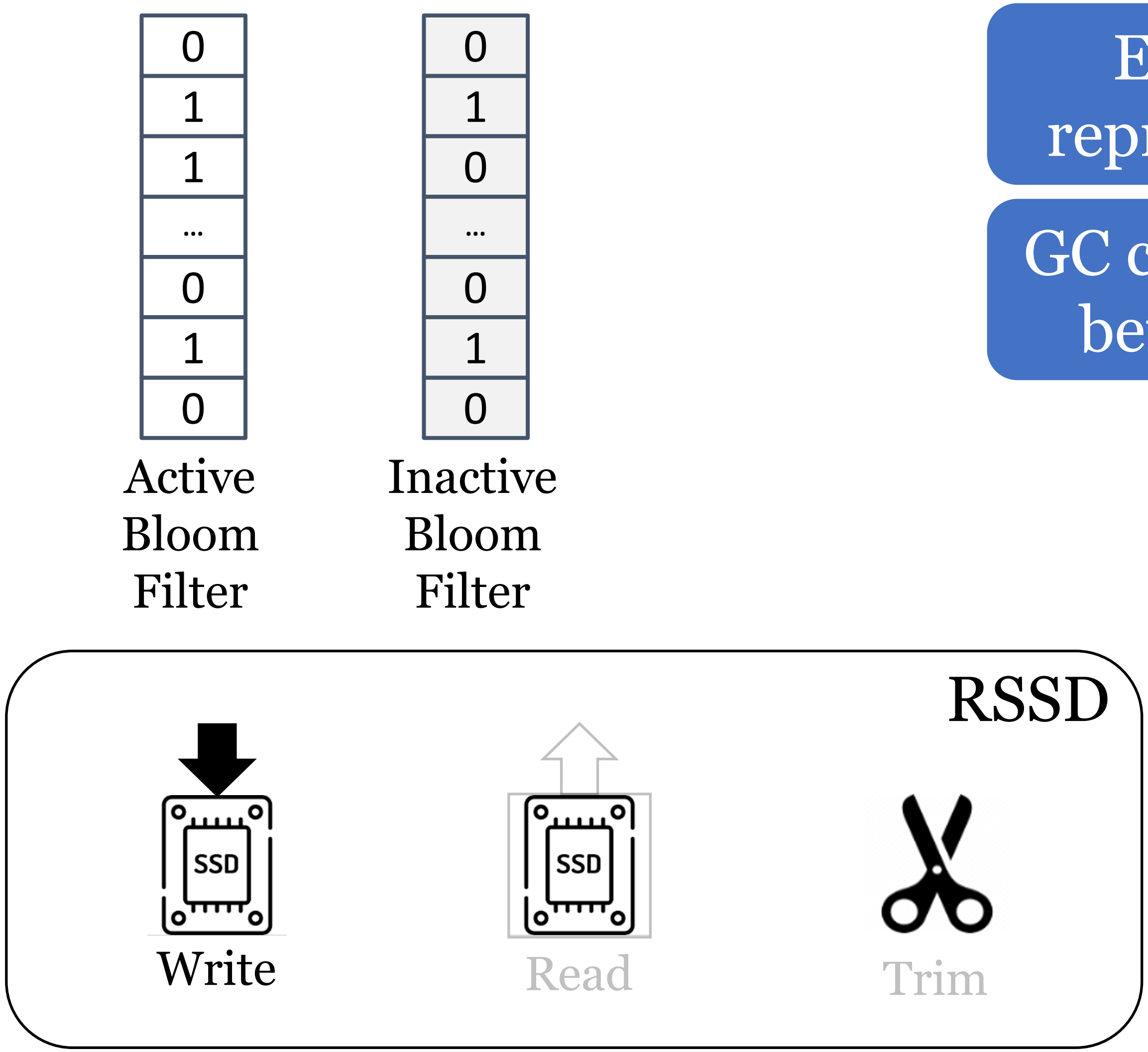
Tracking Invalid Data in Time Order

Each bloom filter represents one epoch!



Active Bloom Filter	Inactive Bloom Filter
0	0
1	1
1	0
…	…
0	0
1	1
0	0

Tracking Invalid Data in Time Order

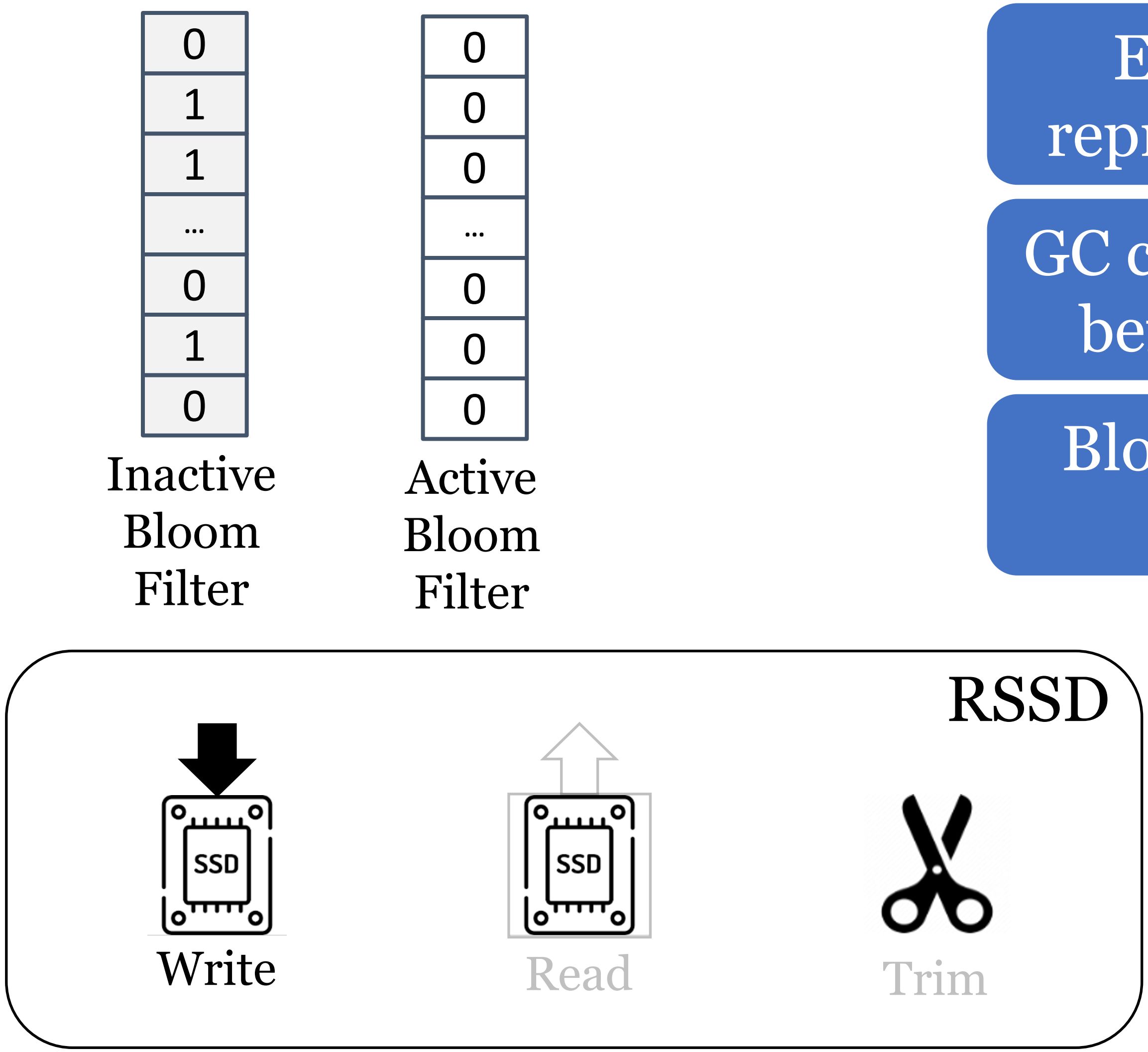


Active Bloom Filter	Inactive Bloom Filter
0	0
1	1
1	0
…	…
0	0
1	1
0	0

Each bloom filter represents one epoch!

GC checks bloom filters before transferring!

Tracking Invalid Data in Time Order



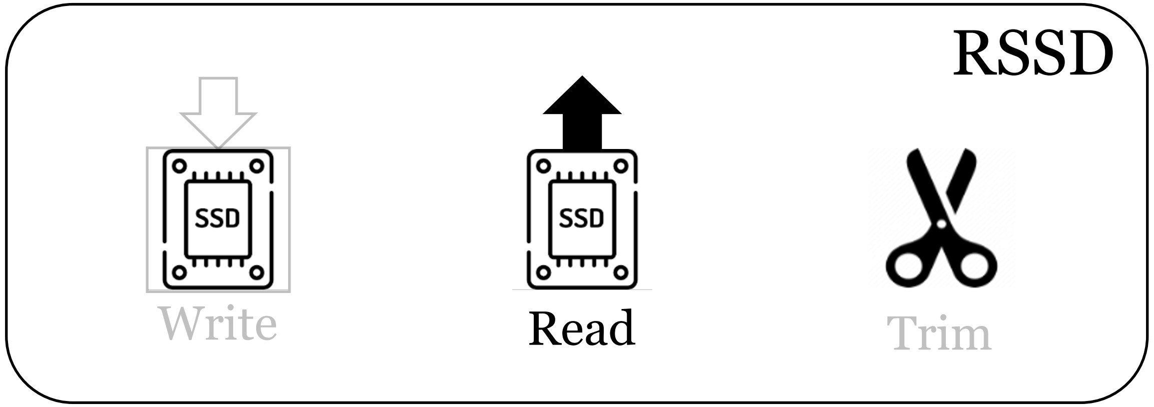
Inactive Bloom Filter	Active Bloom Filter
0	0
1	0
1	0
…	…
0	0
1	0
0	0

Each bloom filter represents one epoch!

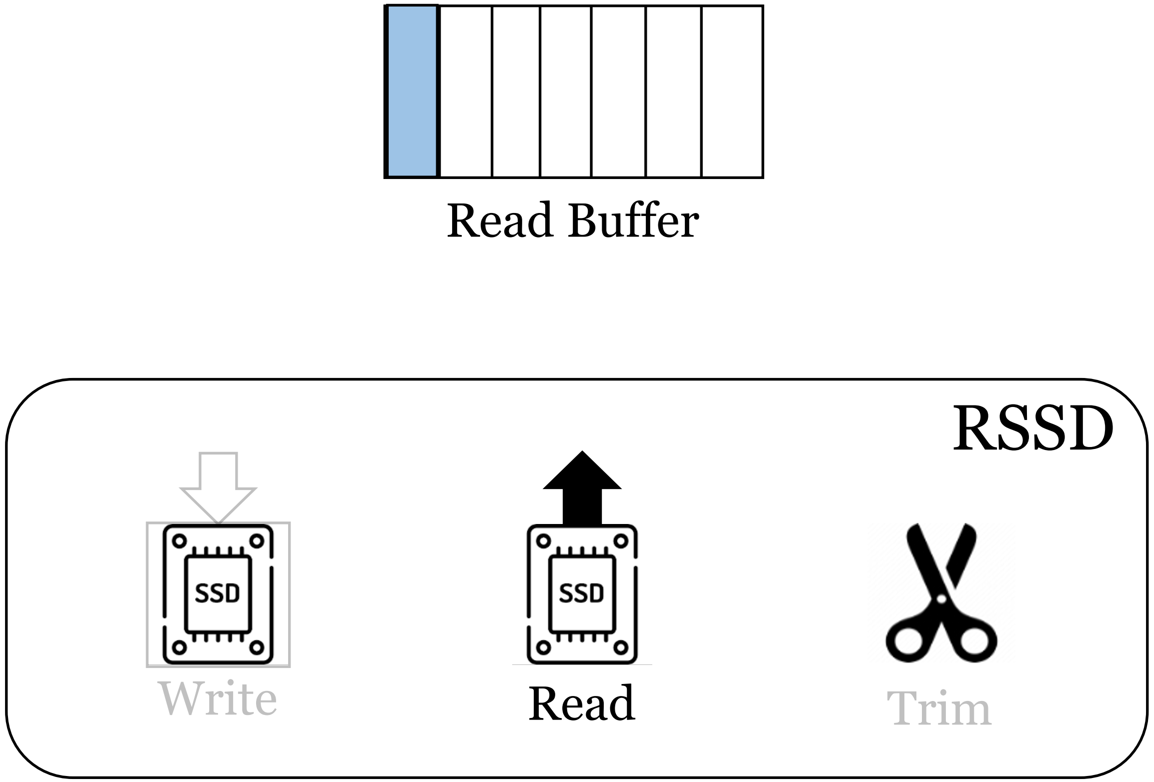
GC checks bloom filters before transferring!

Bloom filters reset in time order

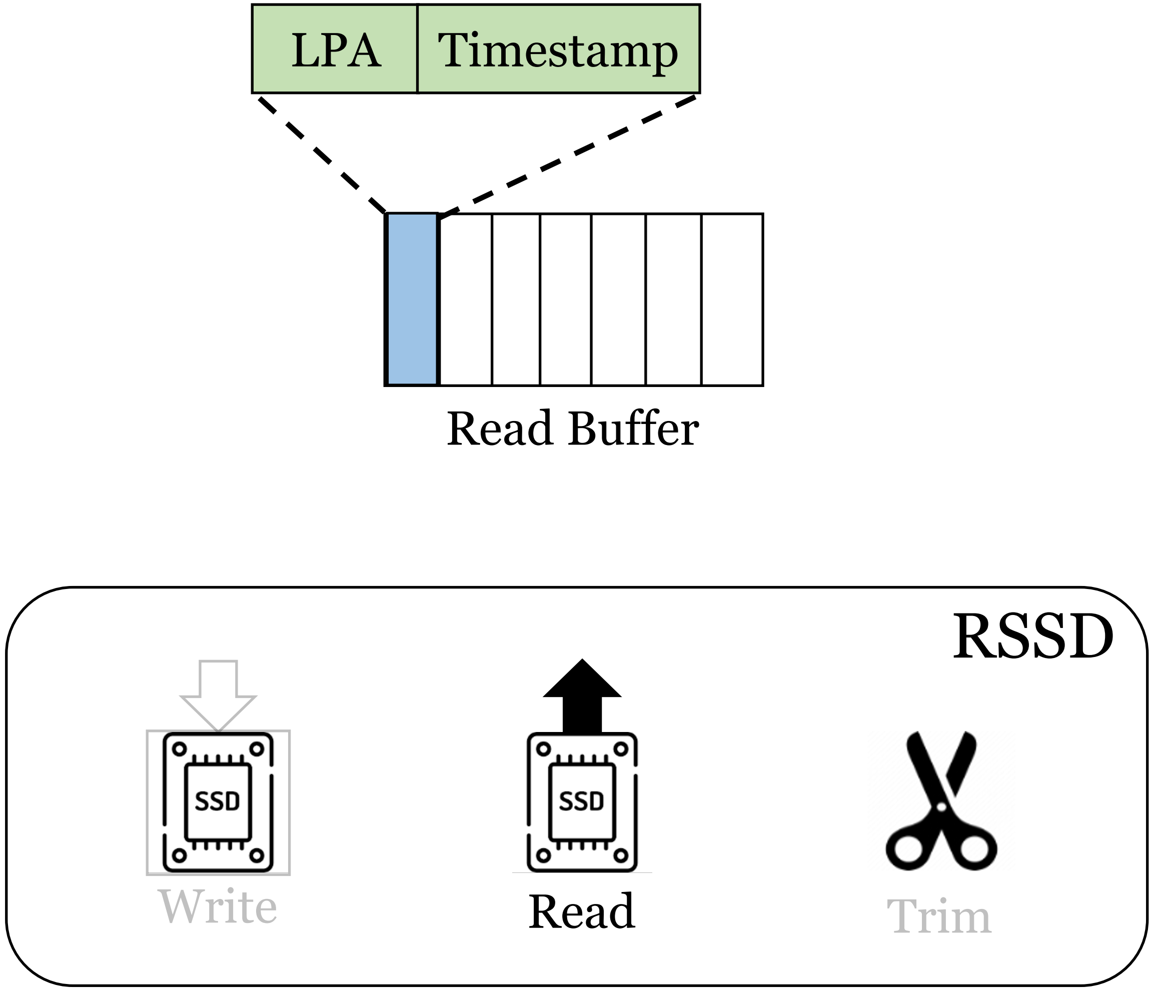
Tracking Reads in Time Order



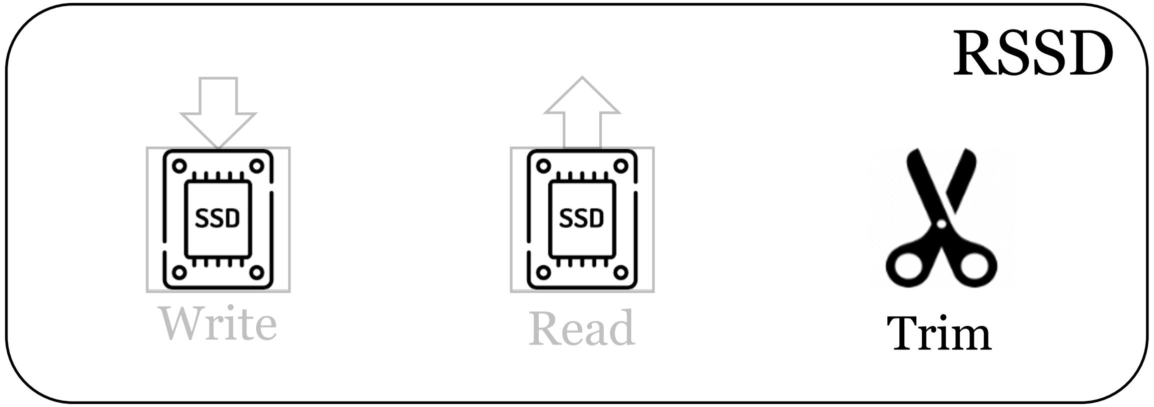
Tracking Reads in Time Order



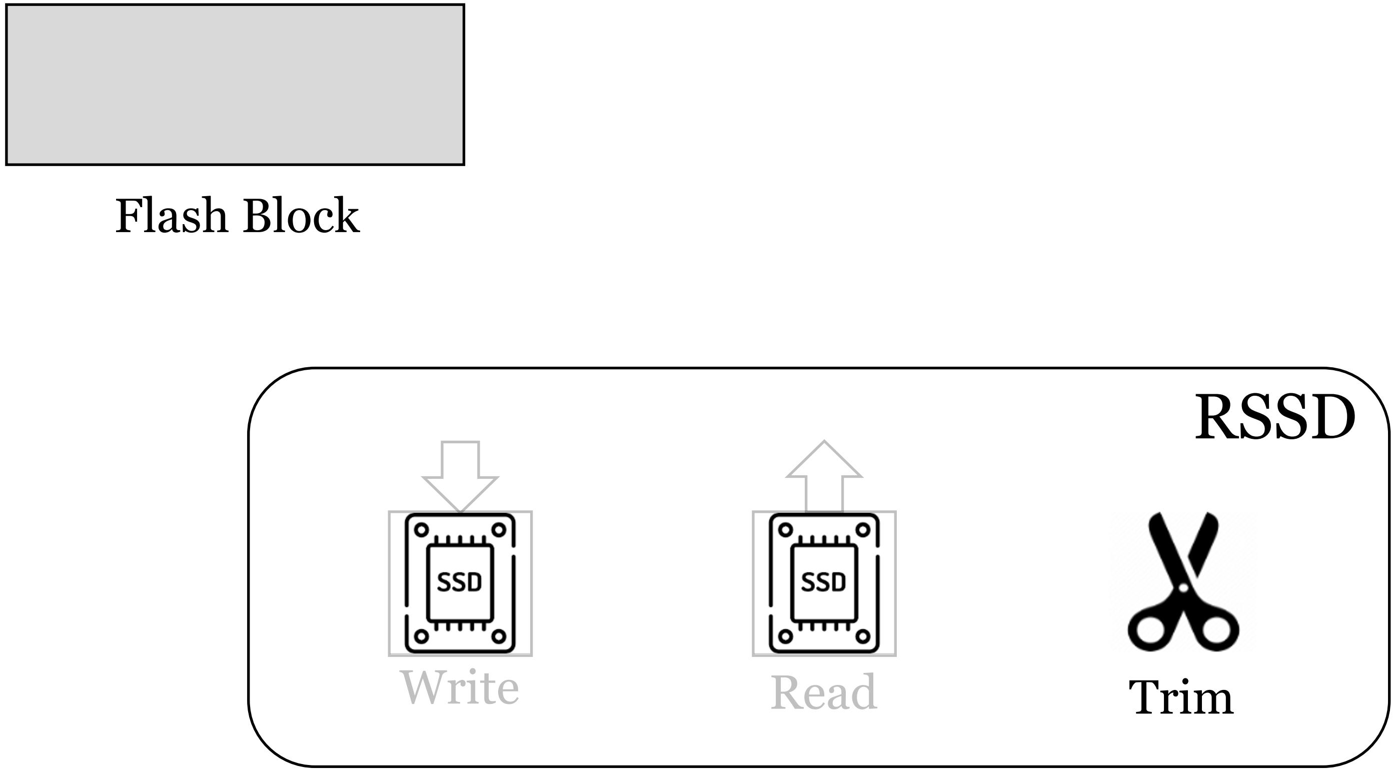
Tracking Reads in Time Order



Tracking Trims in Time Order



Tracking Trims in Time Order



Flash Block

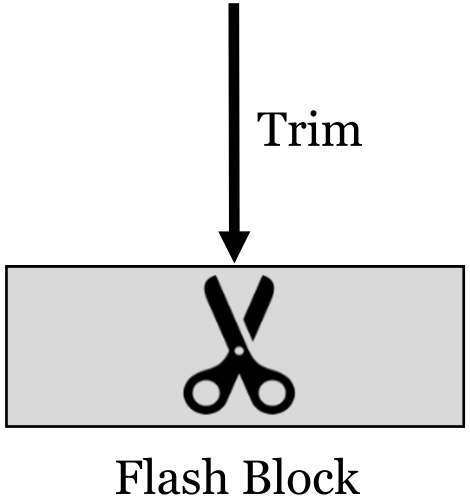
RSSD

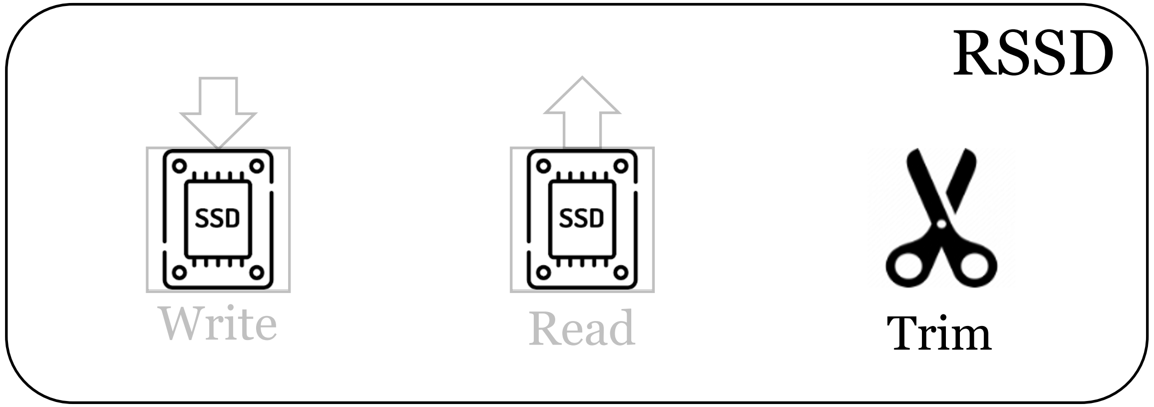
Write

Read

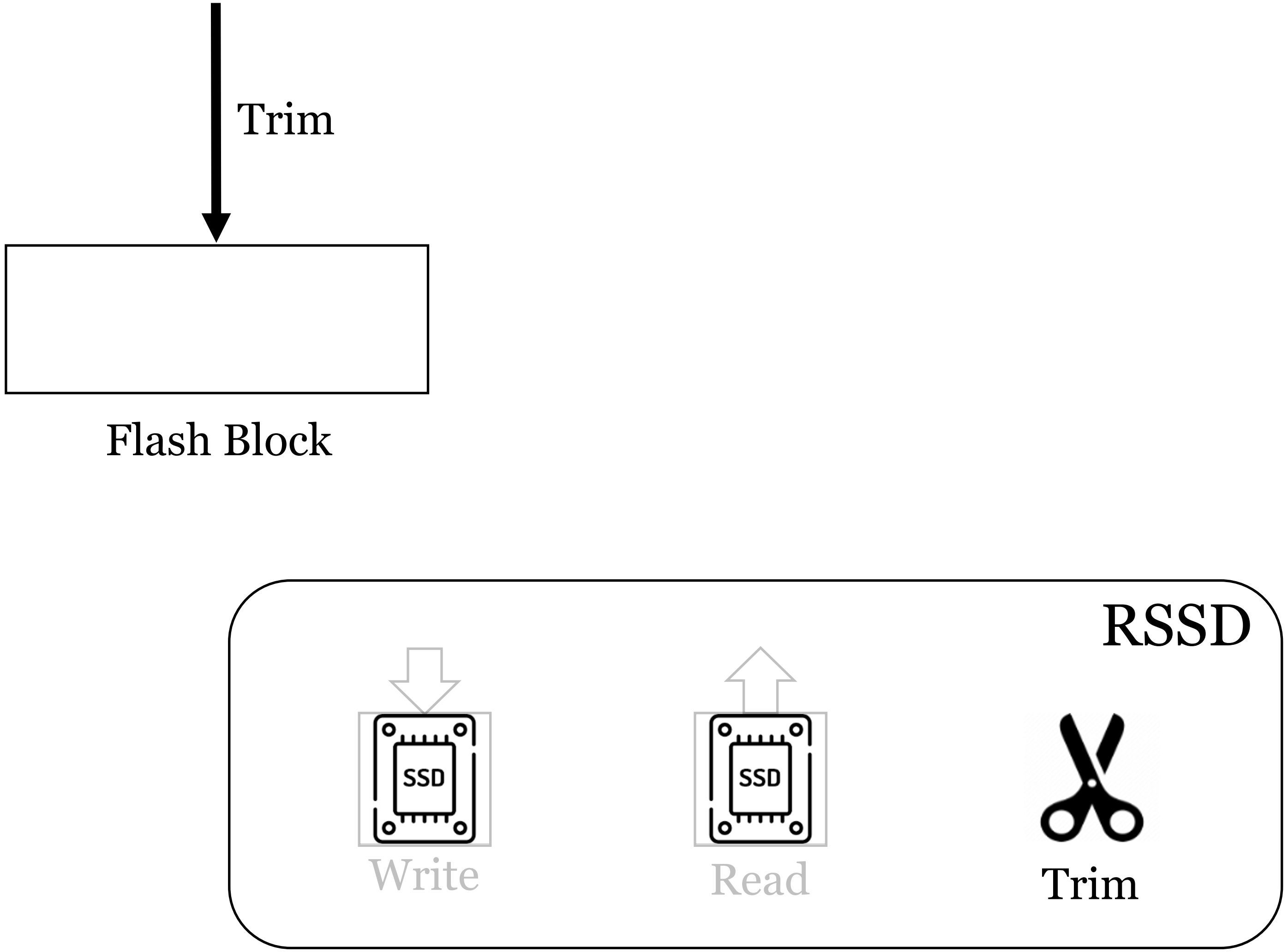
Trim

Tracking Trims in Time Order

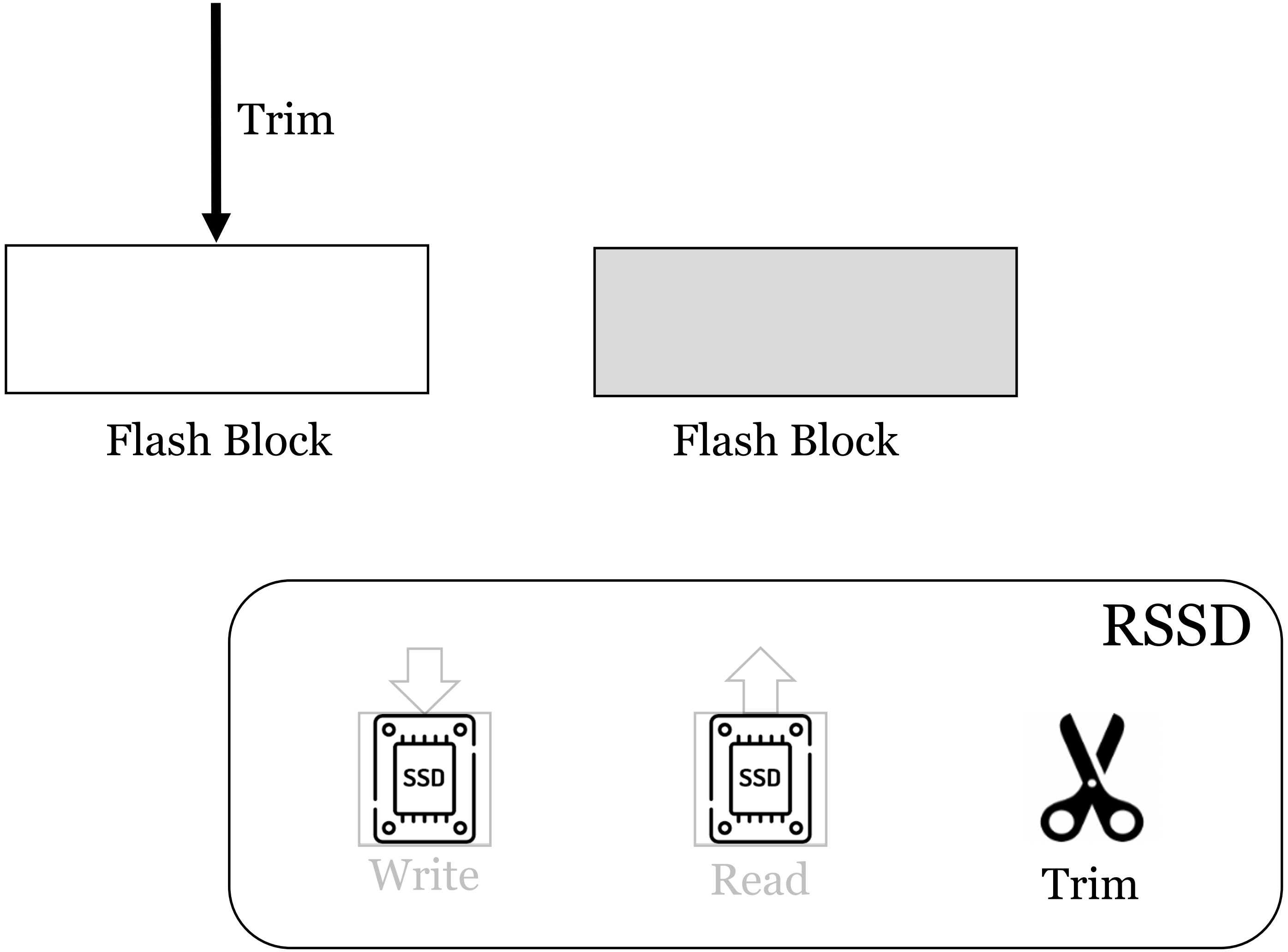




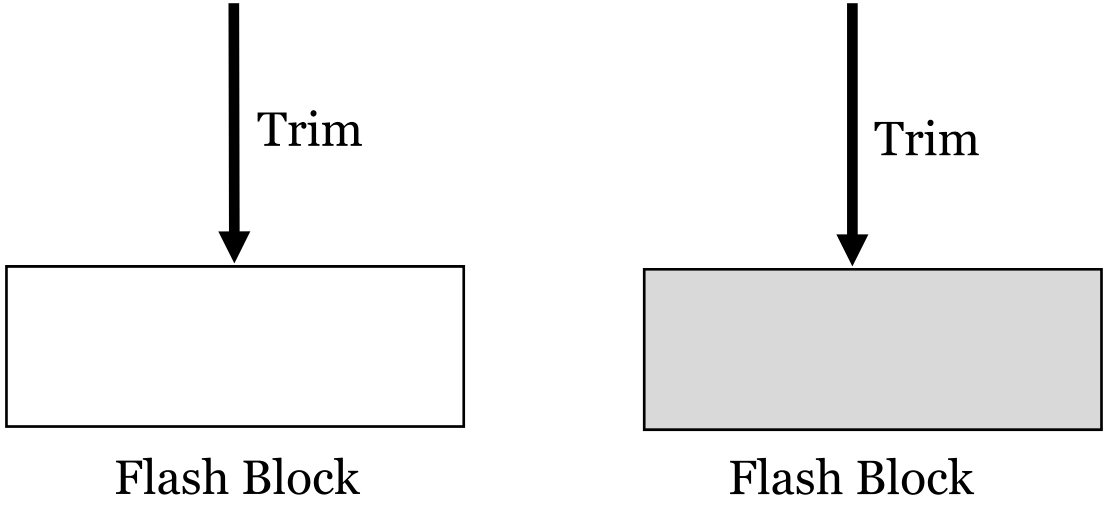
Tracking Trims in Time Order

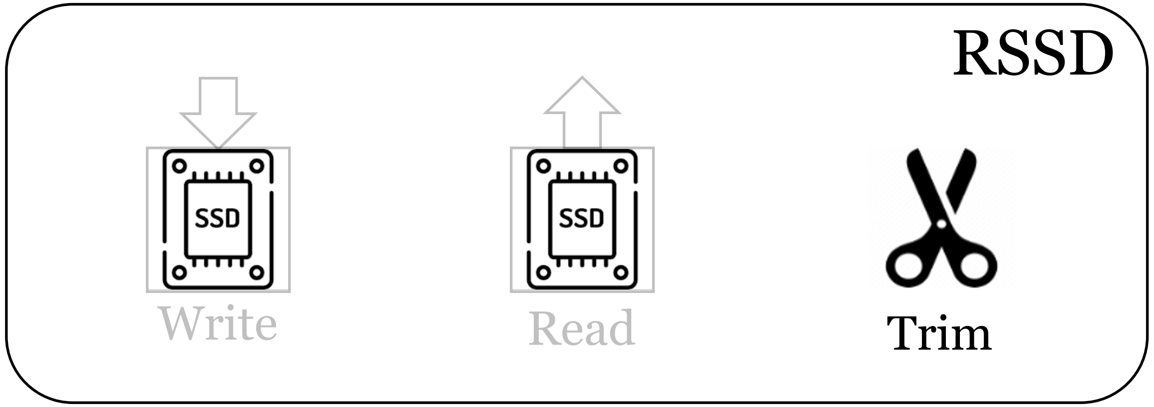


Tracking Trims in Time Order

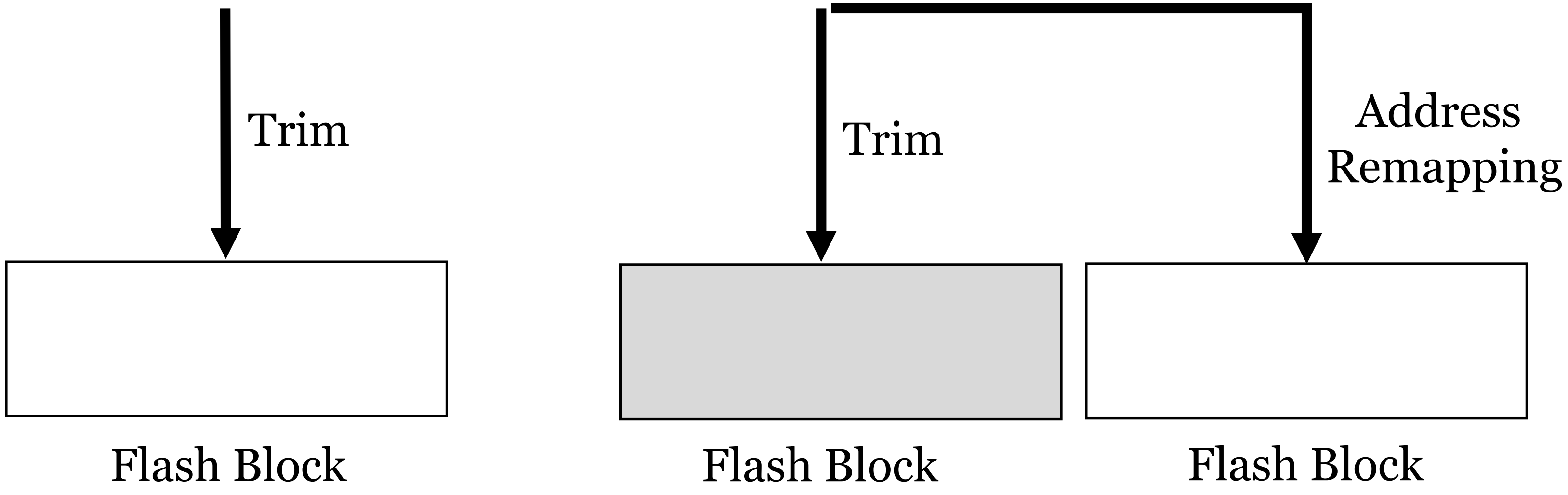


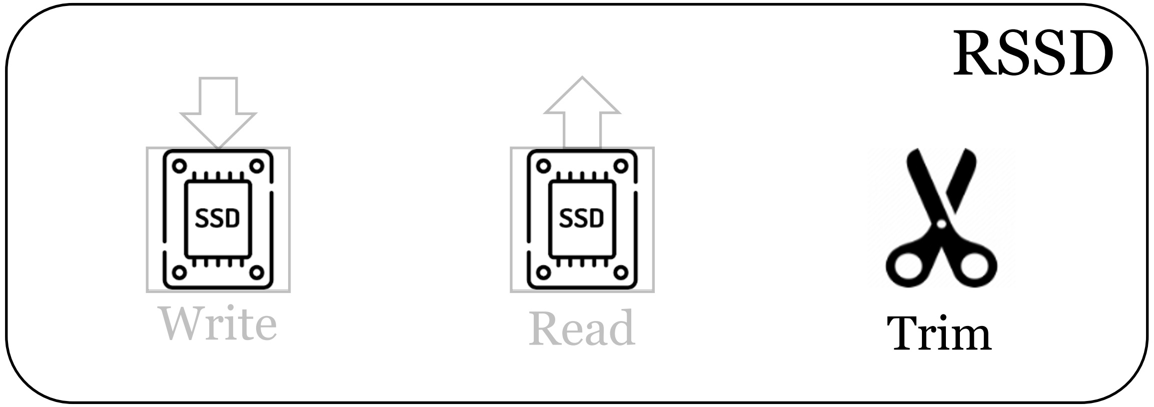
Tracking Trims in Time Order



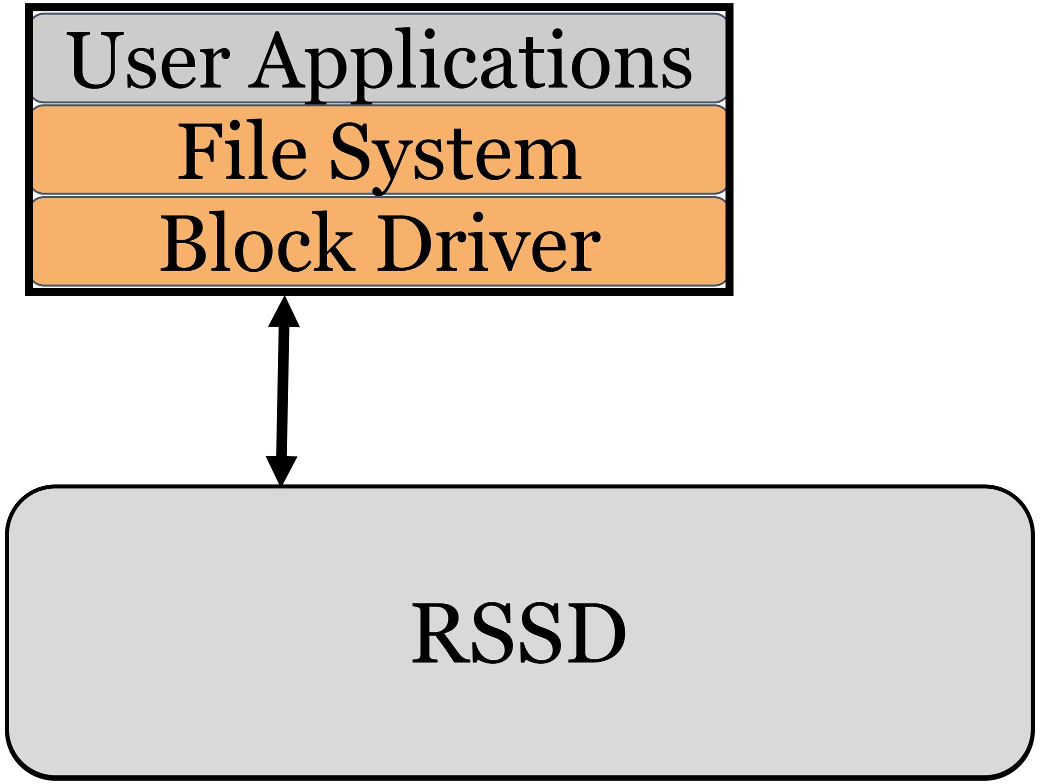


Tracking Trims in Time Order

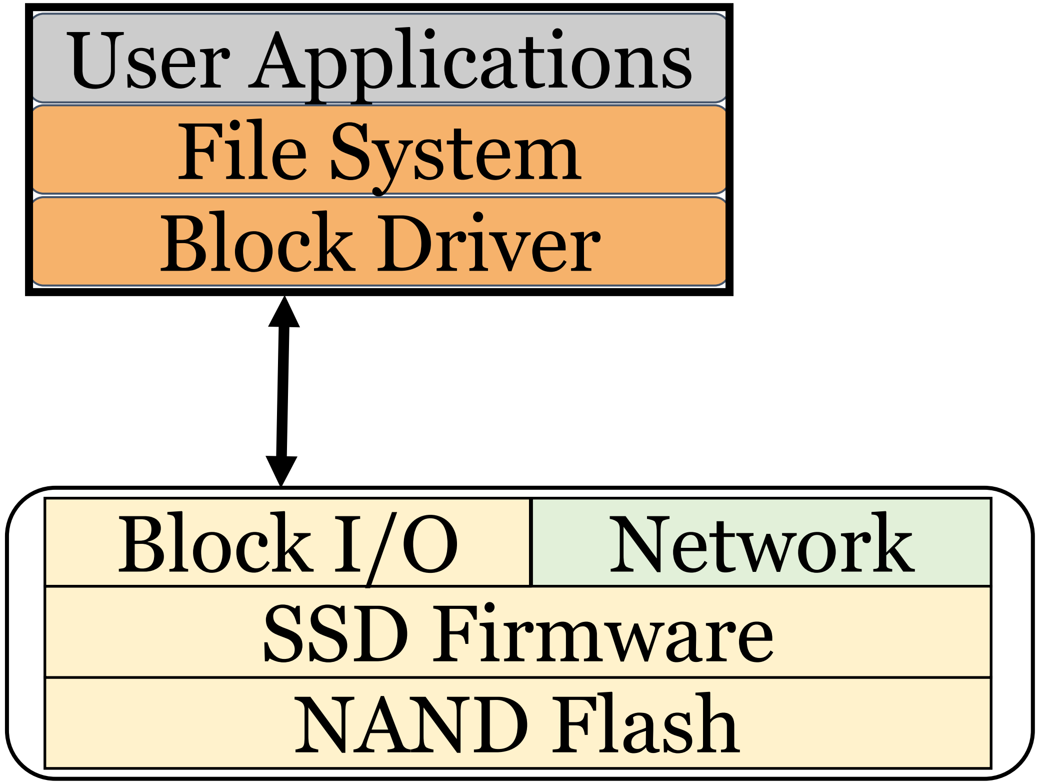




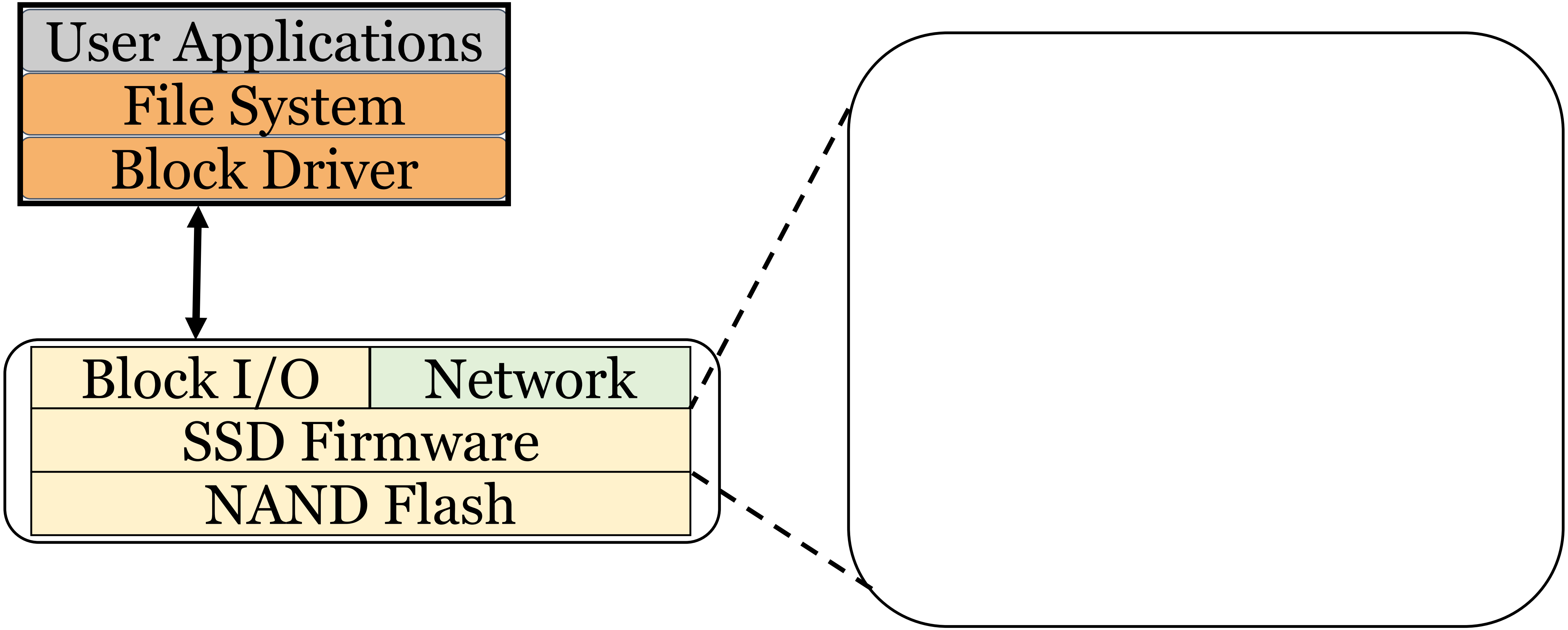
Putting It All Together



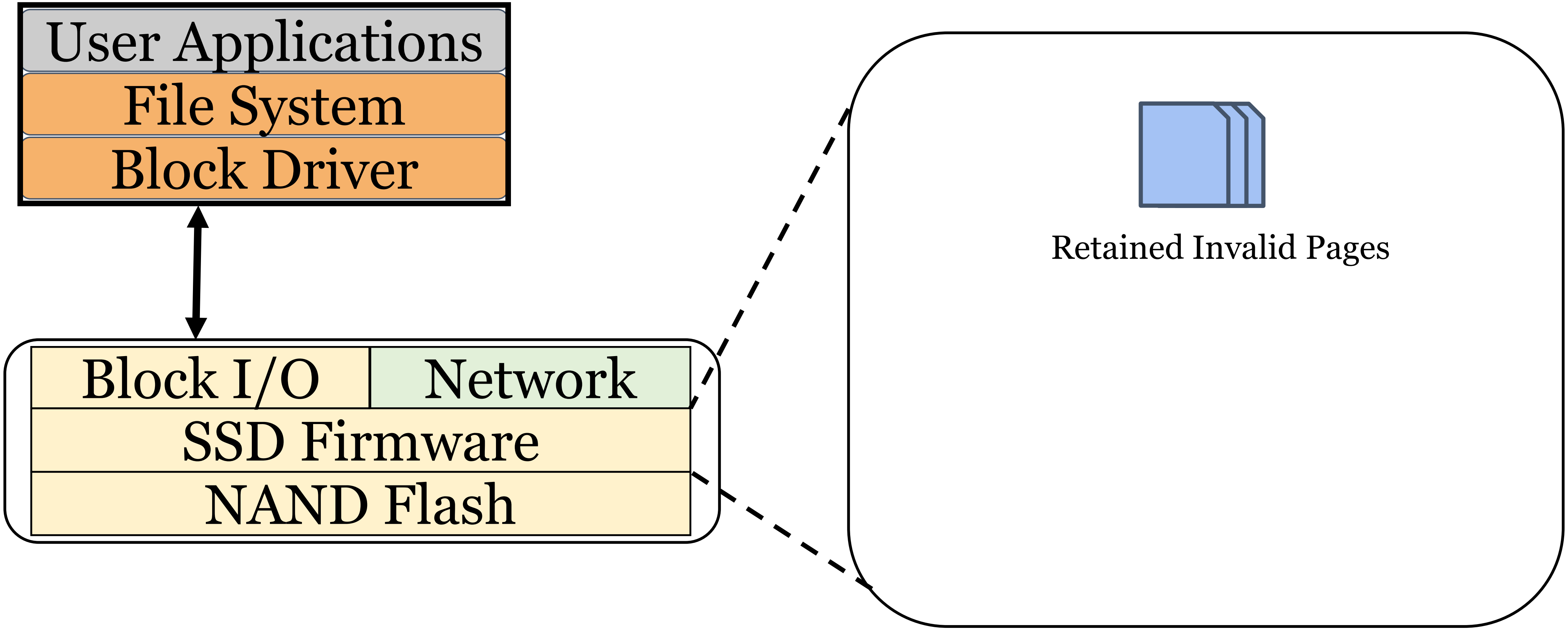
Putting It All Together



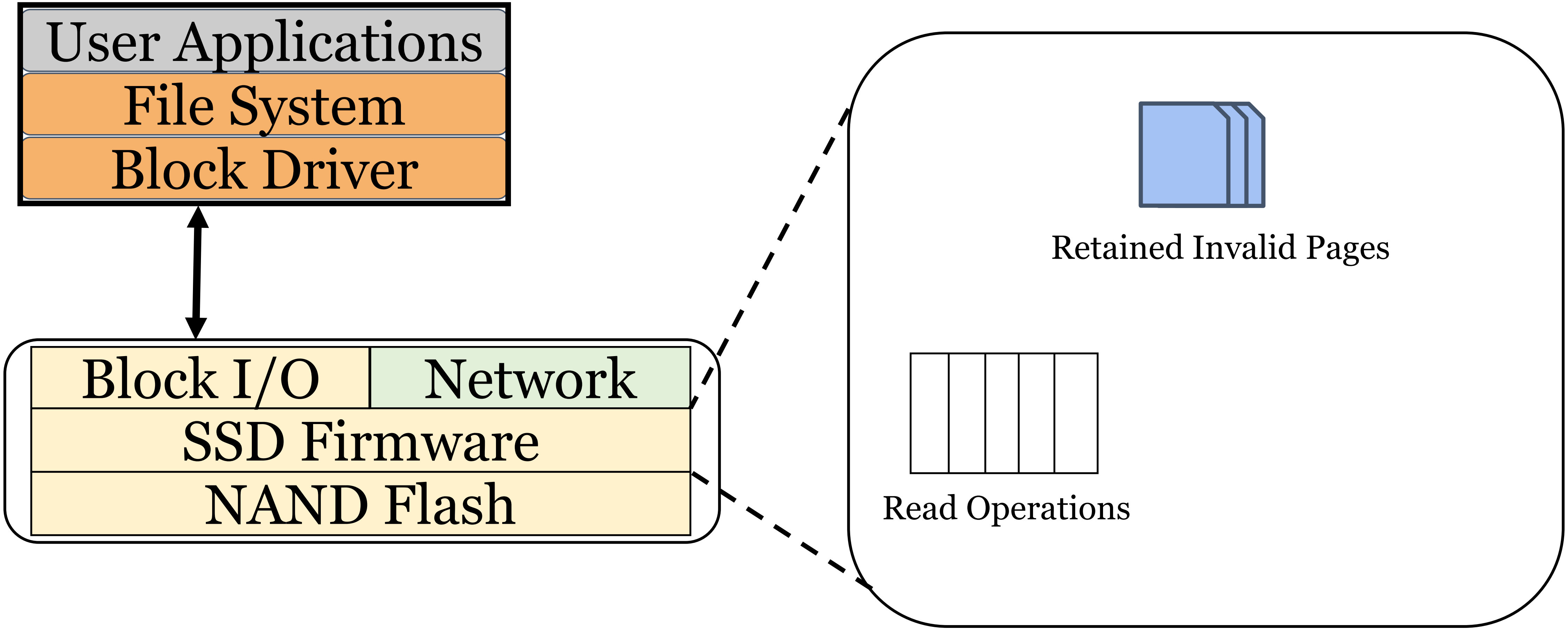
Putting It All Together



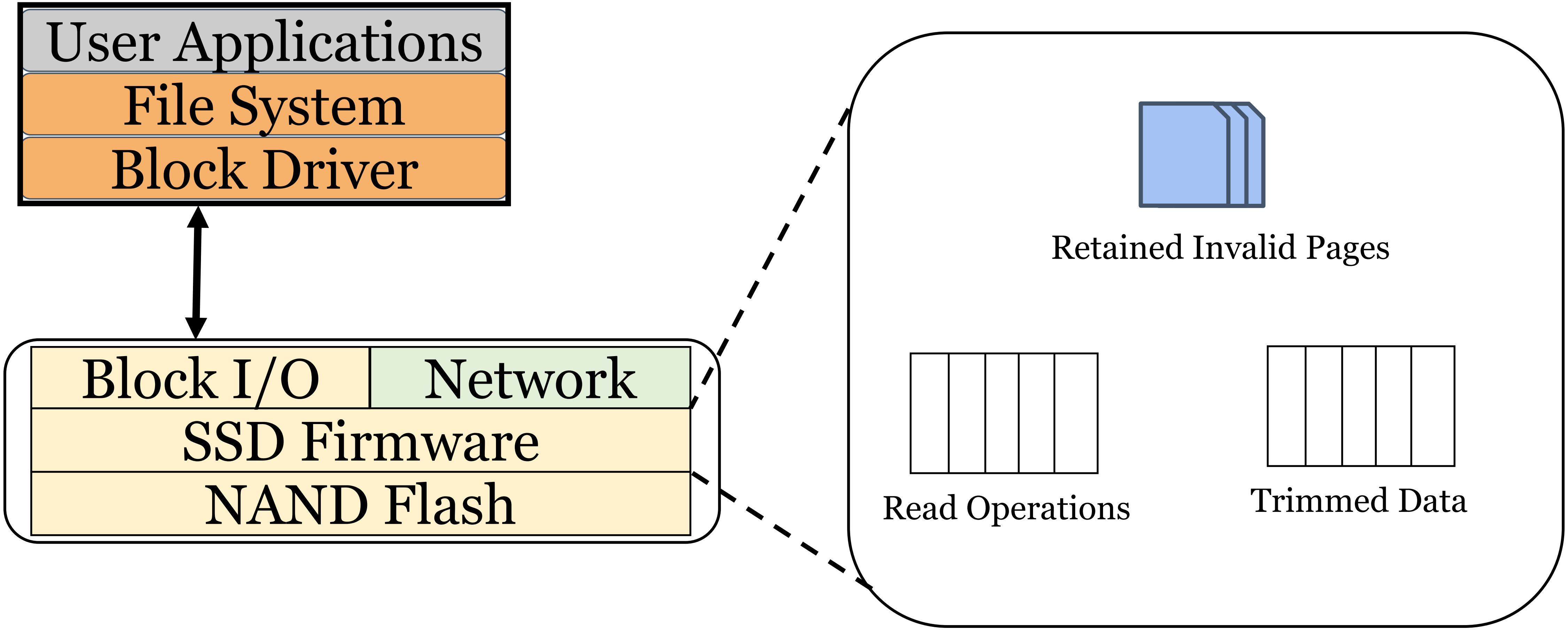
Putting It All Together



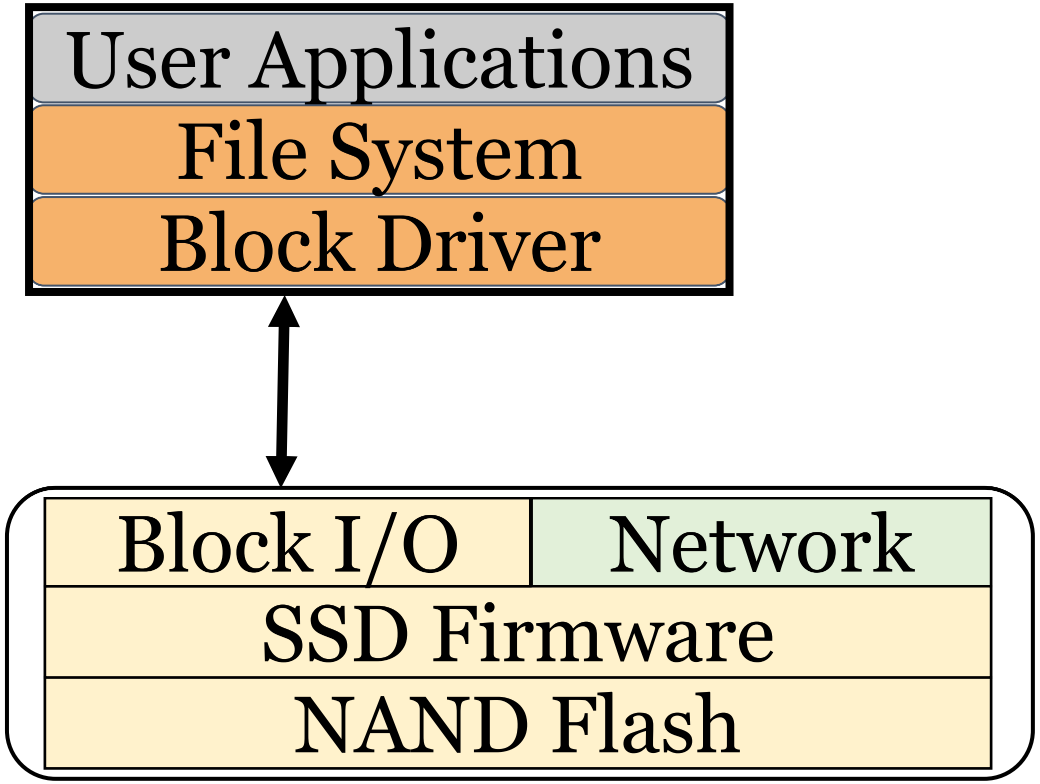
Putting It All Together



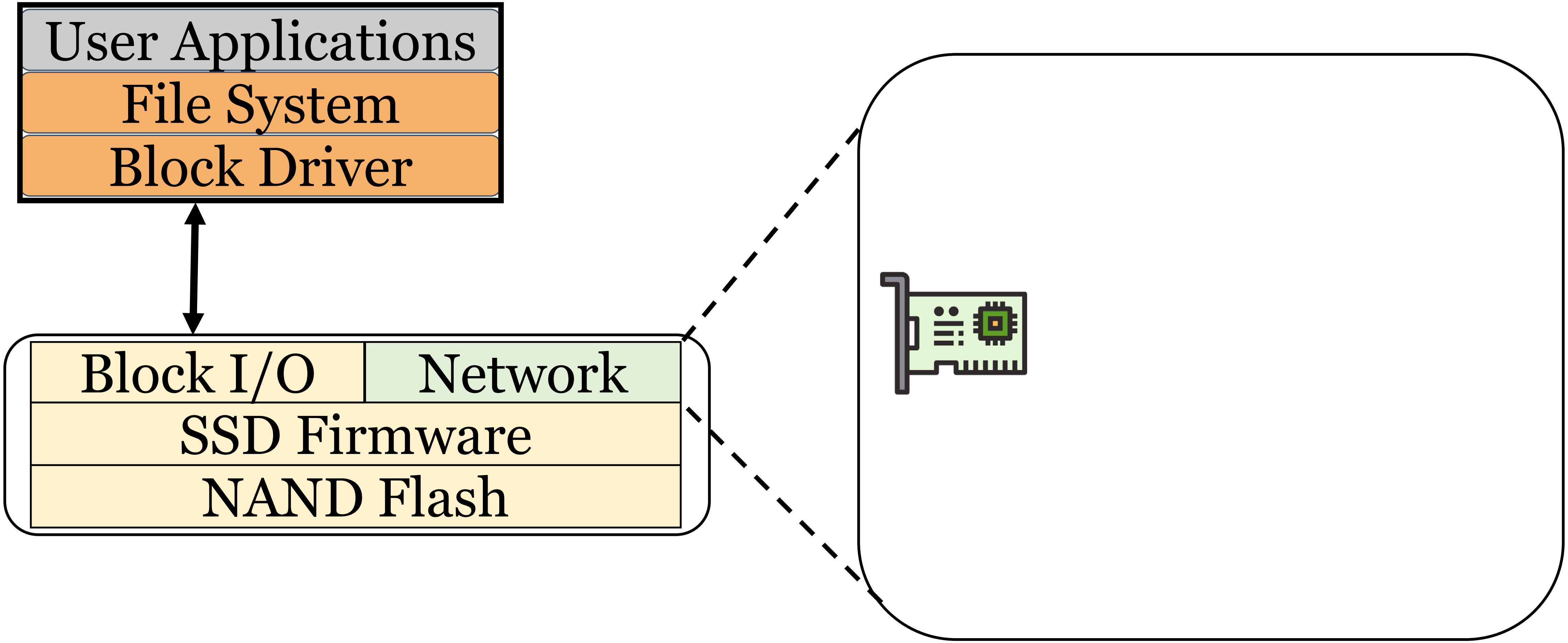
Putting It All Together



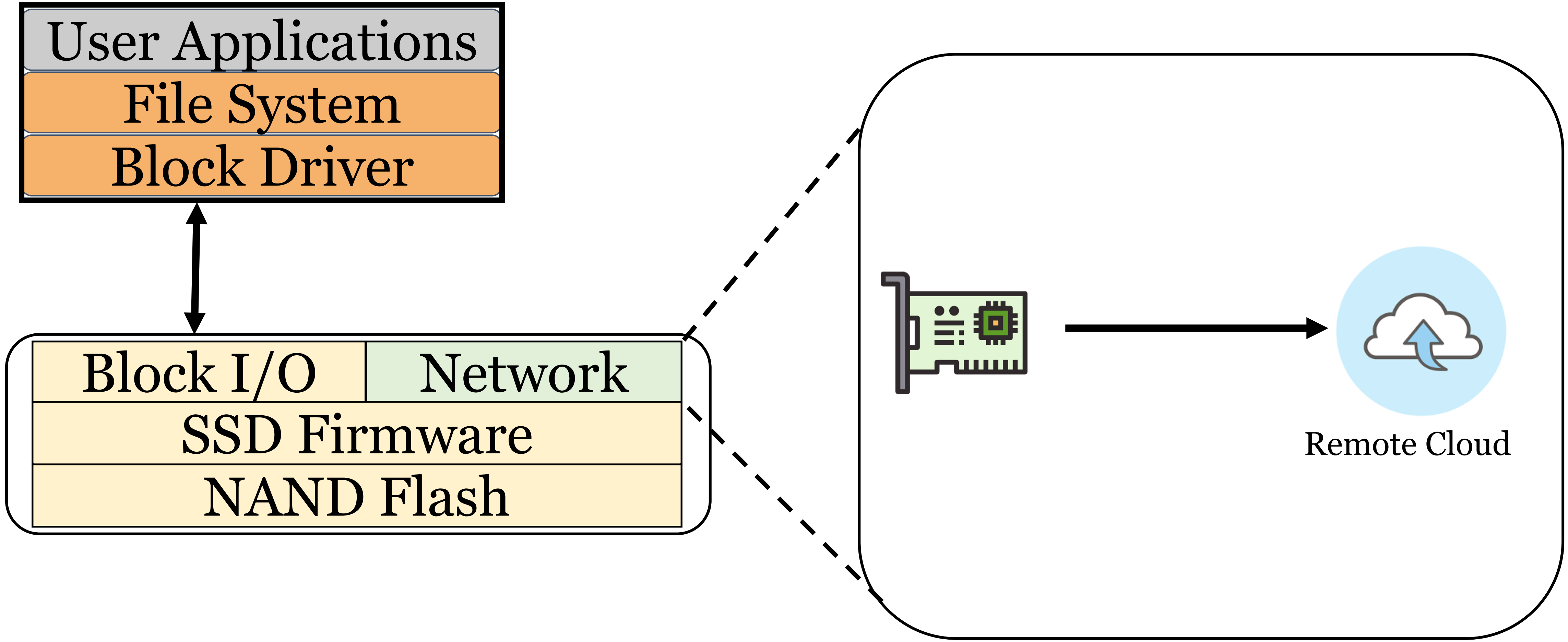
Putting It All Together



Putting It All Together



Putting It All Together



Defending Against Ransomware 2.0

Defend against GC and timing attacks

Retained data is used to recover!

Defending Against Ransomware 2.0

Defend against GC and timing attacks

Defend against trim attack

Retain trimmed data by repurposing the trimming function!

Defending Against Ransomware 2.0

Defend against GC and timing attacks

Defend against trim attack

Defend against unknown future attacks

Zero data loss recovery and trusted post-attack analysis!

RSSD Implementation

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

RSSD Implementation

Experimental Setup

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

Ransomware Samples

1,477 ransomware samples (VirusTotal)

RSSD Implementation

Experimental Setup

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

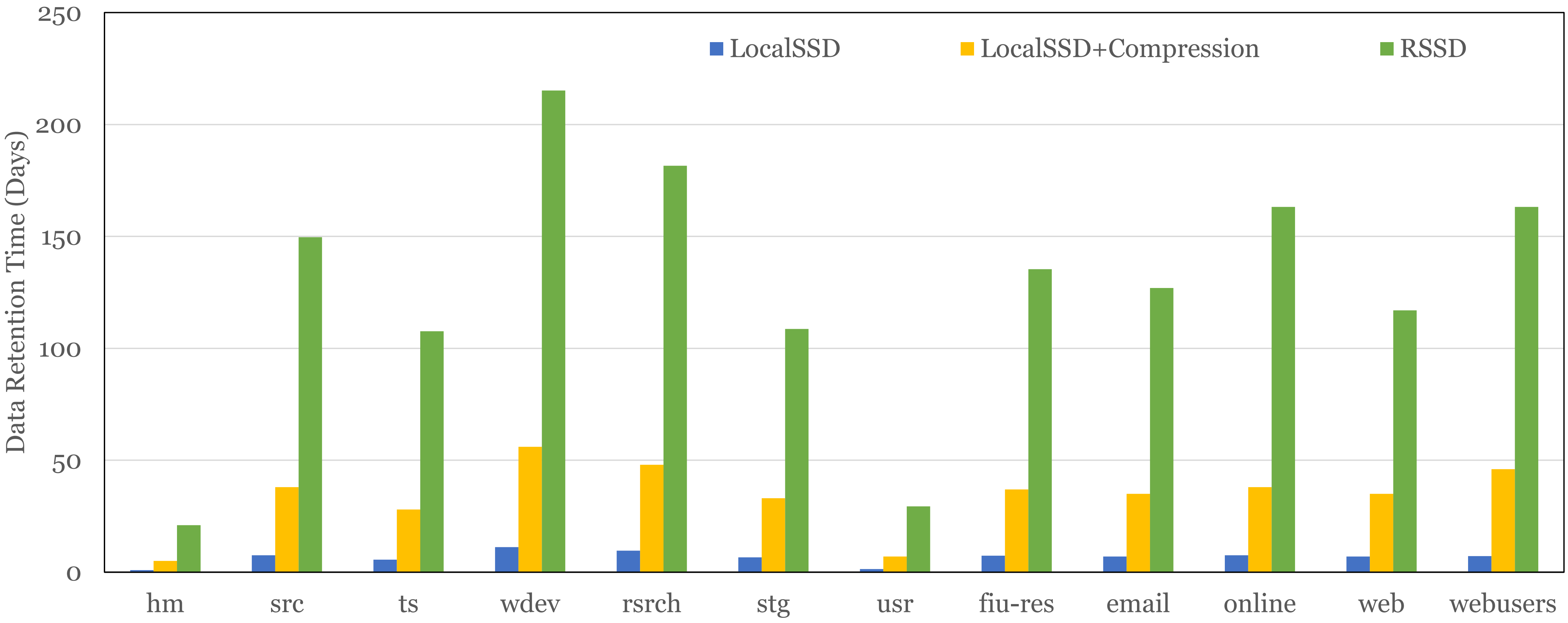
Ransomware Samples

1,477 ransomware samples (VirusTotal)

Storage Workloads

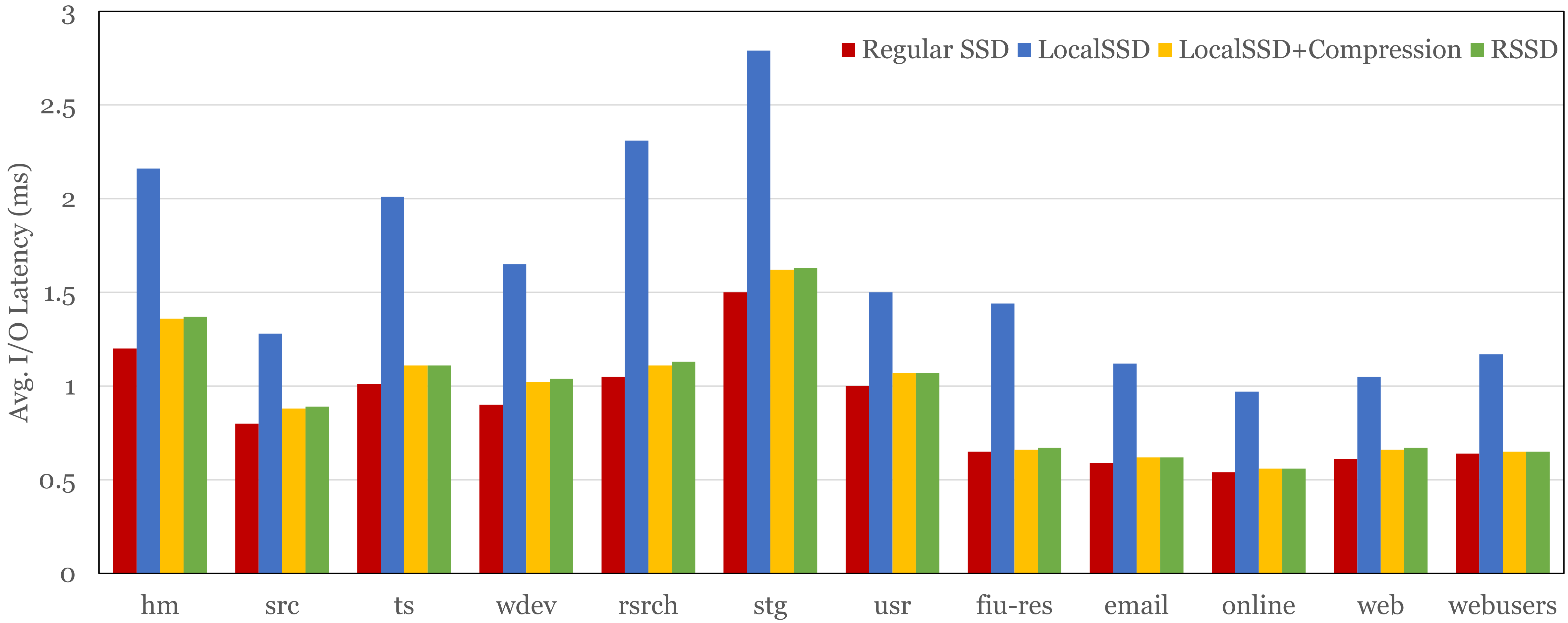
Enterprise servers (11 workloads)
University machines (6 workloads)
Storage benchmarks: IOZone/Postmark
Database workloads (TPCC/TPCE)

Impact on Data Retention Time



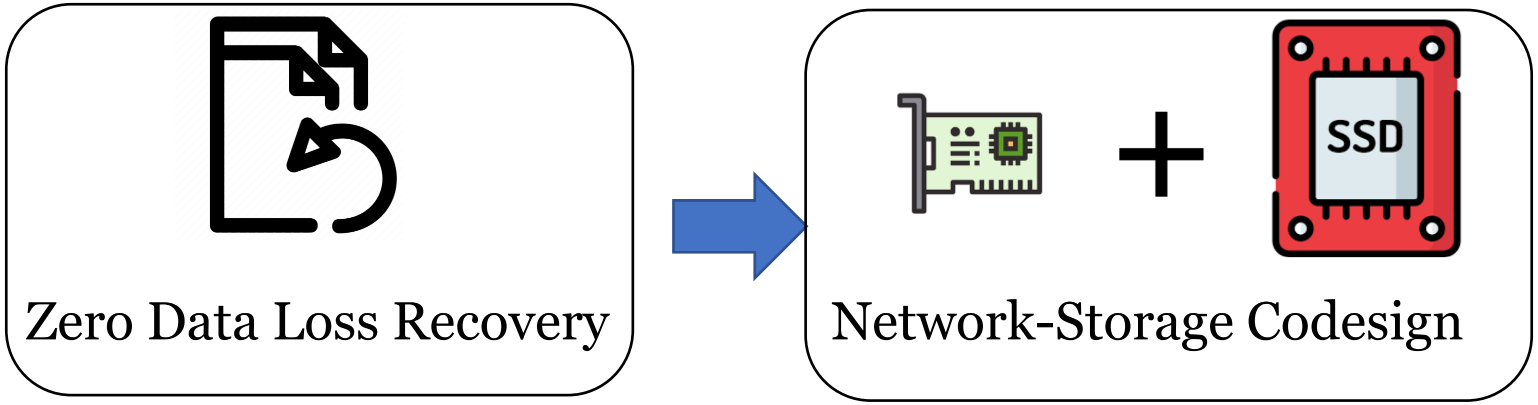
RSSD can retain data for over 200 days!

Impact on Storage Performance



RSSD introduces less than 1% performance overhead!

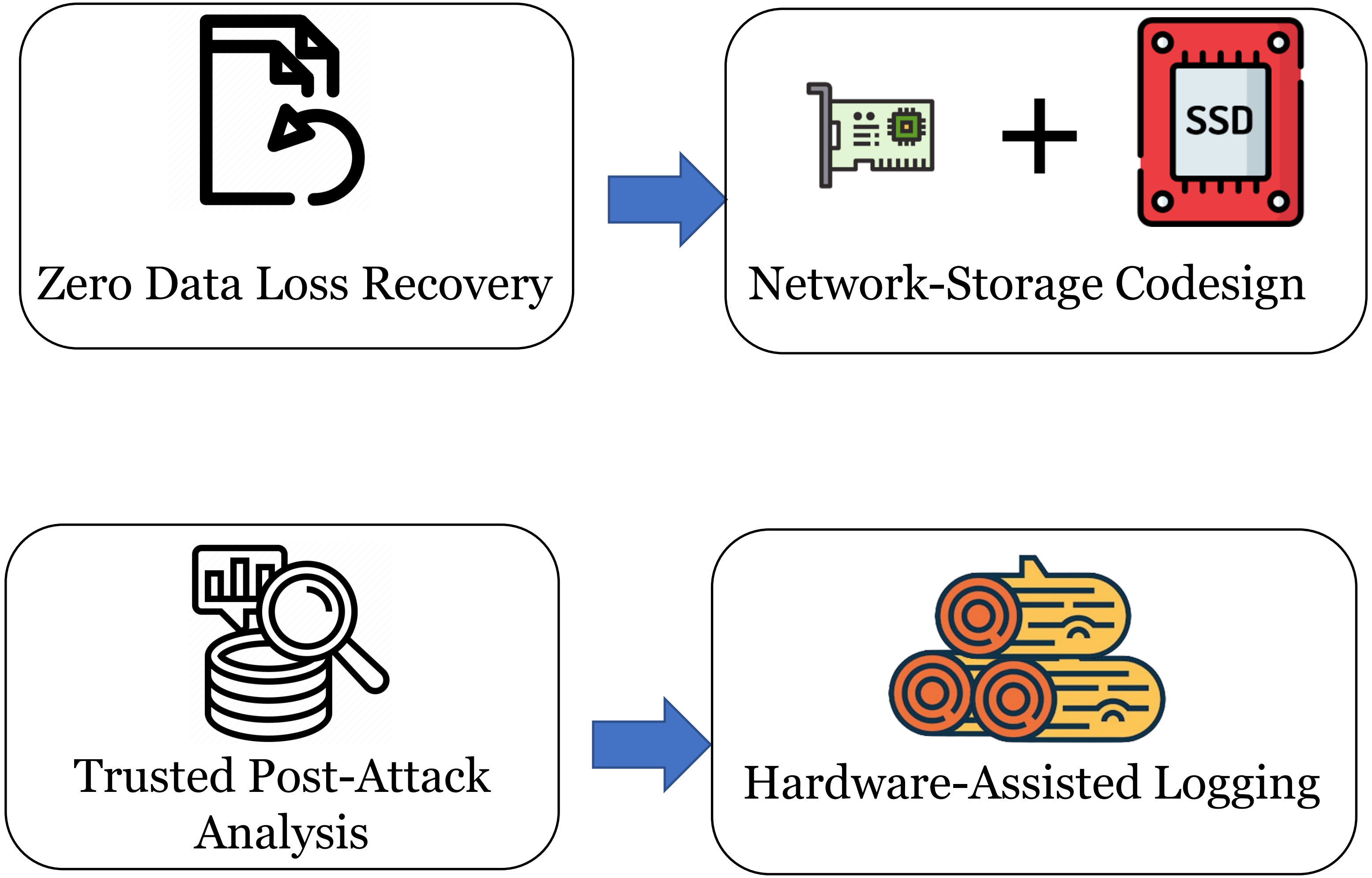
RSSD Summary



Zero Data Loss Recovery

Network-Storage Codesign

RSSD Summary



Zero Data Loss Recovery

Network-Storage Codesign

Trusted Post-Attack Analysis

Hardware-Assisted Logging

Thank You!

Benjamin Reidys, Peng Liu, Jian Huang

breidys2@illinois.edu, pxl20@psu.edu, jianh@illinois.edu

UNIVERSITY OF
ILLINOIS
URBANA-CHAMPAIGN