HETEROGENEOUS CLUSTER

- Master (INTEL NUC)
- 8 Starfive VisionFive2 RISC-V Nodes

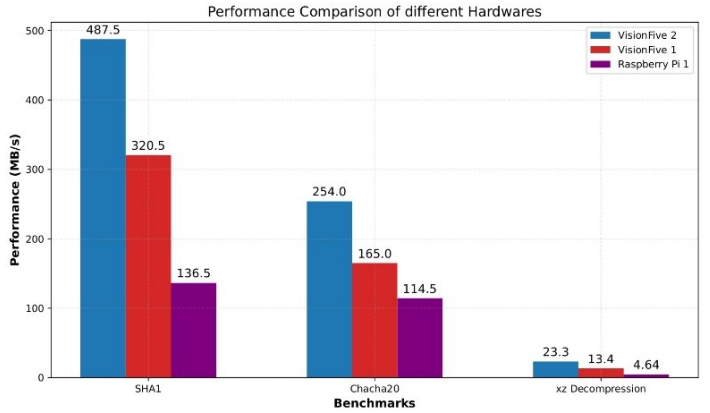
COMPARISON & BENCHMARKS

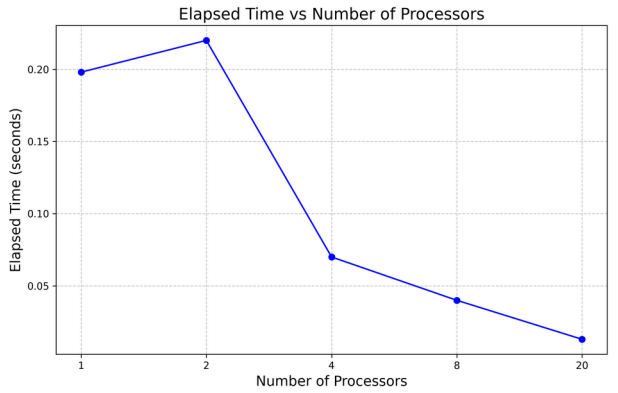
TABLE III
MONTE CARLO PI ESTIMATION RESULTS

Number of Processors	Elapsed time	Estimated Value
1	0.198 seconds	3.141532
2	0.220 seconds	3.143832
4	0.070 seconds	3.140976
8	0.040 seconds	3.141000
20	0.013 seconds	3.141530

TABLE II
PERFORMANCE COMPARISON

Hardware	SHA1 (MB/s)	Chacha20 (MB/s)	xz Decompression
VisionFive2	487.5	254.0	23.3
VisionFive1	320.5	165.0	13.4
Raspberry Pi 1	136.5	114.5	4.64



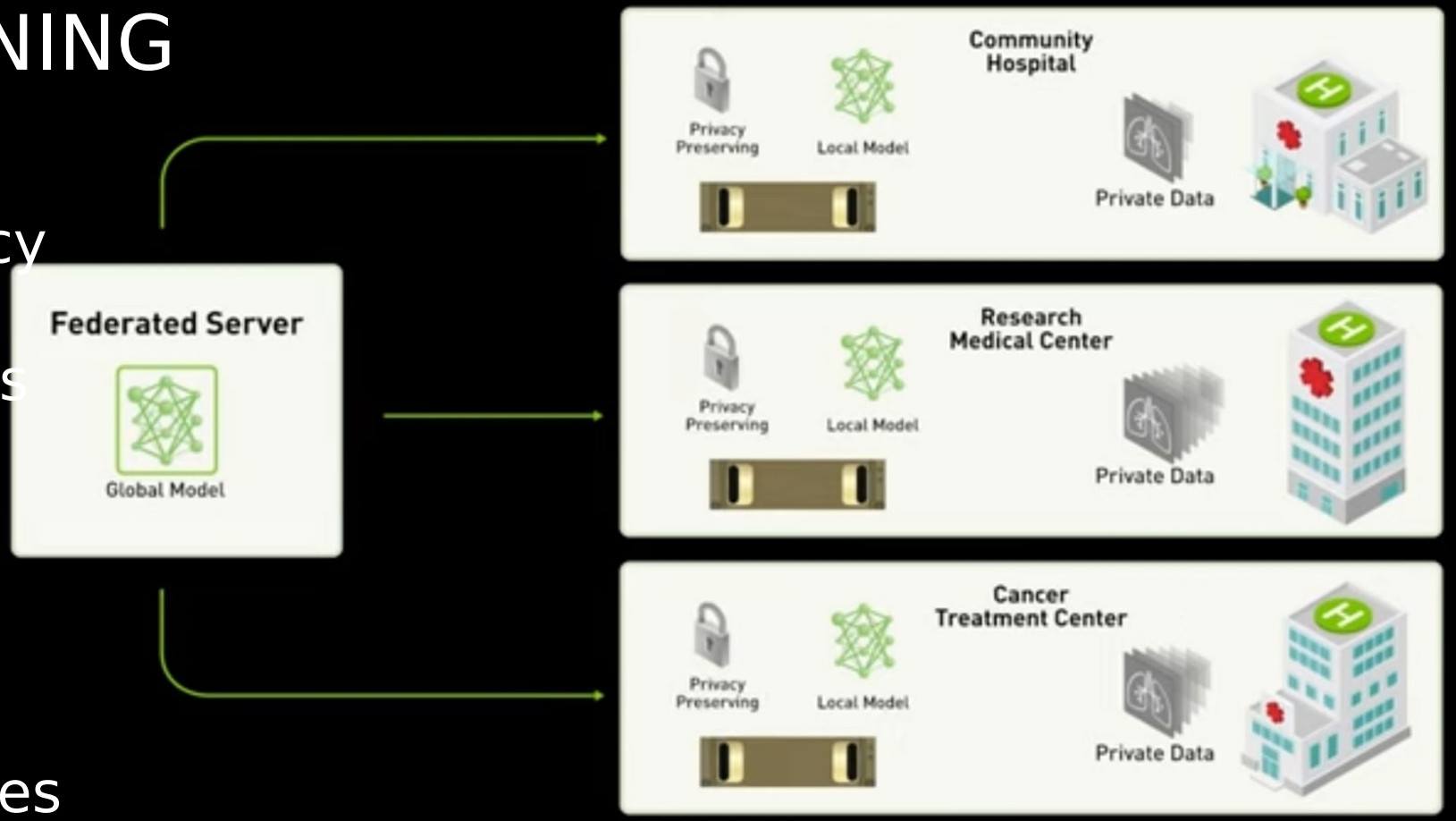


FEDERATED LEARNING

- Enhanced Privacy
- Bandwidth Efficiency
- Scalability
- Personalized Models

Use Cases:

- Healthcare
- Finance
- Smart Devices
- Autonomous Vehicles
- Retail



Federated Learning in our Heterogeneous Cluster

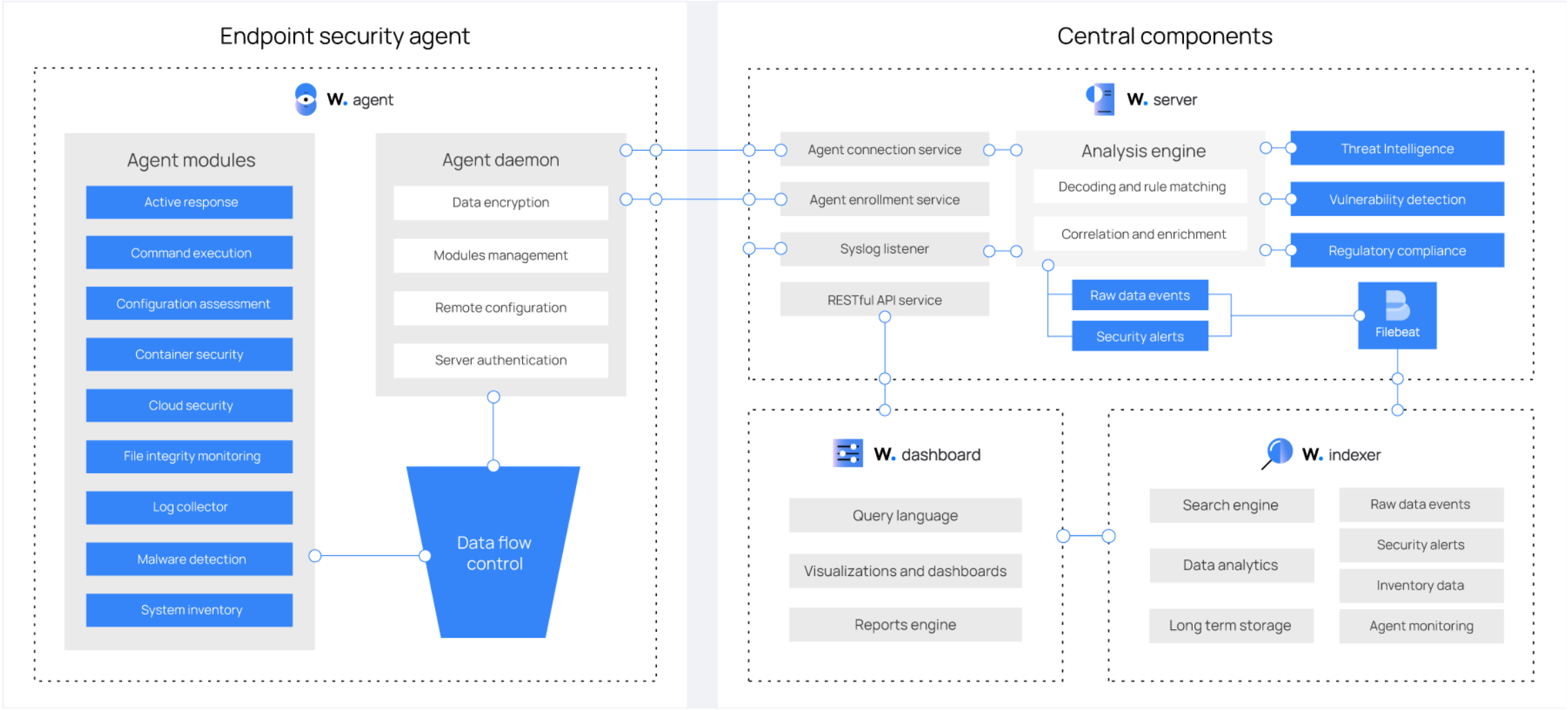
Global Model Prediction

```
[0.2743351  0.32396628 0.32396628 0.28159331 0.27434259 0.274335
 0.27434636 0.32396623 0.2743549  0.32396628 0.28455367 0.32379316
 0.32396628 0.27818714 0.27526988 0.32396628 0.27507644 0.32368501
 0.32396628 0.32396628 0.32396628 0.32396628 0.32396628 0.32396628
 0.274335   0.32396628 0.29648179 0.32396628 0.30986975 0.32396544
 0.27433627 0.2919739  0.32396628 0.32396628 0.32396628 0.30697051
 0.27433536 0.274335   0.28676772 0.274335   0.27437508 0.32396628
 0.274335   0.32396628 0.27482303 0.2743354  0.3239636  0.32234898
 0.3168088  0.27433514 0.32396628 0.27565298 0.2758254  0.33188186
 0.27435272 0.27461465 0.27476665 0.27468193 0.27440081 0.32396628
 0.28133734 0.27433505 0.28464681 0.32396628 0.29104265 0.32396628
 0.274335   0.29008198 0.32396628 0.29936989 0.27436069 0.28573137
 0.28365435 0.2743354  0.32396628 0.27437222 0.27433509 0.27433506
 0.32396628 0.32396627 0.27433753 0.32327231 0.28743212 0.32396626
 0.28324394 0.3317465  0.32396628 0.32396628 0.27479913 0.27484739
 0.27433768 0.27438793 0.27434589 0.32396626 0.27434923 0.32396628
 0.32396624 0.27434409 0.27434067 0.274335   0.32295151 0.2898177
 0.32396628 0.32396628 0.274335   0.2743358  0.32396628 0.27444617
 0.27467004 0.32396628 0.32396628 0.32388224 0.27433579 0.32396417
 0.29564856 0.32396628 0.28742808 0.32396628 0.32396608 0.32396628
 0.32396628 0.32273236 0.27443707 0.32396628 0.32396441 0.27433653
 0.32396628 0.32396628 0.32396581 0.27438121 0.32396628 0.32396628
 0.32396628 0.32396628 0.32396628 0.32396628 0.27514036 0.31833963
 0.27436374 0.31133979 0.30726175 0.27434379 0.27434491 0.2743352
 0.32396628 0.32160899 0.3229369  0.27983575 0.32396628 0.29539794
 0.32396628 0.32396628 0.32396628 0.32396628 0.32396628]
Accuracy: 62.58%
```

WAZUH

- An Open-source Security Information and Even Management (SIEM) system.
- Provides centralized logging, monitoring, and analysis of security events.
- Detects and responds to threats in real-time.

WAZUH


Endpoint security agent
W. agent
Agent modules
Active response
Command execution
Configuration assessment
Container security
Cloud security
File integrity monitoring
Log collector
Malware detection
System inventory
Agent daemon
Data encryption
Modules management
Remote configuration
Server authentication
Data flow control
Central components
W. server
Agent connection service
Agent enrollment service
Syslog listener
RESTful API service
Analysis engine
Decoding and rule matching
Correlation and enrichment
Threat Intelligence
Vulnerability detection
Regulatory compliance
Raw data events
Security alerts
Filebeat
W. dashboard
Query language
Visualizations and dashboards
Reports engine
W. indexer
Search engine
Data analytics
Long term storage
Raw data events
Security alerts
Inventory data
Agent monitoring

WAZUH

Wazuh Agent:

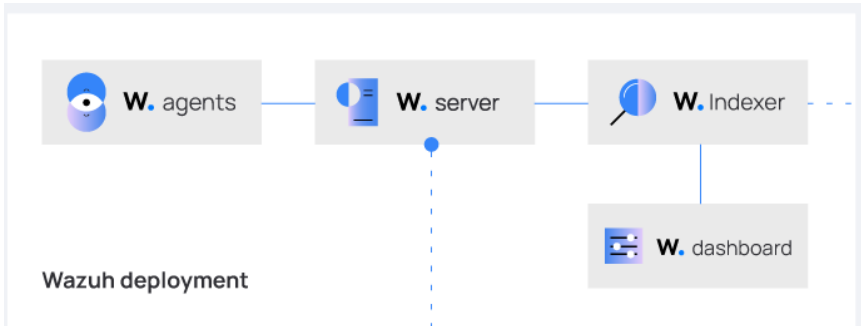
- Lightweight agent on endpoints (servers/workstations) collects logs, monitors security events, and reports to the Wazuh server.

Wazuh Server:

- Central hub analyzes logs/events for threats, generates alerts, manages agents, and monitors their health.

Wazuh Indexer:

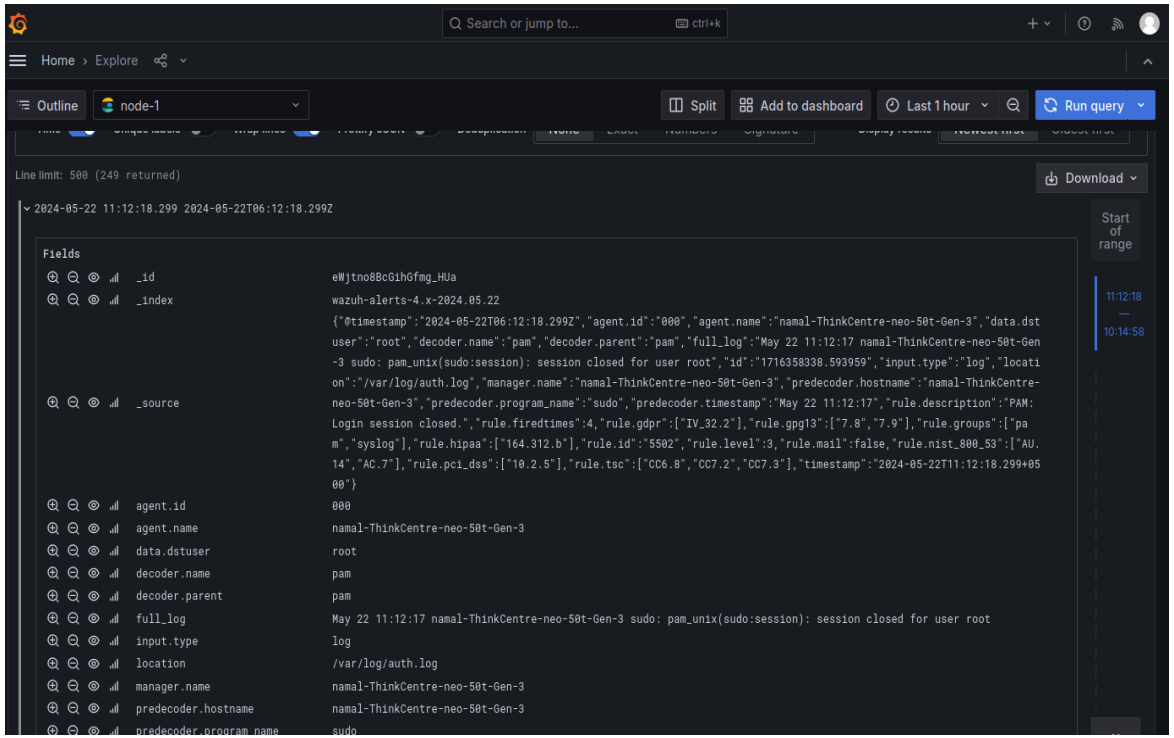
- High-performance storage efficiently stores and indexes logs/events for historical analysis and trend identification.



WAZUH

Wazuh agent deployed at master node of the heterogenous cluster.

SNORT



- An open-source intrusion detection system (IDS) and intrusion prevention system (IPS).
- Monitors network traffic for suspicious activity.

Why Integrate Snort with Wazuh?

- Enhances threat detection capabilities.
- Provides detailed network traffic analysis.
- Correlates Snort alerts with other security data in Wazuh.

GRAFANA

- An open-source platform for monitoring and observability.
- Supports diverse data sources, including Elasticsearch, Prometheus, and more.

Why Use Grafana with Wazuh?

- Provides advanced data visualization capabilities.
- Customizable dashboards for real-time monitoring.
- Enhances the ability to analyze security metrics and trends.