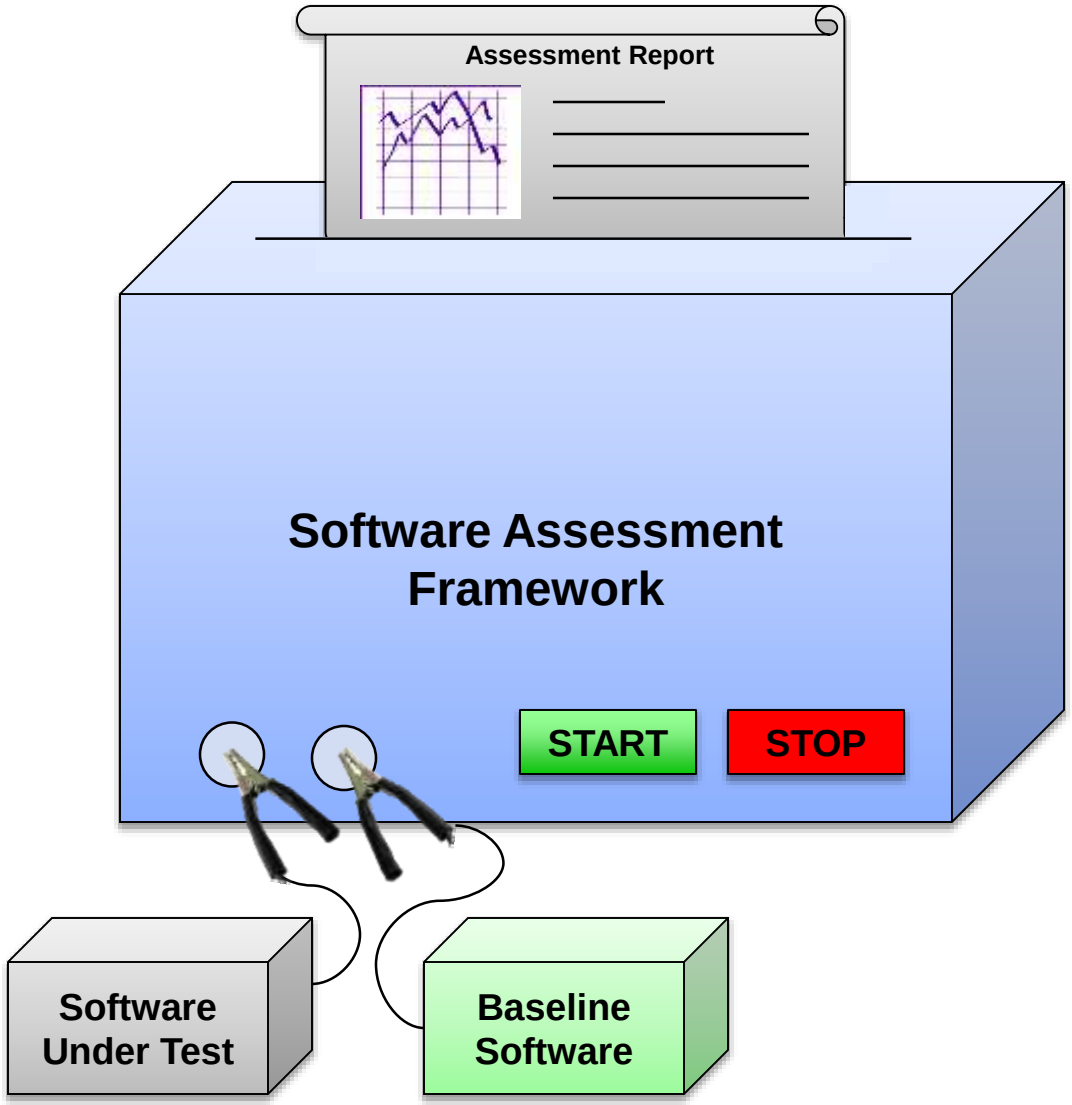
Automated Assessment of Secure Search Systems

Nicholas Hwang
on behalf of the MIT LL SPAR T&E Team

nicholas.hwang@ll.mit.edu
spar-lincoln@ll.mit.edu

October 7, 2014

How Should We Assess Software?



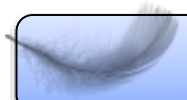
Software T&E Mantras

Black box treatment of systems

End-to-end automation

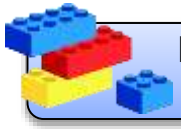
Test-time agility

Real-time status reports



Minimal system overhead

Repeatability



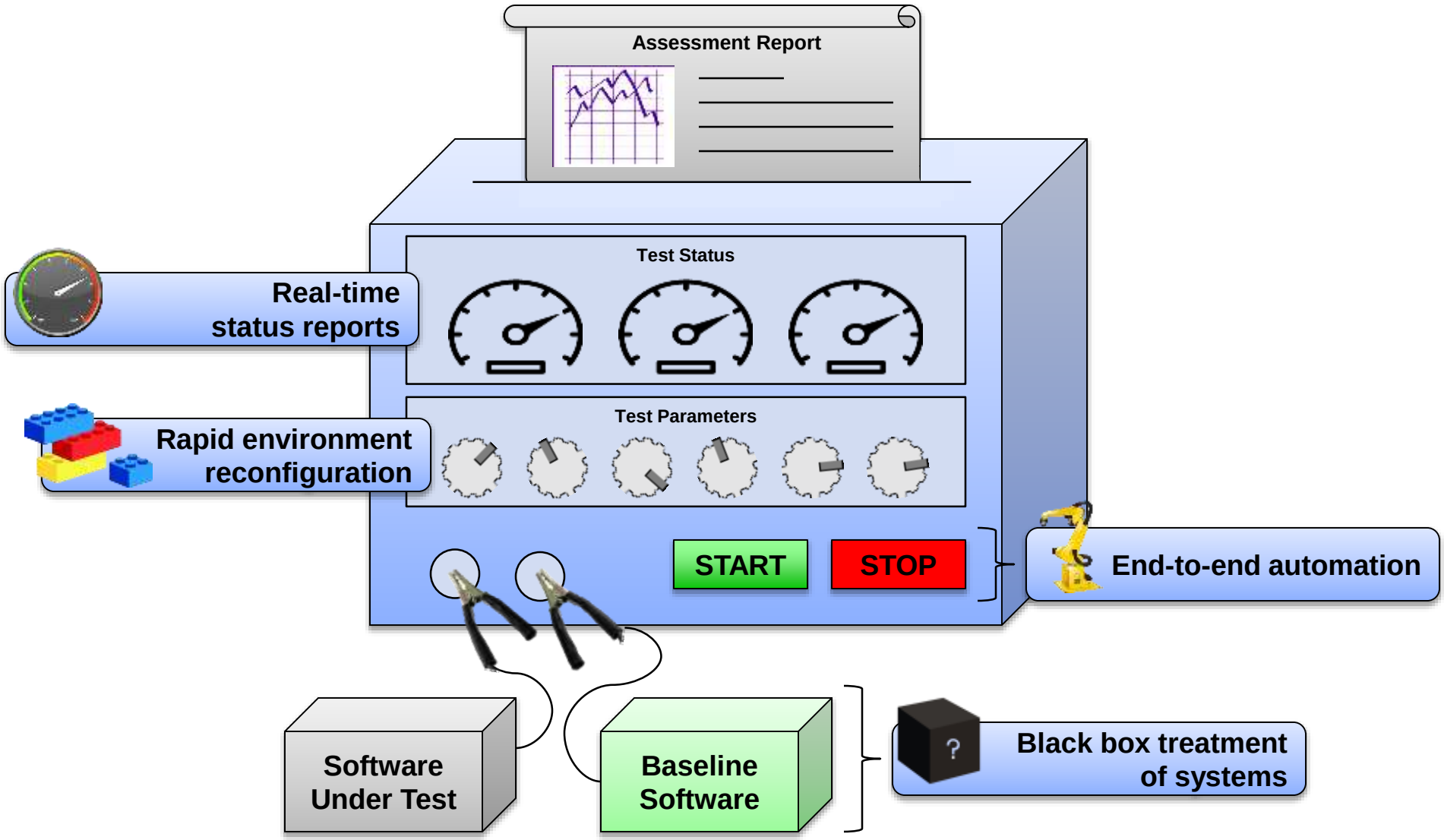
Rapid environment reconfiguration

Extensibility

Comprehensive data capture

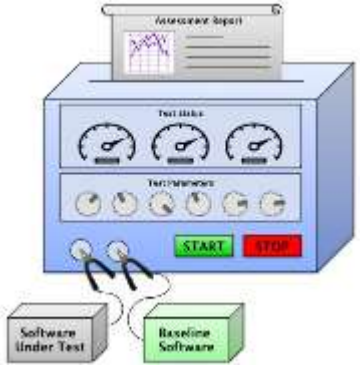
Reusability

Incorporating Software T&E Mantras



Our Contributions

Mantras for Effectively Performing Effective Software Assessments



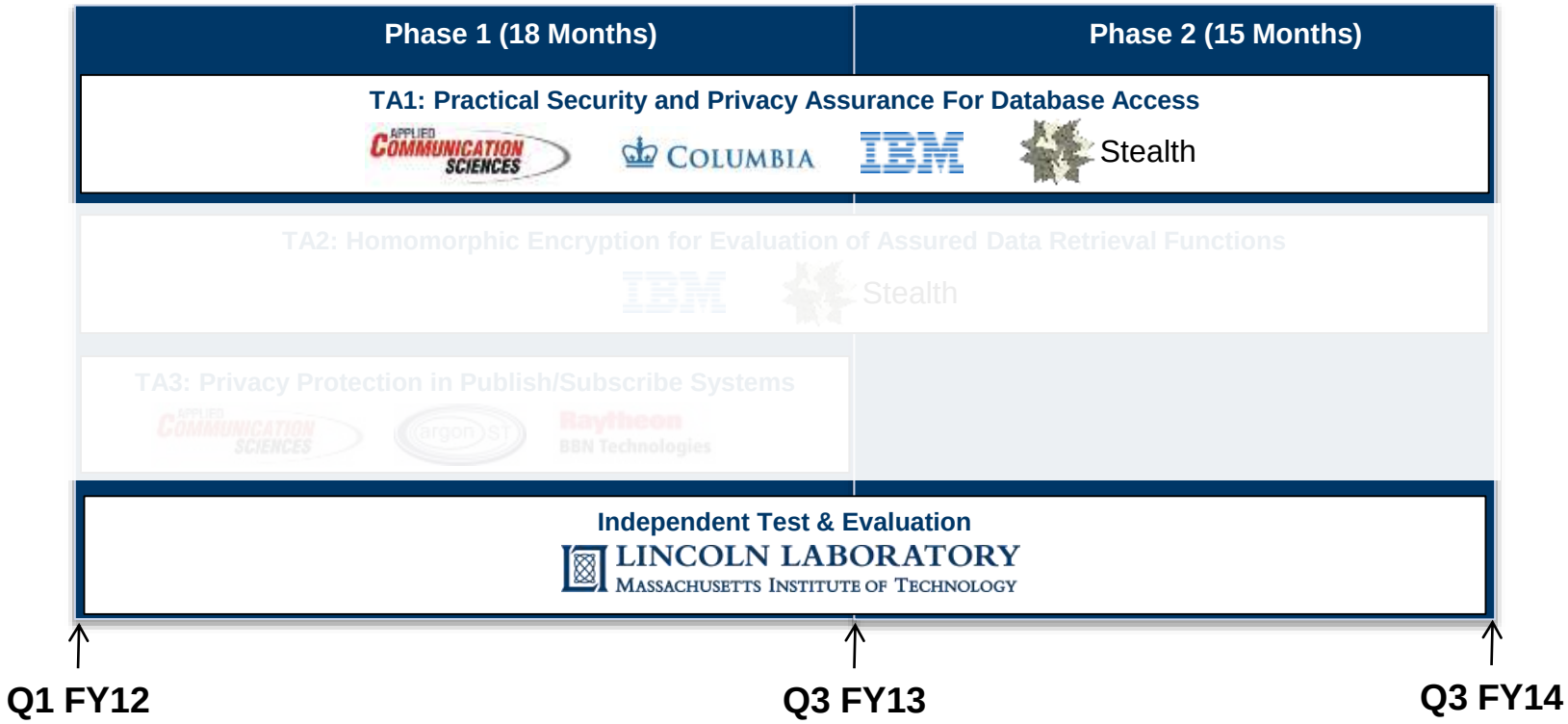
An Exemplar Software Assessment Framework

GitHub

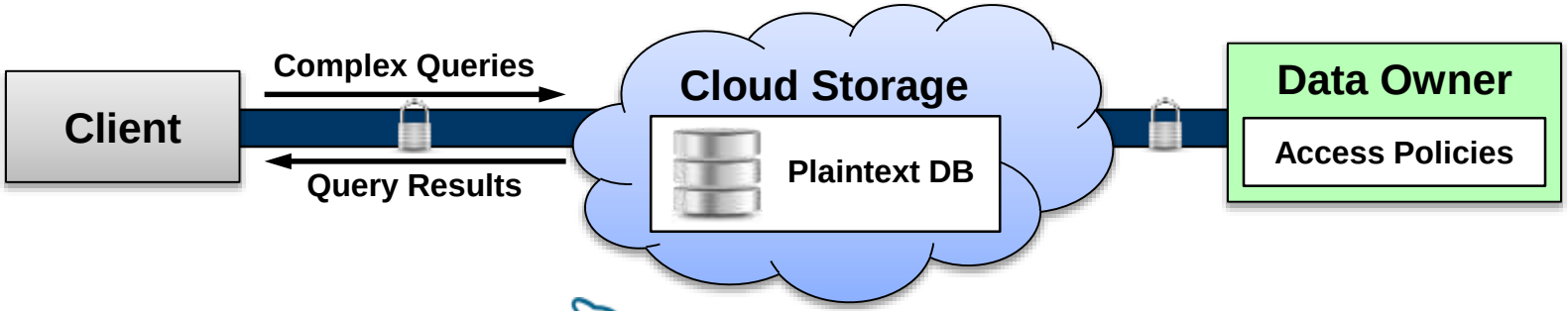
https://github.com/mitll-csa/sparta

T&E Case Study: SPAR

- **Security and Privacy Assurance Research (SPAR)**
- **IARPA-funded program, managed by W. Konrad Vesey**
- **Nine research teams in three Technical Areas (TAs)**



Traditional Database Systems

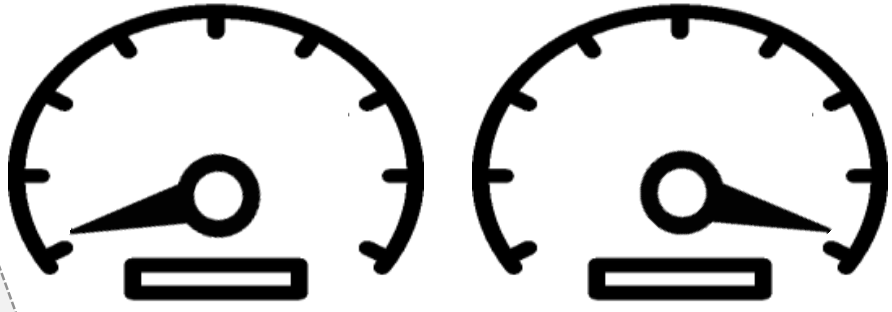


MySQL ORACLE PostgreSQL SQL Server 2014 IBM DB2

Client learns:
- Access policies

Cloud learns:
- Access policies
- Queries
- Query results
- Query access patterns

Owner learns:
- Queries
- Query results
- Query access patterns

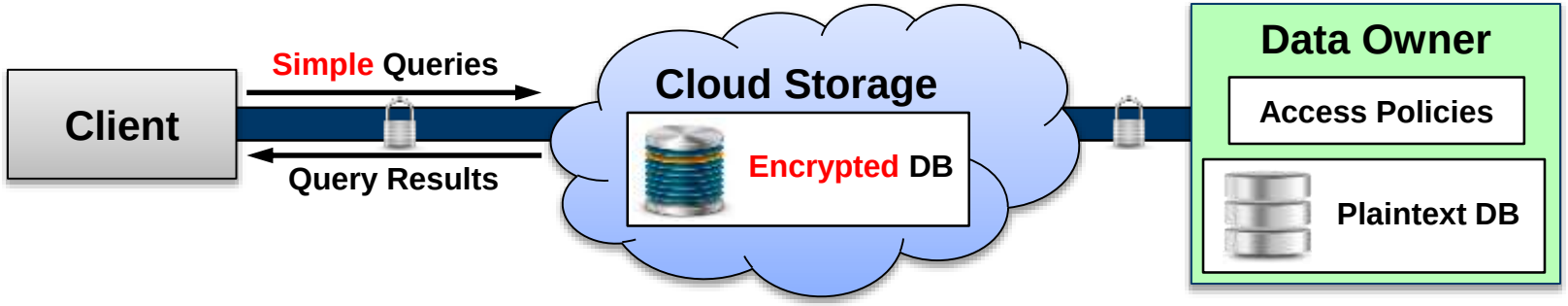


Security and Privacy Guarantees

Operation Speed

COTS products optimized for speed, not security or privacy.

Theoretical SPIR Database Systems



Client learns:
- ~~Access policies~~

Cloud learns:
- ~~Access policies~~
- ~~Query~~
- ~~Query results~~
- Query access patterns

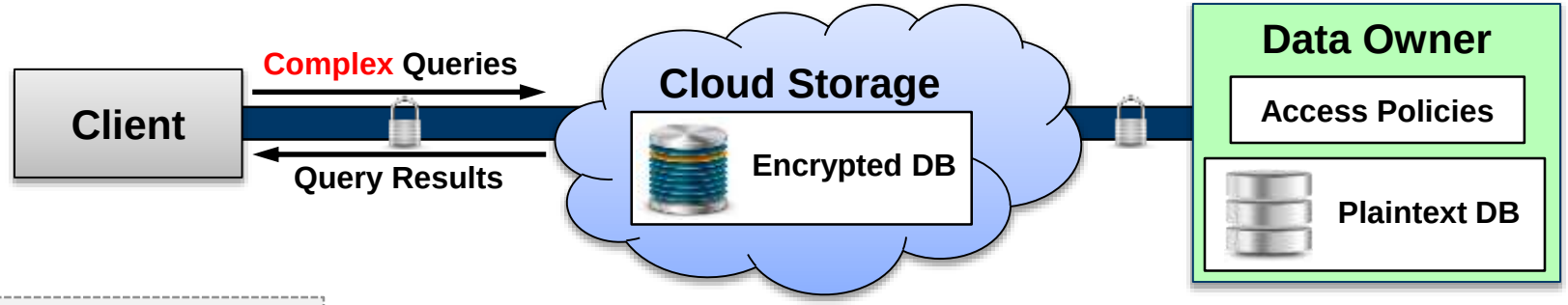
Owner learns:
- ~~Query~~
- ~~Query results~~
- ~~Query access patterns~~

Security and Privacy Guarantees

Operation Speed

SPIR achieves security and privacy, but is impractical and slow.

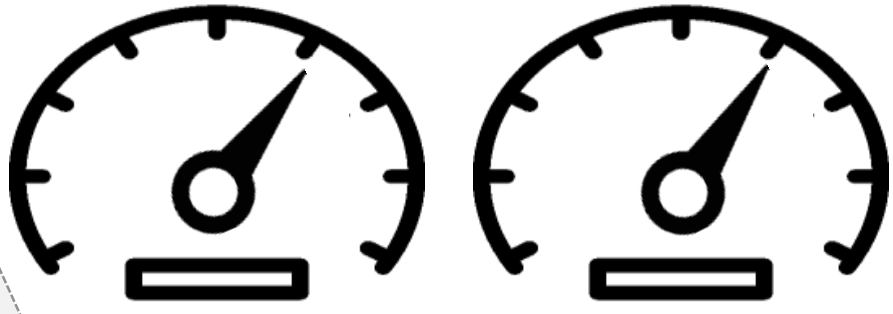
SPAR Database System Goals



Client learns:
- ~~Access policies~~

Cloud learns:
- ~~Access policies~~
- ~~Query~~
- Query structure
- ~~Query results~~
- Result set size
- Query access patterns

Owner learns:
- ~~Query~~
- ~~Query results~~
- ~~Query access patterns~~

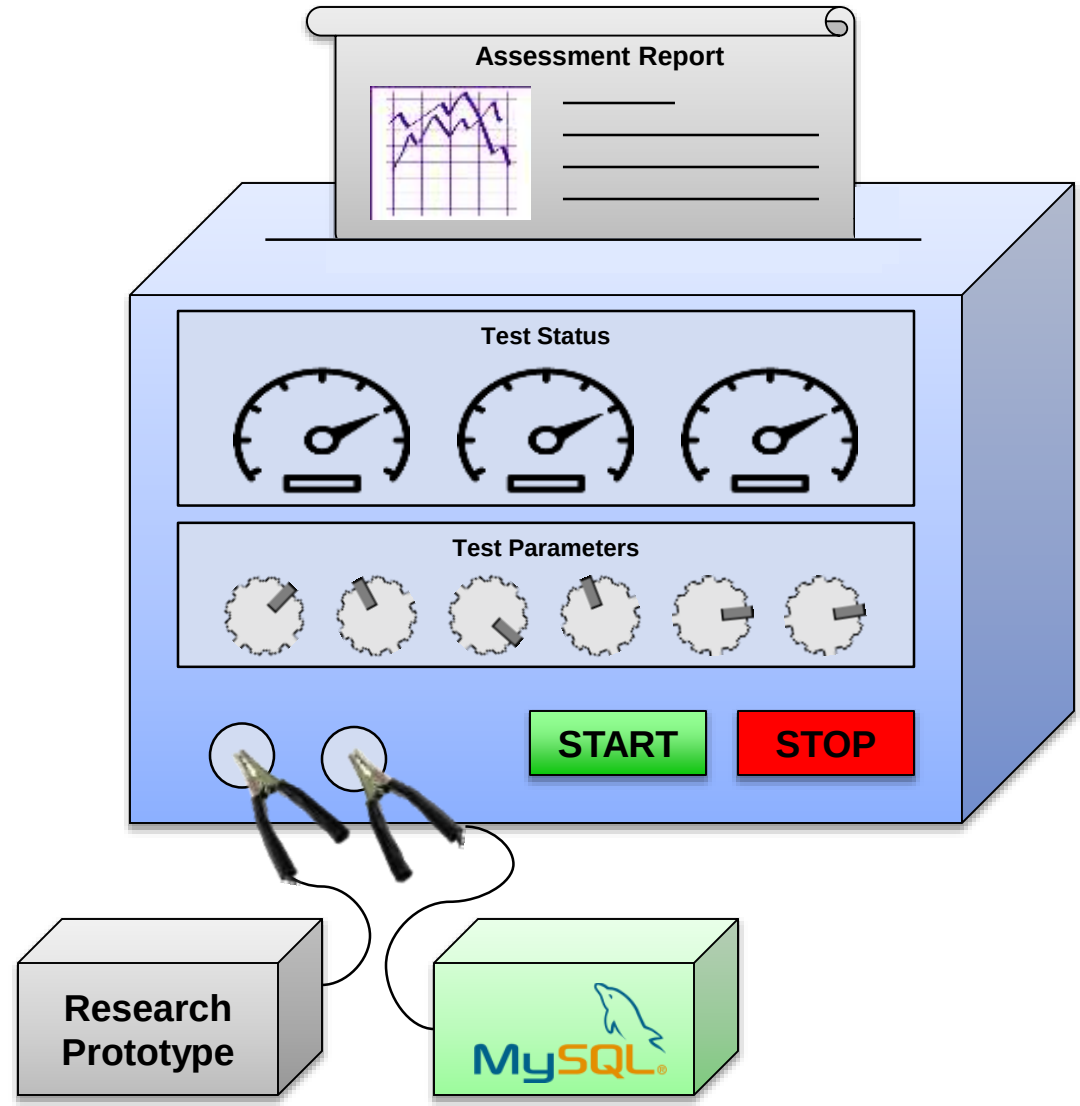


Security and Privacy Guarantees

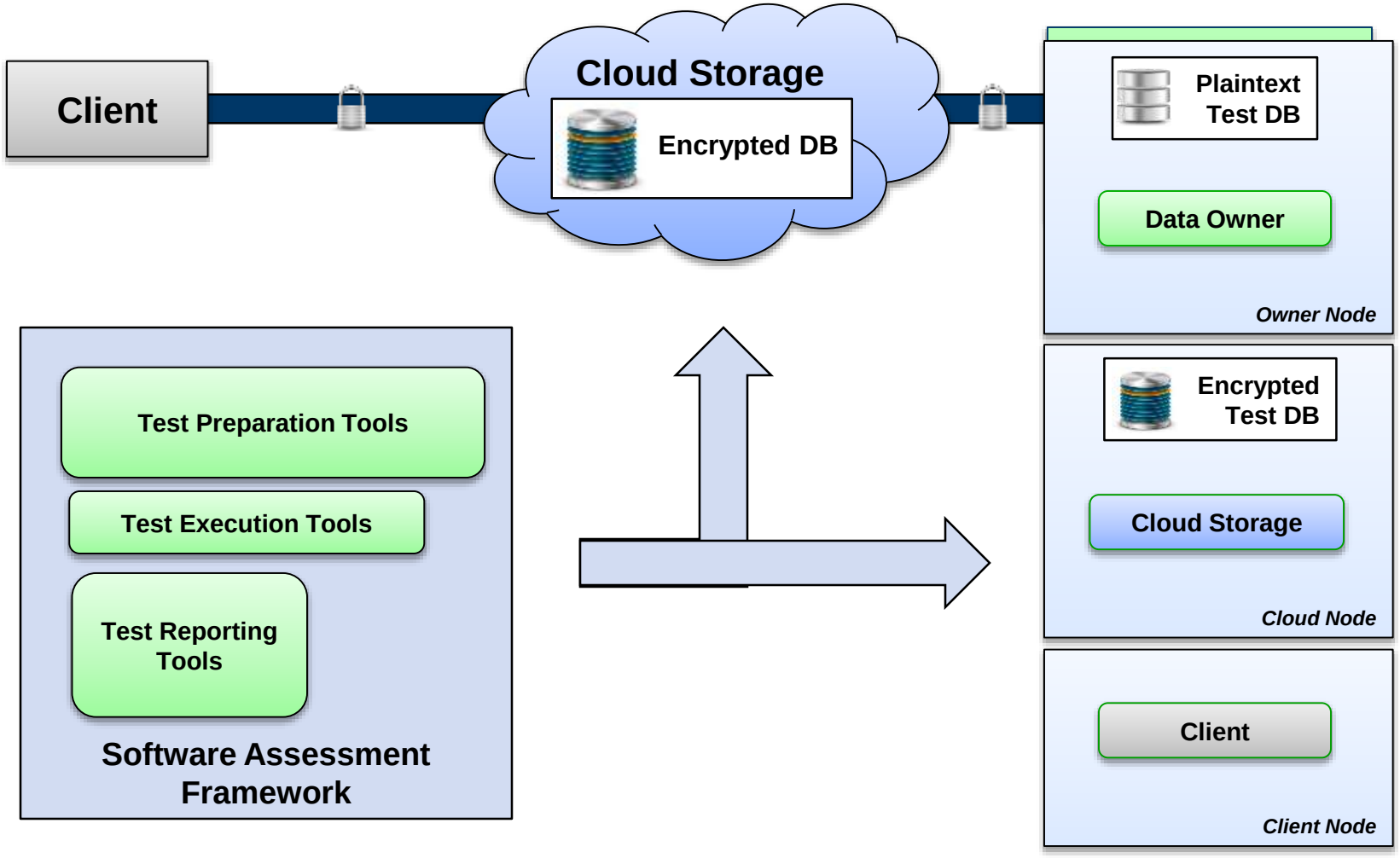
Operation Speed

SPAR systems achieve a practical balance between security, privacy, and performance.

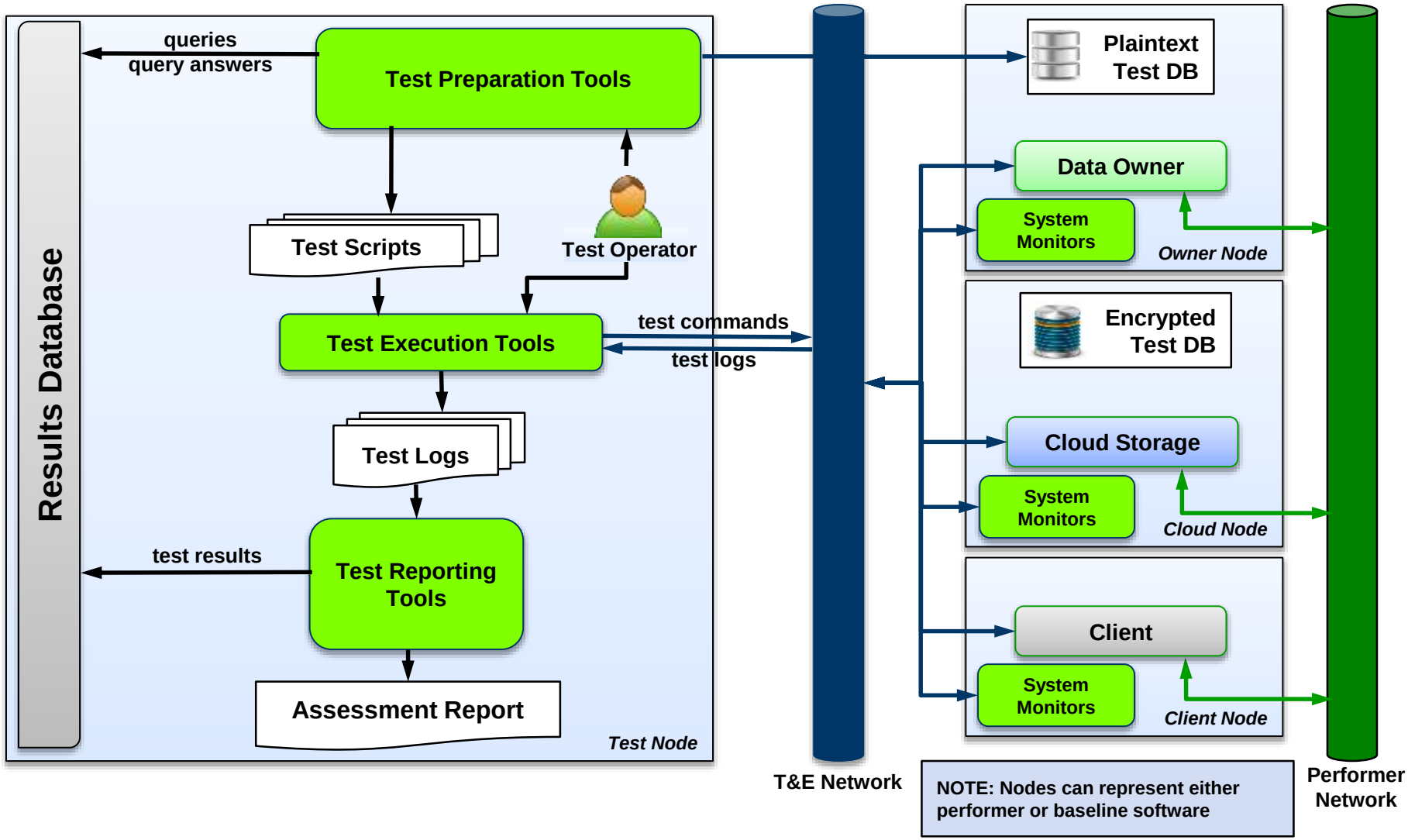
Lincoln's T&E Role



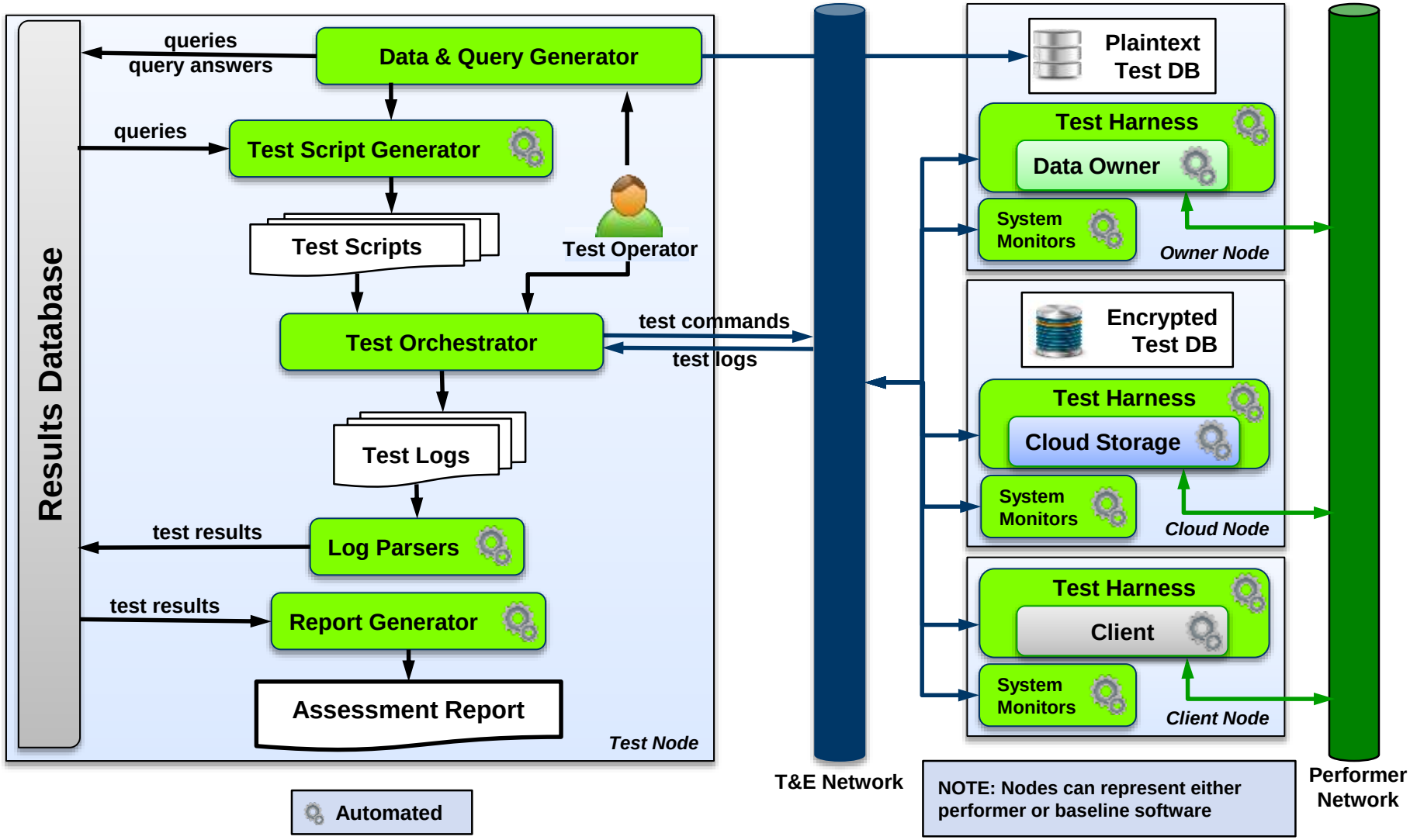
Assess SPAR research prototypes for correctness, functionality, and performance


Client
Cloud Storage
Encrypted DB
Plaintext
Test DB
Data Owner
Owner Node
Test Preparation Tools
Test Execution Tools
Test Reporting
Tools
Software Assessment
Framework
Encrypted
Test DB
Cloud Storage
Cloud Node
Client
Client Node

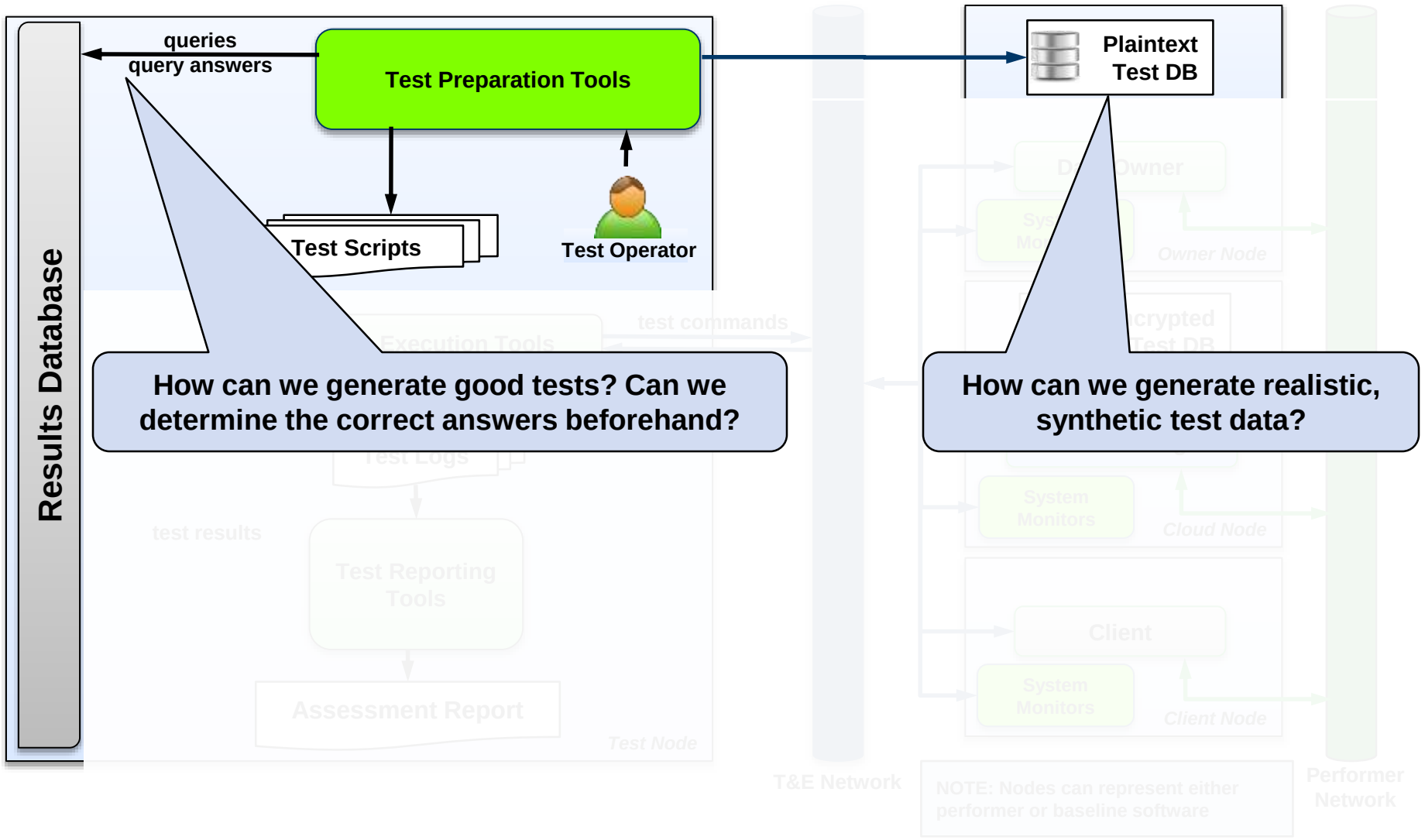
Notional Assessment Framework



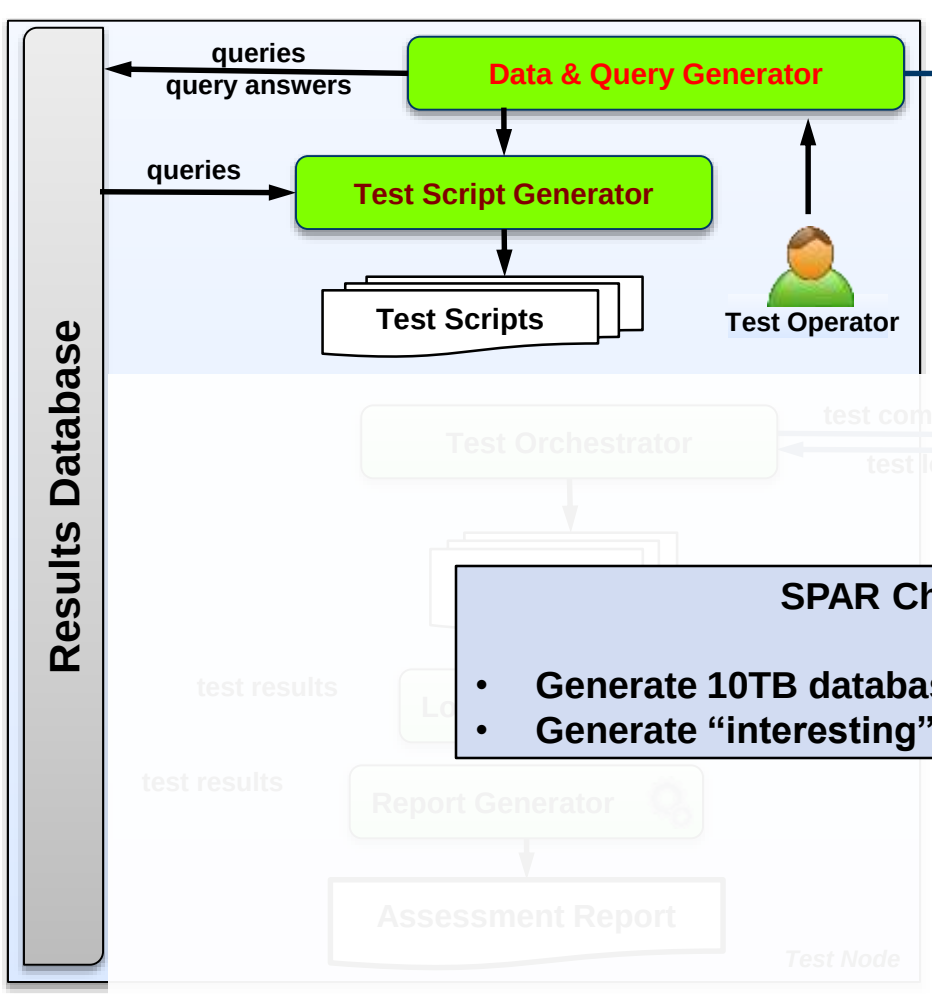
Our Assessment Framework



Common Test Preparation Challenges



Our Test Preparation Tools



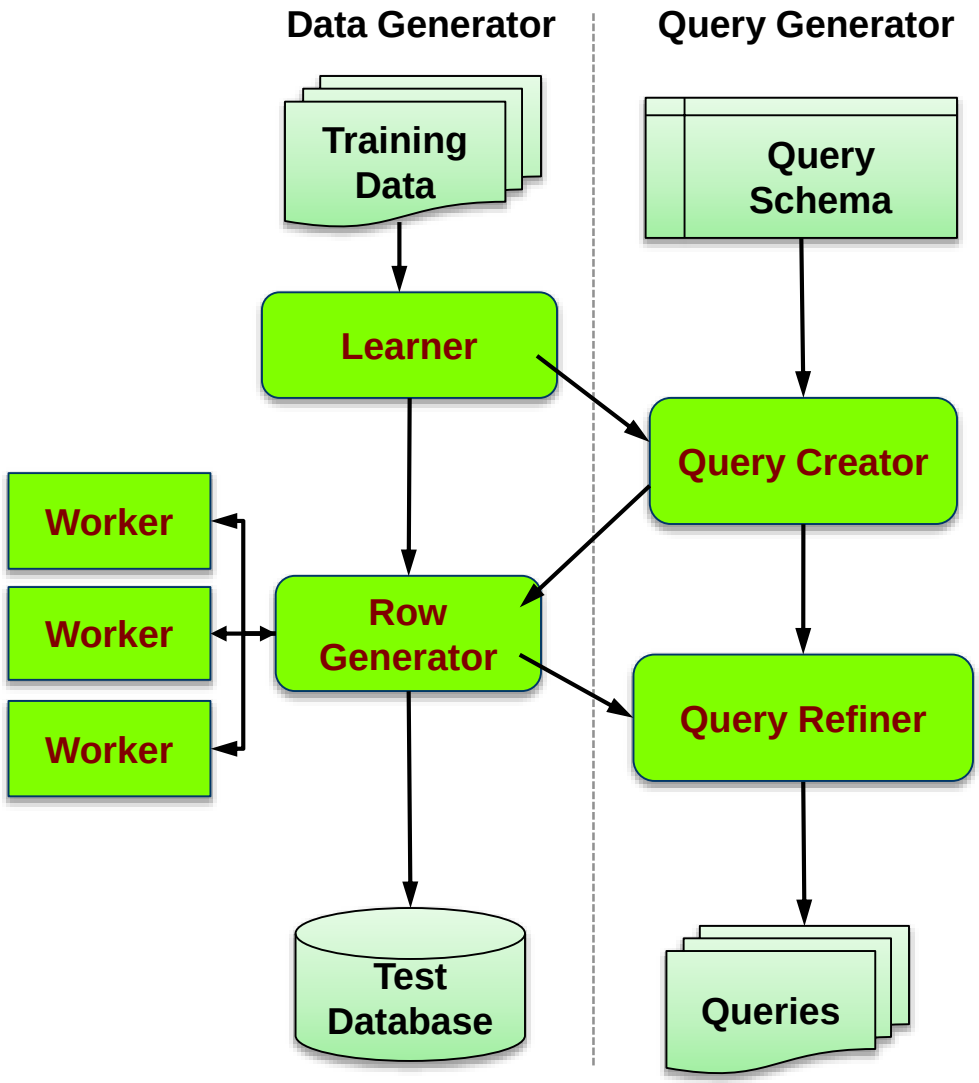
SPAR Challenges

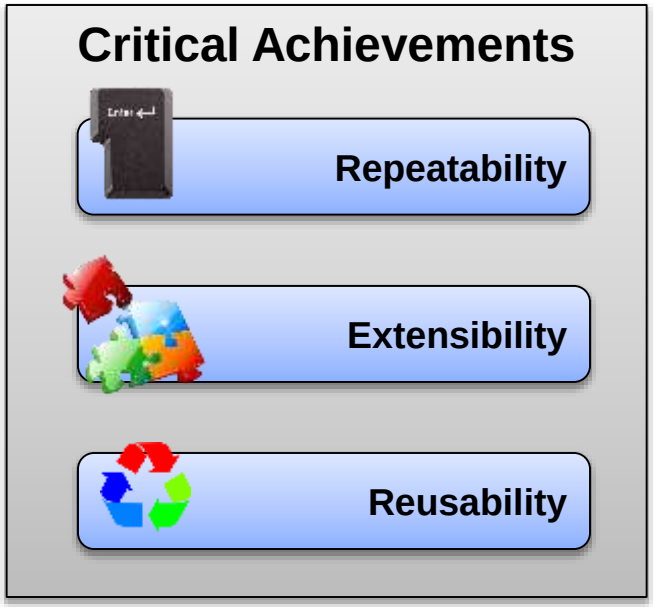
- **Generate 10TB databases within 12 hours**
- **Generate "interesting" queries**

SPAR Query Types

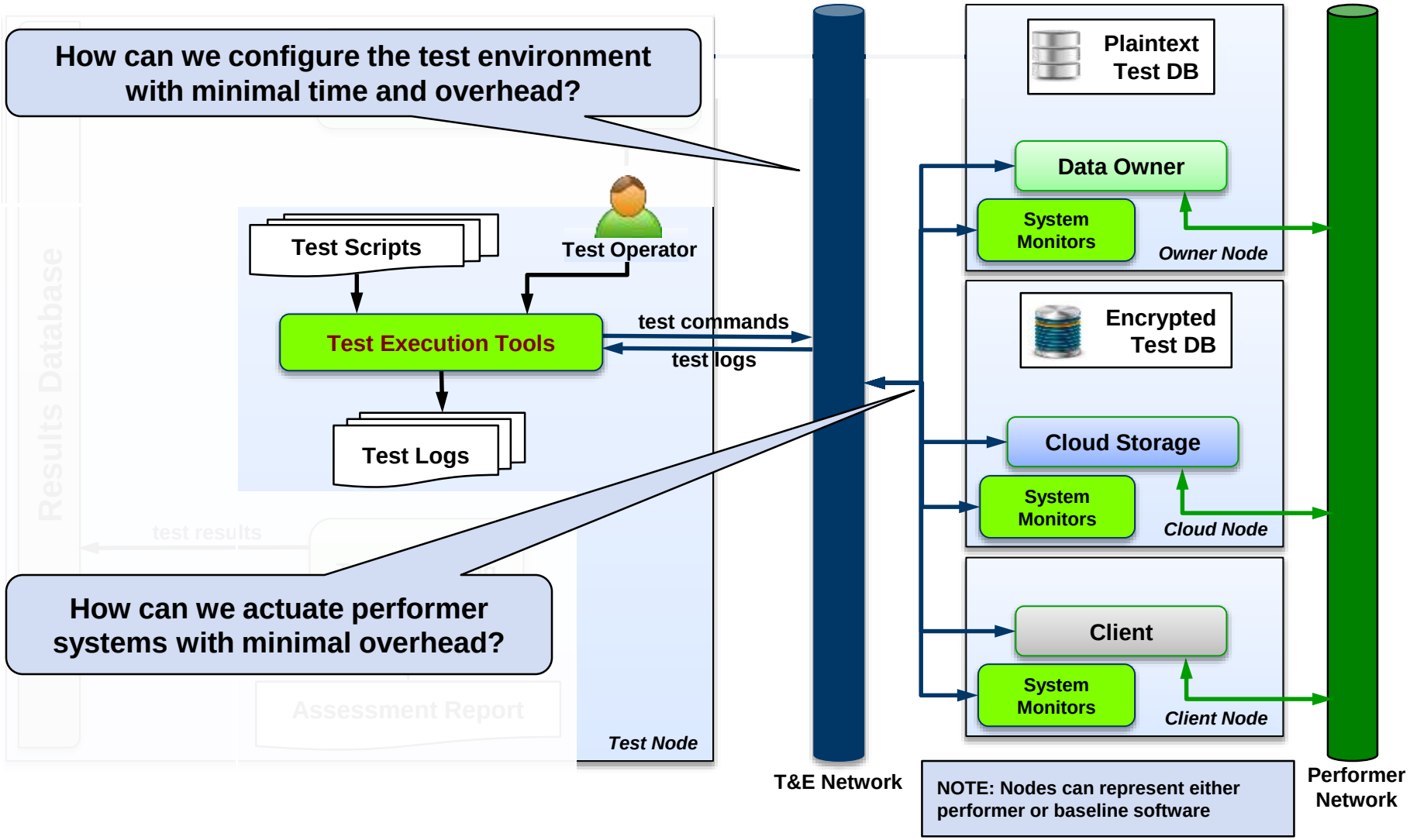
Type ID	Description	Example
Eq	Single-field equality	fname = ‘Homer’
P1	Boolean operations	lname = ‘Simpson’ AND city = ‘Springfield’
P2	Numeric ranges	age BETWEEN 38 and 40
P3	Free-text keyword	CONTAINED_IN(notes1, ‘donut’)
P4	Stemming	CONTAINS_STEM(notes2, ‘work’)
P6	Wildcard	notes3 LIKE ‘%oo %oo!’
P7	Substring	notes4 LIKE ‘%mmm%’
P8	Threshold	M_OF_N(2, 3, income > 40000, citizenship = ‘Yes_Born_In_US’, marital_status = ‘Married’)
P9	Ranking	M_OF_N(2, 3, income > 40000, citizenship = ‘Yes_Born_In_US’, marital_status = ‘Married’) ORDER BY RANK
P11	Searching on XML	xml XPATH xml//company = ‘Springfield Nuclear Power Plant’

Data & Query Generators

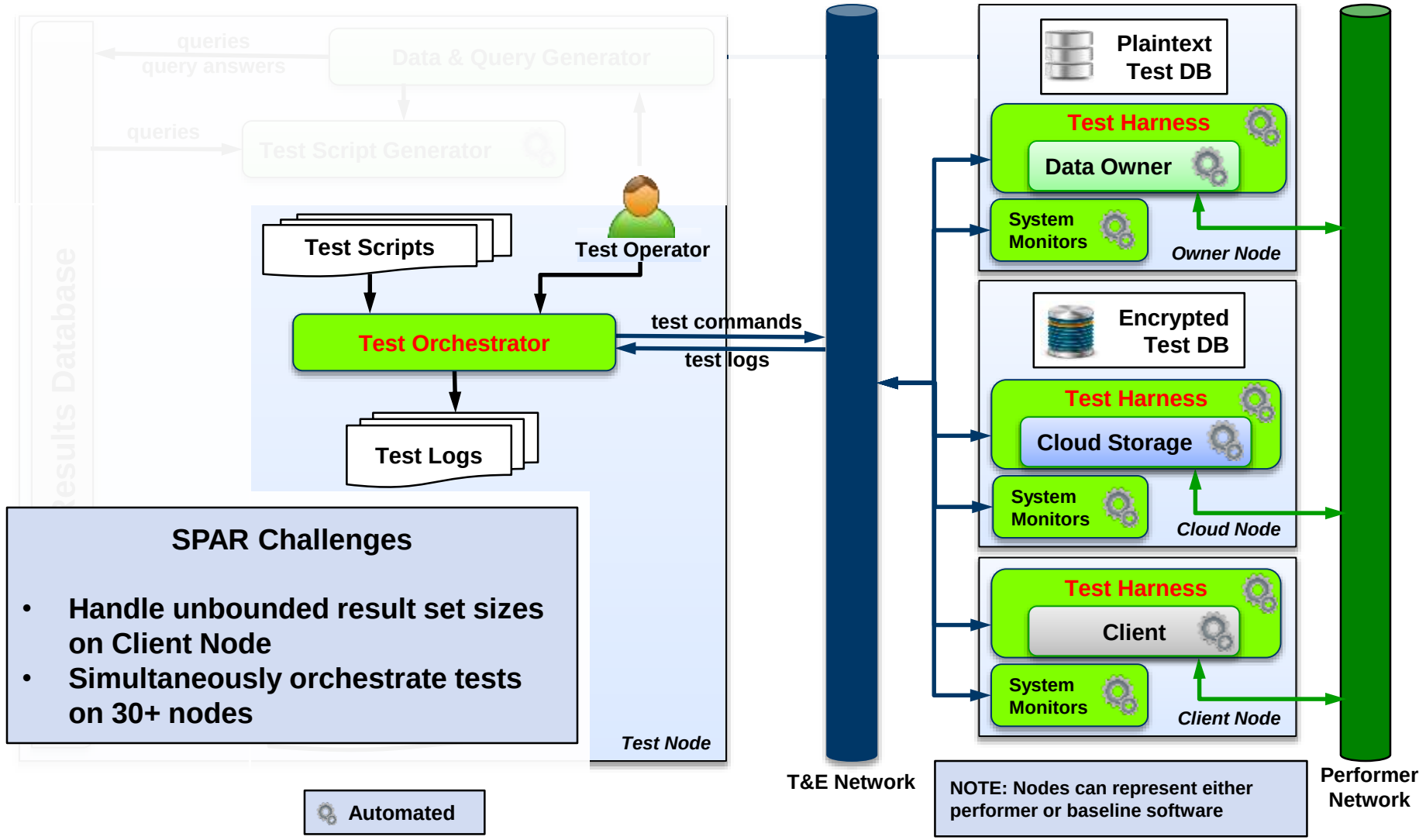




Common Test Execution Challenges



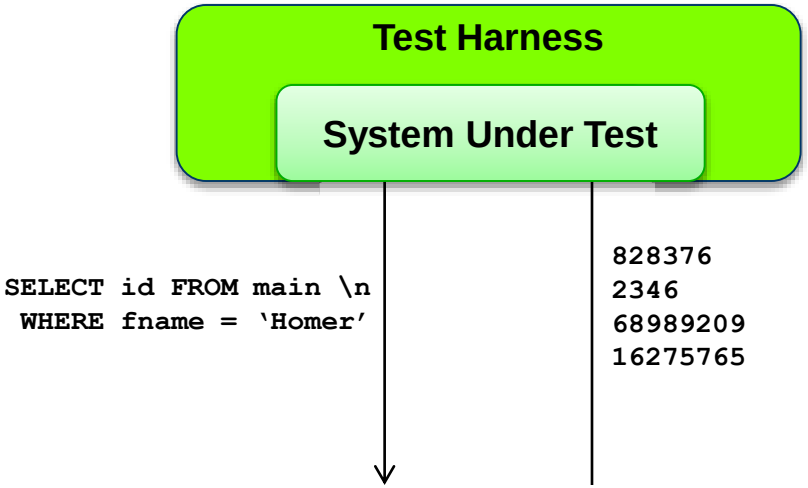
Our Test Execution Tools



SPAR Challenges

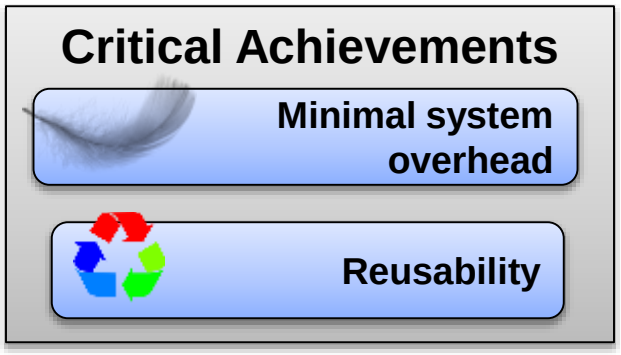
- Handle unbounded result set sizes on Client Node
- Simultaneously orchestrate tests on 30+ nodes

Test Harness Protocol Handler



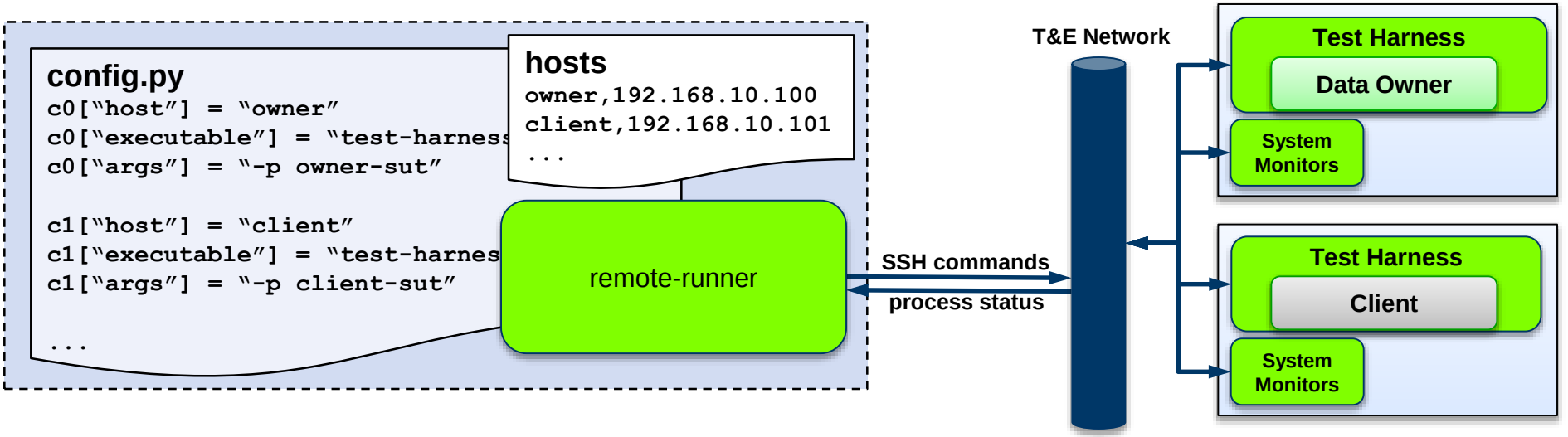
Operation	string	rope	knot
Index	O(1)	O(log n)	O(log n)
Concatenate	O(n)	O(1) [lazy] O(log n) [else]	O(1)
Delete	O(n)	O(log n)	O(1)
Substring	O(n)	O(log n)	O(1) [left/right] O(log n) [else]
Iteration	O(n)	O(n)	O(n)

Average case run-time



Boehm, Hans-J; Atkinson, Russ; and Plass, Michael (December 1995). "Ropes: an Alternative to Strings" (PDF). Software—Practice & Experience (New York, NY, USA: John Wiley & Sons, Inc.) 25 (12): 1315–1330.

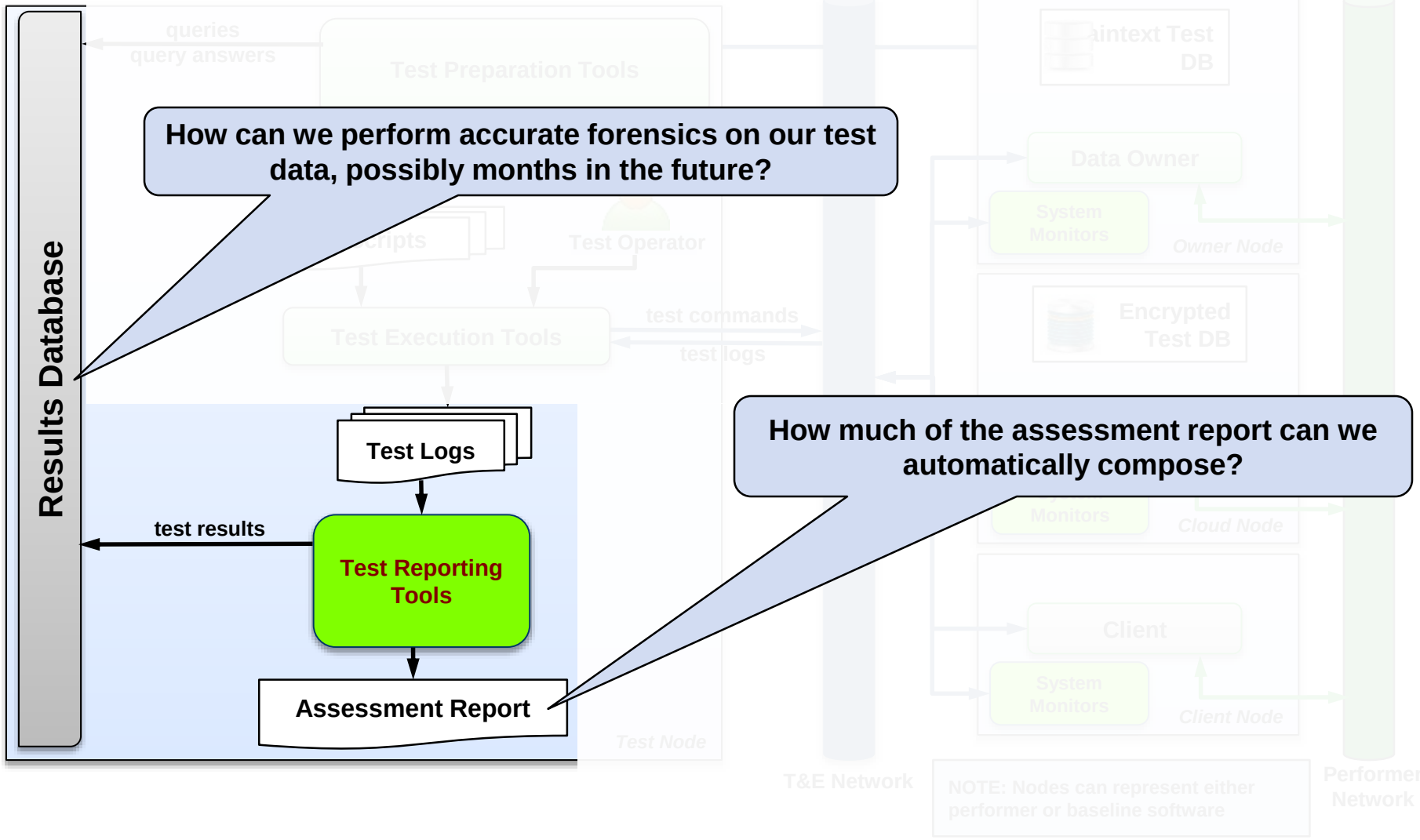
Test Orchestrator



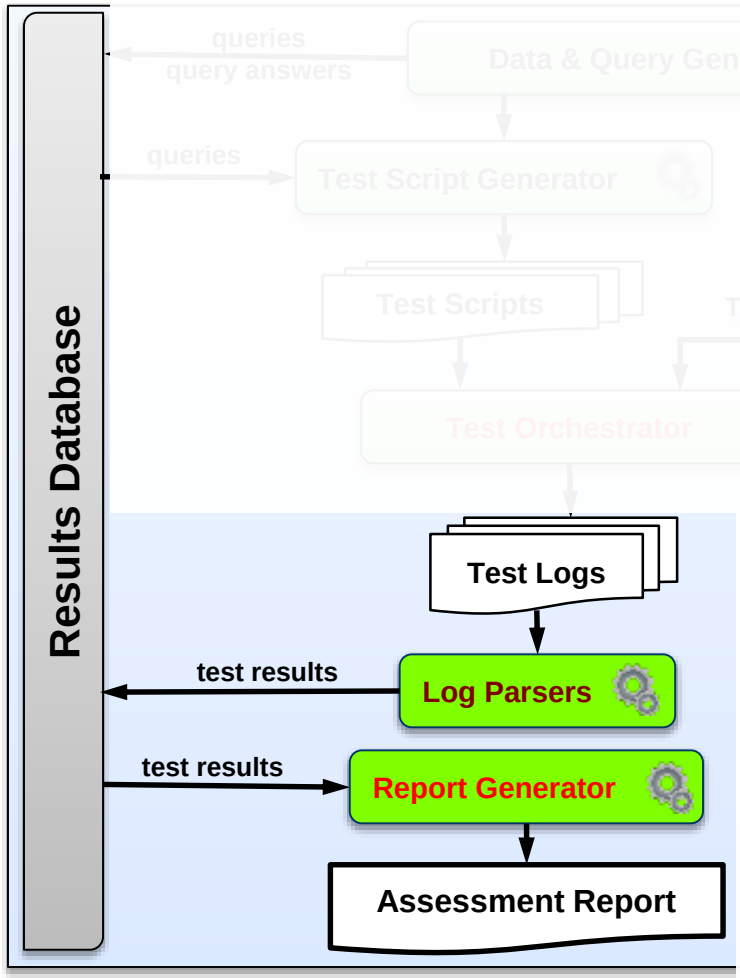
Critical Achievements

- Minimal system overhead
- Real-time status reports
- Rapid environment reconfiguration
- Comprehensive data capture
- End-to-end automation
- Test-time agility
- Reusability

Common Test Reporting Challenges



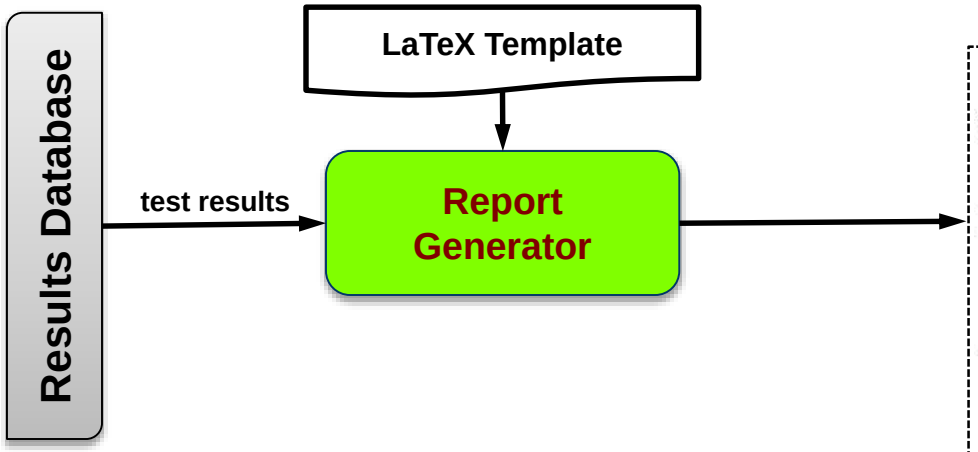
Our Test Reporting Tools

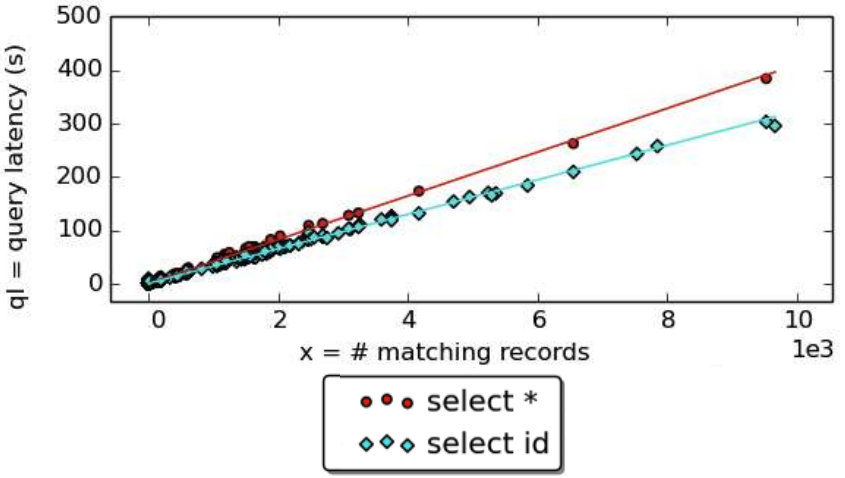


SPAR Challenge

Sponsor-ready draft report one day after test completion

Report Generator





	b= 1	b= 2	b= 3	b= 4	b= 5
a= 0	0	13	74	87	90
a= 1	86	89	96	96	97
a= 2	86	90	96	99	100
a= 3	88	90	100	100	100
a= 4	89	94	100	100	100

% queries where performer ≤ *a* + *b* · baseline

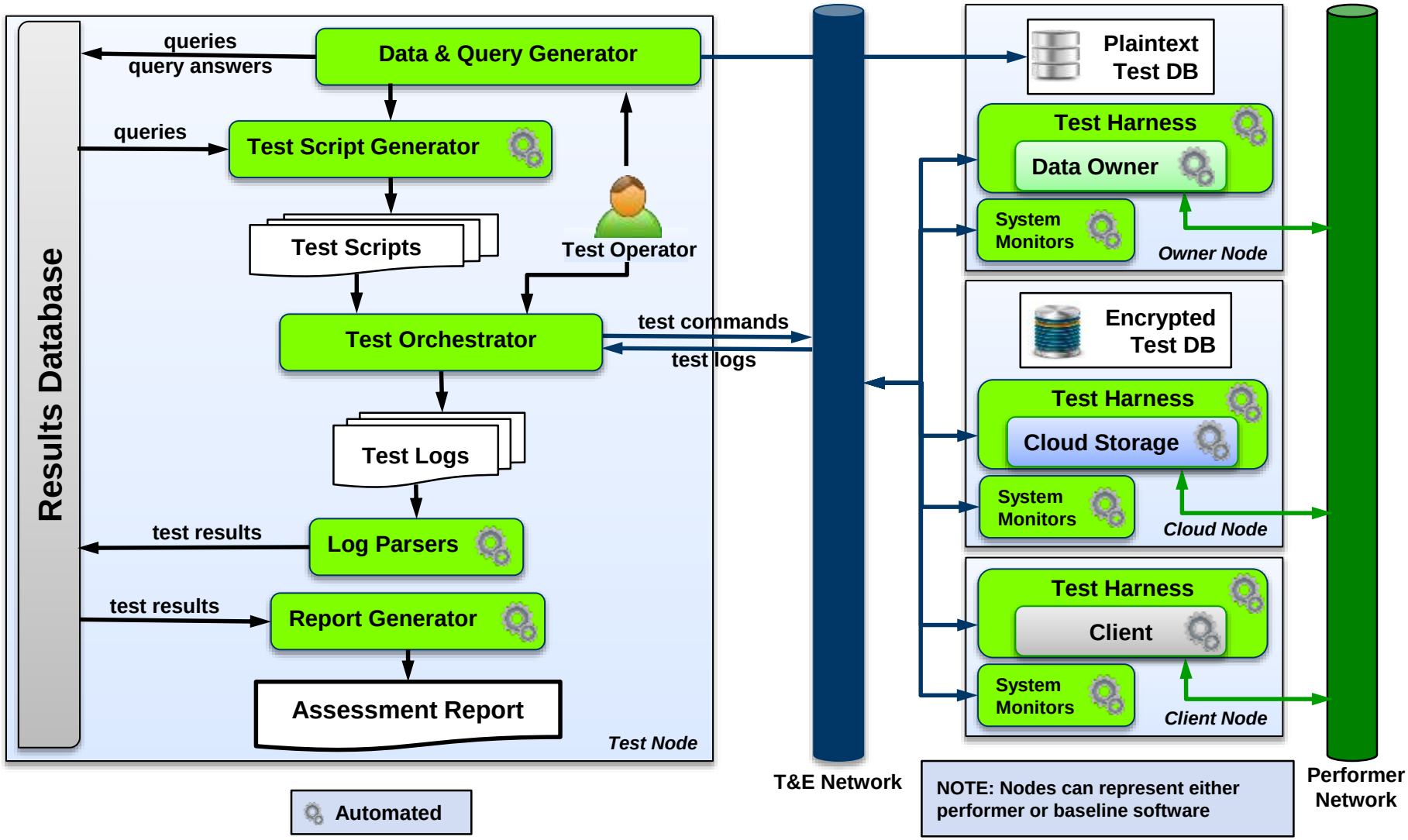
Critical Achievements

Comprehensive data capture

Extensibility

End-to-end automation

Our Assessment Framework



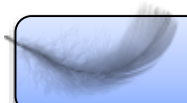
Software T&E Mantras

Black box treatment of systems

End-to-end automation

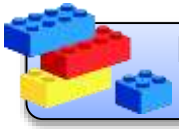
Test-time agility

Real-time status reports



Minimal system overhead

Repeatability

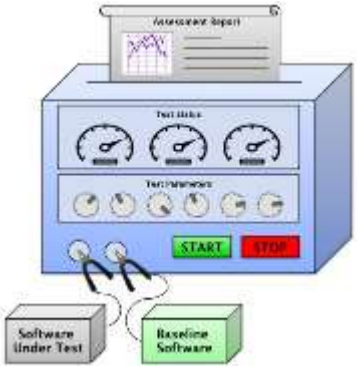


Rapid environment reconfiguration

Extensibility

Comprehensive data capture

Reusability



GitHub

https://github.com/mitll-csa/sparta

Questions?

nicholas.hwang@ll.mit.edu
spar-lincoln@ll.mit.edu