

MICROSHARD™ TECHNOLOGY: AN ENABLER FOR GDPR SCHREMS II COMPLIANCE

Data resilience, security, and privacy for hybrid-
and multi-cloud environments

PASCAL CRONAUER



GDPR/SCHREMS II COMPLIANCE OVERVIEW

- On 16 July 2020, the Court of Justice of the European Union (the Court) in its Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called “Schrems II case”) invalidated the EU-US Privacy Shield adequacy decision.
- The Court also casts doubt over the extent data transfers from the EU and the EEA to the US and to other jurisdictions with significantly less data protection can be legitimized by the European Commission’s Standard Contractual Clauses (SCC).
- The Court upheld the general validity of SCCs as a transfer tool but stressing that SCCs are nothing but a contract only binding the parties, not public authorities of third countries.
- Therefore, the SCCs cannot be used as a transfer tool alone if the laws or practices of the third country impinges on the effectiveness of the appropriate safeguards.
- In those situations, the Court leaves open the possibility for exporters to implement supplementary measures to compensate for the contractual shortcomings.

**Prepared by Hans-Peter Erlingsson - Specialist Lawyer - GDPR



GDPR/SCHREMS II COMPLIANCE OVERVIEW – TRANSLATED

- Am **16. Juli 2020** erklärte der **Gerichtshof** der Europäischen Union ("der Gerichtshof") in der Rechtssache C-311/18 Datenschutzbeauftragter gegen Facebook Irland und Maximilian Schrems ("Rechtssache Schrems II") das **EU-US-Privacy-Shield-Abkommens für ungültig**.
- **Der Gerichtshof bezweifelt** auch, **dass Datenübermittlungen** aus der EU und dem EWR in die USA und in andere Länder mit deutlich geringerem Datenschutz durch die Standardvertragsklauseln (SCC) der Europäischen Kommission **legitimiert werden können**.
- Der Gerichtshof bestätigte die allgemeine Gültigkeit von SCCs als Transfer-Tool, betonte jedoch, dass SCCs nichts anderes als ein Vertrag sind, der nur die Parteien bindet, nicht aber die Behörden von Drittländern.
- Daher können die SCC nicht als alleiniges Transfer-Tool verwendet werden, wenn die Gesetze oder Praktiken des Drittlandes die Wirksamkeit der entsprechenden Schutzmaßnahmen beeinträchtigen.
- In diesen Fällen lässt der Gerichtshof den Ausführern die Möglichkeit offen, zusätzliche Maßnahmen zu ergreifen, um die vertraglichen Mängel auszugleichen.



CLOUD ADOPTION IS NOW IN QUESTION

- Seit dem Urteil des EU-Gerichtshofs in der Rechtssache Schrems II ist die Nutzung globaler Cloud-Dienste durch EU/EWR-Organisationen deutlich schwieriger geworden.
- Dies hat Auswirkungen auf die Strategien zur digitalen Transformation und auf die Fähigkeit der EU-Organisationen, die Betriebskosten für Strom und Speicher zu senken und gleichzeitig die Flexibilität zu verringern.





SCHREMS II RULING AND ITS IMPLICATIONS ON CLOUD ADOPTION IN THE EU

Copyright© 2022, ShardSecure, Inc. This content is privileged and confidential.

MAIN POINTS

1

Mit der Aufhebung des EU-US-Privacy-Shield durch den Gerichtshof wurde die gesamte Rechtsgrundlage für den freien Datenverkehr mit den USA außer Kraft gesetzt.

2

SCCs (und andere von der DSGVO genehmigte Übermittlungs-tools) können ohne die Umsetzung zusätzlicher Maßnahmen nicht mehr als vertrauenswürdig angesehen werden.

3

Am 18. Juni 2021 verabschiedete der Europäische Datenschutzausschuss (EDPB) Empfehlungen zu Maßnahmen, die die Übermittlungs-tools ergänzen, um die Einhaltung des EU-Niveaus für den Schutz personenbezogener Daten zu gewährleisten.

4

Die Empfehlungen zielten darauf ab, die Daten in viel kleinere Teile aufzuteilen, um sicherzustellen, dass die Teile nicht rekonstruiert werden können. Use Case 5



MICROSHARDING

THE ANSWER TO UNLEASHING CLOUD ADOPTION BENEFITS

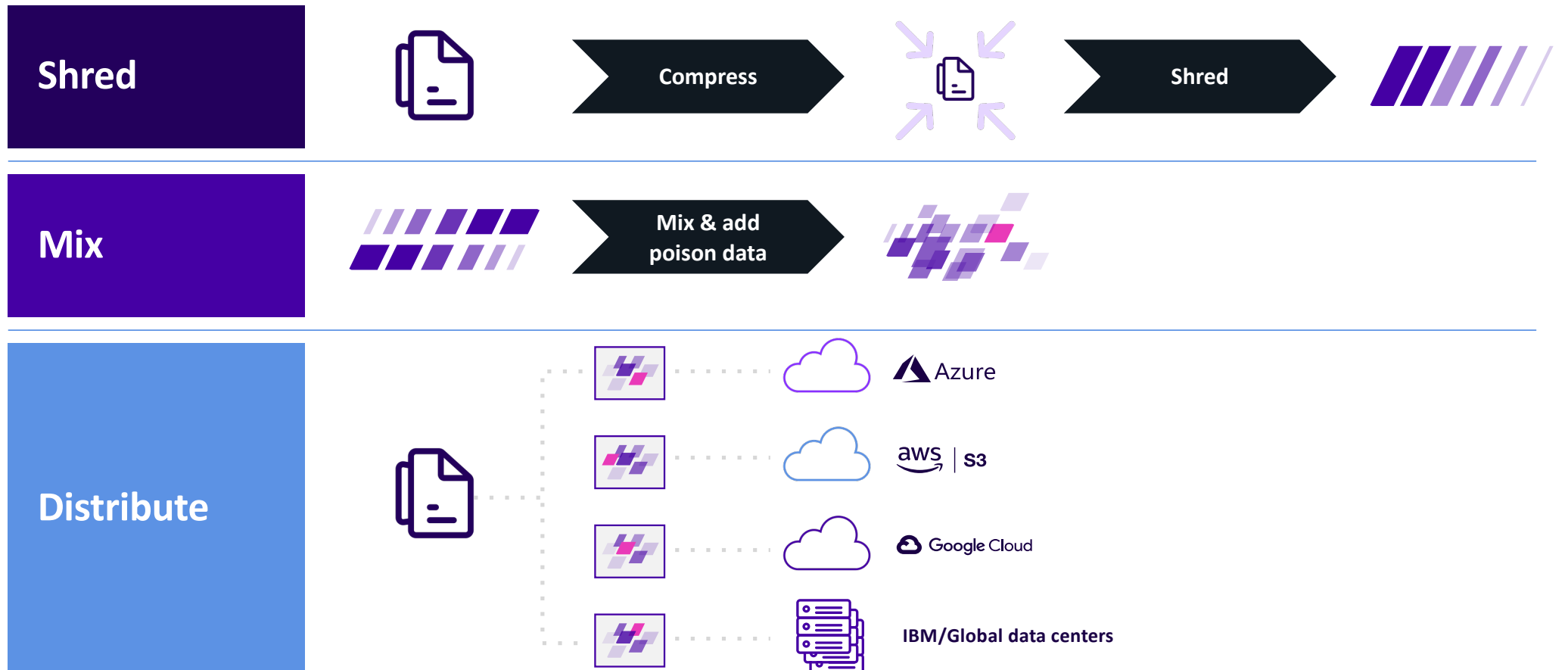




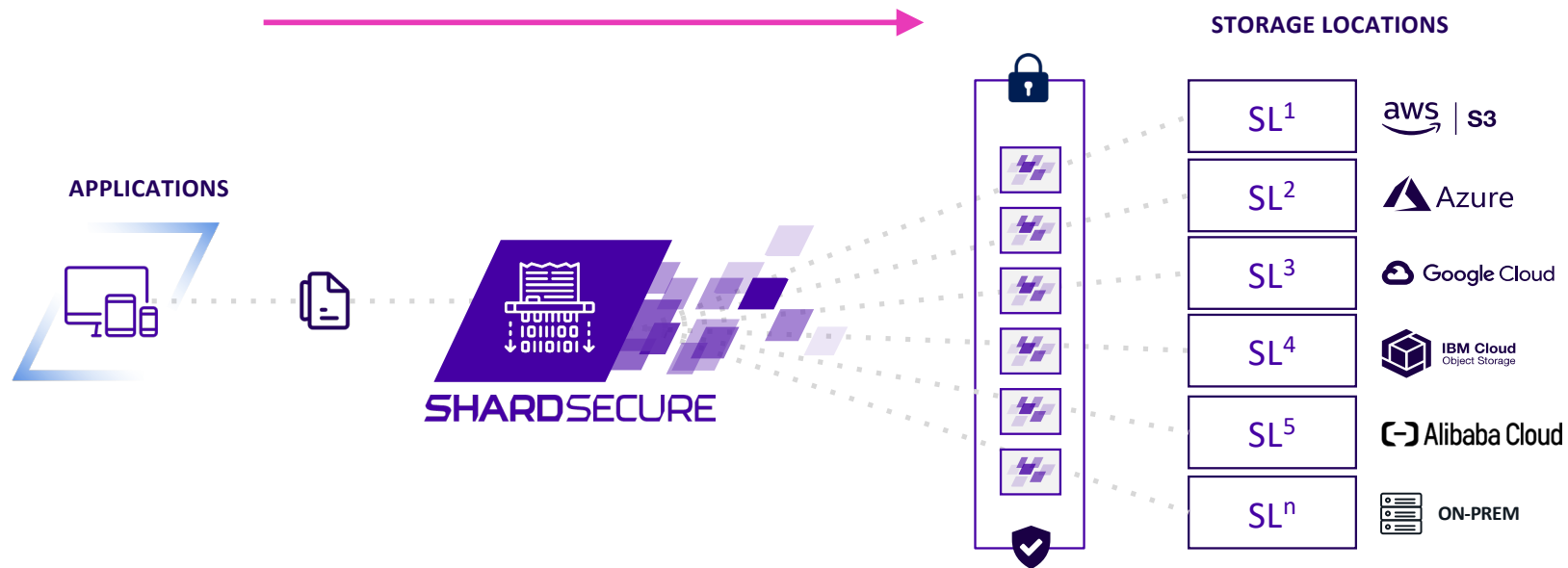
“With MicroSharding all organizations can easily and securely enjoy the benefits of cloud adoption without surrendering control of their data.”



HOW MICROSHARDING WORKS?



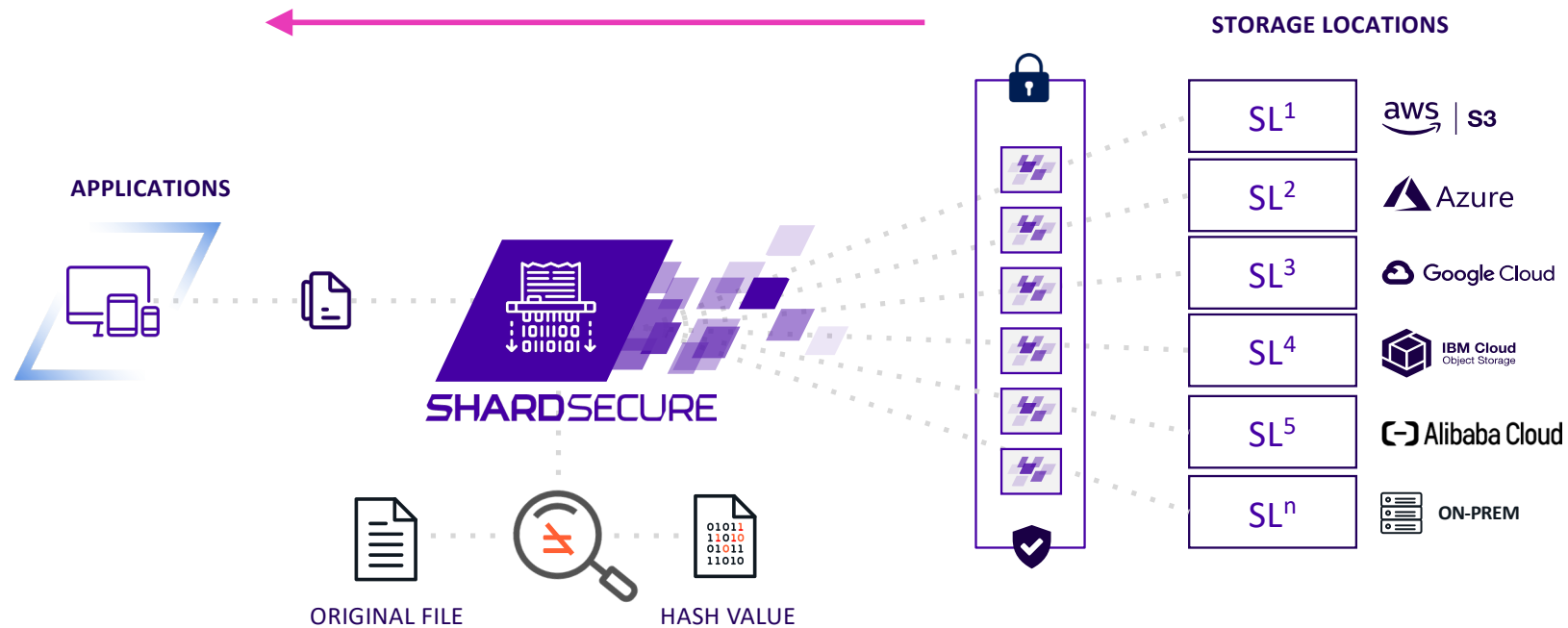
DATA CONFIDENTIALITY



Files are:

- Shredded into four-byte microshards
- Mixed into multiple logical containers
- Distributed across multiple storage locations

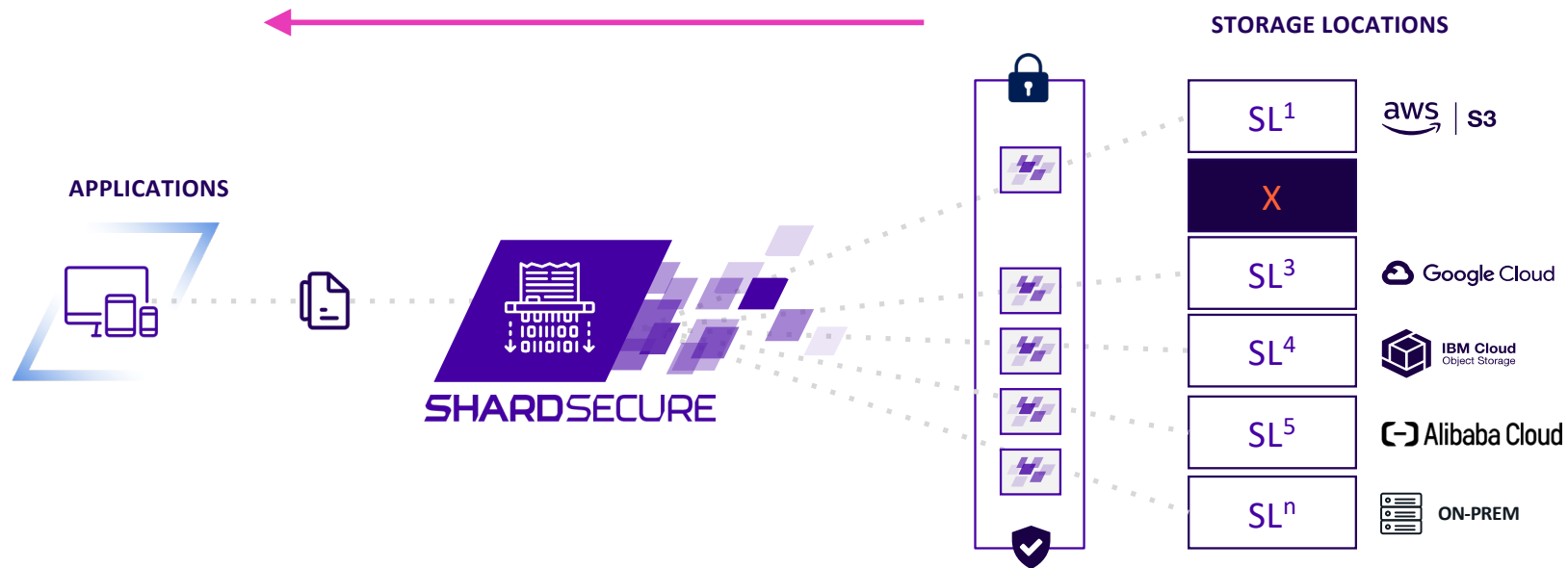
DATA INTEGRITY



Automatic integrity checks to:

- Detect file tampering or deletion at rest
- Tampered/deleted data restored to last known good
- Neutralizes cloud-based ransomware

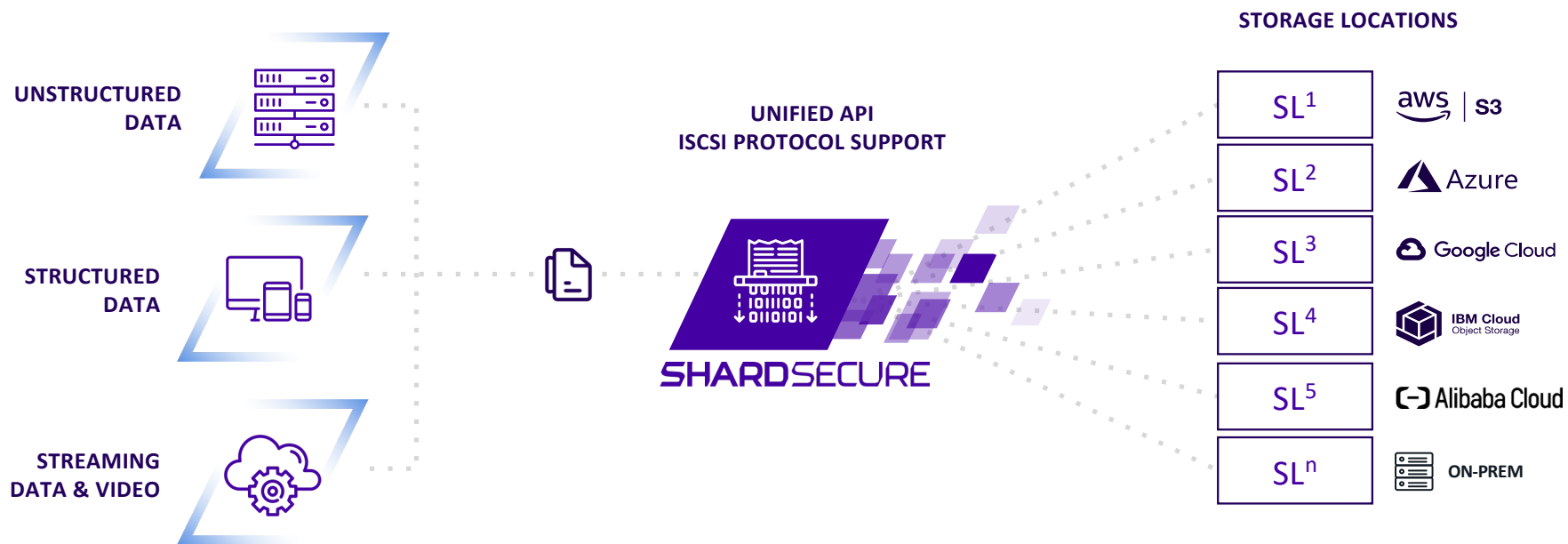
DATA AVAILABILITY



In case of service outage:

- Affected containers are reconstructed in real-time
- Business continuity is maintained
- ShardSecure instances are virtual clusters; multiple may be configured for HA/failover

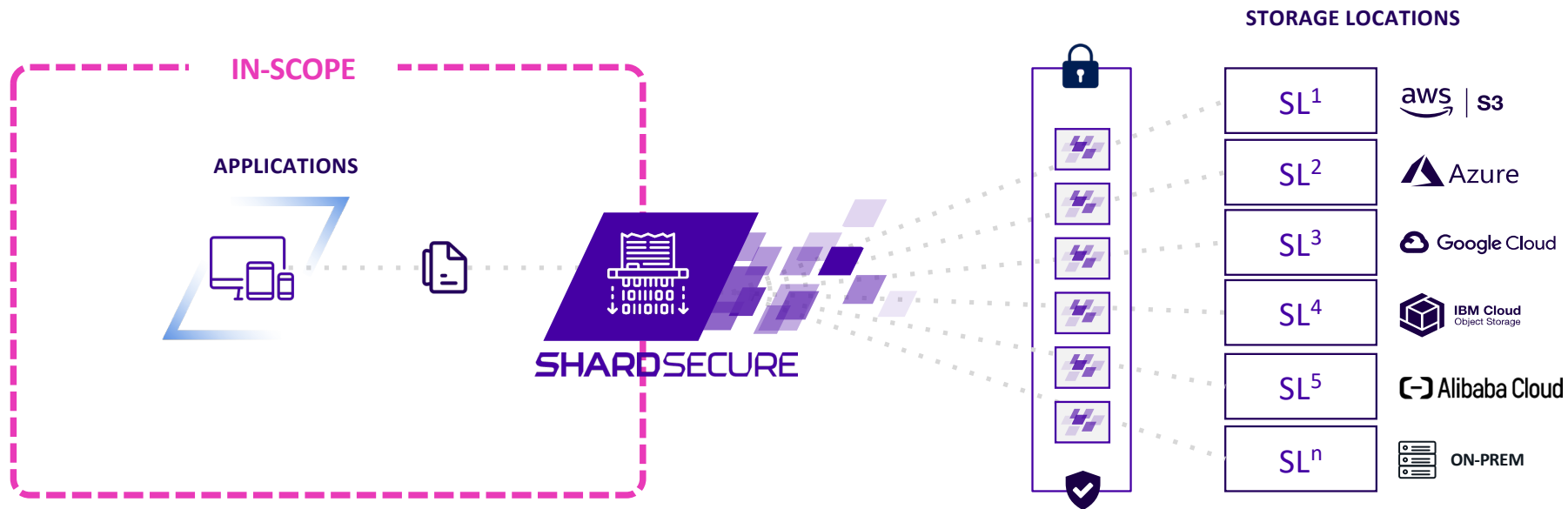
MULTI-REGION/MULTI-CLOUD/HYBRID ARCHITECTURES



COMPLIANCE SCOPE BEFORE MICROSHARDING



COMPLIANCE SCOPE AFTER MICROSHARDING



SHARDSECURE

THANK YOU