POLYMER

Polymer DLP Virtual Compliance Officer

A quantitative risk-management approach to data governance within SaaS platforms

No one wants their organisation to lose or expose sensitive customer data via third-party SaaS applications for collaboration. On average, Gartner estimates 90% of cloud breaches happen due to human error. The flexibility of third-party SaaS allows greater collaboration opportunities but introduces risks that did not exist in the pre-cloud era. Access controls for data stores, shared folders and applications are not sufficient in SaaS eco systems where 'data' can be created by anyone in the network and shared on a global basis to all other participants. SaaS platforms differ as a data store from databases or shared folders from a clear absence of a defined process or workflow feeding into them.

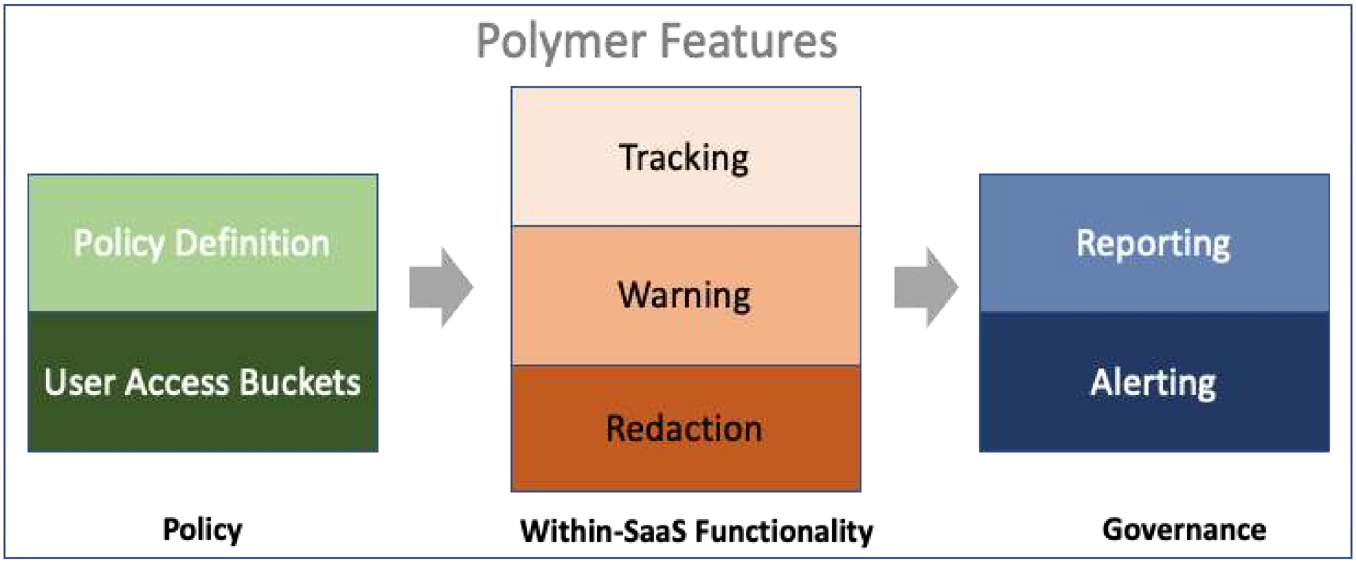
A data warehouse will maintain its ontology of data types while an online object store or chat platform by nature will have data classifications that shift constantly. This quickly renders qualitative controls and process documentations obsolete.

Operational risk management is very important in getting a handle on risk over cloud-hosted solutions but the range of security options have been limited. Other than behavioral controls or best-effort process implementations, there have been limited methods to apply op-risk policies. A more rigorous approach should reduce human involvement and allow for targeted policies that can be applied in real time.

For a more holistic risk framework, risk scorecards need to be enriched with quantitative metrics. A simple heuristic in assessing risk over a given SaaS platform can be summed up as follows:

$$P(data\_breach\_or\_exposure) \propto \sum(sensitive\_data\_elements)$$

Polymer reduces the sensitive data footprint over third-party SaaS applications—basically the right hand side of the equation. At a high level, Polymer is designed to permission PII/PHI data elements in *near* real time. This is accomplished based on three distinct aspects of the architecture summarized here:



Polymer is a tightly coupled integration with any SaaS platform that delivers the most informed and accurate real-time assessment of data exposure risk based on actual traffic. Organizations can apply risk and data governance frameworks quantitatively with a ‘trust but verify’ approach. Documents and unstructured datasets can be decomposed into the same reporting formats as structured data to create a single view of your PII/PHI/HIPAA traffic over any platform.

Why Polymer?

Accurately Measure Your SaaS Data Exposure Risk: Get real-time metrics on the frequency, quantity, and sources of sensitive data in SaaS platforms. With the built-in Policy Engine, get a true picture of what data elements are being exposed to groups of users within chats, documents, database records and object stores. It comes with out-of-the-box support for 100+ data elements with the flexibility to add *n* types of custom elements and policies.

Leverage Existing Investments: Polymer easily integrates with existing SaaS platforms such as Slack, Gmail, Dropbox, Zendesk and others without an expensive buildout or specialized infrastructure. With the availability of Polymer over the SaaS app stores, the product is designed to be tightly integrated and work over existing workflows.

Align IT, Security, Risk & Compliance Efforts with Business Objectives: Increasing governance has the potential side effect of creating friction for business objectives. With automated and granular permissioning, there is one common framework that helps Security and IT communicate clearly and succinctly with management, so they can make data-driven decisions. In addition, dissemination of information between departments and across organizations can be automated and clearly defined.

Automate Actions to Enhance your Compliance Team’s Capabilities: Real-time redaction of sensitive data molecules removes sensitive data without manual supervision. Predefined rules can be created to set categories of sensitive data that should be immediately redacted. As opposed to wholesale removal of a document, this is a targeted response that reduces friction without interrupting regular workflows.

Attenuate Your Policy Application: At the core of Polymer’s Policy Engine is a data element-level permissioning interface that allows an organization to map user groups to defined PII/PHI/HIPAA data elements. This feature allows highly targeted policy frameworks where alerts, reporting, and redaction can all be controlled based on access levels.

Security via Social Engineering: With over 50% of data breaches due to avoidable mistakes, Polymer’s optional alerting is designed to affect choice-architecture & social influence. Polymer ‘nudging’ (Thaler & Cass Sunstein “Nudge: Improving Decisions about Health, Wealth & Happiness”) creates heuristics that are designed to promote privacy-aware choices within your organization.