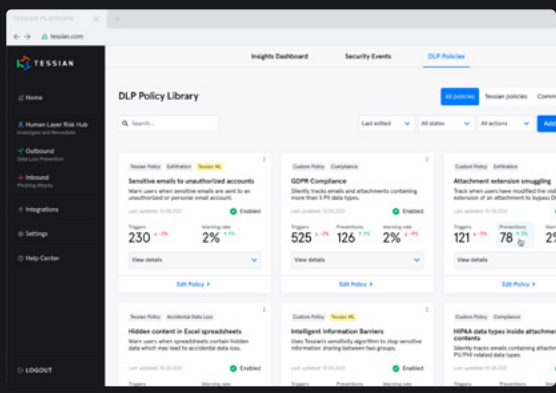
TESSIAN



Tessian Architect

Advance your Data Loss Prevention Strategy with Custom Intelligent Policies

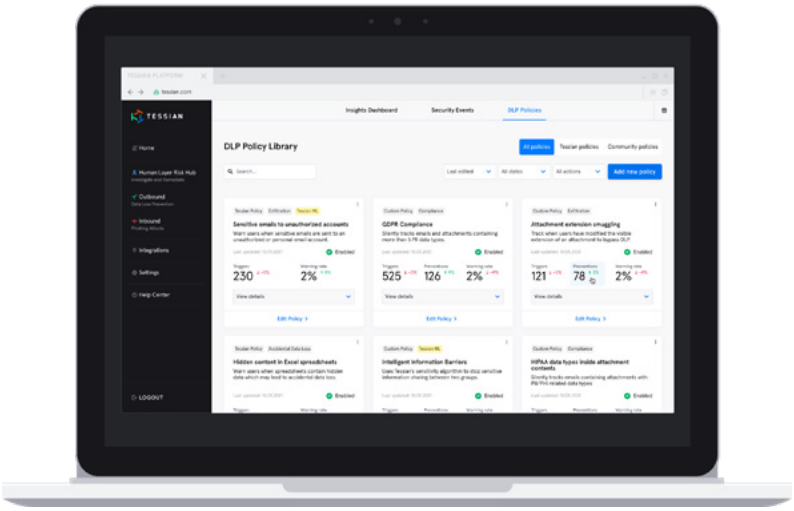
Tessian Architect is a powerful policy engine for real-time email data loss prevention. It features a combination of the classic elements of DLP policies, as well as intelligent policies that provide custom protection against sensitive data loss.

Tessian Architect: The Industry's Only Intelligent Data Loss Prevention Policy Engine

The industry has seen first hand how Data Loss Prevention has become too reliant on static rules and places far too much burden on admins to identify, investigate and remediate sensitive data loss.

However, we have also seen that custom policies, when combined with dynamic behavioral analysis, plays an important role for an organization's DLP strategy. When policies are used, they should be intelligent where applicable, be easy to configure and manage, and leverage end-user remediation to reduce administrative burden.

With Tessian Architect, enterprises can now deploy powerful intelligent DLP policies. Architect completes Tessian Guardian and Enforcer to provide the market's best-in-class Email DLP platform.



Product Highlights

PRE-BUILT AND CUSTOM POLICIES THAT SOLVE FOR YOUR SPECIFIC DATA LOSS USE CASES

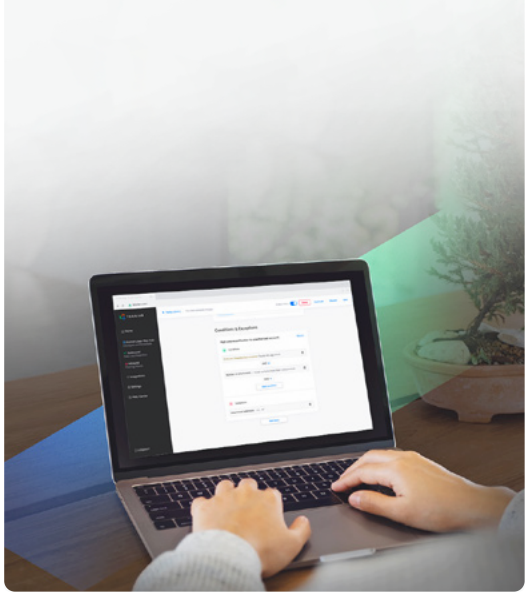
Policies may contain any number of DLP conditions and can be simple or complex, rely entirely on machine learning, basic rules, or both. Testing, tuning and rolling out policies can be done within hours, not days, weeks, or months. Test a policy change in production in as little as one minute.

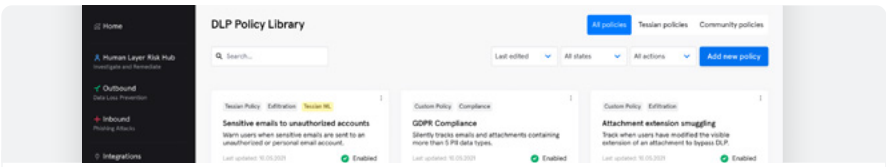
POLICY EDITOR PROVIDES MAXIMUM PROTECTION FOR SENSITIVE DATA

Build advanced, nested-logic policies and consolidate multiple policies that are related to similar topics. This is needed for advanced use cases to allow companies to consolidate and simplify policies as they're migrating legacy DLP policies.

INTEGRATE WITH ANY DATA CLASSIFICATION SYSTEM, INCLUDING MICROSOFT INFORMATION PROTECTION

Combine the behavioral approach of Tessian with Data Classification tools, such as Microsoft Information Protection, to further protect against sensitive data loss. Tessian detects sensitive attachments without Data Classification labels.





Tessian Architect addresses the following use cases to advance your data loss prevention strategy, all without the costly and cumbersome, static rules of traditional DLP solutions:

- Detect hidden content in Excel spreadsheets to prevent accidental disclosure of sensitive data
- Use regular expressions to detect specific data types and identify high severity breaches by defining unique match thresholds (e.g. more than 5 unique records)
- Warn on sensitive attachments without Microsoft Information Protection labels, and detect when attachments labelled as 'Confidential' are sent to unauthorized accounts
- Educate and remind users when a sensitive attachment has been labelled as 'Public' or 'General'
- Set up intelligent information barriers to prevent sensitive data sharing between teams
- Detect PII/PHI shared externally in bulk
- Detect financial data such as credit card numbers and bank account numbers
- Detect unencrypted personal health information shared externally
- Block attachments containing high volumes of PII from being sent to unauthorized accounts
- Use Architect to migrate and simplify DLP policies from legacy tools and consolidate related policies using powerful logic blocks.
- Use Architect to enhance rule-based legacy DLP policies with machine learning such as Tessian's sensitivity algorithm and minimize the number of false positives

Feature Highlights

POLICY LIBRARY

- Choose from pre-built policies provided by Tessian and sourced from the Tessian network
- Quickly understand the performance of a policy and compare key stats between policies
- Identify policies with potential for improvements at a glance
- Build, test and deploy policies within hours, not weeks

POLICY EDITOR

- Flexibly combine conditions using logic blocks
- Combine machine learning + rule-based conditions
- Flag on data classification labels such as in MIP/AIP
- Use risk-adaptive protection (assign policies based on risk levels of a user group)

DLP EVENTS PAGE AND EVENT VIEWER

- Review and triage any DLP event via the Events page or Tessian API
- Assign status tags to security events
- New Event viewer to get more context about security events flagged by Tessian

DLP INSIGHTS DASHBOARD

- Track and report on DLP policy impact
- Review and take action on policy performance
- Filter insights per policy, time period, etc.

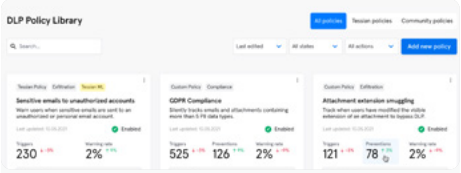
END USER REMEDIATION

- In-the-moment training educates and empowers users to build continuous email security awareness.
- Risk will quickly trend downward as users learn more about security, and more careful when sending emails.

INTELLIGENT DLP POLICIES

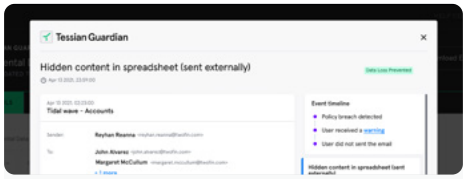
Architect Differentiators

With Tessian Architect, enterprises can now deploy powerful intelligent DLP policies. Architect completes Tessian Guardian and Enforcer and provides the market's best-in-class Email DLP platform.



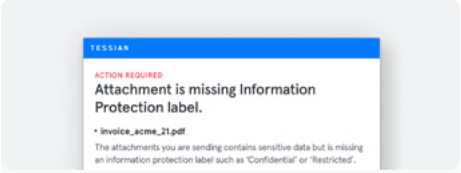
PRE-BUILT AND CUSTOM POLICIES

Take the guesswork out of building DLP with Tessian's policy library, with the flexibility to build your own to adhere to your organization's unique data protection requirements.



STOP DATA LOSS AND ENSURE REGULATORY COMPLIANCE

Stop data loss incidents that legacy DLP tools are unable to detect. Solve hard to detect data loss including accidental data loss and sensitive data exfiltration risks by combining Tessian Enforcer with intelligent pre-built and custom DLP policies.



REDUCE ADMIN BURDEN OF DLP BY 10X

Reduce admin overhead with end-user remediation and powerful policy logic that simplifies DLP configurations in minutes. Cut through noisy DLP alerts and gain new visibility of high severity incidents and anomalous activity.

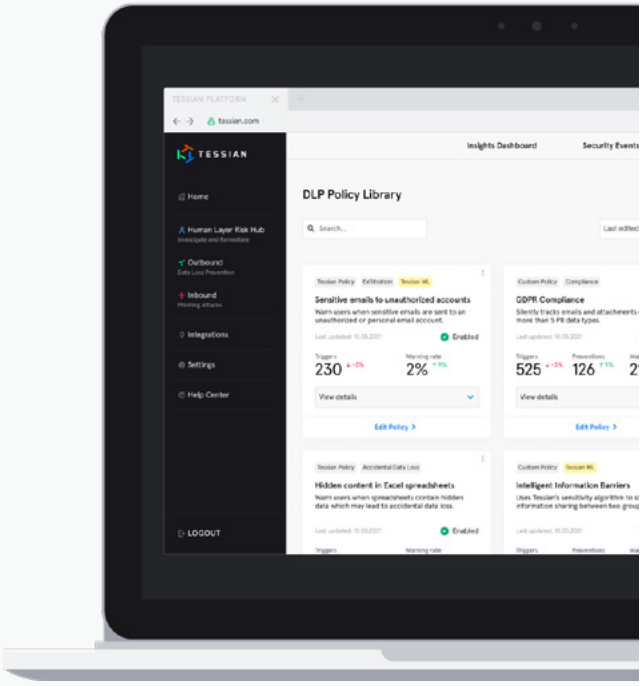
How Tessian Architect Works

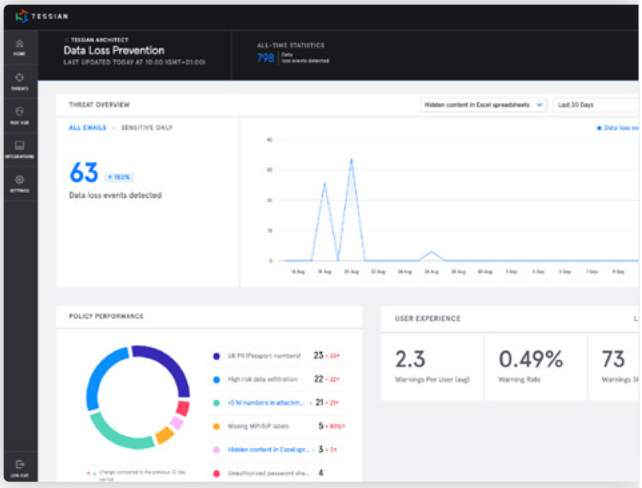
AUTOMATED AND CUSTOM POLICIES

Automated and Custom Policies that Solve for Your Specific Data Loss Use Cases

Policies may contain any number of DLP conditions and can be simple or complex, rely entirely on machine learning, basic rules, or both. Choose from pre-built policies that solve specific use-cases or industry requirements, or build custom policies for your unique requirements.

- Policy Directory: Manage all Tessian policies via a new policy directory page and view policies in a gallery or table format. See at a glance how policies are performing and how they're functioning, without going into the details of the policy editor.
- Tessian pre-built policies: Choose from a range of policies pre-built by Tessian
- Select from policies built by other Tessian customers (vetted by Tessian)
- Sort, filter, explore, manage policies: Search for policies, sort by last updated and filter by state, alert type and policy scope.
- Label: Assign labels to policies to organize policies into groups.
- Prioritize: View and change the order of priority of policies to determine which warning a user should see if two policies flag on one email.





INSIGHT INTO DATA LOSS EVENTS

Real-time Insights into Data Loss Events and Policy Performance

Quickly view real-time policy performance and determine what types of data loss are most prevalent in your organization. Insights are provided such as the number of data loss events detected, as well as information about those data loss incidents within specified time periods.

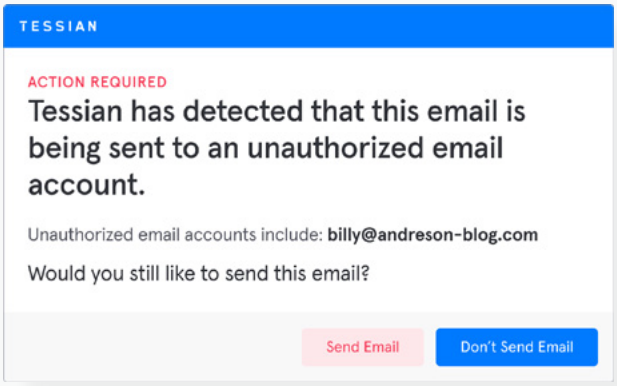
- Insights Page: Insights dashboard provides DLP policy performance and most important stats
- Slice and dice insights per user group, policy, time period
- Filtering: Filter and view insights for a specific policy (one or multiple)
- Data Points: Quickly view the number of triggers, warnings, preventions and top policies
- Review and take action on policy performance

SECURITY AND AWARENESS TRAINING

In-the-Moment Educational Warnings

Tessian warnings act as in-the-moment training for employees, continuously educating them about threats, reinforcing your policies, and nudging them toward safe email behavior. Automatically build individualized policies at scale to reduce high-risk email use and track trends in unsafe activity over time.

- In-the-moment training educates and empowers users to build continuous email security awareness.
- Risk will quickly trend downward as users learn more about security and be more careful when sending emails.

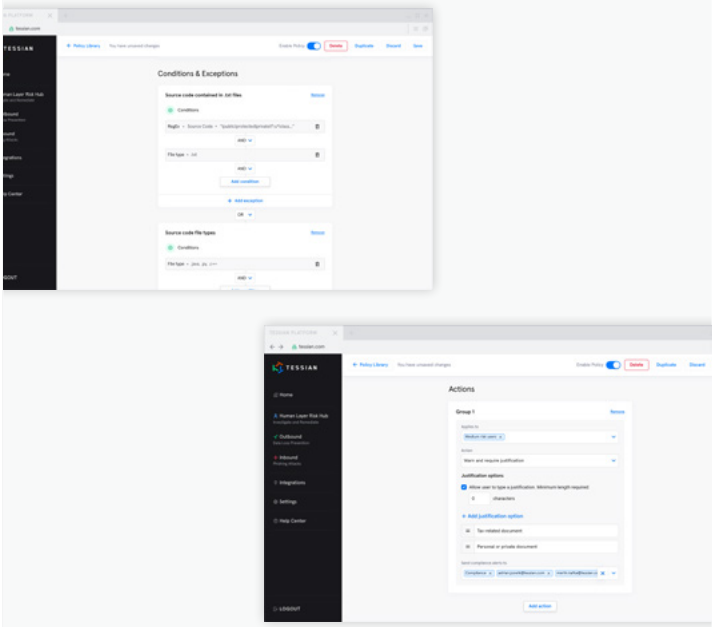


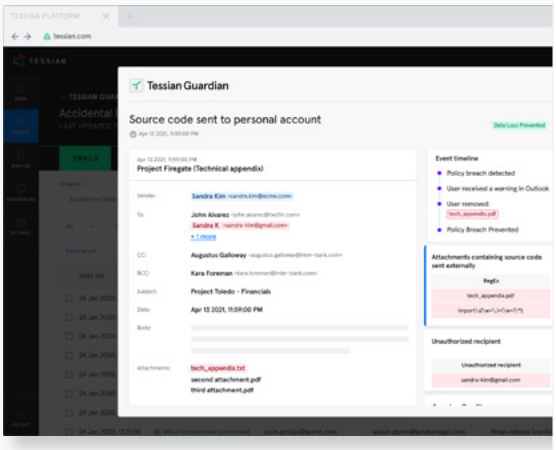
POLICY EDITOR

Policy Editor Provides Maximum Protection for Sensitive Data

Build advanced, nested-logic policies and consolidate multiple policies that are related to similar topics. This is needed for advanced use cases to allow companies to consolidate and simplify policies as they're migrating legacy DLP policies.

- Standard DLP: Build DLP policies using standard conditions and exceptions, such as keywords, regex, recipients, and attachments, and many others.
- Combine Tessian Enforcer with Rules: Flexibly combine Tessian Enforcer with any number of conditions and exceptions to detect specific types of exfiltration.
- Combine Sensitivity and Rules: Combine sensitivity with any number of conditions and exceptions to detect specific types of exfiltration.
- Preset Justification Options: On policy breach, provide users with preset justification options or allow users to provide their own justification (or both).





INTEGRATE WITH DATA CLASSIFICATION TOOLS

Integrate with Any Data Classification System, Including Microsoft Information Protection (MIP)

Combine the behavioral approach of Tessian with Data Classification tools, such as Microsoft Information Protection, to further protect against sensitive data loss. Tessian detects sensitive attachments without Data Classification labels.

- Detect when data labeled "confidential" is being sent to unauthorized parties.
- Detect when important documents are missing labels.

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

Evercore · arm · Herbert Smith Freehills · RealPage · affirm · Investec · Graphcore · sanne · K&L Gates · PeaceHealth · MSCI · ERT · Man Group plc · Bracewell · Rand Merchant Bank

See Tessian in Action.

Automatically stop data breaches and security threats caused by employees on email.

REQUEST A DEMO →

TESSIAN

Tessian Cloud Email Security intelligently prevents advanced email threats and protects against data loss, to strengthen email security and build smarter security cultures in modern enterprises.