TESSIAN

TESSIAN SOLUTIONS BRIEF

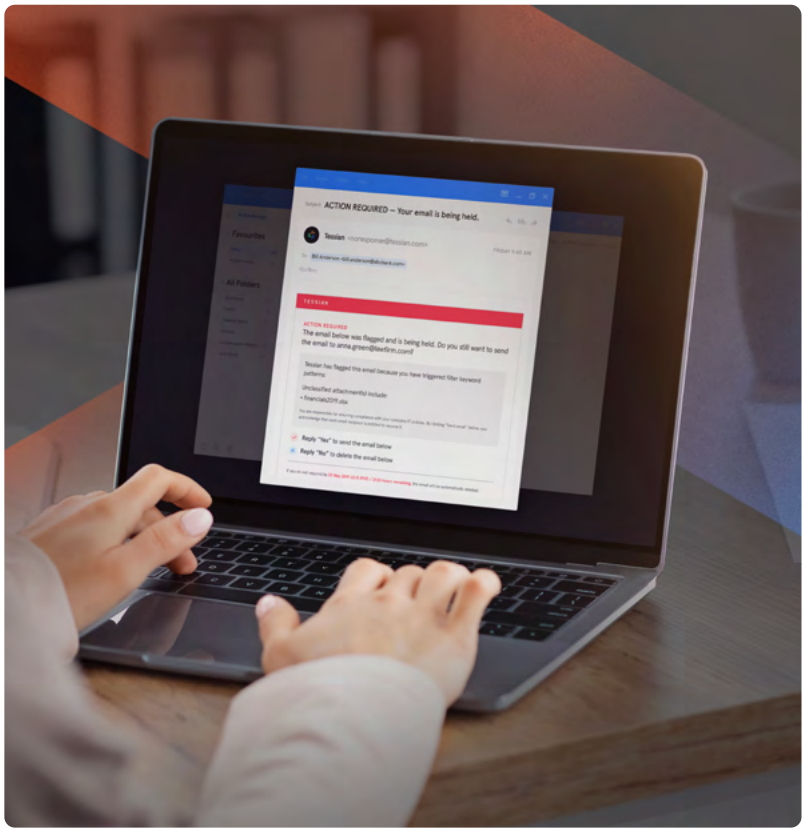
The Industry's Best-in-Class Email Data Loss Prevention Platform

Tessian's Email DLP suite provides security teams with an automated data protection solution to predict, prevent, detect and respond to data loss events caused by employees on email.

Legacy DLP Has Failed the Modern Enterprise

Legacy DLP solutions are quickly becoming an anti-quated technology that isn't evolving to meet the needs of enterprise organizations. Most of these solutions rely on rules, create massive overhead for admin teams, and typically require constant manual fine-tuning to manage the myriad of false alerts. And data breaches continue to happen.

There is a better way with Tessian.



Solution Highlights

AUTOMATICALLY PREVENT ACCIDENTAL DATA LOSS

Detect anomalies that indicate whether emails are being sent to the wrong person before it leaves your organization.

PREVENT DATA EXFILTRATION TO UNAUTHORIZED ACCOUNTS

Automatically prevent data exfiltration via email to employee personal, unauthorized and non-business accounts.

POWERFUL POLICY ENGINE

Automatic and custom policy capabilities, and real-time visibility into data loss events, all without cumbersome, manual rules found in traditional DLP solutions.

ESTABLISH AND MAINTAIN REGULATORY COMPLIANCE

Protect against non-compliant activity and prevent users from sharing confidential data with non-business, personal addresses /unauthorized recipients; track and block compliance breaches in real-time.

The Problems with Legacy Data Protection Methods

Perhaps the most important aspect to consider with legacy data loss prevention solutions, is that the context of the data and attachments in emails are never thoroughly examined and understood, and security and awareness training is an ineffective tick-box exercise. Instead, cumbersome solutions based on known signatures are used, which don't account for unknown anomalies, or consider the friction and latency they produce when implemented. It also doesn't help that email infrastructure hasn't changed in three decades. Anytime we are securing information in legacy infrastructure, there are bound to be challenges. To prevent today's email security incidents, your security controls must bring the perimeter down to the employee level, so that you can understand their unique human behavior.

Here are the primary ways that DLP fails organizations in their data protection projects:

RULES-BASED DLP DOES NOT PROTECT AGAINST DATA EXFILTRATION

Rules-based approaches simply cannot detect when emails are sent to the wrong people because there are no regex or pattern matches that can be applied. This level of protection requires context that DLP just doesn't have.

DLP FOCUSES ON A NEGATIVE CONTROL MODEL

Legacy DLP is very strict with a binary approach to protecting data. It either allows it or blocks it. In a post-perimeter architecture, this is highly disruptive to business and unsustainable.

SLOW, CUMBERSOME AND NON-ADAPTIVE

85% of security leaders say DLP is admin-intensive. Legacy DLP must analyze all content and try to match it to block lists. This requires extensive analysis and the matching can be wrong as enterprise email content is constantly changing. As content and locations get more complex, legacy DLP can develop problems very quickly.

DIFFICULT AND EXPENSIVE TO IMPLEMENT

While DLP may be regarded as a check-the-box solution for compliance, it is incredibly cumbersome, complex and expensive to deploy, often requiring huge spend in professional services to implement and maintain. Typical deployments are at least 12 months which make it hard to justify the return on investment vs. the security it provides.

LIMITED THREAT VISIBILITY

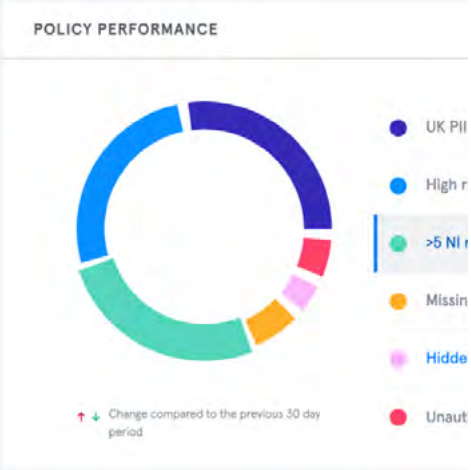
Legacy DLP, including Email DLP, Endpoint DLP and Network DLP offer little to no visibility into personal email, webmail or other unauthorized email accounts.

PRONE TO FALSE POSITIVES

DLP technologies have traditionally been prone to false positives, and as such, some of their best use cases are for controlling very predictable and structured content in very specific situations. In other words, it has extremely limited capabilities.

ASK YOURSELF...

- → How do you make sure that employees are sending emails and attachments to the right people?
- → How are you currently managing your blind spots?
- → How often are you conducting security awareness training and how effective has it been?
- → How long does it take to update your DLP policies?
- → How effective are your DLP policies in preventing data exfiltration?
- → What is the value of being able to report to the board and executives how technology is helping to reduce risk in the organization?
- → What would be the benefit of implementing email DLP without impacting your users' current workflow?



A NEW APPROACH TO EMAIL DATA PROTECTION

Stop Data Loss You Can't Make Rules For with Tessian's Next-Gen Email DLP Platform.

Automatically Prevent Accidental Data Loss to Unauthorized Parties

Tessian's Email DLP platform automatically stops accidental data loss that leads to organizations putting their customer's data at risk, breaching mandatory industry and data protection regulation and losing mission critical intellectual property.

LEARN MORE →

Automatically Stop Exfiltration of Sensitive Data to Unauthorized or Personal Accounts

Whether it's an employee negligently sending emails to unauthorized or personal accounts, or individuals maliciously stealing company intellectual property, Tessian's Email DLP platform automatically stops sensitive data from being sent to any unauthorized recipients.

LEARN MORE →

Custom Policies that Solve for Your Specific Data Loss Use Cases

Manage all Tessian policies via a new policy directory pages and view policies in gallery or table format. Quickly see how policies are performing and how they're functioning within your environment.

LEARN MORE →

Robust Capabilities and User Benefits to Protect Your Most Sensitive Data.

COMPREHENSIVE EMAIL DLP (POLICIES OPTIONAL)

Tessian's machine learning algorithms use relationship graphs, deep content inspection, and behavioral analysis to automatically identify highly sensitive data, and incorrect/unauthorized email recipients. Tessian offers out-of-the-box policies or the ability to build your own.

ENABLE THE RIGHT CONTROLS FOR YOUR ORGANIZATION'S UNIQUE EMAIL DLP NEEDS

Design and deploy email filters by role and classifier to restrict access and prevent email communications across ethical walls, monitor abusive language, and prevent sensitive information like social security numbers and healthcare data from leaving the organization.

GRANULAR VISIBILITY AND CONTROL

Granular visibility into data exfiltration and view incidents in a single dashboard for easy remediation. Get complete insight into email data exfiltration, insider threats, and accidental data loss facing your email environment.

AUGMENT YOUR EXISTING MICROSOFT 365 DLP SOLUTIONS

Tessian augments MS365 with enhanced data and insider threat protection by closing critical DLP gaps such as accidental data loss, and sensitive data exfiltration to unauthorized and personal accounts.

ESTABLISH AND MAINTAIN REGULATORY COMPLIANCE

Protect against non-compliant activity and prevent users from sharing confidential data with non-business, personal addresses /unauthorized recipients; track and block compliance breaches in real-time.

RISK-ADAPTIVE PROTECTION

Comprehensive protection using adaptive machine learning to predict, prevent, detect and respond to data breaches. Personalized protection is based on individual users' risk level.

REDUCE BURDEN OF ONGOING OPERATIONS FOR SECURITY TEAMS

Reduce admin overhead with powerful policy logic that simplifies DLP configurations by an order of magnitude.

ENTERPRISE SCALABILITY

Tessian's DLP suite is cloud-delivered and offers simplified deployment, cross platform coverage, and flexible controls to stop high risk behavior.

SUPPORTS A ZERO TRUST APPROACH TO DATA PROTECTION

Tessian offers a range of capabilities across the email security environment with a rich set of integrations that allow for ease of deployment and management.

DATA LOSS PREVENTION FOR THE HUMAN LAYER:

Shift from Static, Rules-Based Methods, to a Dynamic Behavioral Approach

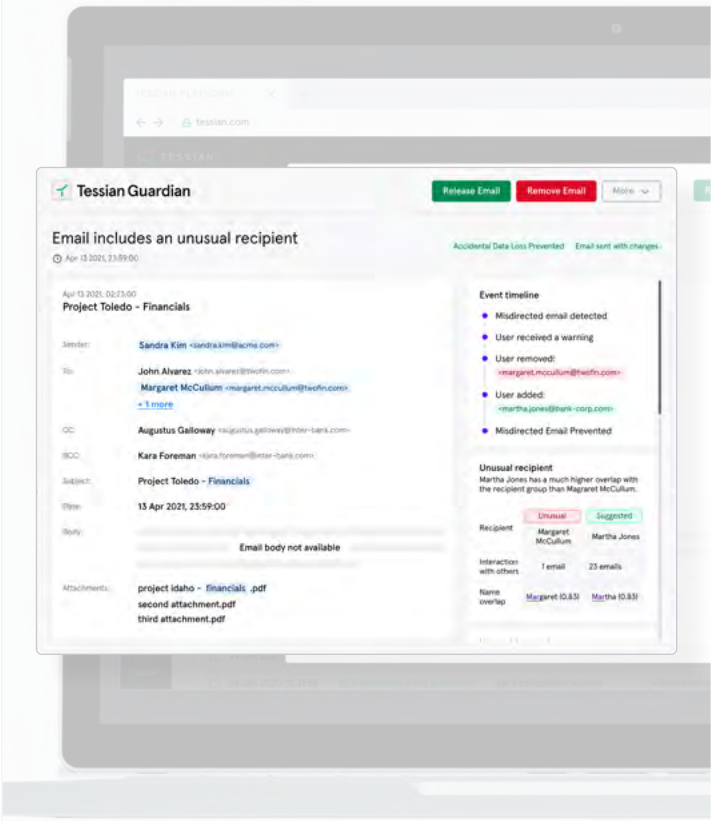
STOP ACCIDENTAL DATA LOSS

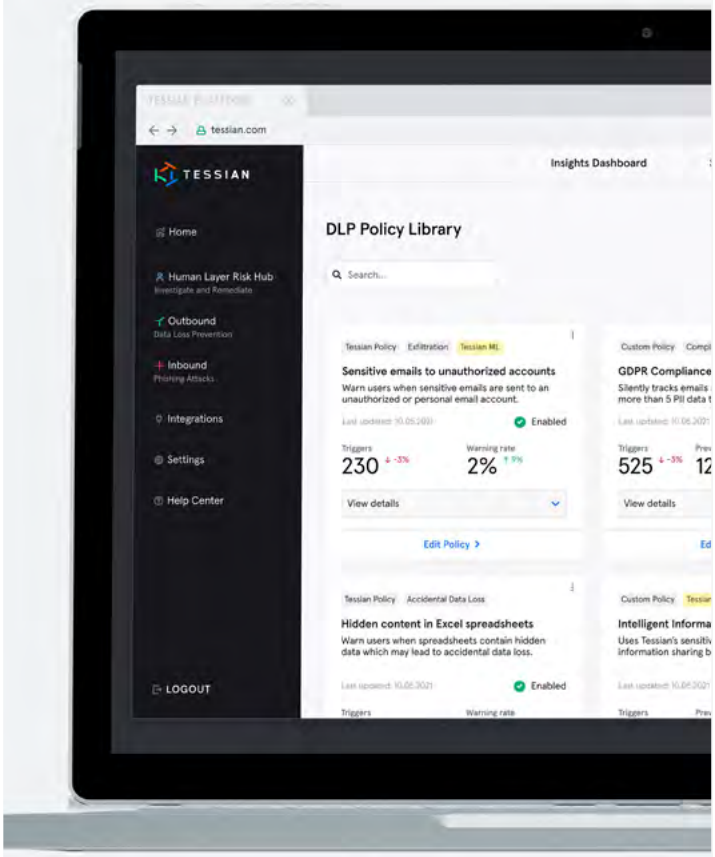
Automatically Prevent Accidental Data Loss to Unauthorized Parties

Tessian Guardian is the industry's only solution that automatically prevents accidental data loss from misdirected emails. Powered by Tessian's machine learning model, Guardian analyzes millions of data points for every outbound email and detects anomalies that indicate whether the email is being sent to the wrong person before it leaves your organization.

- Automatic protection using machine learning. No predefined rules required.
- Prevent accidental data breaches due to misdirected emails that are impossible-to-detect with legacy DLP controls.
- Safeguard your intellectual property, comply with customer confidentiality agreements and eliminate the risk of reputational damage.
- Meet GDPR, CCPA, and other mandatory data protection regulations.
- No behavior change required for employees, minimal end user disruption and zero admin for security teams.
- Reinforce security awareness and data protection policies through in-situ training.

LEARN MORE ABOUT TESSIAN GUARDIAN →





AUTOMATED AND CUSTOM DLP POLICIES

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 (Bonus: 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.

LEARN MORE ABOUT TESSIAN ARCHITECT →

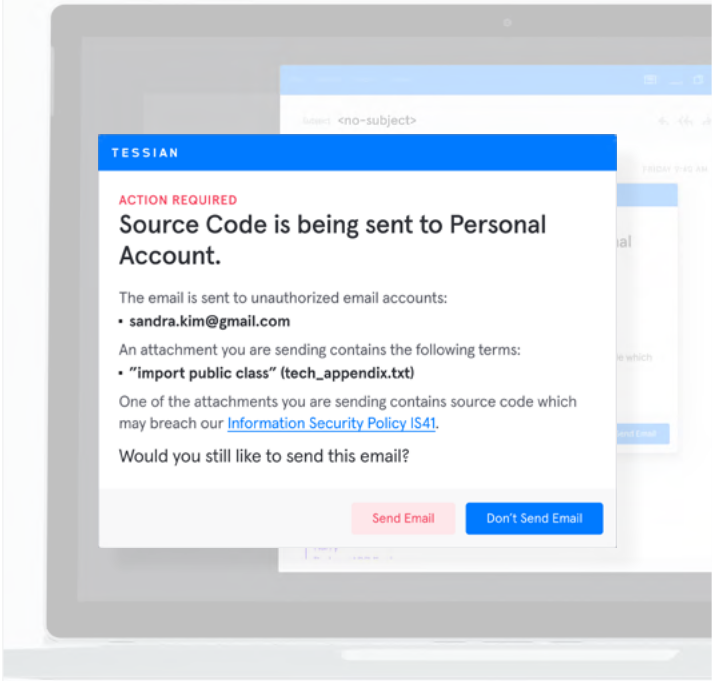
PREVENT DATA EXFILTRATION

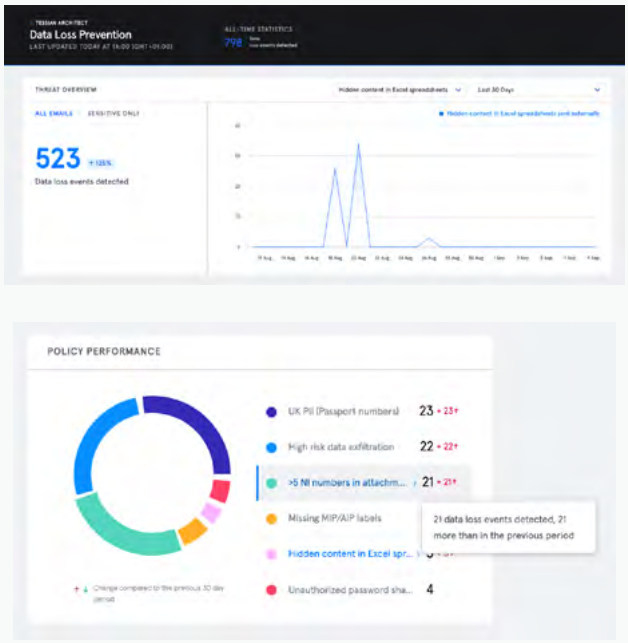
Automatically Stop Exfiltration of Sensitive Data to Unauthorized or Personal Accounts

Prevent data exfiltration via email to employee personal, unauthorized and non-business accounts. Tessian Enforcer analyzes millions of data points for every outbound email and detects anomalies that indicate data exfiltration before it leaves your organization.

- Automatically protect against data exfiltration via email. No predefined rules or denylists required.
- Instant visibility into high risk data exfiltration events, trends, and insiders, to take immediate actions.
- Safeguard intellectual property, comply with customer confidentiality agreements and eliminate risk of reputational damage.
- Meet GDPR, CCPA, PHI, HIPAA, and other mandatory data protection regulations.

LEARN MORE ABOUT TESSIAN ENFORCER →





CUSTOM DLP POLICY INSIGHTS

Analyze DLP Policy Performance Across Your Email Environment

Quickly and easily view 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

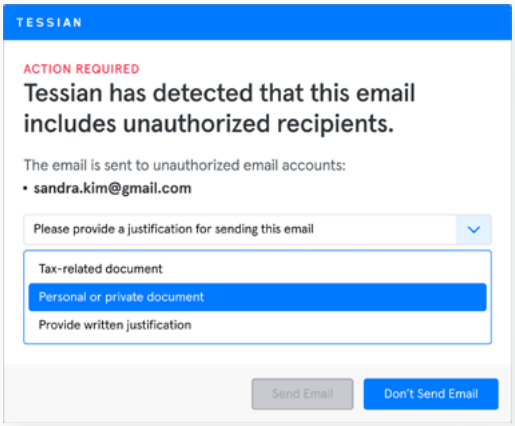
LEARN MORE ABOUT TESSIAN ARCHITECT →

SECURITY AND AWARENESS TRAINING

In-the-Moment Educational Warnings

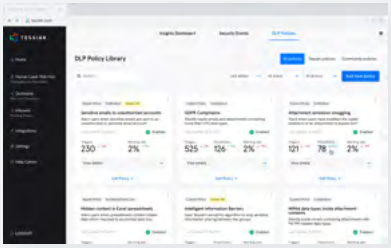
Tessian warnings act as in-the-moment training for employees, continuously educating them about threats, reinforcing your policies, and nudging them toward safe email behavior. Automatically build individualized policies at scale to reduce high-risk email use and track trends in unsafe activity over 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, becoming better at spotting inbound attacks and more careful when sending emails.



TESSIAN HUMAN LAYER SECURITY PLATFORM

Explore the Human Layer Security Platform

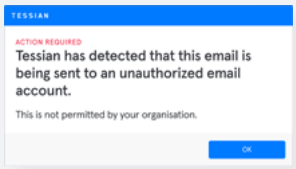


AUTOMATIC AND CUSTOM DLP POLICIES

Tessian Architect

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

LEARN MORE →

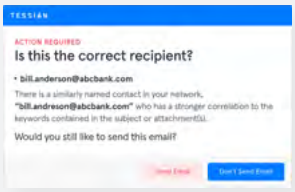


STOP DATA EXFILTRATION

Tessian Enforcer

Automatically prevent data exfiltration over email. Whether it's careless, negligent or malicious, Enforcer automatically detects data exfiltration and non-compliant activities on emails. No rules required.

LEARN MORE →



AUTOMATICALLY PREVENT DATA LOSS

Tessian Guardian

Stop accidental data loss from misdirected emails and misattached files before they happen. Ensure the right email is shared with the right person and prevent data breaches that are impossible to detect with legacy DLP controls.

LEARN MORE →

FLEXIBLE DEPLOYMENT AND SEAMLESS INTEGRATIONS:

Exchange · Office 365 · G Suite · splunk> · Radar · exabeam · SGS · AICPA SOC · DUO · ALIEN VAULT · RAPID7 · RSA

TRUSTED BY ENTERPRISE CUSTOMERS ACROSS ALL INDUSTRIES:

EVERCORE · arm · HERBERT SMITH FREEHILLS · REALPAGE · affirm · Schroders · rightmove · Investec · GRAPHCORE · sanne · K&L GATES · PeaceHealth · GOCARDLESS · MSCI · ERT · CLYDE&CO · BRACEWELL · RAND MERCHANT BANK · Intertrust · ManGroup plc

See Tessian in Action.

Book a demo and see first hand how Tessian's Human Layer Security Platform detects inbound and outbound email attacks that bypass legacy email security solutions.

REQUEST A DEMO →

TESSIAN | Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error - like data exfiltration, accidental data loss, business email compromise and phishing attacks - with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like March Capital, Sequoia, Accel, and Balderton.