Datasheet

Advanced Data Loss Prevention (DLP)

Advanced DLP from Censornet provides enterprise-class Data Loss Prevention (DLP) for email and web and cloud application data, enabling real-time discovery and blocking of confidential or sensitive data in flight.

Advanced DLP protects organisations against data loss associated with email and cloud application use, reducing risk and ensuring compliance with legislation and regulations, including GDPR, with support for personal data (Personally Identifiable Information) in 59 countries and 38 languages.

It is fully integrated with Censornet's autonomous integrated cloud security platform with a single central DLP policy engine. DLP rules can identify personal data (PII), payment card industry (PCI) and protected health information (PHI) data types using predefined out-of-the-box templates.

Censornet DLP is fully extensible. Custom data types can be defined quickly and easily to detect data that is of particular interest, or unique to an organisation - such as sensitive project codenames or keywords and phrases relating to specific intellectual property (IP).

Critical protection layer

Organisations of all sizes and in all sectors are increasingly focused on better protecting their data. Whether it's GDPR, PCI DSS, HIPAA, or other legislation, regulations and external audits - or organisational policies and internal assessments - data protection is critical.

Simply allowing upload of any file to an approved or sanctioned cloud application – such as M365 (OneDrive, SharePoint) – is no longer sufficient.

ADVANCED DLP

- Instant protection, just enable add-on licenses for Censornet Email, Web or Cloud Application Security (CASB)
- Prevents data loss in email message text (and attachments) by quarantining outbound emails
- Prevents data leaks associated with cloud application actions such as 'upload'
- Upload scanners isolate files and block uploads in real-time where files contain confidential and/or sensitive data, that breaches DLP policy
- Enforce uniform DLP on any combination of apps, users, devices and locations

The ability to extract and scan file content against a DLP policy, and preventing the action if confidential or sensitive data is identified, is rapidly becoming mandatory - even outside regulated industries.

Advanced DLP enables a 'DLP Scanner' tile for Email Security and extends the 'Content Scanner' tile for Web/CASB within the existing visual rule builders of the Censornet platform.

Adding DLP to Censornet rules takes seconds.

Exact DLP content analysis and actions can be implemented on top of existing rules to provide immediate data centric intelligence – and prevent data loss in real-time.

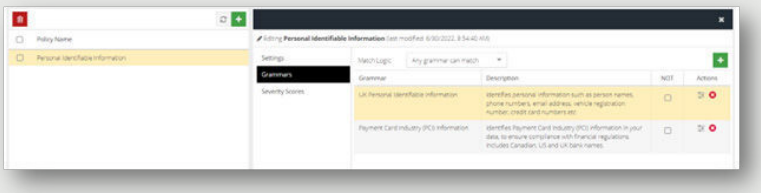
THE VALUE OF DATA LOSS PREVENTION

- Up to 94% of companies that experience a severe data loss never recover.
- Human error is among the top three causes of data loss, and plays a part in 82% of breaches.
- 72% of employees have accidentally sent sensitive information to the wrong person.

[Consoltech] [Verizon] [Egress]

Advanced Data Loss Prevention (DLP) datasheet

Policies, Grammars and Entities (data types)



DLP polices are built using Grammars (a.k.a. Dictionaries).Grammars contain Entities (data types) that include words or keywords, patterns (Reg Ex) and synonyms.
The out-of-the-box pre-configurations are extensive, providing flexibility that translates into rapid policy definition. Grammars can be combined in rules and policies using AND, OR and NOT logic. Once created, DLP Polices can be used in email, web and inline CASB rules.

For greater control, Severity Scores can be tuned for data types representing the highest risk or exposure based on organisational attributes and activities. Polices can also be applied to specified file types (default is 'all').

Advanced DLP is fully integrated with the Censornet platform and the admin portal provides rich data visualization and reporting across an extensive set of attributes and criteria. Analysis and reporting is available by time, user, device, app class, app name, app action, keywords, risk level and outcome (block or allow).

Whether audit data is required purely for visibility into data in flight, or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, Advanced DLP will provide the evidence needed.

KEY FEATURES

Pre-defined Policies	• Personal Data (PII) – UK – inc. names, passport and NI numbers • Personal Data (PII) – US – inc. names, passport and social security numbers • Payment Card Industry Data Security Standard (PCI DSS) • Personal Health Information (PHI) – inc. medical conditions, procedures and drugs • API Credentials – credential and key information for common web services • Computer Addresses – inc. HTTP, FTP, IP (v4/v6) MAC and file addresses • Profanity – inc. social, homophobic and sexually offensive terms
Policy Configuration	• Select whether the policy should apply to 'All Products', 'Email Security', 'Web Security / CASB Inline' • Match Case Sensitive/Case Insensitive, Locale (tokenisation of Chinese, Japanese, Korean, Thai languages), include punctuation characters, Whole Word • Severity Levels – Low, Medium, High, Critical. Each Grammar is evaluated and returns a normalised score (0-100) – defaults can be modified if required
Grammars	• Grammars are dictionaries that define what data types (Entities) are detected • Grammars contain Entities in multiple languages and regional formats • All Grammars are extensible • Multiple Grammars can be combined using AND, OR, and NOT logic
Grammar Customisation	• Remove Entities • Add/change Entities – based on Patterns/Regular Expressions inc. Synonyms
File Types	• Policies are applied to all content by default • Policies can be limited to specific file types – by extension and MIME type

Grammar Categories	• Address – physical addresses, post code, ZIP code • API credentials – inc. AWS, Facebook, LinkedIn, Twitter • Car Licence Plate – vehicle registrations in multiple regional formats • Companies – significant companies in different countries • Computer – IP address (v4/v6), HTTP, FTP, MAC address and file address • Date/Time – in different regional formats • Driver Licence – driving licence numbers in different regional formats • Job Titles – job titles including abbreviations inc. government and cabinet titles • Medical – didease names, medical terms, medication (trade and generic drug names) • Passport – passport numbers in different regional formats • PCI – credit card numbers (PANs), bank account numbers, sort codes, IBAN/SWIFT • Phone Numbers (requires tangible characters such as '+' and '(' • PII – age, nationality, ethnicity, email addresses, NI/Social Security numbers, medical ID, person first and last names, salutations • Places – identifies settlements in different countries inc. population size • Profanity – blasphemous, homophobic, racial derogatory, sexual, biological or censored words for different regions and countries

DEPLOYMENT

Email Security	• Advanced DLP add on license for Email Security is required
CASB Inline and Web	• Advanced DLP add on license for CASB and Web is required
CASB API Mode	• Advanced DLP for CASB API mode coming soon • Apps supported include box, Dropbox, Google Drive, Microsoft OneDrive and SharePoint • Enables DLP scanning of all data at rest (Data Security Posture Management)

Advanced Data Loss Prevention (DLP) datasheet

Censornet Platform

E. EMAIL

Secure your entire organization from known, unknown & emerging email security threats - including email fraud.

S. SAT

Defend your organisation against cybercriminals by strengthening your engaging and stimulating automated training.

W. WEB

Protect users from webborne malware, offensive or inappropriate content & improve productivity.

C. CASB

Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.

M. MFA

Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.

ID. IDaaS

Control user access with complete identity-threat protection. Automatically authenticate users using rich contextual data.

Our Platform

Our cloud security platform integrates email, web, and cloud application security, working seamlessly with powerful identity management to activate the Autonomous Security Engine (ASE).

This takes you beyond alert driven security and into real-time automated attack prevention.

Autonomous Security Engine

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence. Prevent attacks before they enter the kill chain.

ASE provides 24x7 security so you don't need to.

Full access to threat intelligence without the cost.

CENSORNET LTD
Matrix House, Basing View, Basingstoke, RG21 4FF, UK
Phone: +44 (0) 845 230 9590

CENSORNET LTD
Park Allé 350D, 2605 Brondby, Denmark
Phone: +45 61 80 10 13

CENSORNET LTD
700 Lavaca Street Suite 1400-PMB#100122 Austin, TX 78701
Phone: +1 (877) 302-3323