SASE/SSE WHITE PAPER

An overview of Data Loss Prevention (DLP) from Windstream Enterprise

How does an organization prevent against crippling data loss? DLP, a key component of Secure Access Service Edge (SASE) and Security Service Edge (SSE), protects sensitive enterprise data from modern day cybersecurity threats.

Ever wonder how much data is created every day? Thanks to the widespread adoption of mobile technology, along with incredible access to anywhere network connectivity and WiFi, the creation and consumption of data is unstoppable on its exponential growth trajectory.

Data has such a critical value to all enterprises, yet it has becoming more difficult to guard, especially considering how much of it resides in the cloud. While there are numerous tools available for an organization to restrict access to enterprise assets, nothing offers a more efficient solution to protecting the movement of information to-and-from enterprise assets than SASE/SSE DLP.

Executive takeaways

Here's what you'll learn from this whitepaper:

1. The severe implications of data loss and what makes enterprise information "sensitive".
2. Which assets your organization needs to protect, and why you'll benefit from Windstream Enterprise's effective DLP solution.
3. Ways to identify data types through a DLP engine, and how to define which policies will best protect against data loss within your organization.
4. What insights can be gained into DLP-related events with the complete visibility and control of Windstream Enterprise's customer management portal.

WINDSTREAM ENTERPRISE | CATO NETWORKS

How do you measure the value of data?

A modern enterprise's most valuable asset is its data. The growing importance and value of intangible assets has risen from 17% of the value of the S&P 500 in 1975 to around 90% in 2022[1]. Be it intellectual property like source code or blueprints, sensitive business information like financial metrics or customer data, or sensitive personal information like Personally Identifiable Information (PII) or Personal Health Information (PHI)—their combined value far exceeds physical assets. If sensitive enterprise information were to reach the wrong hands, it could have devastating implications for the victim organization's business, also leading to damaged reputation and exposure to legal action.

Protecting sensitive corporate information is also often required for regulatory compliance, such as the Payment Card Industry (PCI) data security standard or the Health Insurance Portability and Accountability Acts (HIPAA).

How to protect your enterprise data?

One of the most effective tools to help enterprises protect their sensitive information and ensure regulatory compliance is Data Loss Prevention (DLP). DLP can scan all traffic being sent to, or from, enterprise assets in order to detect sensitive information and take the appropriate action. But what does this mean exactly? What makes information sensitive? How do we identify it? And which assets do we need to protect? Let's take a deeper look.

What makes information "sensitive"?

Sensitive information appears in two main forms:

Sensitive data

Sequences of characters which contain sensitive data, such as social security numbers, IP addresses, credit card numbers, etc.

Sensitive file types

Files of a certain type that the enterprise regards as being sensitive, such as source code (e.g., Java) or design files (e.g., AutoCAD).

How do we identify sensitive data?

Sensitive data is detected by matching content with known data type structures. For example, U.S. social security numbers have a structure of 123–45–6789. When a matching sequence of digits is found within the scanned data, it is marked as having a high potential of being a social security number, and the defined action is taken.

Windstream Enterprise DLP scans data within files, for example a Microsoft Word document, as well as stand-alone information sent to or from an application via a form.

The Windstream Enterprise DLP engine includes more than 350 data types covering globally sensitive information (e.g., credit card numbers) as well as county-specific information (e.g., U.S. postal codes) covering more than 30 countries.

In order to enable fast and efficient lookup, Windstream Enterprise's DLP classifies data types using two main attributes: Category and country.

Category-based data types

Data categories include general classifications, such as PII and regulatory classifications, such as HIPAA. The categories covered by Windstream Enterprise DLP are listed in fig.1.

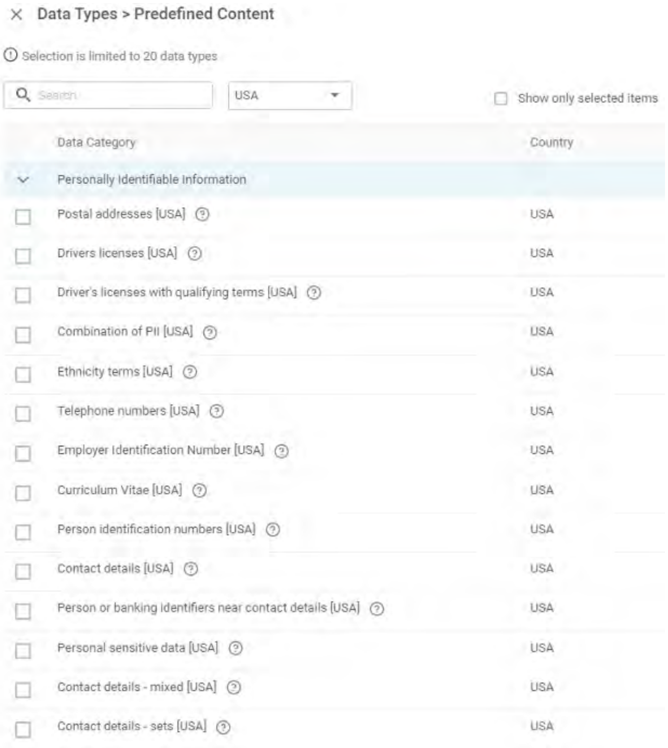
Country-based data types

Data types can also be filtered by country to view localized content types. When selecting the Canada for example, all data types relevant to the Canada are shown, such as postal addresses and personal identification numbers. The Canada specific PII data types are shown in fig. 2.

In order to simplify the selection of several data types from a certain category, Windstream Enterprise DLP groups data types that are commonly selected together into a combined data type, for example, "Combination of personally identifiable information [UK]".

Windstream Enterprise DLP also enables searching the full list of data types in order quickly find data types by name or based on a known term, such as "personal" or "post".

Fig.1: PII for USA



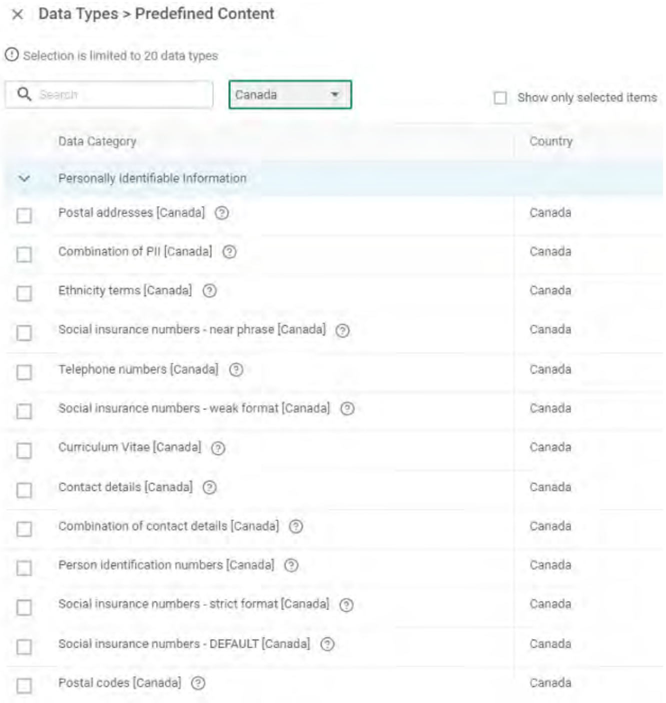
× Data Types > Predefined Content

ⓘ Selection is limited to 20 data types

Search | USA ▾ | □ Show only selected items

	Data Category	Country
⌄	Personally Identifiable Information	
□	Postal addresses [USA] ?	USA
□	Drivers licenses [USA] ?	USA
□	Driver's licenses with qualifying terms [USA] ?	USA
□	Combination of PII [USA] ?	USA
□	Ethnicity terms [USA] ?	USA
□	Telephone numbers [USA] ?	USA
□	Employer Identification Number [USA] ?	USA
□	Curriculum Vitae [USA] ?	USA
□	Person identification numbers [USA] ?	USA
□	Contact details [USA] ?	USA
□	Person or banking identifiers near contact details [USA] ?	USA
□	Personal sensitive data [USA] ?	USA
□	Contact details - mixed [USA] ?	USA
□	Contact details - sets [USA] ?	USA

Fig. 2: PII for Canada



× Data Types > Predefined Content

ⓘ Selection is limited to 20 data types

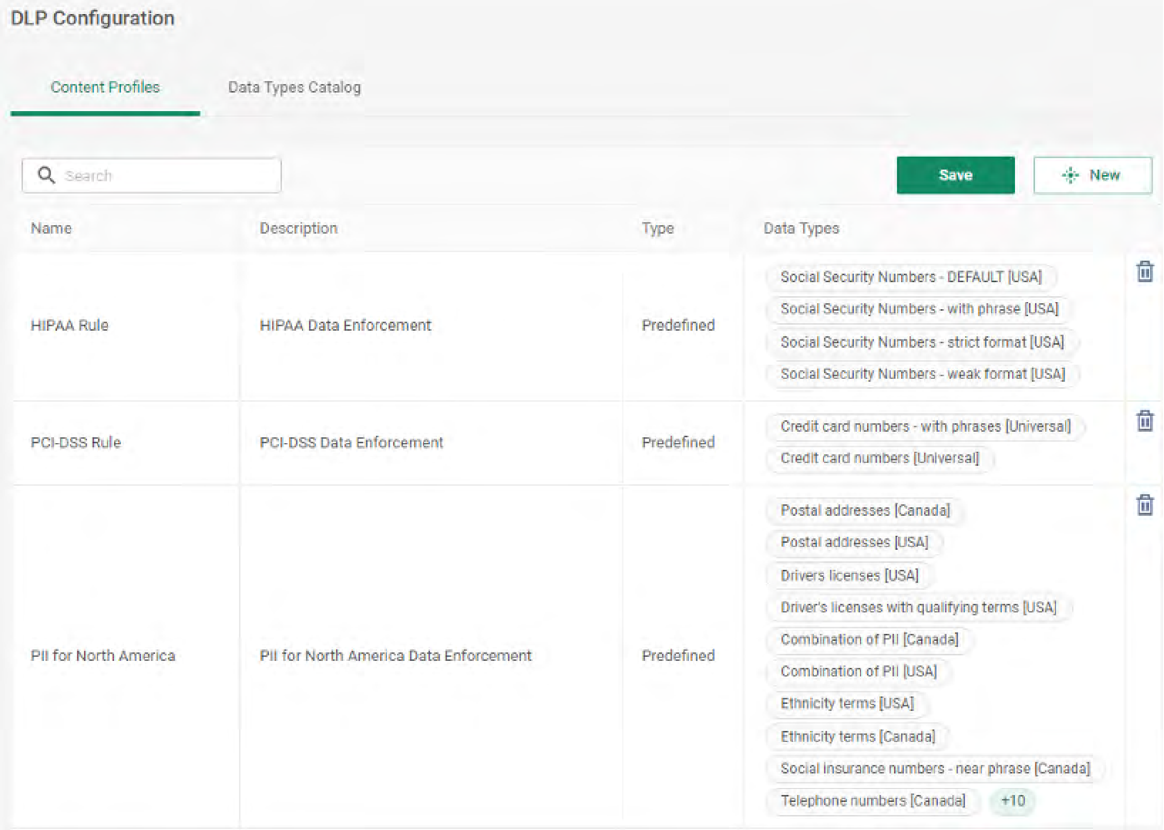
Search | Canada ▾ | □ Show only selected items

	Data Category	Country
⌄	Personally Identifiable Information	
□	Postal addresses [Canada] ?	Canada
□	Combination of PII [Canada] ?	Canada
□	Ethnicity terms [Canada] ?	Canada
□	Social insurance numbers - near phrase [Canada] ?	Canada
□	Telephone numbers [Canada] ?	Canada
□	Social insurance numbers - weak format [Canada] ?	Canada
□	Curriculum Vitae [Canada] ?	Canada
□	Contact details [Canada] ?	Canada
□	Combination of contact details [Canada] ?	Canada
□	Person identification numbers [Canada] ?	Canada
□	Social insurance numbers - strict format [Canada] ?	Canada
□	Social insurance numbers - DEFAULT [Canada] ?	Canada
□	Postal codes [Canada] ?	Canada

Creating modular DLP data types and policies at scale

When defining DLP rules we will typically use a combination of data types. These combinations will be relevant to more than one application. In order to avoid the need to select the same set of data types repeatedly, potentially hundreds of times, Windstream Enterprise's DLP takes a "building block" approach to defining rules in order to simplify the process, yet make it as flexible and customizable as needed. Windstream Enterprise's DLP enables grouping data types into profiles which can then be used to quickly define DLP rules. For example, we can create a profile called, "PII for North America" which also includes PII data types used in North American countries—see fig. 3.

Fig. 3: DLP profile for PII in North America



Name	Description	Type	Data Types
HIPAA Rule	HIPAA Data Enforcement	Predefined	Social Security Numbers - DEFAULT [USA] Social Security Numbers - with phrase [USA] Social Security Numbers - strict format [USA] Social Security Numbers - weak format [USA]
PCI-DSS Rule	PCI-DSS Data Enforcement	Predefined	Credit card numbers - with phrases [Universal] Credit card numbers [Universal]
PII for North America	PII for North America Data Enforcement	Predefined	Postal addresses [Canada] Postal addresses [USA] Drivers licenses [USA] Driver's licenses with qualifying terms [USA] Combination of PII [Canada] Combination of PII [USA] Ethnicity terms [USA] Ethnicity terms [Canada] Social insurance numbers - near phrase [Canada] Telephone numbers [Canada] +10

DLP policies in action

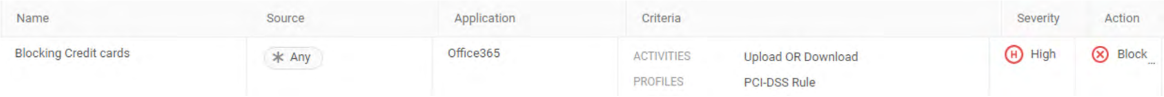
DLP rules are where we define the actual policies we want to implement. They combine the data profiles we have defined for matching sensitive information with the behavior we want to enforce the policy to. The following are examples of common DLP use cases. Each will demonstrate the policy we want to enforce and the DLP rule that will implement it.

Use case #1

Required policy: Block any downloads of credit card information in Office365

The rule implementing this policy can be seen in Fig. 4. We can see the request to "block" defined in the Action parameter, "download" defined in the Criteria: Activities, "credit card" represented in Criteria: Profile, and "Office365" defined in the Application parameter. "Any" is defined in the Source parameter to indicate this should be applied to all sources.

Fig. 4: DLP policy for blocking credit card information in Office365



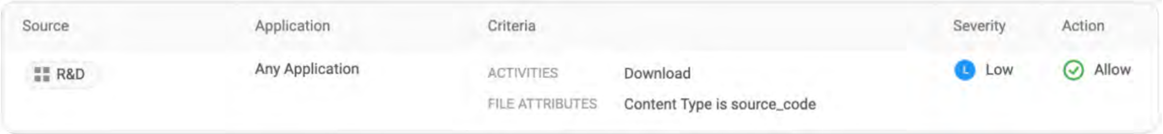
Name	Source	Application	Criteria		Severity	Action
Blocking Credit cards	Any	Office365	ACTIVITIES PROFILES	Upload OR Download PCI-DSS Rule	High	Block

Use case #2

Required policy: Enable only R&D users to download source code files

In this case, we want to allow only the Research and Development (R&D) group to download files, so the Action parameter in Fig. 5 will be set to "Allow" and the Source parameter to "R&D". Since we're not limiting this rule to specific applications, the Application parameter value will be "Any Application". The Criteria: File Attributes will be set to "Content Type is source_code", meaning the rule will be applied to this file type, rather than any specific matching content within the file.

Fig. 5: DLP policy for allowing R&D users to download source code files



Source	Application	Criteria		Severity	Action
R&D	Any Application	ACTIVITIES FILE ATTRIBUTES	Download Content Type is source_code	Low	Allow

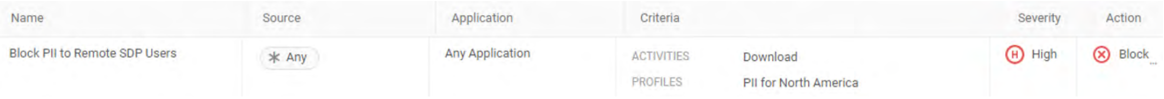
What is important to note in this example, is that in order for all non-R&D traffic to be blocked, we will need to add rule blocking "Any" other source traffic. As rules are applied in their define order, all R&D traffic will be allowed to download files, while all other user types will reach the subsequent block rule.

Use case #3

Required policy: Block downloads of PII to remote Software Defined Perimeter (SDP) users

What is unique in this case is that we want to restrict data access to remote SDP users from downloading sensitive PII information from other locations. As can be seen in Fig. 6,

Fig. 6: DLP Policy to block downloads of PII to remote SDP users



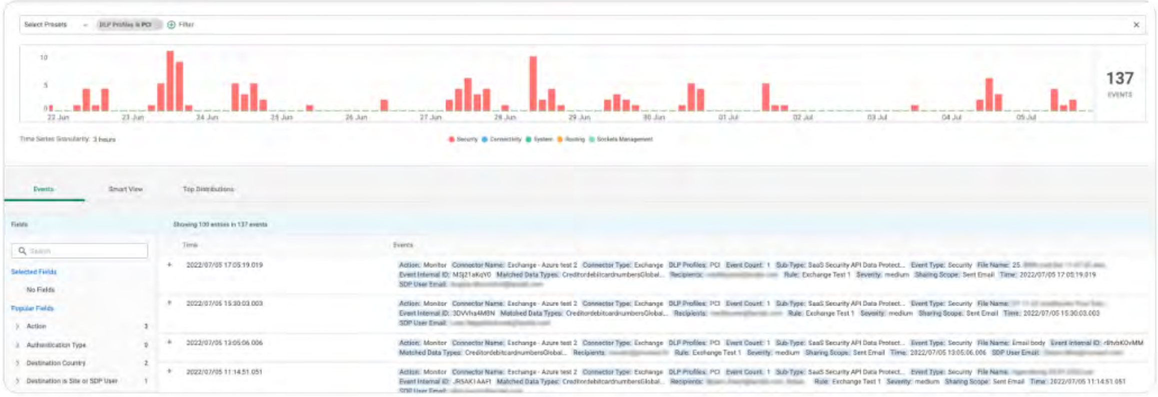
Name	Source	Application	Criteria		Severity	Action
Block PII to Remote SDP Users	✱ Any	Any Application	ACTIVITIES PROFILES	Download PII for North America	Ⓗ High	⊗ Block

Gaining insight into DLP activity

All DLP-related events can be seen in the events view (Fig. 7), which lives in the Windstream Enterprise customer management portal.

Events can be searched and filtered in numerous ways to help explore DLP trends or investigate a specific event. Events of interest can be drilled down into, providing rich data and insight into their origins and cause.

Fig. 7: DLP events view



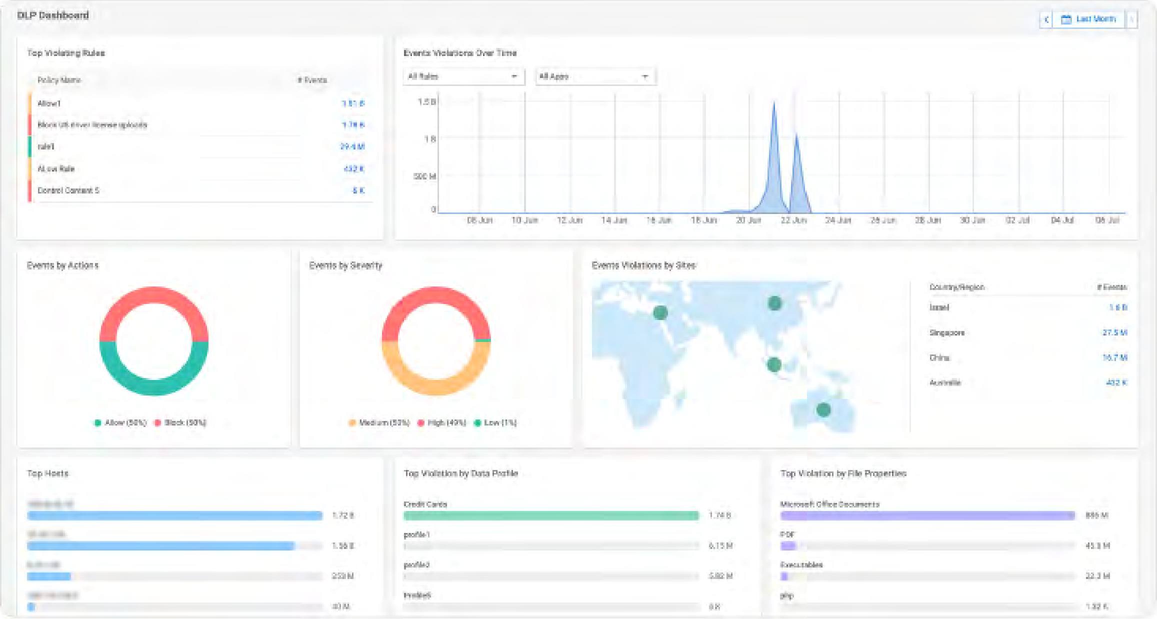
Popular Fields	
Action	3
Authentication Type	0
Destination Country	2
Destination is Site or SDP User	1

Showing 100 entries in 137 events

Time	Events
2022/07/05 17:05:19.019	Action: Monitor Connector Name: Exchange - Azure test 2 Connector Type: Exchange DLP Profiles: PCI Event Count: 1 Sub-Type: SaaS Security API Data Protect... Event Type: Security File Name: 25. [redacted] Event Internal ID: MSj21aKqY0 Matched Data Types: CreditordebitcardnumbersGlobal... Recipients: [redacted] Rule: Exchange Test 1 Severity: medium Sharing Scope: Sent Email Time: 2022/07/05 17:05:19.019 SDP User Email: [redacted]
2022/07/05 15:30:03.003	Action: Monitor Connector Name: Exchange - Azure test 2 Connector Type: Exchange DLP Profiles: PCI Event Count: 1 Sub-Type: SaaS Security API Data Protect... Event Type: Security File Name: [redacted] Event Internal ID: 3DVvha4M8N Matched Data Types: CreditordebitcardnumbersGlobal... Recipients: [redacted] Rule: Exchange Test 1 Severity: medium Sharing Scope: Sent Email Time: 2022/07/05 15:30:03.003 SDP User Email: [redacted]
2022/07/05 13:05:06.006	Action: Monitor Connector Name: Exchange - Azure test 2 Connector Type: Exchange DLP Profiles: PCI Event Count: 1 Sub-Type: SaaS Security API Data Protect... Event Type: Security File Name: Email body Event Internal ID: r8tvbKOvMM Matched Data Types: CreditordebitcardnumbersGlobal... Recipients: [redacted] Rule: Exchange Test 1 Severity: medium Sharing Scope: Sent Email Time: 2022/07/05 13:05:06.006 SDP User Email: [redacted]
2022/07/05 11:14:51.051	Action: Monitor Connector Name: Exchange - Azure test 2 Connector Type: Exchange DLP Profiles: PCI Event Count: 1 Sub-Type: SaaS Security API Data Protect... Event Type: Security File Name: [redacted] Event Internal ID: JRSAK1AAFI Matched Data Types: CreditordebitcardnumbersGlobal... Recipients: [redacted] Rule: Exchange Test 1 Severity: medium Sharing Scope: Sent Email Time: 2022/07/05 11:14:51.051 SDP User Email: [redacted]

Windstream Enterprise DLP also offers a dashboard which provides a high-level view of DLP related activity in the network. This enables quick insight into key data movement metrics, such as top violating DLP rules, hosts, profiles, file types and locations. Additionally, it includes a breakdown of events by action and severity. The DLP dashboard provides a unique vantage point which can help identify anomalies or changes in data usage, indicating to possibly suspicious user behavior.

Fig. 8: DLP dashboard



Top Violating Rules

Policy Name	# Events
Allow1	1.51 B
Block US driver license uploads	1.78 K
rule1	29.4 M
ALow Rule	432 K
Control Content 5	5 K

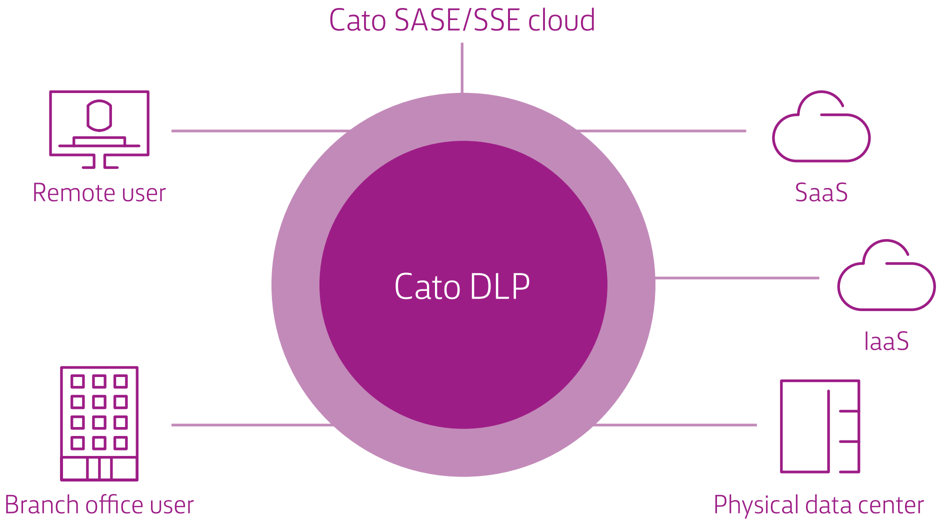
Country/Region	# Events
Israel	1.6 B
Singapore	27.5 M
China	16.7 M
Australia	432 K

Which assets do you need to protect?

Sensitive information typically resides within enterprise applications. These can be proprietary applications managed by the enterprise itself or 3rd party Software-as-a-Service (SaaS) applications, like Salesforce, Office 365 and Box. As most SaaS applications used in a typical enterprise are unsanctioned, an effective DLP solution must cover them too.

Windstream Enterprise DLP is delivered as part of a comprehensive SASE/SSE Cloud service and provides coverage for all traffic to all enterprise assets (fig. 9). This includes also on-prem applications hosted in the enterprise's physical data centers, which most DLP solutions do not have visibility into and therefore do not cover. Additionally, Windstream Enterprise DLP follows Zero Trust principles in which we can define DLP rules for applications and activities for which no explicit rules have yet been defined. This means that through this solution, clients can enforce restrictive policies for unsanctioned applications (AKA shadow IT) and ensure sensitive content isn't uploaded to, or downloaded from, these applications before there's been a better chance to understand their purpose and potential risk.

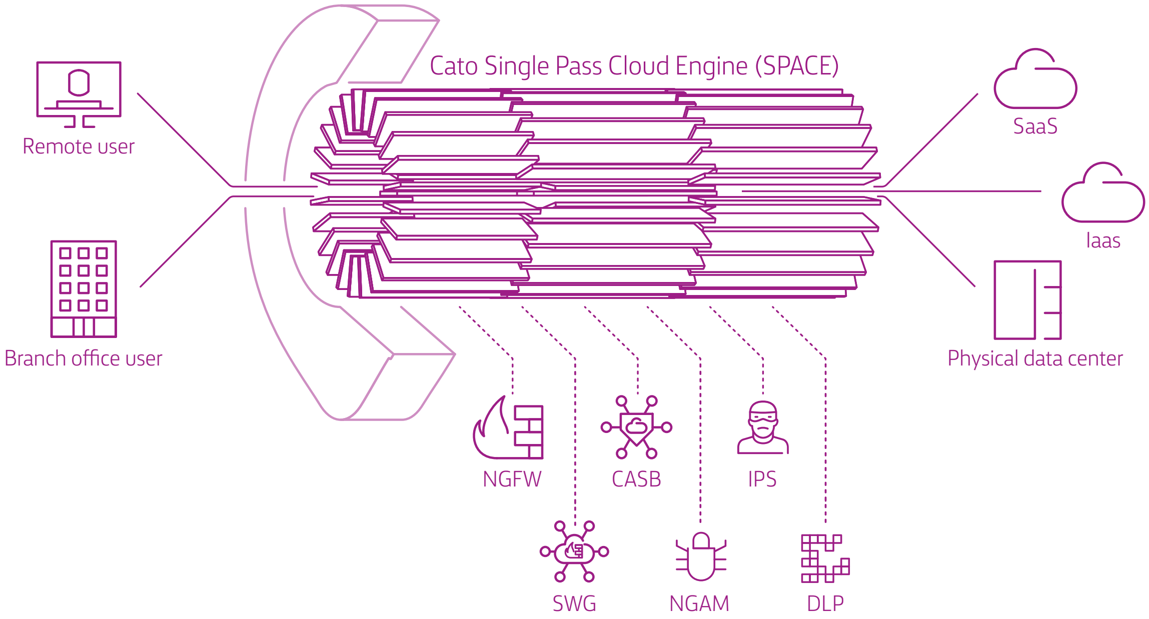
Fig. 9: SASE/SSE coverage for all traffic



A fully converged SASE/SSE solution from Windstream Enterprise

Secure Access Service Edge (SASE) and Security Service Edge (SSE) from Windstream Enterprise, powered by Cato Networks, converges DLP with additional application access and threat mitigation services. Windstream Enterprise SASE/SSE uses a Single Pass Cloud Engine (SPACE) to employ these services concurrently and with a shared context, enabling visibility into information collected and processed by the others, to enable them to make better informed decisions (fig 10). This also shortens the overall processing time and reduces latency, which is further optimized by the fact that Transport Layer Security (TLS) encryption and decryption needs to be done once for all services.

Fig. 10: Single Pass Cloud Engine (SPACE)



SASE/SSE from Windstream Enterprise also advances the enterprise's overall security posture by implementing a layered access and content inspection approach. In the context of DLP protection of sensitive information, users will need to pass several security services before they get to the position where they can even attempt uploading or downloading sensitive information.

Users must first pass Windstream Enterprise's Next Generation Firewall (NGFW), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and for remote users also Zero Trust Network Access (ZTNA) service to gain access to any application. Only then will they be able to attempt to transfer sensitive information, at which point, DLP will take action.

In tandem, Windstream Enterprise's Intrusion Prevention System (IPS) will scan the traffic to detect malicious infiltration attempts. The Next Generation Anti-Malware (NGAM) will scan traffic to detect attempts to transfer malicious content into enterprise assets.

Cloud-enabled connectivity, communications and security—guaranteed.

1. BrandFinance®, Alex Haigh, November 29, 2022.

To learn more about SASE, visit windstreamenterprise.com/solutions/sase

To learn more about SSE, visit windstreamenterprise.com/solutions/sse

WINDSTREAM ENTERPRISE | CATO NETWORKS