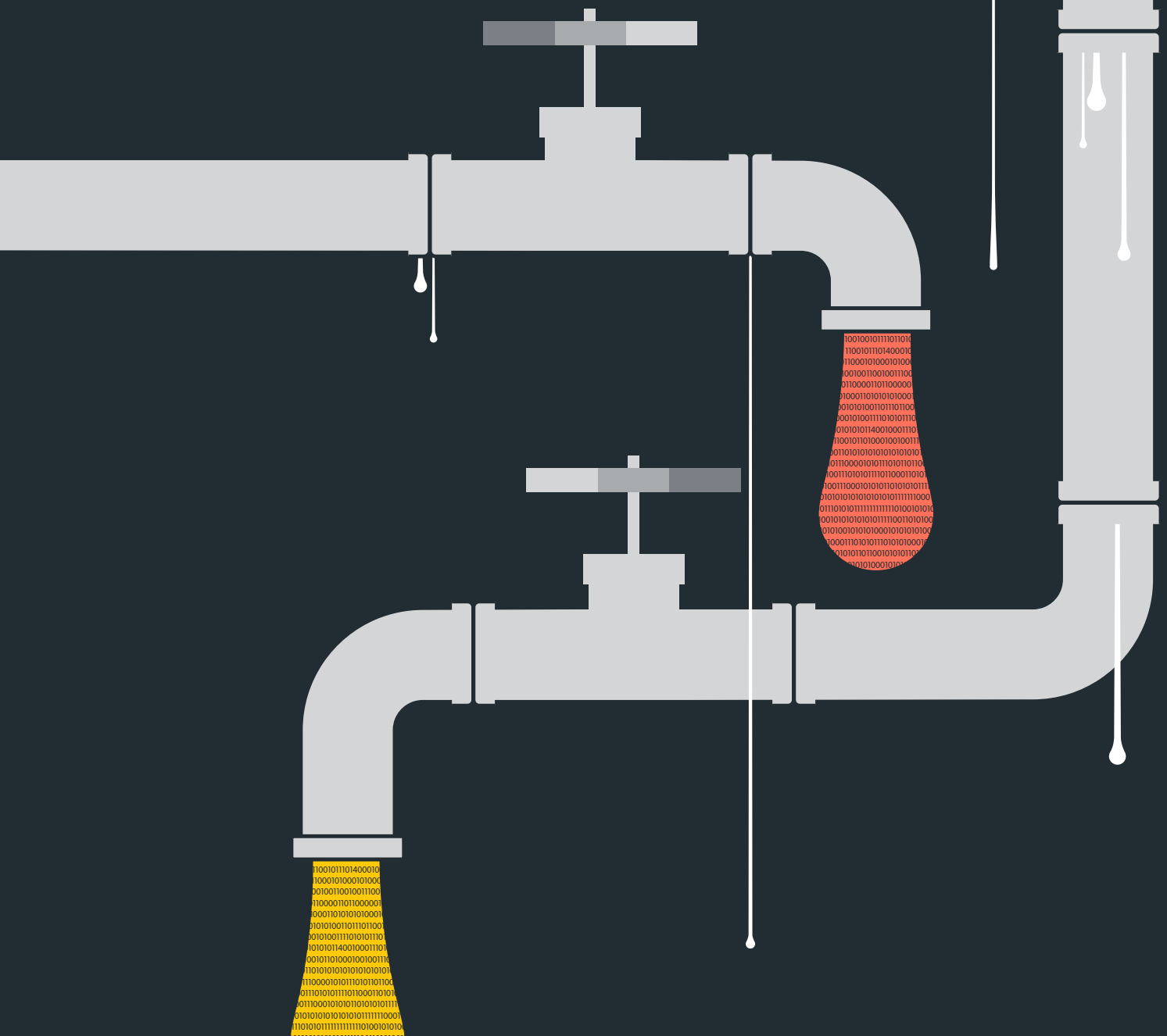


An Overview of

# Cato Data Loss Prevention (DLP)



# How Do You Measure the Value of Data?

A modern enterprise's most valuable asset is its data. A recent study of S&P 500 companies showed that intangible assets constitute 90% of their total value. Be it intellectual property such as source code or blueprints, sensitive business information such as financial metrics or customer data, or sensitive personal information such as Personally Identifiable Information (PII) or Personal Health Information (PHI) of employees or customers—their combined value far exceeds that of the company's physical assets. If sensitive enterprise information were to reach the wrong hands, it could have devastating implications for the victim organization's business, leading also 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). A 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 number, 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, US social security numbers have a structure of 123-45-6789 (3 numbers, 3, 2, and 4 digits long, respectfully). 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.

**Cato's DLP** scans data within files, for example a Word document, as well as stand-alone information sent to or from an application via a form.

Cato's 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. US postal codes) covering more than 30 countries.

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



## Category-based Data Types

Data categories include general classifications such as Personal Identifiable Information (PII) and regulatory classifications such as Health Insurance Portability and Accountability Act (HIPAA). The categories covered by Cato's DLP are listed in fig.1.

×

Data Types > Predefined Content

ⓘ Selection is limited to 20 data types

🔍 Search

France ▾

☐ Show only selected items

Data Category	Country
▼ Personally Identifiable Information	
<input type="checkbox"/> Postal addresses [France] ⓘ	France
<input type="checkbox"/> Combination of PII [France] ⓘ	France
<input type="checkbox"/> INSEE numbers [France] ⓘ	France
<input type="checkbox"/> Telephone numbers [France] ⓘ	France
<input type="checkbox"/> INSEE numbers with qualifying terms [France] ⓘ	France
<input type="checkbox"/> Contact details [France] ⓘ	France
<input type="checkbox"/> Person identification numbers [France] ⓘ	France

Figure 1: Data Type Categories



## Country-based Data Types

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

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

× **Data Types > Predefined Content**

! Selection is limited to 20 data types

UK ▾

☐ Show only selected items

Data Category	Country
<div> <div>▼</div> <div>Personally Identifiable Information</div> </div>	
<input type="checkbox"/> Postal addresses [UK] ⓘ	UK
<input type="checkbox"/> Combination of personally identifiable information [UK] ⓘ	UK
<input type="checkbox"/> Personal identifiers near contact details [UK] ⓘ	UK
<input type="checkbox"/> Ethnicity terms [UK] ⓘ	UK
<input type="checkbox"/> Telephone numbers [UK] ⓘ	UK
<input type="checkbox"/> Curriculum Vitae [UK] ⓘ	UK
<input type="checkbox"/> Contact details [UK] ⓘ	UK
<input type="checkbox"/> Combination of contact details [UK] ⓘ	UK
<input type="checkbox"/> Person identification numbers [UK] ⓘ	UK
<input type="checkbox"/> Personal sensitive data [UK] ⓘ	UK
<input type="checkbox"/> National Insurance numbers - strict format [UK] ⓘ	UK
<input type="checkbox"/> National Insurance numbers - flexible format [UK] ⓘ	UK
<div> <div>&gt;</div> <div>PCI DSS</div> </div>	
<div> <div>&gt;</div> <div>Document classification</div> </div>	
<div> <div>&gt;</div> <div>Health Care</div> </div>	

Figure 2: Personally Identifiable Information (PII) for the UK

Cato's 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".

# Creating Modular DLP Data Types and Policies at Scale

When defining DLP rules we will typically use a combination of data types and 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, Cato's DLP takes a "building blocks" approach to defining rules in order to simplify the process, yet make it as flexible and customizable as needed. Cato'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 "Europe PII" which includes PII data types used in European countries (fig. 3).

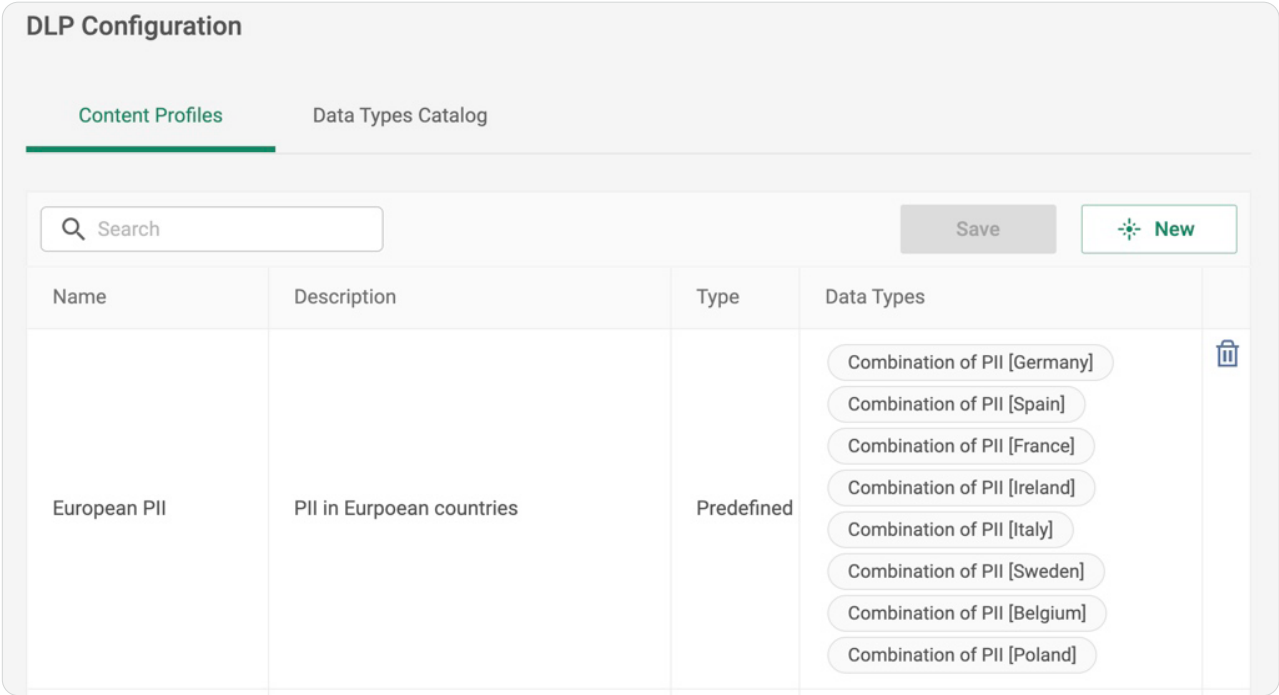


Figure 3: DLP Profile for PII in Europe

# Cato 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 example will show the policy we want to enforce and the DLP rule implementing it.

## Use-case #1

### Required policy: Block any downloads of German 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, "German 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 attempting such a download.




Source	Application	Criteria		Severity	Action
 Any	Office365	ACTIVITIES	Download	 High	 Block
		PROFILES	PCI Germany		

Figure 4: DLP Policy for Blocking German Credit Card Information in Office365

## Use-case #2

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

In this case we want to allow only the 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 we're not limiting this rule to specific applications, the Application parameter value will be "Any Application". The Criteria: File Attribute will be set to "Content Type is source\_code", meaning the rule will be applied to this filetype, rather than any specific matching content within the file.




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

Figure 5: DLP Policy for Allowing R&D users to Download Source Code Files

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 European PII to a Chinese site

What is unique in this case is that we want to restrict data access to users from a site in a specific location. As can be seen in Fig. 6, the Source parameter is set to the name of the site as defined in the enterprise's network: "Beijing".




Source	Application	Criteria		Severity	Action
 Beijing	Any Application	ACTIVITIES	Download	 High	 Block
		PROFILES	Europe PII		

Figure 6: DLP Policy for Blocking European PII to China Site

# Gaining Insight into DLP Activity

All DLP related events can be viewed in the events viewer (Fig. 7) in the Cato Management Application (CMA).

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.

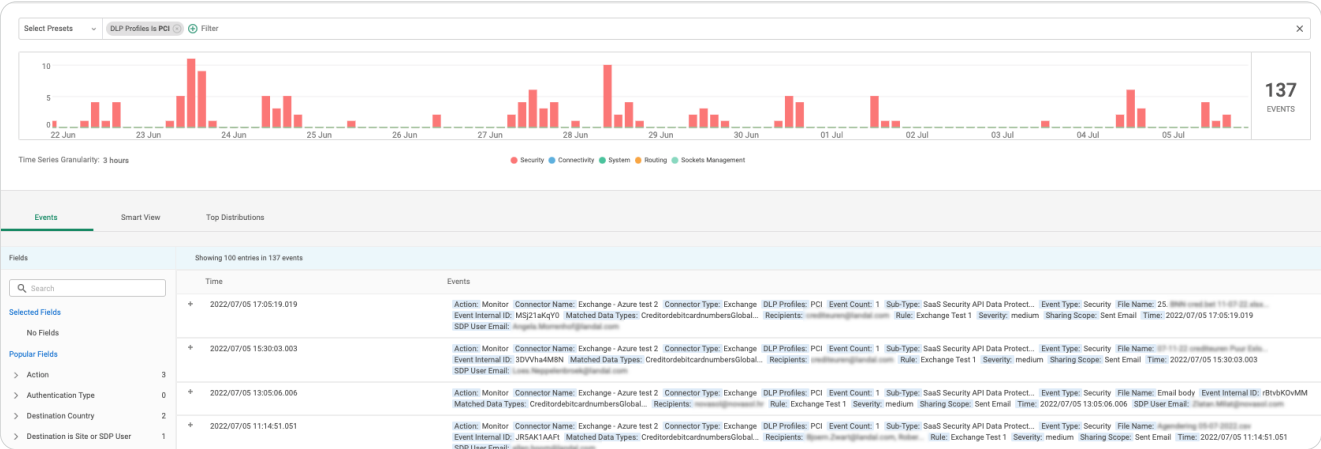


Figure 7: DLP Events View

Cato's 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, filetypes 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.

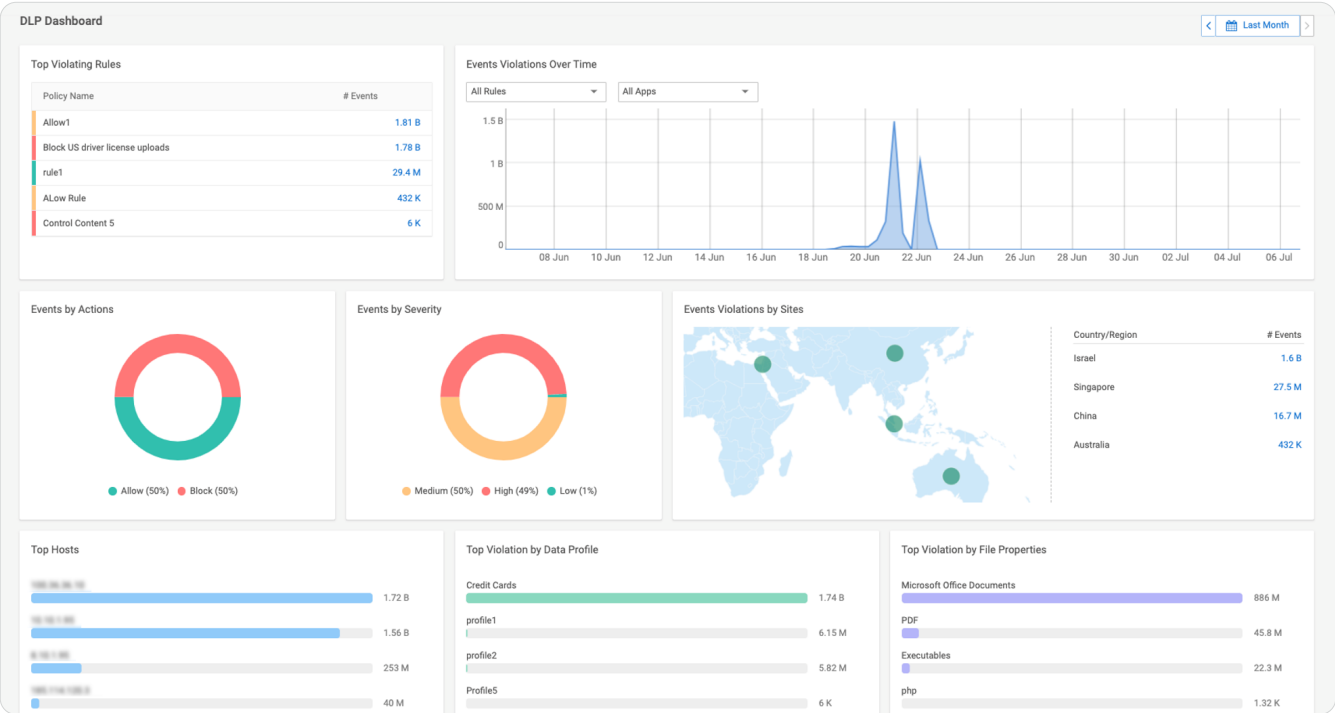


Figure 8: Cato DLP Dashboard

## Which Assets Do We Need to Protect?

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

Cato's DLP is delivered as part of a SASE Cloud service and provides coverage for all traffic to all enterprise assets (fig. 8). 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, Cato's DLP follows Zero Trust principles in which we can define DLP rules for applications and activities for which no explicit rules have been defined. This means that we can enforce restrictive policies for unsanctioned applications (AKA shadow IT) and ensure sensitive content isn't uploaded to, or downloaded from, these applications before we have had a chance to better understand their purpose and potential risk.

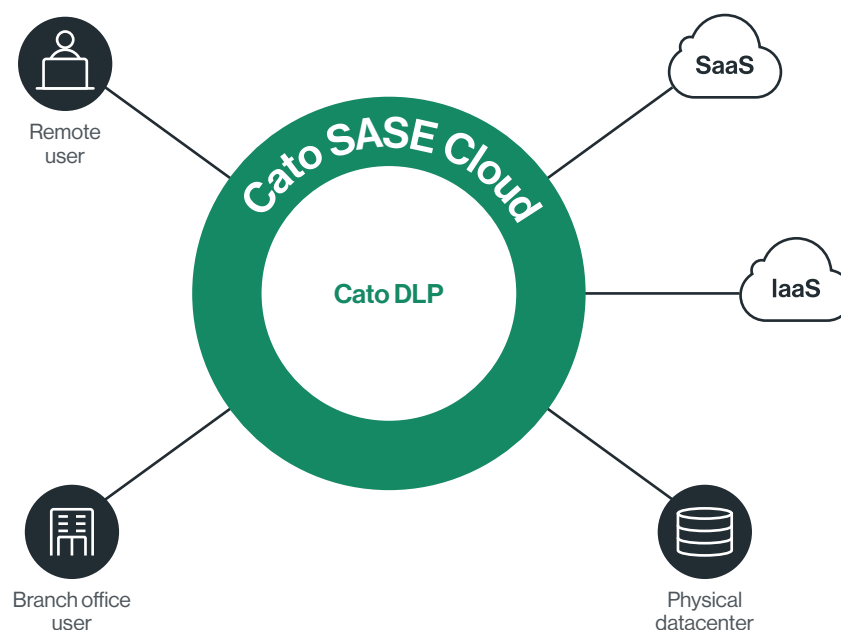


Figure 8: Cato SASE Coverage for All Traffic



# Cato's DLP as Part of a Fully Converged SSE and SASE Service

Cato's Security Service Edge, SSE 360 , which is part of Cato's Secure Access Service Edge (SASE), converges DLP with additional application access and threat mitigation services. Cato SSE 360 uses a Single Pass Cloud Engine (SPACE) to employ these services concurrently and with a shared context, enabling each one visibility into information collected and processed by the others, to enable them to make better informed decisions (fig 11). This also shortens the overall processing time and reduces latency, which is further optimized by the fact that TLS encryption and decryption needs to be done once for all services.

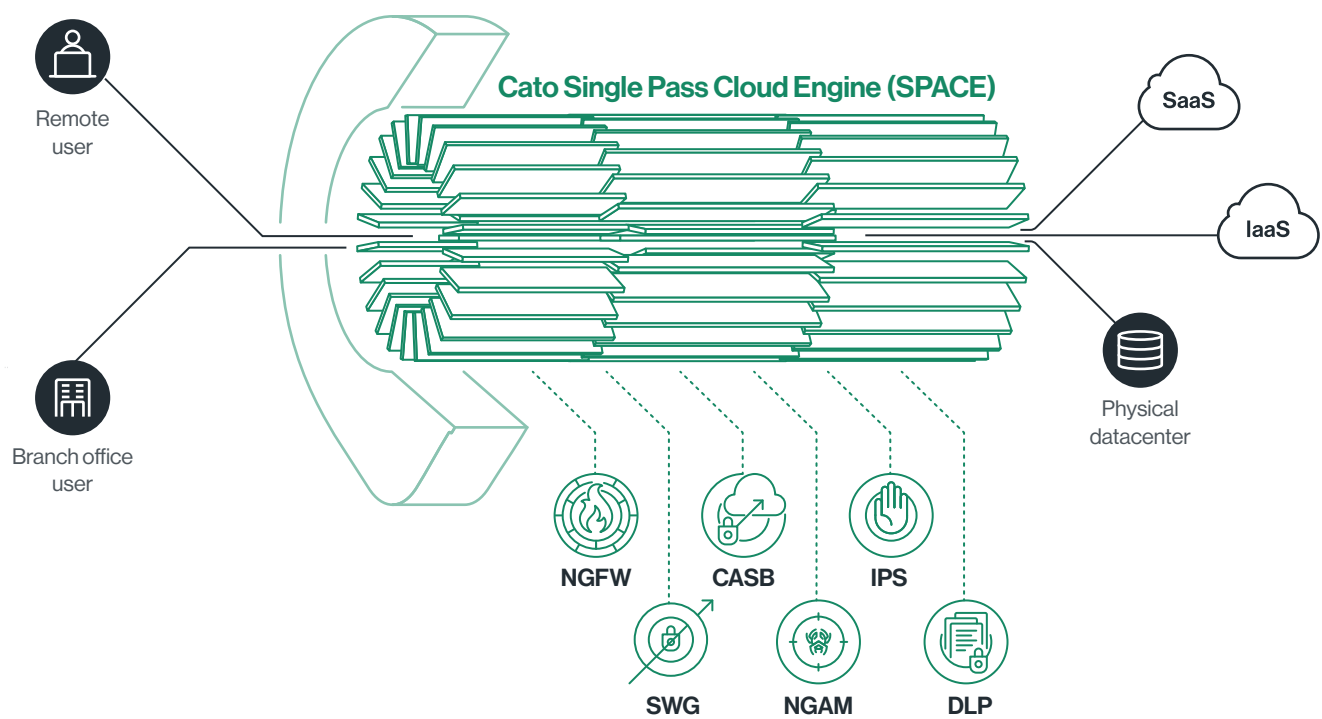


Figure 11: Cato SPACE

Cato's SSE 360 also improves 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.

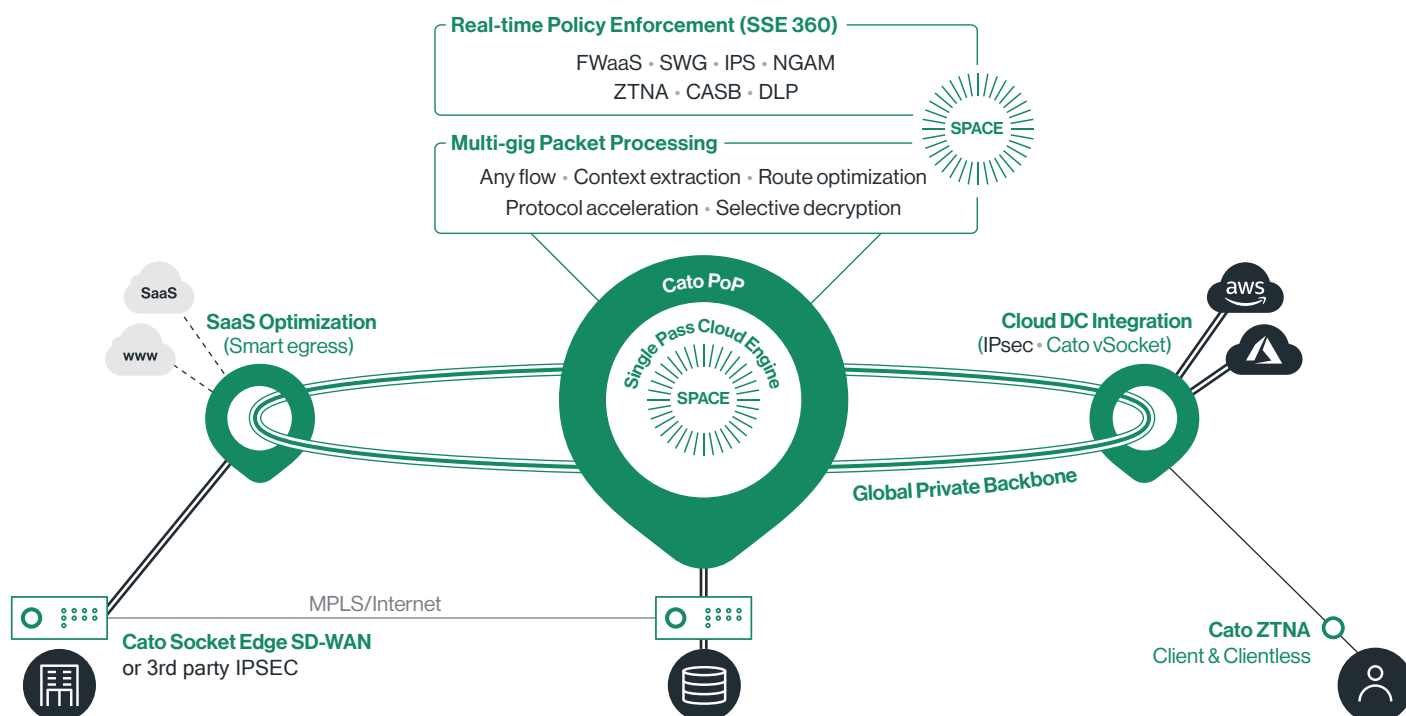
Users must first pass Cato's Next Generation Firewall (NGFW), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and for remote users also Zero Trust Network Access (ZTNA) service to even gain access to an application. Only then will they be able to attempt to transfer sensitive information,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

In tandem, Cato's threat prevention services such as the 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.

Cato's SSE 360 is a holistic security solution which provides comprehensive and robust enterprise network security. Cato's DLP is a critically important piece of the security puzzle, which leverages Cato's unique SPACE architecture to deliver superior security and performance, and truly demonstrates that the whole is far greater than the sum of its parts.

# About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato SASE Cloud, customers easily migrate from MPLS to SD-WAN, improve connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud data centers and remote users into the network with a zero-trust architecture. With Cato, your network and business are ready for whatever's next.



## Cato SASE. Ready for Whatever's Next

### Cato SASE Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Datacenter Integration

Cloud Application Acceleration

Secure Remote Access

Unified Management Application

### Use Cases

MPLS migration to SD-WAN

Optimized Global Connectivity

Secure Branch Internet Access

Cloud Acceleration and Control

Remote Access Security and Optimization

Flexible Management

