

## Press Release

### Cato Networks、すべてのアプリケーションへのアクセスを保護 および最適化する初のSSEプラットフォーム「Cato SSE 360」と その一機能として「Smart DLP」を発表

Cato DLP (Data Loss Prevention) は、レガシーDLPの実装や運用に伴う煩雑性を解消します。Cato SSE 360は、WAN、クラウド、インターネットトラフィックを完全に可視化、最適化、制御する初のSSEプラットフォームです。

テルアビブ（イスラエル）2022年7月19日 - [世界初のSASEプラットフォーム](#)のプロバイダー、[Cato Networks](#)は、複雑なDLPルールを設定する手間なく、あらゆるエンタープライズアプリケーションのデータを保護する初のDLP（情報漏洩対策）エンジン、「Cato DLP」を発表しました。Cato DLPは、SASE（Secure Access Service Edge）へのシームレスな完全移行を可能にしつつ、すべてのトラフィックを完全に可視化、最適化、制御する唯一のSSE（Security Service Edge）アーキテクチャ、「[Cato SSE 360](#)」の一機能です。また、Catoは、SSEアーキテクチャの理解促進を目的として、業界をリードする[Cato SASEエキスパート認定](#)に[Cato SSEエキスパート認定](#)を追加しました。

Cato Networksの共同創業者兼CEOであるShlomo Kramer（シュロモ・クレイマー）は、次のように述べています。「従来型のSSEアーキテクチャだけでは、企業を十分に守ることはできません。WANトラフィックの可視化および制御に限界があるため、複数のネットワークとセキュリティアーキテクチャを構築する必要があります。必要なのはエンドポイント、アプリケーション、リソースを問わず、あらゆるトラフィックを可視化および制御できる単一のアーキテクチャです。Cato SSE 360は、このニーズに対応する初のSSEソリューションです。」

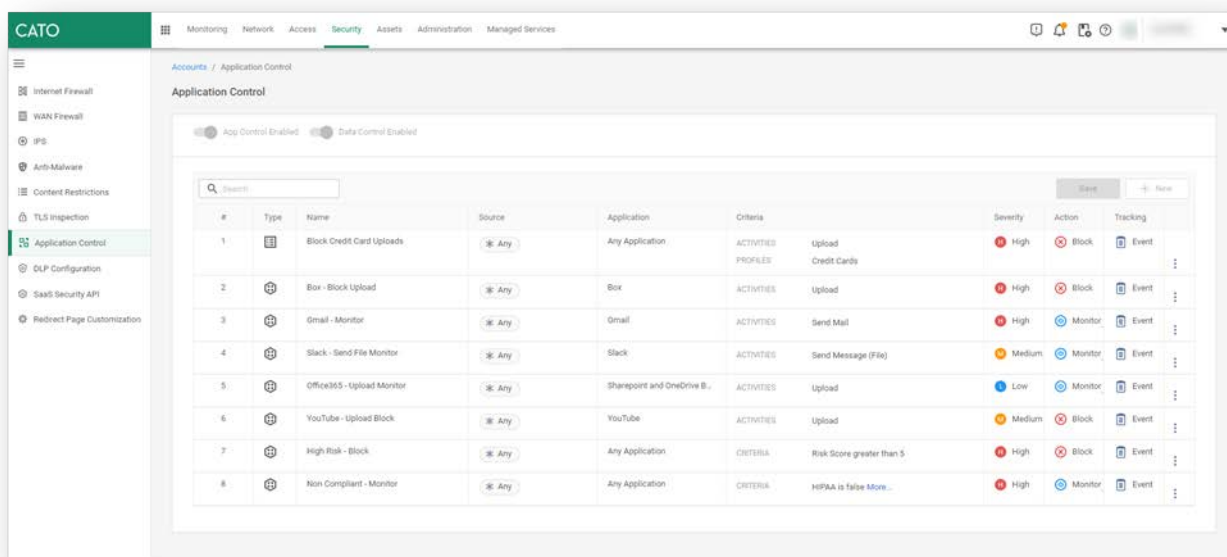
#### Cato DLPは、レガシーDLPの運用に伴う煩雑性を解消

DLPは、データ資産の保護、スキャン、ユーザーによる重要ファイルや機密情報（クレジットカードや顧客情報など）の送信防止に有効なツールです。

しかし、レガシーDLPには多くの限界があります。不正確なDLPルールが原因で、正当な動作を阻害される、あるいは不正な動作が許可されるといった事象が頻繁に発生しています。パブリッククラウドアプリケーションに注目するあまり、専有または非承認のアプリケーションに格納される機密データはDLPで保護されないまま放置され、DLPに投資しても他の脅威ベクターには対応できていません。

このような問題をCato DLPが解決します。Cato DLPはすべてのネットワークトラフィックをスキャンし、お客様の定義に基づき機密ファイルやデータを検出します。Catoは現在、クレジットカード番号のような世界共通で使用される機密データから、郵便番号のような国ごとに異なるデータまで、350種

類以上のデータタイプの識別に対応しています。DLPルールがデータ識別後、お客様が定義したポリシーに従ってブロック、アラート、許可等のアクションを適用します。



Cato DLPは、Cato SASE Cloudのセキュリティを支えるCato SSE 360に完全統合されています。アプリケーション制御ルールに基づく粒度の高いDLPポリシーが、すべてのアプリケーションとリソースに適用されます。

Cato DLPは、[Cato SPACE \(Single Pass Cloud Engine\) アーキテクチャ](#)の一部として、Catoが提供するクラウドネイティブなネットワークおよびセキュリティポートフォリオに完全統合されているため、レガシーDLPソリューションよりも詳細なネットワークフローの可視化および制御を実現します。具体的には、次のように機能します。

### スマート DLP ルールが実装をサポート

CatoのスマートDLPルールを使えば、DLPの実装がより簡単になります。セキュリティチームはアプリケーションごとに定義されたアクション（GitHubにおける「コミット」、Outlookにおける添付ファイル付きの「送信」、SharePointにおける外部フォルダへの「コピー」など）を明示的にブロックするのではなく、チームの意図をより反映したかたちでルール（「アップロードをブロック」など）を作成することができます。作成したDLPルールは、設定されたアクションごとにCatoが該当するアプリケーションを全て特定し、実装します。

### 機械学習で DLP の運用を簡素化

レガシーDLPルールが不正確であるため、業務に支障がでてしまう、といったケースは少なくありません。Cato DLPは、「特定のデータを扱えない」というクレームがユーザーから入って初めて対処するのではなく、不正確なDLPルールをプロアクティブに特定します。異常検知アルゴリズムが事前定義済みベースラインを超えたDLPルールを検出し、Catoのセキュリティコンテンツチームに既定のデータタイプを精緻化・改善するよう通知します。

## 多層構造による保護でセキュリティ体制を強化

Catoは、各種セキュリティユースケースのトラフィックをすべて同時に検査することで、効率的な多層構造による保護を実現します。アクセス制御層は、ユーザーが許可されたアプリケーション以外にアクセスできないようにするほか、許可されていないリソースや不正サイトへのアクセスを防止します。脅威防御層はトラフィックをスキャンし、ネットワークベースの脅威や不正コンテンツを検出します。Catoのインスペクション機能はすべて並行して行われるため、暗号化されたトラフィックでも、ラインレート並みのパフォーマンスを実現します。

## Cato SSE 360：今日のセキュリティ、明日への備え

Catoは、Cato DLPとともに、WAN、クラウド、インターネットトラフィックを可視化、最適化、制御する唯一のSSEプラットフォーム「Cato SSE 360」を発表しました。

Gartnerは、SSEとは、SWG（セキュアWebゲートウェイ）、CASB（クラウドアクセスセキュリティブローカー）、DLP、ZTNA（ゼロトラスト・ネットワークアクセス）によって、インターネットアクセス、クラウドアプリケーションアクセス、リモートアクセスのセキュリティを確保するものと定義しています。

Cato SSE 360は通信元や通信先を問わずすべてのポートとプロトコルに対して、SSEの基本機能のほか、Cato SASE Cloudが誇るクラウドネイティブのセキュリティ機能（FWaaS（サービスとしてのファイアウォール）、ATP（高度な脅威保護；不正侵入防止システムや次世代マルウェア対策など）、MDR（検知と対応のマネージドサービス）など）を拡張しています。Cato SSE 360は、Cato SASE Cloudのスケラビリティ、レジリエンス、グローバル性、セルフメンテナンス機能を網羅しています。

Catoを導入することにより、ITリーダーはSSEまたはSASEのプラットフォームを一元化できます。Cato SSE 360があれば既存のネットワークを維持したまま、現行のセキュリティ運用業務を転換し、世界中のアプリケーションへのアクセスを保護および最適化することができます。各拠点、ハイブリッドワークフォース、クラウドリソースをCatoに接続することでネットワーク構築のコストや煩雑性の削減、アプリケーションパフォーマンスの向上、自己回復力に優れたインフラによるレジリエンスの強化、単一UIによるネットワークおよびセキュリティインフラの可視化強化が実現されるため、ITリーダーは準備が整い次第、SASEへの完全移行に向けた取り組みを進めることができます。

## Catoは、SASEエキスパート認定にSSE認定を追加

ITチームによるSSEの理解促進を目的として、業界初のSASE認定資格である[Cato SASEエキスパート認定](#)に[Cato SSEエキスパート認定](#)を追加しました。この専門的なコースでは、SSEアーキテクチャを分析し、SSEとSASEの根本的な違いについて説明するほか、SSEの推進要因、ユースケース、重要なメリットについて詳しくお伝えします。本コースへのご登録方法については、

<http://www.catonetworks.com/sase/sase-certification/sse-expert/>をご覧ください。

以上

## 【Cato Networksについて】

Catoは、Cato SD-WANとクラウドネイティブなSSE（セキュリティサービスエッジ）であるCato SSE 360をグローバルクラウドサービスに統合した、世界で最も堅牢なシングルベンダー方式のSASEプラットフォーム・プロバイダーです。Cato SASE Cloudは、場所を問わずあらゆるユーザーや拠点からのアプリケーションアクセスを最適化および保護します。Catoを使用することで、お客様は高コストで柔軟性の低いレガシーMPLSをSD-WANベースの近代的なネットワークアーキテクチャに簡単に入れ替えることができるだけでなく、様々な場所で働くハイブリッドワークフォースを保護および最適化することで、シームレスにクラウドへ移行することができます。また、粒度の高いアクセスポリシーの適用、脅威からのユーザー保護、機密データ漏洩防止などの制御を、すべて単一のUIから簡単に行うことも可能です。Catoがお客様の未来のビジネスをサポートします。

<国内法人>

商号：Cato Networks 株式会社／所在地：東京都千代田区大手町 1-6-1 大手町ビル  
SPACES 大手町 1 階／設立：2020 年 10 月 1 日／カントリーマネージャー：田島弘介

### 【お問い合わせ先】

Cato Networks 株式会社 営業部  
japan.sales@catonetworks.com