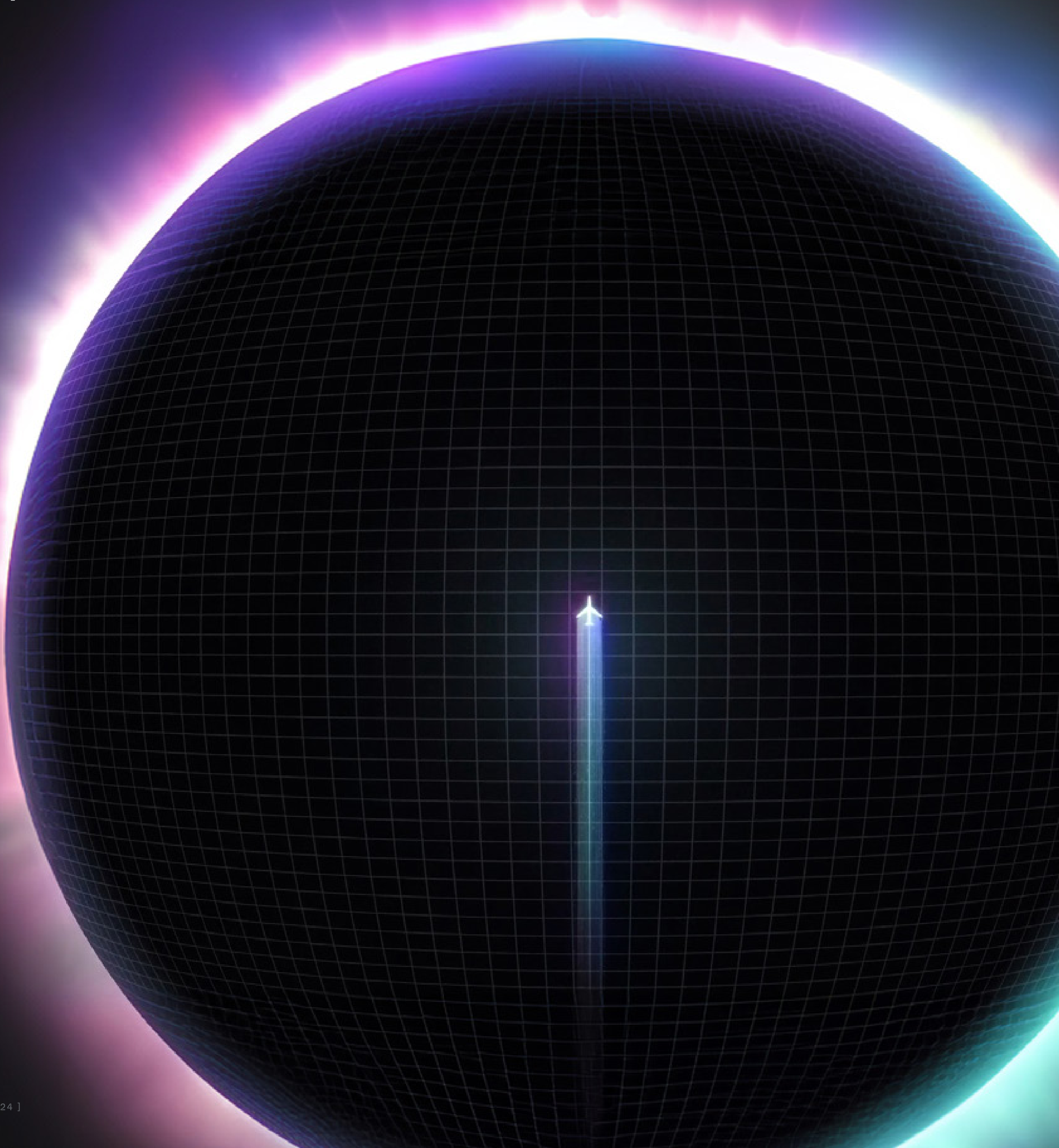
DOPE.SECURITY

Secure Web Gateway + CASB Reinvented

Whitepaper



[DOPE.SECURITY_MAY2024]

Table of Contents

01

Building a *dope* company

Shortcomings of the Legacy SWG

The way we secured corporate workforces 20 years ago worked well for a while.

The legacy secure web gateway (SWG) sat on-premises and enforced a company policy via a hardware appliance proxy. These policies were set up by administrators and put in place to protect users from malicious content as well as blocking unwanted website categories like *Social Media*, *Gambling* or *Adult Content*.

Over time we've seen a "lift and shift" of this on-premises technology, to the cloud, in order to connect employees from outside the office. At the foundation of this cloud model is a heavy reliance on data centers and points of presence (POP) which are spread across the world. So instead of running policy checks and enforcement through hardware in the office, these requests are backhauled to these worldwide data centers. While this network of data center hops and backhauling can connect users on the go, it also results in slower internet speeds and load times, unreliable connections, and massive privacy concerns.

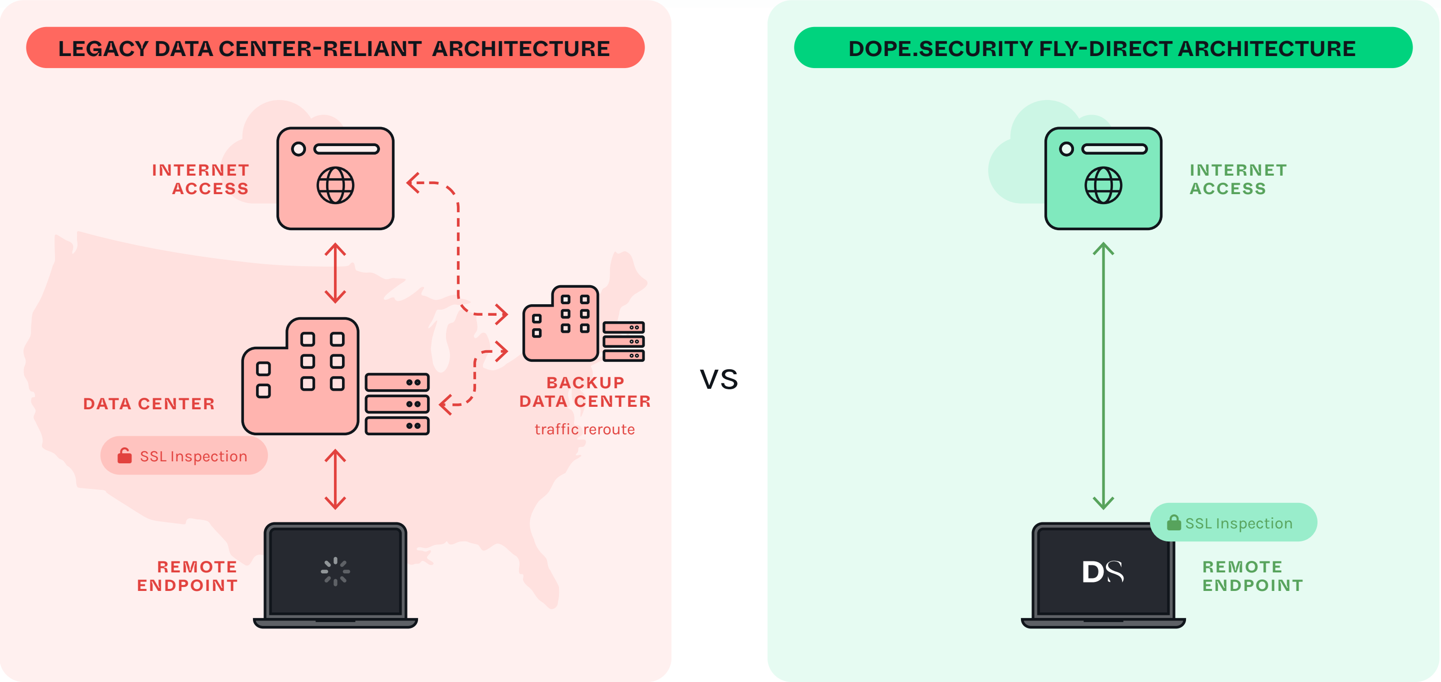
What the industry needs is a new direct-to-internet SWG that places reliability, privacy, and performance at the user's fingertips, and does not compromise end user experience.

WHY DO LEGACY COMPANIES STILL USE DATA CENTERS?

It's difficult for legacy companies to fully transition to the cloud due to their deep-rooted reliance on data center architectures developed over two decades. Despite adopting a "lift-and-shift" model to incorporate cloud technologies, completely abandoning data centers is challenging because they are ingrained in their systems. This setup keeps them from fully modernizing and leaves them open to security risks.

This is where dope.security comes in as a rearchitected solution.

Stopover data centers create a backhaul of traffic, slowing down access and introducing a point of vulnerability



Re-Architecting the SWG

Stemming from our personal experiences at these legacy cybersecurity companies, we heard first-hand many issues that customers faced with the cloud-proxy architecture. This inspired our team to start from the ground up and build something completely new that actually solved customer problems.

Our philosophy is simple: to provide a first class secure internet experience *that just works*. In order to do that we needed to address 3 key areas where cloud proxies today struggled—reliability, performance, and privacy.

Reliability

LEGACY

- → Connection issues
- → Incorrect locale
- → Proxy restrictions
- → Data center outages

DOPE.SECURITY

- → No data center outages
- → Fallback mode continues to enforce policy
- → Caching of policies on device: remain secured even when our cloud is not reachable

Performance

LEGACY

- → Data backhauling
- → Slower load times
- → Latency across the board
- → 1-hr policy update times

DOPE.SECURITY

- → No data backhauling
- → Direct-to-internet connection
- → 4x performance
- → Instant policy updates: seconds (NOT HOURS) to update policies

Privacy

LEGACY

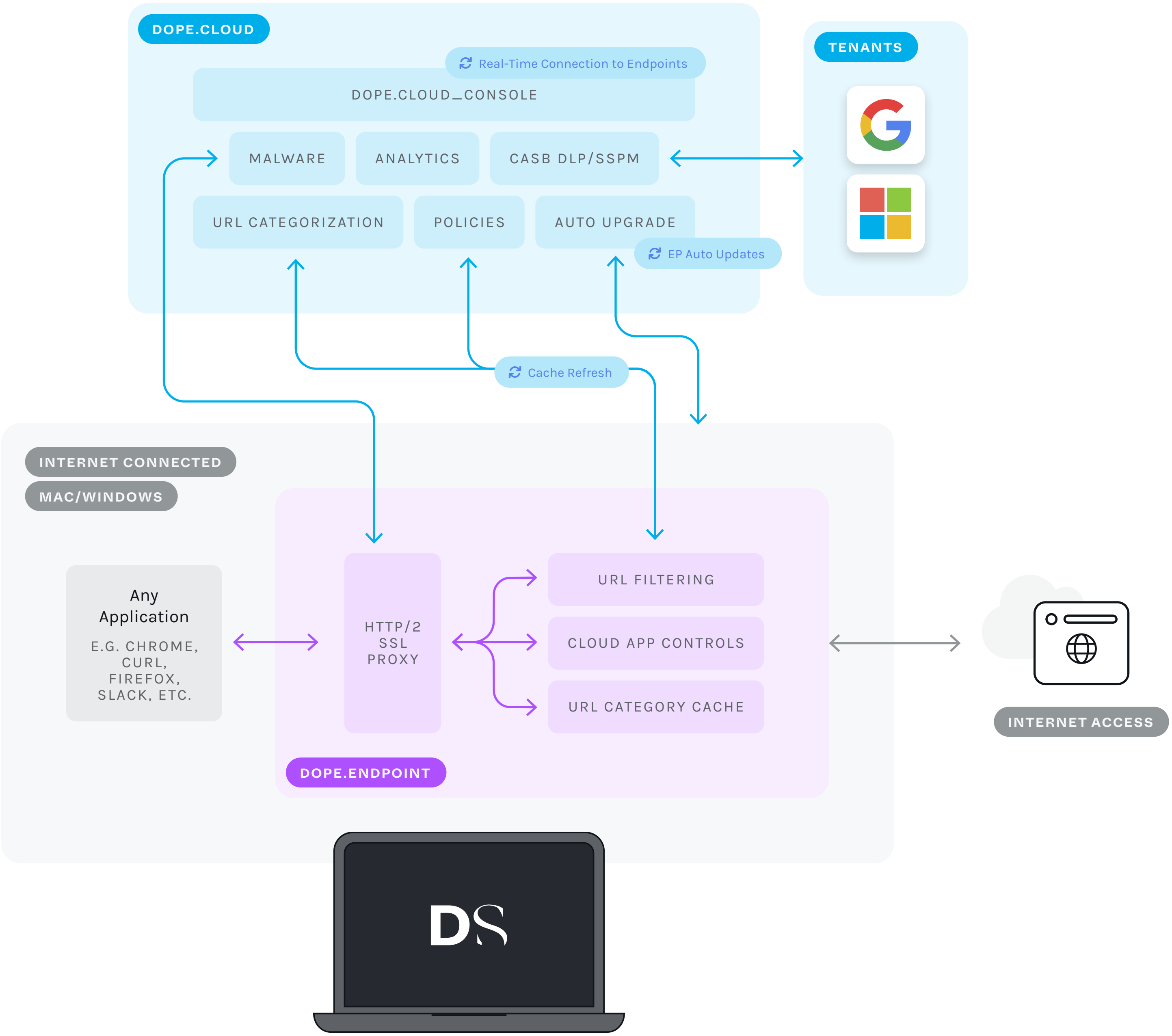
- → SSL inspection and decrypting off-device
- → Bypassing of entire categories to skip SSL inspection (I.E. HEALTHCARE, BANKING)

DOPE.SECURITY

- → Decrypt and inspect SSL directly on your device
- → Data remains locally with you
- → Visibility across every category and web transaction

Today most cloud and on-prem proxy's are "frankensteined" together either through mergers and acquisitions or a multi-console user experience, and you can tell immediately that they just don't work well—they could be better.

dope.security is designed and built from the ground up, ensuring every component works seamlessly together. Our Fly-Direct SWG and CASB Neural live under a single console, so navigating from one to the next is only a click away. We've simplified the complex without sacrificing functionality. That means enterprise grade security with a consumer like ease of use. We've made SSE dope.



02

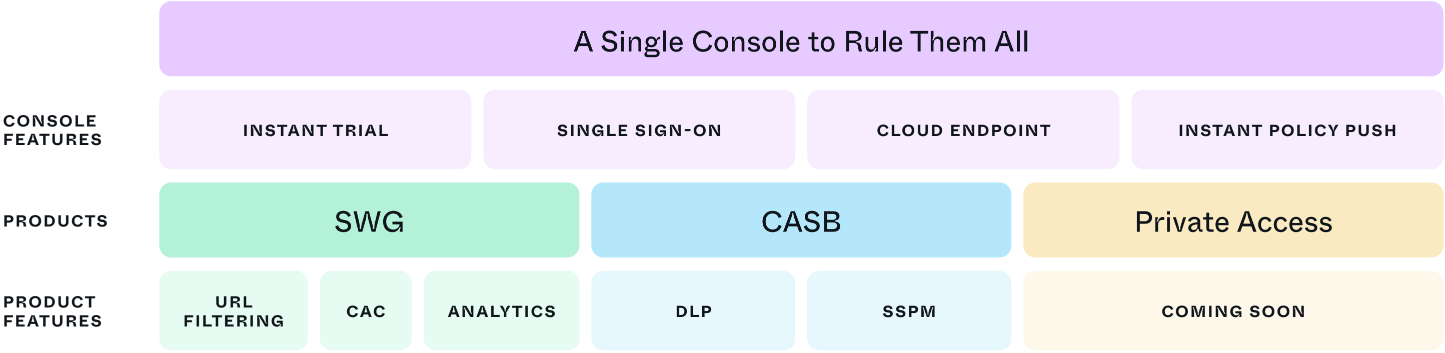
SSE under a single *cloud console*

A First-Class User Experience

Cybersecurity software isn't known for user experience, but that changes with dope.security, which looks and feels like a consumer application—it's easy to sign up for, easy to deploy, easy to manage, and intuitive to use.

The world is going this way across every sector, and cyber needs to catch up. A lot of this first-class user experience offered is due to removing the stopover data center as broken down in **SECTION 1**, but we've considered a lot more when building SSE products. First, all products are housed in a single cloud console. No more flipping through different windows, apps, and tabs to find the product you're looking for, and they all work seamlessly together.

From there, considerations across the console experience have been carefully curated to make your job *and life* easier—instant trial, easy syncing, real-time impact—features right when and where you need them. We're simplifying the process so you can do your complex job....simply.



A Single Console to Rule Them All

CONSOLE FEATURES: INSTANT TRIAL, SINGLE SIGN-ON, CLOUD ENDPOINT, INSTANT POLICY PUSH

PRODUCTS: SWG, CASB, Private Access

PRODUCT FEATURES: URL FILTERING, CAC, ANALYTICS, DLP, SSPM, COMING SOON

Instant Trial

dope.security offers the only SWG you can trial instantly on your own, facilitated through a streamlined setup process enabled by our redesigned cloud-native architecture. Just login using Microsoft 365 or Google Workspace, and you'll install the agent software to your device. It'll begin inspecting traffic immediately without any configuration, extra hardware, or software installs.

Once the initial setup is complete, gain instant access to the platform's features and start testing without a complex proof of concept (POC). Whether your company is small or large, you get a first-class experience.

A REDUNDANT TEST ENVIRONMENT

Legacy companies typically have test environments for POCs. Moving from a test environment to a production tenant requires throwing everything away and reconfiguration.

Single Sign-On

We use Single Sign-On (SSO) through OpenID Connect (OIDC) with Microsoft 365 and Google to authenticate and authorize users. This simplifies admin configuration into a one-click experience, without the pain of Security Assertion Markup Language (SAML) and System for Cross-Domain Identity Management (SCIM). Simple, effective SSO does the following:

1. Integrates automatically with your identity management IDP/IDaaS—i.e. Okta, Microsoft Entra ID (FORMERLY AZURE AD), Ping, Onelogin, etc.

2. Admins, end users, and their groups are automatically updated and deprovisioned

It really is one-click!

ENDPOINT AUTHORIZATION

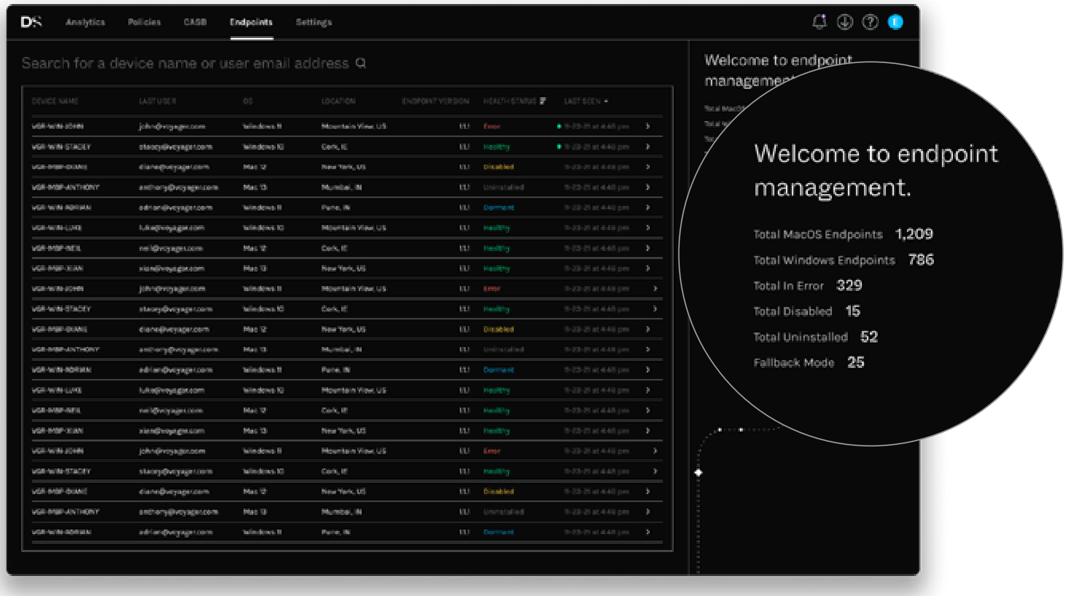
The dope.cloud manages the OIDC authorization between your user and the associated policy.

If you do not enable Endpoint Authentication and import your users, only the Base Policy can be configured. Visibility, policy customization and exceptions, and analytics are limited.

USER IMPORT

Import your users and groups with the click of a button. You'll stay synced—if a user leaves, their access is automatically revoked. If a user's group changes, their policy assignment follows suit.

A Cloud-Managed Endpoint



DEVICE NAME	LAST USER	OS	LOCATION	ENDPOINT VERSION	HEALTH STATUS	LAST SEEN
VGR-WIN-JOHN	john@voyager.com	Windows 11	Mountain View, US	1.1.1	Error	11-23-21 at 4:48 pm
VGR-WIN-STACEY	stacey@voyager.com	Windows 10	Cork, IE	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-DIANE	diane@voyager.com	Mac 12	New York, US	1.1.1	Disabled	11-23-21 at 4:48 pm
VGR-MBP-ANTHONY	anthony@voyager.com	Mac 13	Mumbai, IN	1.1.1	Uninstalled	11-23-21 at 4:48 pm
VGR-WIN-ADRIAN	adrian@voyager.com	Windows 11	Pune, IN	1.1.1	Dormant	11-23-21 at 4:48 pm
VGR-WIN-LUKE	luke@voyager.com	Windows 10	Mountain View, US	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-NEIL	neil@voyager.com	Mac 12	Cork, IE	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-XIAN	xian@voyager.com	Mac 13	New York, US	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-WIN-JOHN	john@voyager.com	Windows 11	Mountain View, US	1.1.1	Error	11-23-21 at 4:48 pm
VGR-WIN-STACEY	stacey@voyager.com	Windows 10	Cork, IE	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-DIANE	diane@voyager.com	Mac 12	New York, US	1.1.1	Disabled	11-23-21 at 4:48 pm
VGR-MBP-ANTHONY	anthony@voyager.com	Mac 13	Mumbai, IN	1.1.1	Uninstalled	11-23-21 at 4:48 pm
VGR-WIN-ADRIAN	adrian@voyager.com	Windows 11	Pune, IN	1.1.1	Dormant	11-23-21 at 4:48 pm
VGR-WIN-LUKE	luke@voyager.com	Windows 10	Mountain View, US	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-NEIL	neil@voyager.com	Mac 12	Cork, IE	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-XIAN	xian@voyager.com	Mac 13	New York, US	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-WIN-JOHN	john@voyager.com	Windows 11	Mountain View, US	1.1.1	Error	11-23-21 at 4:48 pm
VGR-WIN-STACEY	stacey@voyager.com	Windows 10	Cork, IE	1.1.1	Healthy	11-23-21 at 4:48 pm
VGR-MBP-DIANE	diane@voyager.com	Mac 12	New York, US	1.1.1	Disabled	11-23-21 at 4:48 pm
VGR-MBP-ANTHONY	anthony@voyager.com	Mac 13	Mumbai, IN	1.1.1	Uninstalled	11-23-21 at 4:48 pm
VGR-WIN-ADRIAN	adrian@voyager.com	Windows 11	Pune, IN	1.1.1	Dormant	11-23-21 at 4:48 pm

Welcome to endpoint management.

Total MacOS Endpoints	1,209
Total Windows Endpoints	786
Total In Error	329
Total Disabled	15
Total Uninstalled	52
Fallback Mode	25

Endpoint Management lends a helping hand between endpoints and the policies they use. Quickly view the status of each endpoint and confirm they work as expected. After a dope.endpoint is installed, it registers with dope.cloud and reflects under *Endpoints* for real-time visibility.

FALLBACK SAFELY WITHOUT LOSING PROTECTION

Each dope.endpoint regularly checks its connection to the dope.cloud, and also sends its own health status (HEALTHY, FALLBACK, ERROR, ETC). In the event the dope.cloud cannot be reached, the endpoint will go into *Fallback Mode*.

THE LEGACY “FALLBACK” IS INSECURE. WHY?

With Legacy Fallback, when you *Fail Open*, all websites are allowed; when you *Fail Closed*, all websites are blocked. Our Fly-Direct Architecture is more user friendly and safer.

It continues to secure users, even in Fallback Mode, because all policies are cached on-device. Policies remain effective for accessed domains and apps, even if cloud services cannot be reached. This means uninterrupted secure internet access all the time.

FAIL CLOSED ON

Allows previously accessed websites to continue per the policy. New requests will be *disabled for user safety.*

FAIL CLOSED OFF

Allows previously accessed websites to continue per the policy. New requests will be *allowed without security checks.*

Instant Policy Push

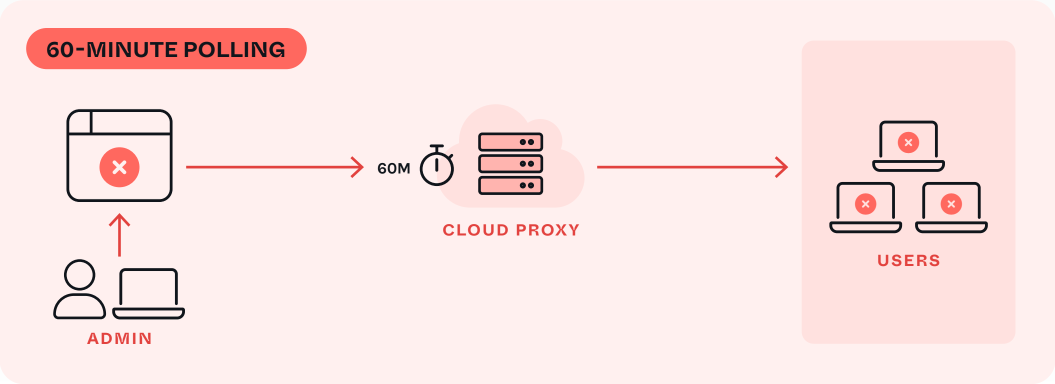
Having to wait 30–60 minutes with existing cloud proxies for a policy update means you are left vulnerable to threat exposure during the time you’re waiting for the refresh. Plus, we know it’s just annoying for you to have to wait to test your changes, then wait, and test again. Our Fly-Direct architecture allows us to instantly update policies in real-time, reducing the policy enforcement wait time to seconds.

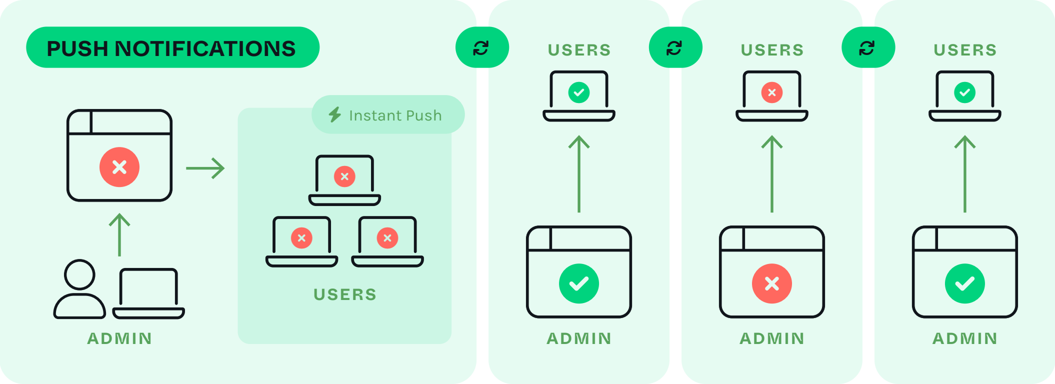
Polling creates frustration and vulnerabilities

Polling is the easiest way to implement a policy update mechanism which is why you see it often. *The downside?* It takes a lot of time before changes take effect leaving you frustrated and vulnerable.

OUR FIRST-CLASS EXPERIENCE

To make the admin’s life easier, we built in push notifications. It’s *bread and butter* in the consumer world, but an exquisite luxury in cybersecurity. In the time it would have taken you with waiting for polling, you can update your dope policy one hundred times over!





03

DOPE.SWG

The *Fly Direct* Secure Web Gateway

DOPE.SWG

The Fly-Direct SWG

With Fly-Direct, we found a way to eliminate the data center and provide a nonstop internet flight.

An on-device SSL Proxy inspects all application and internet traffic locally, keeping your data safe on your device. There are no data center stopovers. It's direct, instant, and invisible.

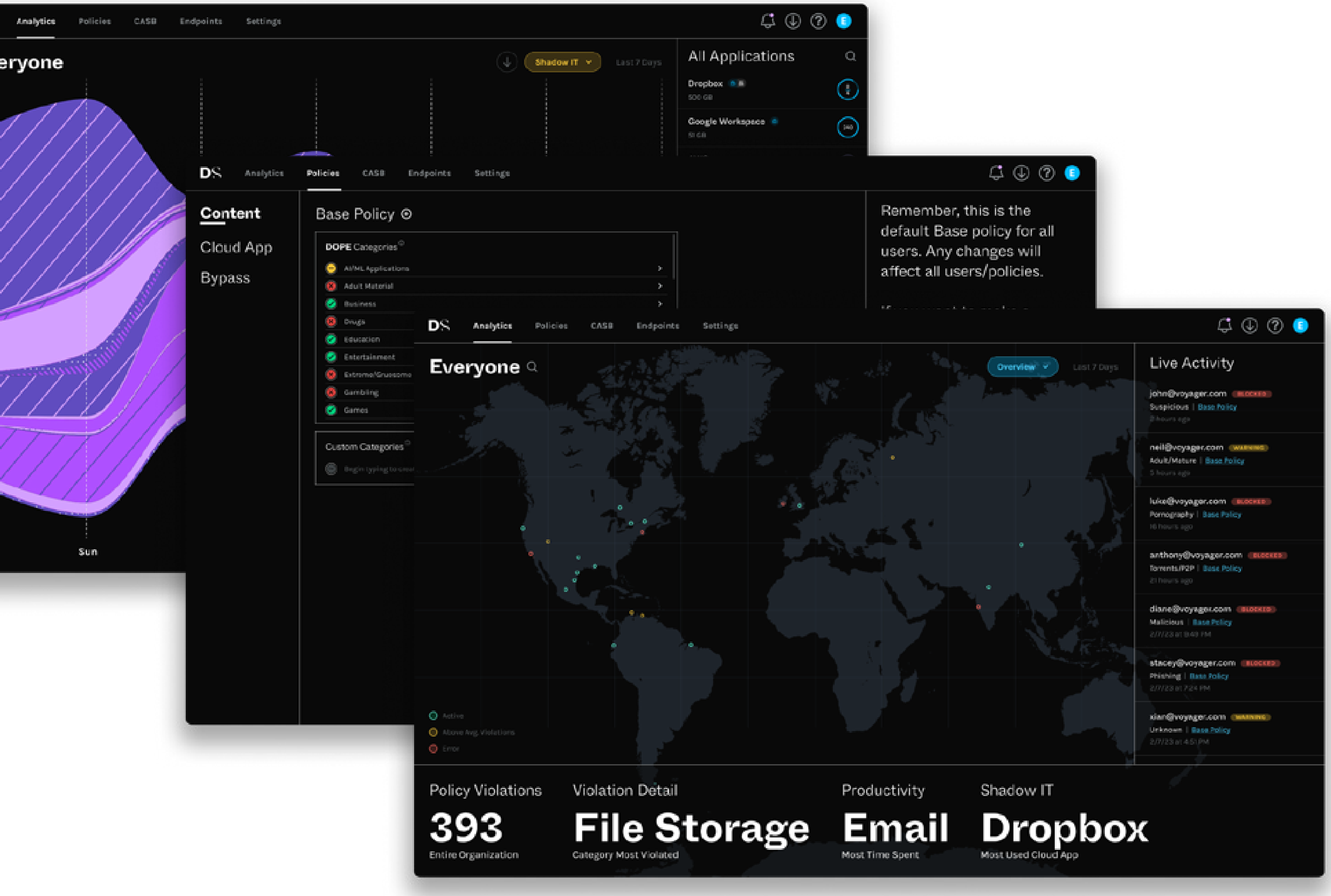
Mac native + Windows

4x
Performance

Compact
Less than 100 MB of RAM

FEATURE BREAKDOWN

1 SSL Inspection
2 URL Filtering
3 Cloud App Controls
4 Analytics
5 Anti Malware



Remember, this is the default Base policy for all users. Any changes will affect all users/policies.

john@voyager.com BLOCKED
Suspicious | Base Policy
2 hours ago

neil@voyager.com WARNING
Adult/Mature | Base Policy
5 hours ago

luke@voyager.com BLOCKED
Pornography | Base Policy
16 hours ago

anthony@voyager.com BLOCKED
Torrents/P2P | Base Policy
21 hours ago

diane@voyager.com BLOCKED
Malicious | Base Policy
2/7/23 at 8:49 PM

stacey@voyager.com BLOCKED
Phishing | Base Policy
2/7/23 at 7:24 PM

xian@voyager.com WARNING
Unknown | Base Policy
2/7/23 at 4:51 PM

Policy Violations	Violation Detail	Productivity	Shadow IT
393	File Storage	Email	Dropbox
Entire Organization	Category Most Violated	Most Time Spent	Most Used Cloud App

SSL Inspection

With dope.swg you not only fly direct, you also fly private. This means your traffic and data do not leave your device with all SSL Inspection performed directly on endpoint.

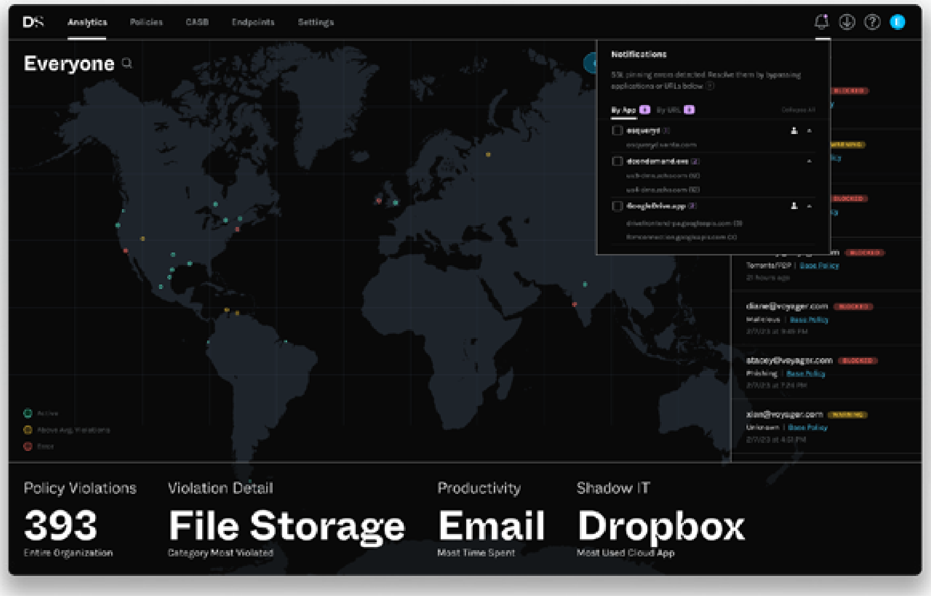
THE BENEFITS OF PERFORMING SSL INSPECTION LOCALLY:

1 It’s safer → Data never leaves your device

2 It’s faster → No more decryption in a potential cross country data center

3 It’s more reliable → Your decryption zone moves with you, so it’s always available

Our approach to SSL inspection produces visibility across every web transaction. By contrast, legacy SWGs bypass entire domains for categories, such as healthcare and banking. These legacy companies know that there can be sensitive data in these categories, which will sit vulnerable decrypted in a data center.



Torrents/P2P | Base Policy
21 hours ago

diane@voyager.com BLOCKED
Malicious | Base Policy
2/7/23 at 9:49 PM

stacey@voyager.com BLOCKED
Phishing | Base Policy
2/7/23 at 7:24 PM

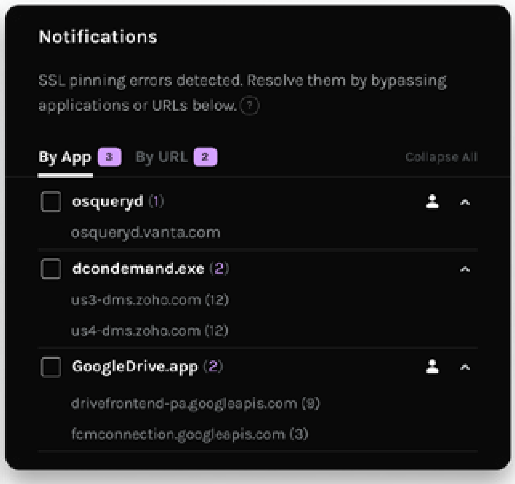
xian@voyager.com WARNING
Unknown | Base Policy
2/7/23 at 4:51 PM

Policy Violations
393
Entire Organization

Violation Detail
File Storage
Category Most Violated

Productivity
Email
Most Time Spent

Shadow IT
Dropbox
Most Used Cloud App



Notifications

SSL pinning errors detected. Resolve them by bypassing applications or URLs below. ?

□ osqueryd (1)
osqueryd.vanta.com

□ dcondemand.exe (2)
us3-dms.zoho.com (12)
us4-dms.zoho.com (12)

□ GoogleDrive.app (2)
drivefrontend-pa.googleapis.com (9)
fcmconnection.googleapis.com (3)

Instant SSL Inspection Error Resolution

Sometimes SSL Inspection can cause certain URLs or applications to break, which is why SWG products have bypass lists. Typically when SSL inspection errors occur, admins must wait for a user to realize there is an issue, log a support a ticket, and then figure out what is causing it.

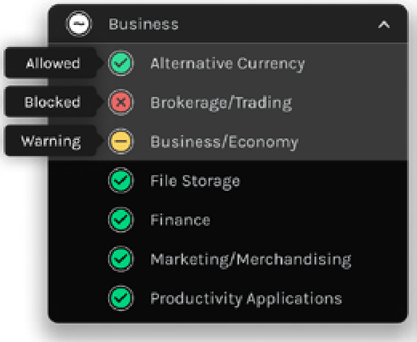
OUR FIRST-CLASS EXPERIENCE

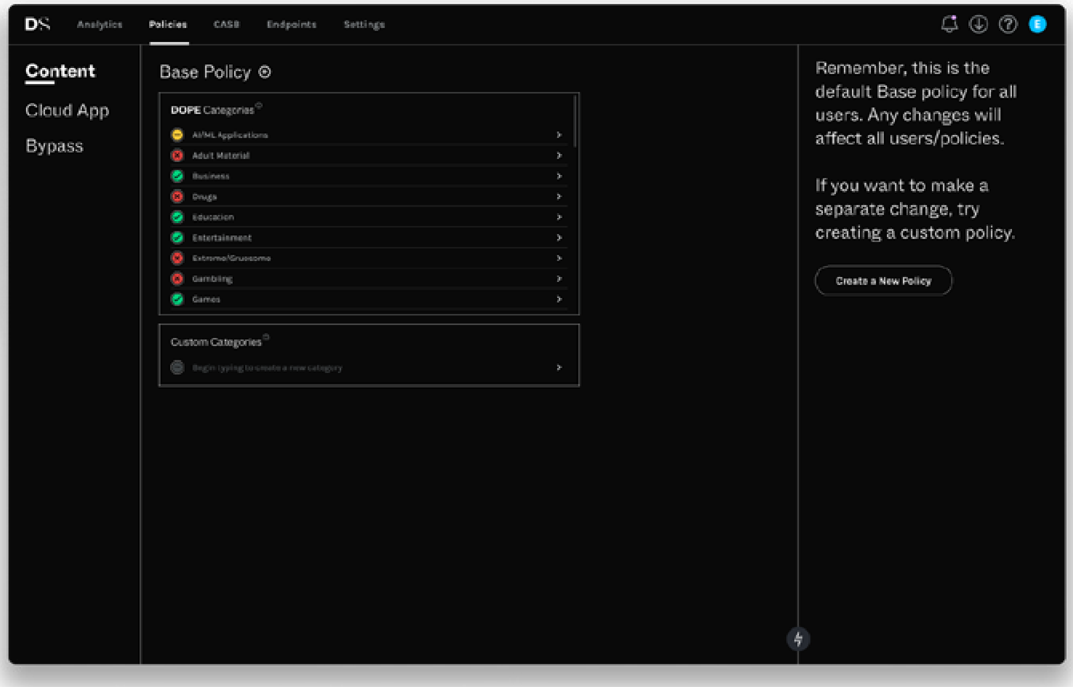
When an SSL inspection error occurs, the dope.endpoint will report the URL/application to the dope.cloud. Admins can view these errors from the notification panel and add to bypass lists across the organization.

URL Filtering

Once you download the agent, a base policy is automatically deployed and enforces policy based on the most common category rules.

If you want to customize it, you can toggle the restriction levels for these website categories between *Allow*, *Block*, and *Warn*.





Remember, this is the default Base policy for all users. Any changes will affect all users/policies.

If you want to make a separate change, try creating a custom policy.

CUSTOM CATEGORIES

Although we have over 80 categories by default, sometimes that's not enough. It's easy to add your own custom categories. By adding a list of domains or URLs, you can create a custom category which can then be assigned a restriction level of *Block*, *Allow*, or *Warn*. Custom categories are shared globally, so toggle an unwanted category to *Ignore* to keep it out of a particular policy.

Policy writing in 3 steps

01 START WITH THE BASE POLICY

By default, we block the typical categories so you don't have to apply them yourself, e.g. Adult Material, Illegal, Piracy, Malicious, and more.

02 TOGGLE RESTRICTIONS

Example: the Base Policy allows "Chat/Messaging." You can toggle to *Block*, which will restrict the use of apps like WhatsApp and Messenger.

03 INSTANT POLICY PUSH

Once you hit save, your policy will be instantly enforced and deployed across your online devices, rather than having to wait up to an hour.

POLICY EXCEPTIONS

The dope.console lets you make category exceptions for certain users and groups in your organization so they can visit required websites. Use this to get granular for your user roles—for example, block "Social Media" across your organization, but allow it for your marketing team. *You know, for research.*

CUSTOM POLICY CREATION

Different geographical locations or specific user groups may require special requirements and customizations— create multiple policies to handle your organization's needs. Upon creation, each new policy inherits the Base Policy, making maintenance of custom categories and Base Policy rules much easier—change once, and it applies everywhere. You'll notice our console is significantly faster than any legacy SWG, and the complex procedural policy is replaced with a simpler user-friendly list.

WHY DO CERTAIN WEBSITES AND APPS BREAK?

- → Certificate validation issues
- → Hard-coded IP addresses or domains
- → Application-specific SSL configurations

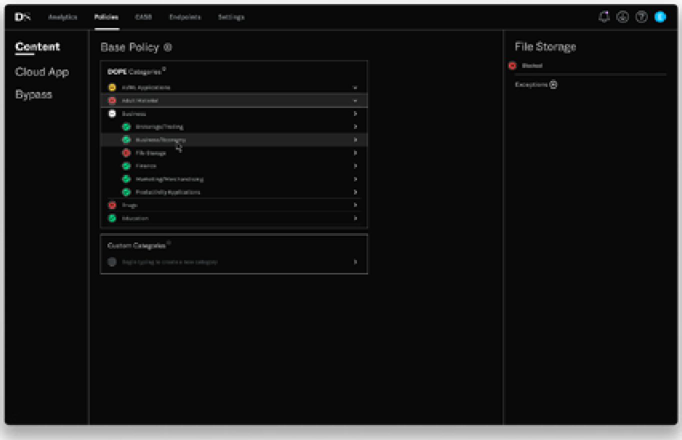
BYPASS SETTINGS

Websites and apps that typically break when proxied by any product can be bypassed, so they always work for your users. We've created a default list of standard URLs and Apps that break, but you can always add to your organization's own custom list.

Cloud Application Control (CAC)

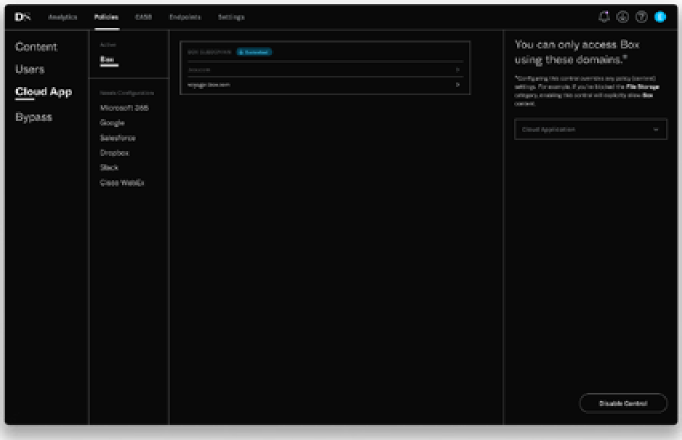
CAC add an additional layer of security by restricting specific app domains or tenants a user can access. Using this in parallel with URL filtering can drastically reduce the risk of data exfiltration while increasing end user productivity by limiting access to personal application accounts. Easily keep your data within the bounds of corporate-sanctioned apps.

Toggle consumer logins on and off and prevent users from accessing SaaS applications with unapproved logins, such as personal consumer accounts.



URL FILTERING

By setting "File Storage" to *Blocked* in your Policy, websites and apps such as Dropbox, WeTransfer, and Box cannot be accessed...



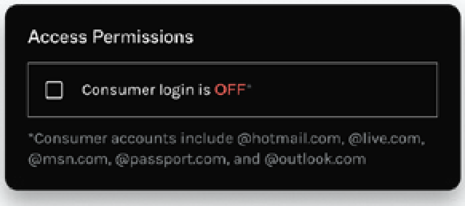
CLOUD APP CONTROL

...However if you enable File Storage Cloud apps like Box or Dropbox in the CAC Settings, corporate accounts will be allowed.

CAC READ ONLY: BLOCKING PERSONAL UPLOADS

With our CAC Read Only feature, organizations have the ability to allow personal access to the defined app, Microsoft 365 or Google, but block the ability to upload files and attachments to an employee's personal accounts.

PERSONAL LOGINS

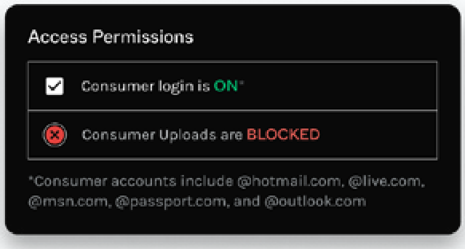


Access Permissions

□ Consumer login is OFF*

*Consumer accounts include @hotmail.com, @live.com, @msn.com, @passport.com, and @outlook.com

ALLOW PERSONAL LOGINS BUT BLOCK PERSONAL UPLOADS TO FILE STORAGE/EMAIL



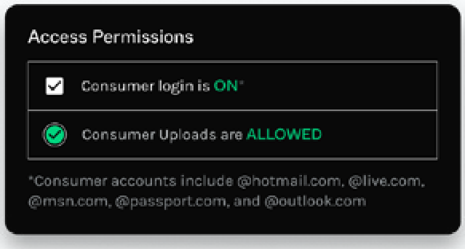
Access Permissions

☑ Consumer login is ON*

☒ Consumer Uploads are BLOCKED

*Consumer accounts include @hotmail.com, @live.com, @msn.com, @passport.com, and @outlook.com

ALLOW PERSONAL LOGINS AND ALLOW PERSONAL UPLOADS TO FILE STORAGE/EMAIL



Access Permissions

☑ Consumer login is ON*

✓ Consumer Uploads are ALLOWED

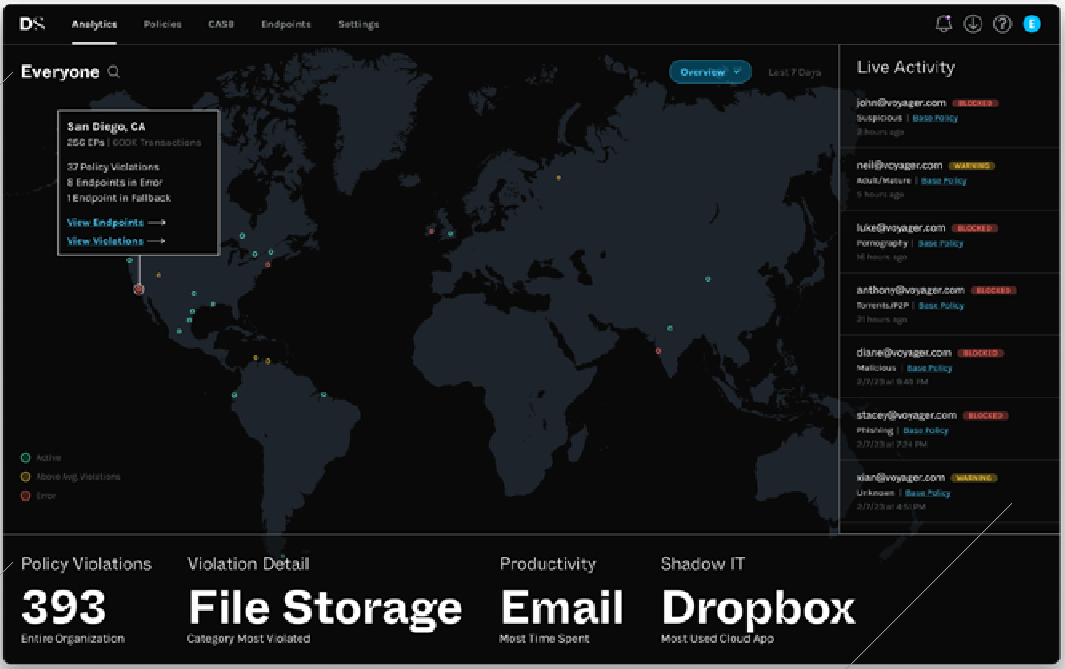
*Consumer accounts include @hotmail.com, @live.com, @msn.com, @passport.com, and @outlook.com

Configuring CAC on most legacy SWGs is not possible. You're often required to purchase and open a separate Cloud Access Security Broker$^{(CASB)}$ console to create a new policy for those apps. Using dope.security, we've integrated these key policy features into the SWG, as they work better together, no separate policy or separate console required. You can control access to these industry cloud applications:

Analytics

Every data point you need under one roof. From policy violations to productivity stats to login detection, we've got you covered. Our analytics offer insights across all connected endpoints. Simple charts and graphs display intelligent and actionable data to help you understand how your policies perform daily, how productive your users are, and the data they access and share.

From first login to the console, the Analytics Overview map provides global visibility and a live view of all endpoint activity connected to your organization. From there, explore data by Policy, Productivity, Shadow IT, or a detailed table of all violations, or search across users, groups, and locations.



DS Analytics Policies CASB Endpoints Settings

Everyone

Overview Last 7 Days

San Diego, CA
256 EPs | 600K Transactions

37 Policy Violations
8 Endpoints in Error
1 Endpoint in Fallback

View Endpoints ⟶
View Violations ⟶

● Active
● Above Avg. Violations
● Error

Live Activity

john@voyager.com BLOCKED
Suspicious | Base Policy
2 hours ago

neil@voyager.com WARNING
Adult/Mature | Base Policy
5 hours ago

luke@voyager.com BLOCKED
Pornography | Base Policy
16 hours ago

anthony@voyager.com BLOCKED
Torrents/P2P | Base Policy
21 hours ago

diane@voyager.com BLOCKED
Malicious | Base Policy
2/7/23 at 9:49 PM

stacey@voyager.com BLOCKED
Phishing | Base Policy
2/7/23 at 7:24 PM

xian@voyager.com WARNING
Unknown | Base Policy
2/7/23 at 4:51 PM

Policy Violations
393
Entire Organization

Violation Detail
File Storage
Category Most Violated

Productivity
Email
Most Time Spent

Shadow IT
Dropbox
Most Used Cloud App

Search by users, groups, or locations

7-DAY STATS

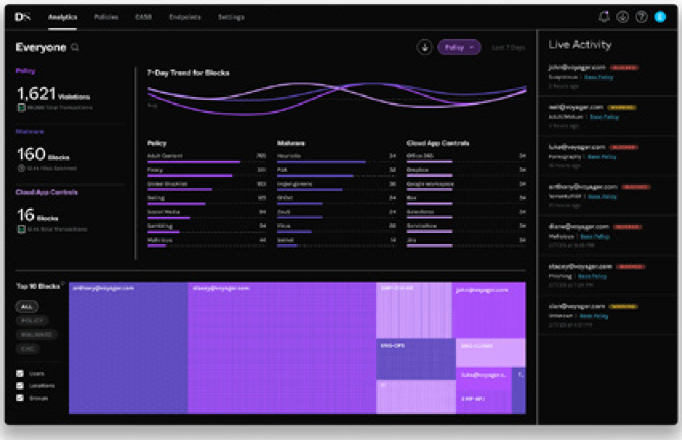
Easy access to policy violations over the last 7 days, including the category most violated, productivity averages, and Cloud SaaS apps being used

LIVE ACTIVITY

Most recent violations across your organization

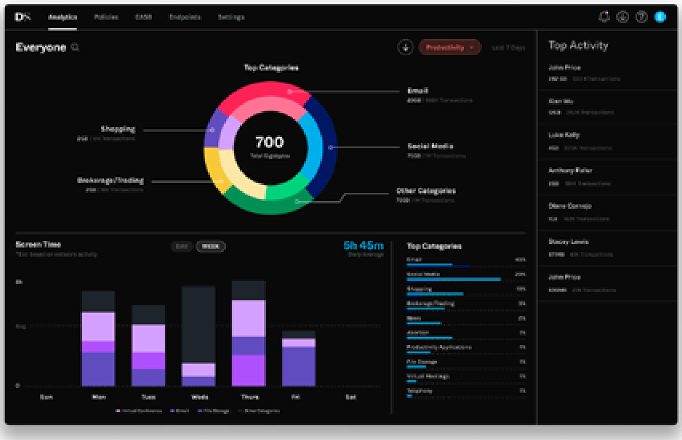
INTELLIGENT CHARTS AND DATA

Under the Policy and Productivity view, enjoy a 7-day view of visualizations that uncover organizational trends, user behavior, and workforce productivity through contextual and actionable features to inform policy adjustments



POLICY

Review number of total transactions, files scanned for malware, and data transactions across the last 7 days organized users and groups.

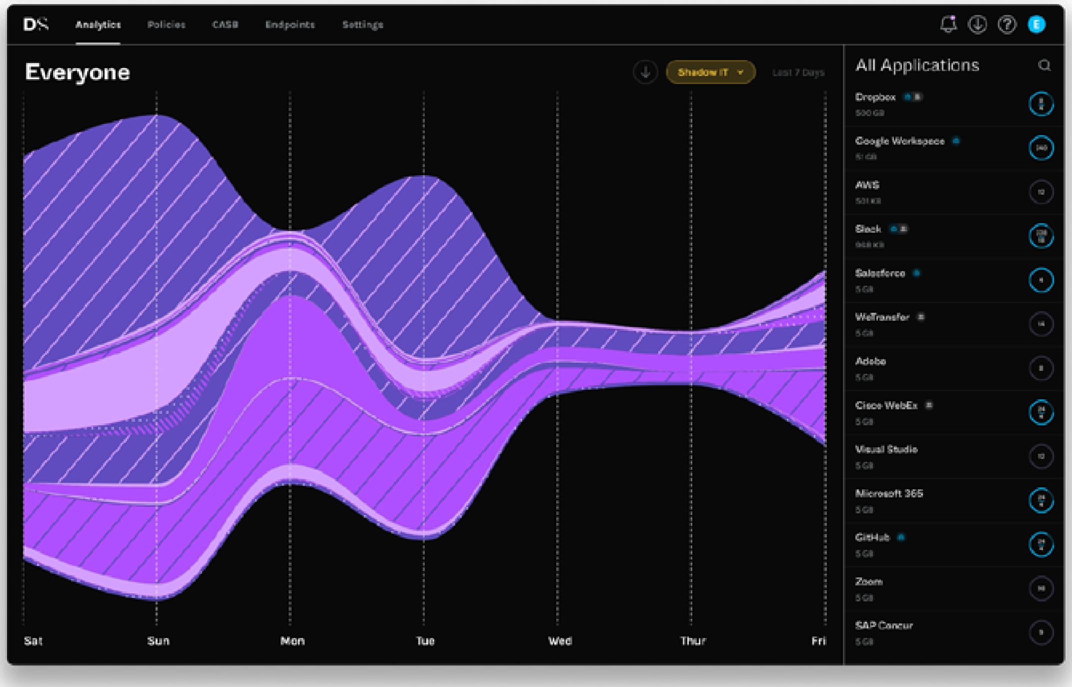


PRODUCTIVITY

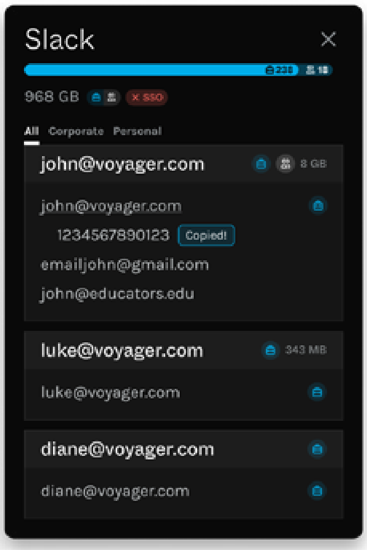
Review where your users are spending their workforce time across network activity per day and week.

SHADOW IT

Extend your visibility to Shadow IT and uncover how users share data across your organization. Features provide application and location visibility on a per-app consumption basis, with a focus on the most data transferred. Use this visibility to take action—inform your policy updates, and assess areas of data exfiltration and non-compliance.



Dropbox	500 GB
Google Workspace	51 GB
AWS	501 KB
Slack	968 KB
Salesforce	5 GB
WeTransfer	5 GB
Adobe	5 GB
Cisco WebEx	5 GB
Visual Studio	5 GB
Microsoft 365	5 GB
GitHub	5 GB
Zoom	5 GB
SAP Concur	5 GB



john@voyager.com 8 GB
john@voyager.com
1234567890123 Copied!
emailjohn@gmail.com
john@educators.edu

luke@voyager.com 343 MB
luke@voyager.com

diane@voyager.com
diane@voyager.com

DIVE EVEN DEEPER

In addition to account emails, view AWS account IDs and Slack workspaces, and use them to update Cloud App Controls.

See a deeper breakdown of app account logins to identify where data is transferring. Identify and track which accounts are used for corporate or personal. You can see account information to these industry cloud applications:

aws box salesforce

Anti-Malware

The dope.swg leverages leading anti-malware service to determine file safety.

The goal is simple—capture and block files that may have malware. dope.swg's anti-malware does the following:

1. Capture all file hashes from all downloads
2. Receive the status from the malware service
3. Cache the result for future use
4. Update the Analytics dashboard of the dope.console
5. Serve the result to the endpoint as *Allowed* or *Blocked*

The dope.endpoint locally inspects all downloads and computes each file hash. Upon a malware verdict, it will send the details to the dope.console for the admin.

EXAMPLE OF THE ANTI-MALWARE PROCESS

1. dope.endpoint captures and decrypts the traffic

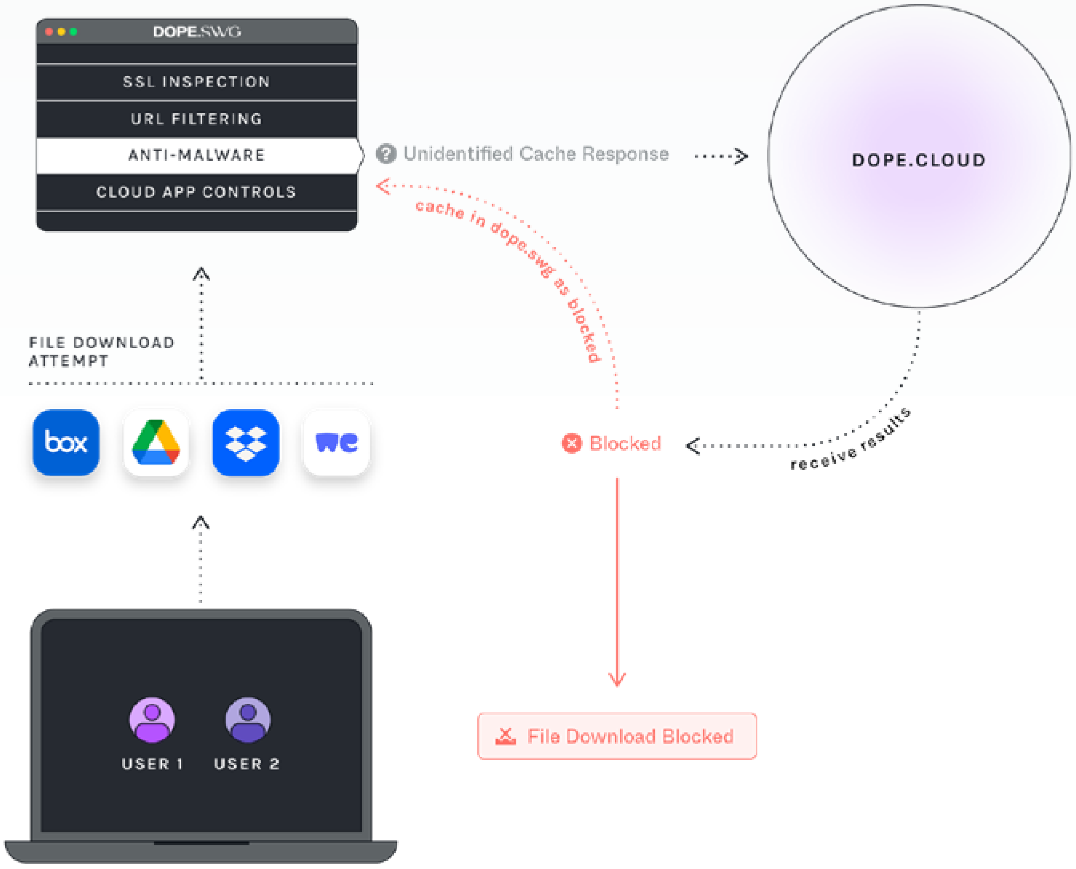
   Box.com is allowed through URL Filtering

2. We detect a file download on the endpoint
3. Before it is fully served to the calling application, we calculate the file hash and check the local cache to verify the file is benign:

   Allowed or *Blocked*

4. If we haven't seen the file before, the hash is sent to the dope.cloud to verify if it is malware:

   Allowed or *Blocked*



04

DOPE.CASB_NEURAL

LLM-Powered CASB Neural DLP

DOPE.CASB_NEURAL

CASB Neural

LLM-powered DLP for Cloud Apps

CASB Neural is the first of its kind leveraging deep learning AI and Large Language Models [(LLM)]. We instantly crawl your Microsoft 365 or Google tenant and identify all publicly and externally shared files containing PII, PCI, PHI, and IP, and will automatically monitor for any file-sharing changes. This is done with zero pre-configurations.

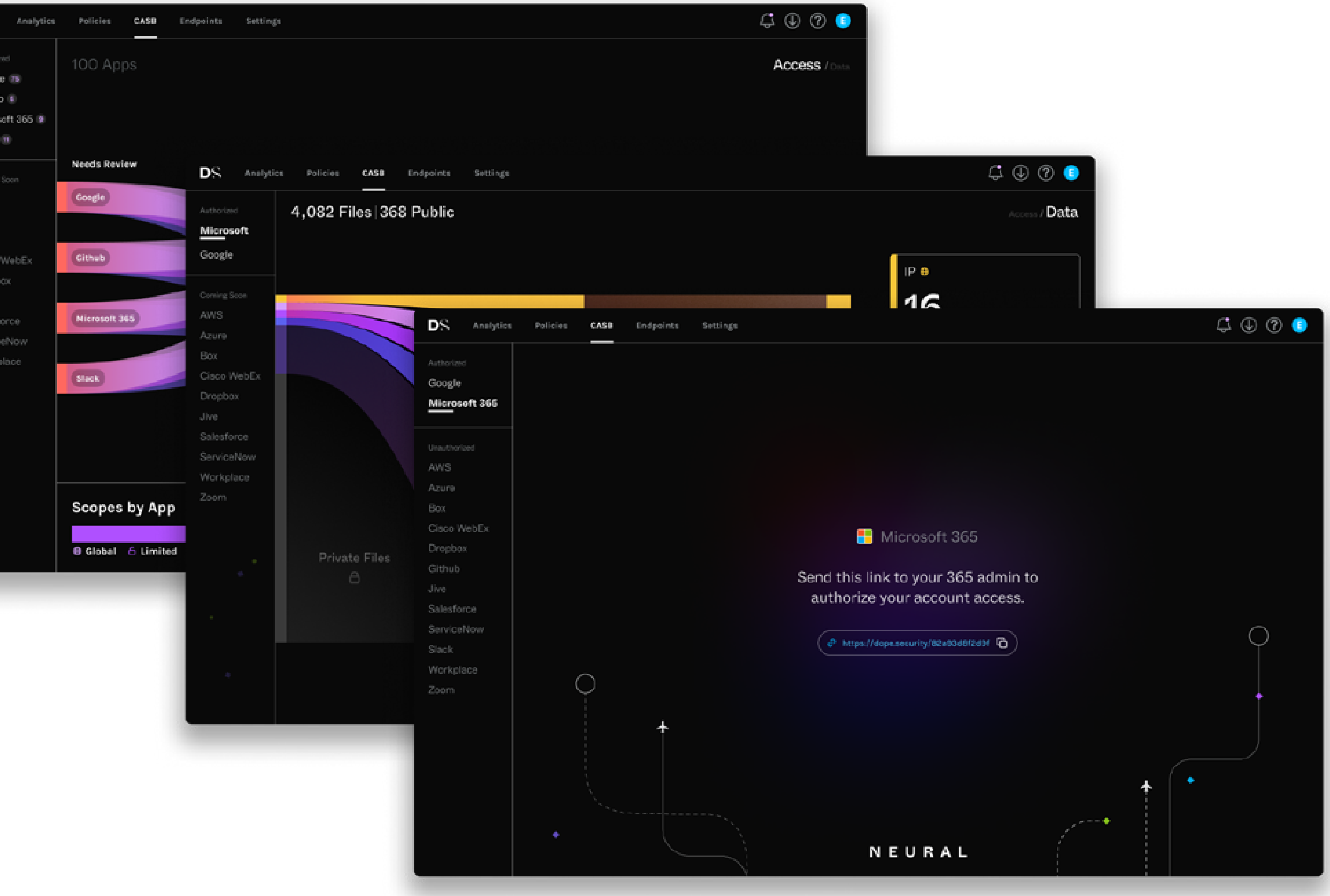
FEATURE BREAKDOWN

1. Data Loss Prevention
2. SaaS Security Posture Management
3. Remediation from the Console

DOPAMINE
File summaries

One-Click
Onboarding and file unsharing

LLM-powered DLP

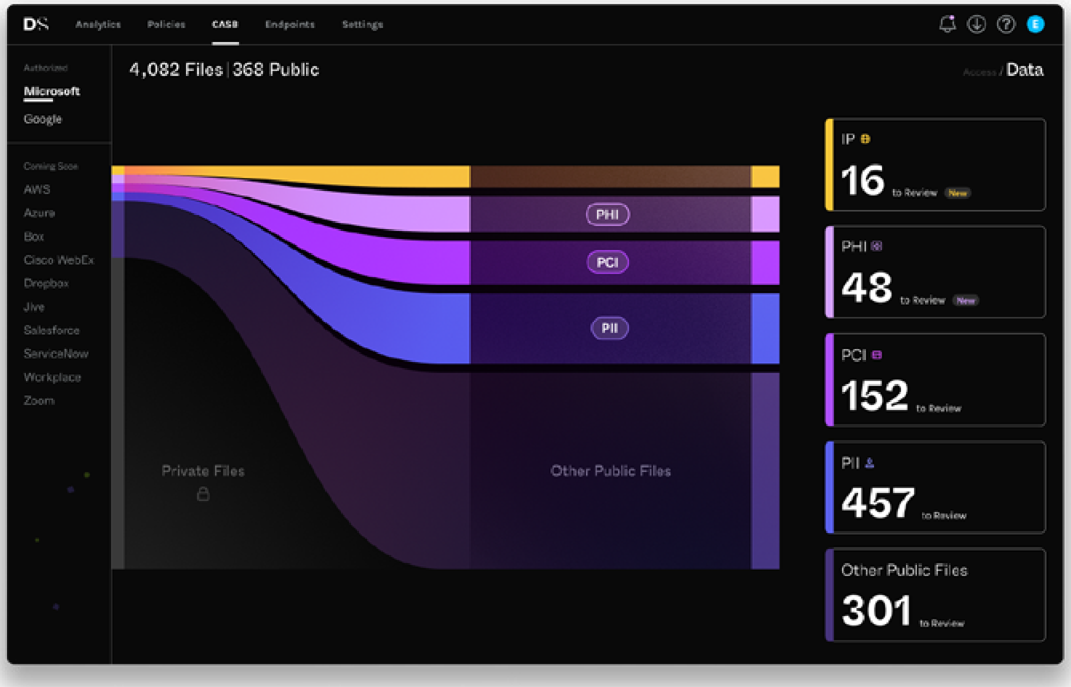


Send this link to your 365 admin to authorize your account access.

LLM-Powered Data Loss Prevention (DLP)

Today's CASBs were supposed to be effective at limiting data exposure; however their DLP classifications rely on pattern matching, regexes, and a series manual rule configurations that result in a high number of false positives.

This is because regexes cannot understand the context of a document like a LLM does. Not to mention, these DLP solutions require pre-configuration before you can get your scan started.



4,082 Files | 368 Public

IP 16 to Review New

PHI 48 to Review New

PCI 152 to Review

PII 457 to Review

Other Public Files 301 to Review

Once activated, CASB Neural automatically scans your SaaS tenant, discovers all public/externally shared files, and monitors for any file-sharing changes. Leveraging deep learning LLM, it comprehends these files to find IP, PII, PCI, and PHI data. In other words, it answers the question, "Is this sensitive?"

By leveraging LLMs and actually comprehending the files, we materially reduce the amount of false positives—this results in higher precision and accuracy. Previously, this had to be done using regex and pattern matching, i.e. a 16-digit number = a credit card. This shift from matching to true file comprehension is an industry first and completely reduces the administrative overhead.

WHAT ARE MY FILES CLASSIFIED AS?

Our LLM reviews your live files to find sensitive data to categorize

IP
Intellectual Property

PHI
Protected Health Information

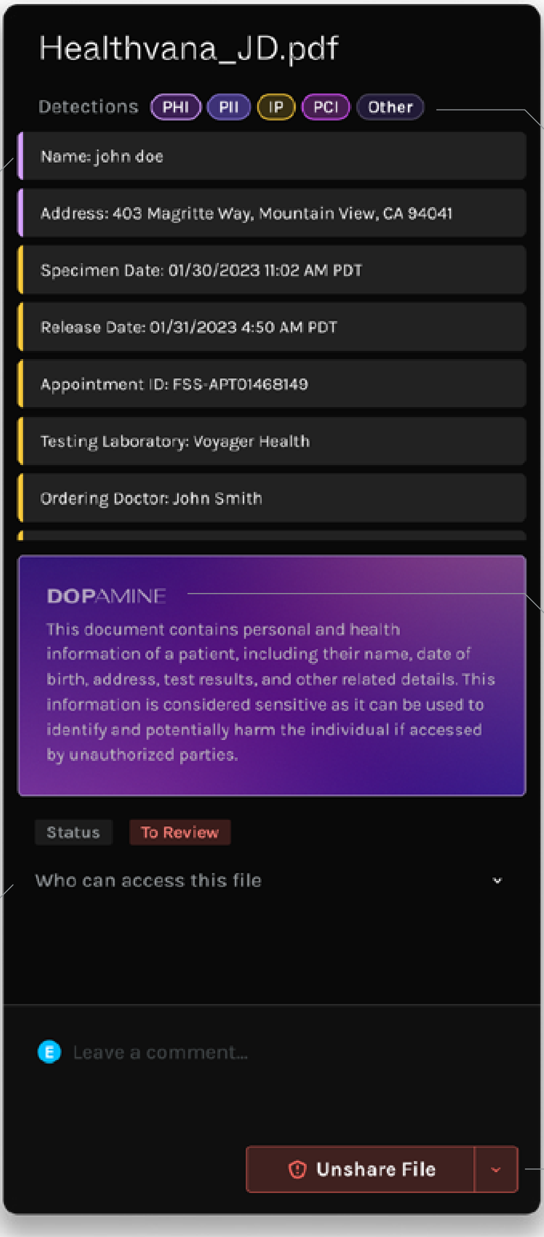
PCI
Payment Card Industry

PII
Personal Identifiable Information

Other Public Files

INTRODUCING DOPAMINE DLP

Dopamine DLP provides a highly precise human-readable document summary alongside any sensitive data extractions. Upgrade your old-school DLP regexes and pattern matching with LLMs, and experience fewer false positives than ever before.



Healthvana_JD.pdf

Name: john doe

Address: 403 Magritte Way, Mountain View, CA 94041

Specimen Date: 01/30/2023 11:02 AM PDT

Release Date: 01/31/2023 4:50 AM PDT

Appointment ID: FSS-APT01468149

Testing Laboratory: Voyager Health

Ordering Doctor: John Smith

DOPAMINE

This document contains personal and health information of a patient, including their name, date of birth, address, test results, and other related details. This information is considered sensitive as it can be used to identify and potentially harm the individual if accessed by unauthorized parties.

Status: To Review

CLASSIFICATIONS

All externally shared files as classified as containing PII, PCI, PHI, Intellectual Property, or just “Other” Public files

Sensitive data detected in document

DOPAMINE HIT

Highly precise human-readable document summary alongside any sensitive data extractions

Users who have access to this file within and outside of your organization

Unshare, mark as reviewed, or reopen your file

DO WE SHARE YOUR DATA?

No! Our off-the-shelf LLM technology is private, with data segregation between clients. Your data will not be used to train the model.

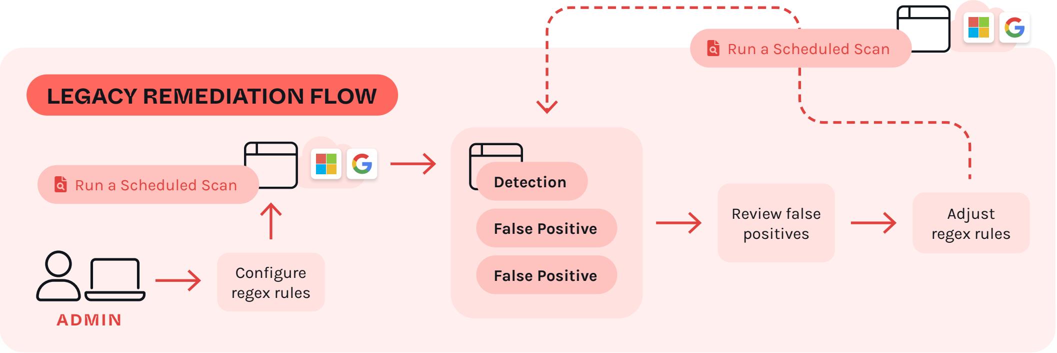
See our Data Processing Agreement to read more.

ONE-CLICK REMEDIATION

Each dopamine hit helps the admin decide what to do next by giving a clear, accurate summary of the document. From there, they can remove the file-sharing permissions with one click from the console.

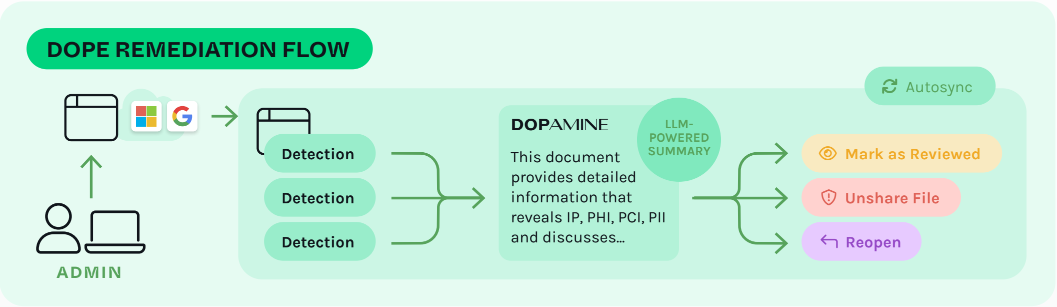
Legacy remediation is tedious

With legacy CASBs, any sensitive file incident is typically a false positive. This creates a flurry of noise and require re-configurations that makes it very difficult to get usable results.

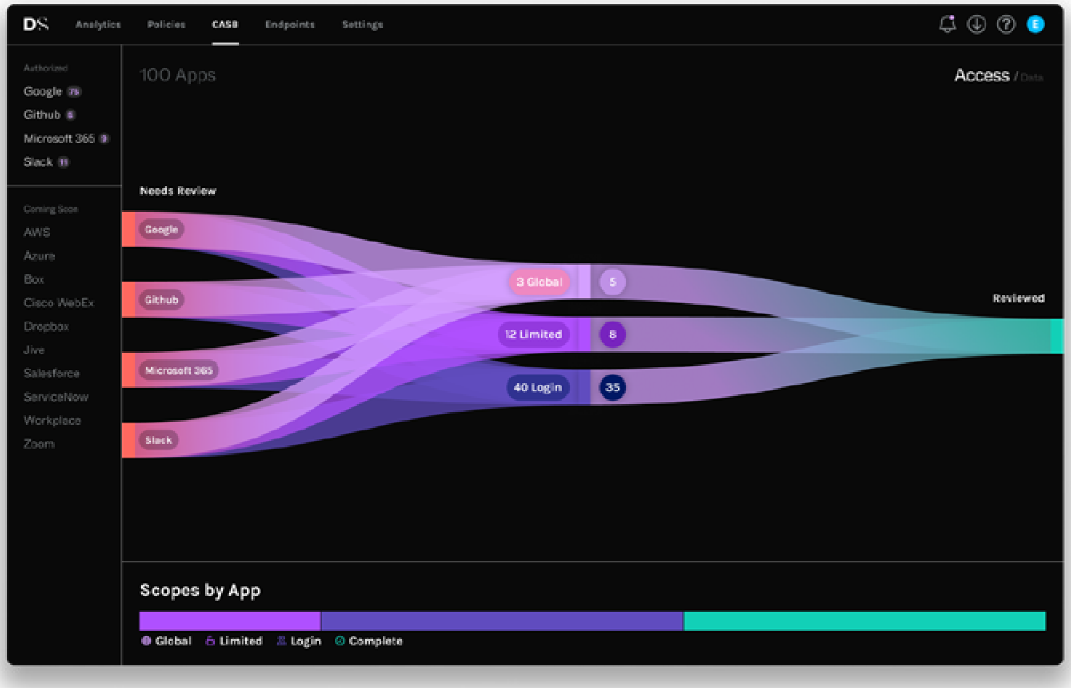


OUR FIRST-CLASS EXPERIENCE

Our dopamine hit accurately summarizes the document, and can be confidently remediated with one-click.



SaaS Security Posture Management (SSPM)



Uncover all third-party apps connected to your Microsoft 365 or Google SaaS tenant, neatly organized by access type: global, limited, or login access. Review detailed data such as app access start date, app access capabilities, and user info.

05 Appendix

Not-so-buzzwords

Some common words you might see around

DOPE COMPONENTS

dope.cloud
A set of security services and APIs that maintain a connection between the endpoint and console

dope.console
The administrator's cockpit. The single point of control for all connected endpoints, providing visibility and troubleshooting capabilities at scale. It maintains the connection between an installed endpoint and cloud to keep defined policies up to date.

dope.endpoint
The on-device proxy that manages and enforces a company-defined policy. It autonomously performs all SWG functions, even when there is no cloud connection, so users remain safe at all times.

dope.swg
The dope.security direct-to-cloud proxy at the endpoint.

dope.casb_neural
The dope.security LLM-powered CASB DLP for Cloud Apps

STOPOVER DATA CENTER

The process of info stopping over at a data center to perform SSL Inspection and cybersecurity checks. Often conducted by many legacy SWG vendors.

ENDPOINT HEALTH STATUS

Healthy
A consistent heartbeat and successfully securing traffic

Dormant
The state that is triggered when an endpoint has not connected to the internet for more than 7 days.

Fallback
If an endpoint cannot reach the cloud it will enter Fallback Mode, triggering either a *Fail Open* or *Fail Close* setting that does not require internet access.

Error
Indicates an error state—i.e. service interruption, configuration error, SSL Certificate not installed.

Disabled
The endpoint is disabled.

Debug Mode
Diagnostics and troubleshooting within the console to restore an endpoint experiencing an error.

LEGACY [LEGACY VENDOR]

An organization's IT infrastructure, systems, hardware, or applications that are impossible to update or improve due to systems from the last 20 years.

Also refers to an organization's approach to building a complex technology or process.

LIFT-AND-SHIFT MODEL

The migration of physical hardware appliances (typically found at corporate headquarters) to the cloud, as a hosted SWG provided by a SWG vendor.

DOPE CATEGORIES

80+ PRECONFIGURED CATEGORIES

AI/ML Applications
Adult Material
Adult/Mature
Lingerie/Swimsuit
Nudity
Pornography
Sex Education
Business
Alternative Currency
Brokerage/Trading
Business/Economy
File Storage
Finance
Marketing/Merch.
Productivity Apps
Drugs
Controlled Substances
Marijuana
Education
Entertainment
Gen. Entertainment
Humor/Comics
Media Sharing
Mixed Content
Music/Audio
Video Streaming
Extreme/Gruesome
Gambling
Games
Government/Legal
Military
Politics/Opinion
Hacking Tools
Hate/Discrim.
Health
Abortion
General Health
Illegal
Child Pornography/Abuse
Piracy/Plagiarism
Scam/Illegal/Unethical
Torrents/P2P
IT
Ads/Analytics
CDN/Content Servers
Cybersecurity Tech.
Dynamic DNS
Hosting
Information Tech.
Infrastructure/IOT
Login/Challenge
Remote Desktop
Search Engines
Software Downloads
Translation
URL Redirect
Internet Comm.
Chat/Messaging
Email
Forums
VOIP/Telephone
Video Conferencing
Job Search
Newly Registered
News
Non-Profit/Advocacy
Parked Site
Religion
Alternative Ideology
Major Religions
Security
Malicious
Phishing
Potentially Unwanted Applications
Promotional Comp.
Proxy Avoidance
Spam
Suspicious
Shopping
Auctions/Classifieds
Stores
Society & Lifestyle
Alcohol
Arts/Culture
Dating
Digital Postcards
For Kids
Hobbies/Recreation
Personal Lifestyle
Personal Sites/Blogs
Real Estate
Reference/Encyclopedia
Restaurants/Food
Social Media
Tobacco
Sports
Travel
Vehicles
Violence
Weapons

Comparing against legacy SSE

		DS	Forcepoint	Zscaler	Symantec	Skyhigh Security	Cisco DNS	Netskope
SECURE WEB GATEWAY (SWG)	DATA CENTER RELIANCE	⊗	✓	✓	✓	✓	✓	✓
	URL FILTERING	✓	✓	✓	✓	✓	⊗	✓
	ANTI MALWARE	✓	✓	✓	✓	✓	⊗	✓
	CLOUD APP CONTROLS	✓	✓	✓	✓	✓	⊗	✓
	INSTANT POLICY UPDATES	✓	⊗	⊗	⊗	⊗	⊗	⊗
	ON DEVICE SSL INSPECTION	✓	⊗	⊗	⊗	⊗	⊗	⊗
	ENDPOINT DLP	Coming Soon	✓	✓	✓	✓	⊗	✓
CLOUD ACCESS SECURITY BROKER (CASB)	REGEX/PATTERN MATCH DLP	⊗	✓	✓	✓	✓	⊗	✓
	AI/LLM POWERED DLP	✓	⊗	⊗	⊗	⊗	⊗	⊗
	FILE SUMMARIES	✓	⊗	⊗	⊗	⊗	⊗	⊗
	ONE-CLICK REMEDIATION	✓	⊗	⊗	⊗	⊗	⊗	⊗
	SSPM	Coming Soon	⊗	✓	⊗	⊗	⊗	✓
FIRST-CLASS EXPERIENCE (UX/UI)	SSO-ENABLED INSTANT TRIAL	✓	⊗	⊗	⊗	⊗	⊗	⊗
	MAC NATIVE	✓	⊗	✓	✓	✓	✓	✓
	SINGLE CONSOLE	✓	⊗	⊗	⊗	⊗	✓	✓
	AUTO-UPDATES	✓	✓	✓	✓	✓	✓	✓

DOPE.
SECURITY

DOPE = *Passion*. Design. Attention to detail. That's the difference with our on-device proxy, the Fly-Direct SWG. Paired with CASB Neural, the LLM-powered DLP, we build beautifully designed enterprise cybersecurity. So whether your company is small or large, you get a first-class experience.

It's not that we're mad at yesterday's solutions—just disappointed. So we made it better. We made it easier. *We made it dope.*

SALES@DOPE.SECURITY