

INTRODUCING THE NEW FLY-DIRECT SECURE WEB GATEWAY

Endpoint-driven
without any stopover
data centers.



Table of Contents

01

Our Fly-Direct Philosophy_3

02

A New Secure Web Gateway is Born_5

03

Feature Breakdown_11

04

Diagnostics & Debug Mode_21

05

Writing Policies_23

06

Analytics, Your Captain's Dashboard_29

07

The DS Appendix_36



01

OUR FLY-DIRECT PHILOSOPHY

Our approach to a faster, more reliable experience is to move the SWG to the endpoint. No more stopovers. No more friction.

What is Our Fly-Direct Philosophy?

Our philosophy is to make security simple. Our vision is to provide a first-class internet experience, no matter what. That's why our approach to a faster, secure experience moves the secure web gateway to the endpoint. No more stopover data centers. No more friction.

We stand by keeping simple, simple—turning the complex into new possibilities. The latest cybersecurity paradigm shift begins with dope.security.

WE ENVISION A WORLD WHERE CYBERSECURITY IS...

01

Invisible

02

Simple

03

Elegant

04

Private

02

A NEW SWG IS BORN

Traditional web filtering and proxy solutions are no longer effective at safeguarding web and cloud app users and their data.

Shortcomings of the Legacy SWG

The way we secured corporate workforces 20 years ago worked well for a while. Endpoints were protected by security tools close to the user, including one of the most fundamental technologies, the Secure Web Gateway (SWG).

The legacy SWG sat on-premises and enforced a company policy via a hardware proxy. These policies protected users from malicious content while blocking non-work related websites like social media, gambling, and entertainment.

Time has moved on. Legacy SWGs haven't.

In the decades that have followed, the SWG technology has stayed the same. We've seen a "lift and shift" of what was once on-prem, to the cloud, in order to connect employees outside of the office. At the foundation of this, however, is a heavy reliance on data centers. This reliance creates a stopover that could be in any location—or even in a different country—with added security risks. It is like taking a stopover flight when you just want to fly direct.

So if an employee visits any website, such as The New York Times or Facebook, their traffic is first redirected to a stopover data center before eventually reaching their final destination—diminishing reliability, performance, and privacy of typical web browsing.

As years have passed, the typical vendor response to fix congestion issues is to "spin up another data center" nearest the bottleneck. It's a fix, but it's a temporary fix. In reality, their architecture is the problem: a new foundation is required.

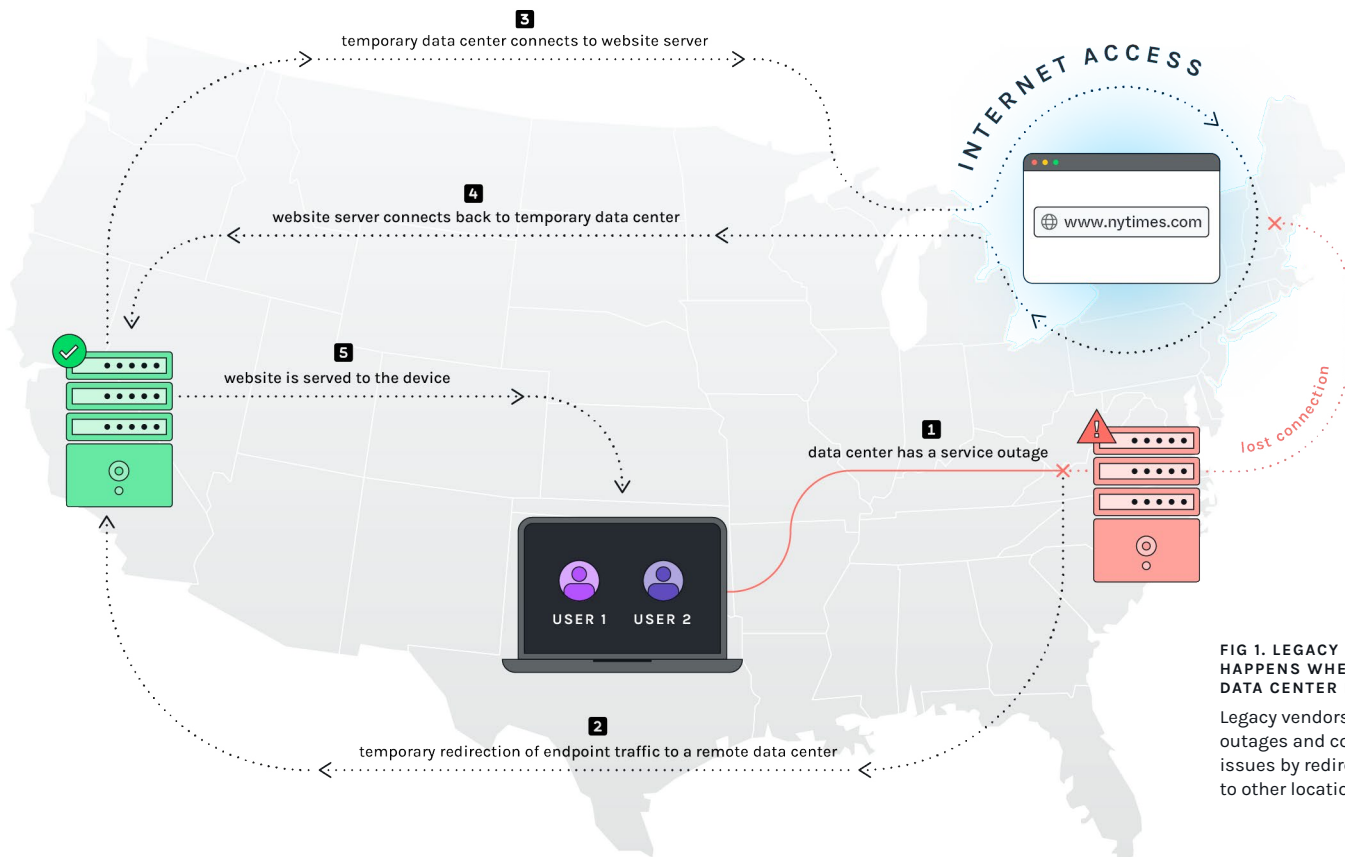


FIG 1. LEGACY SWGS: WHAT HAPPENS WHEN YOUR NEAREST DATA CENTER HAS AN OUTAGE?

Legacy vendors respond to outages and congestion issues by redirecting traffic to other locations.

The Impact on End User Experience

RELIABILITY

Typical end user internet access suffers frequent data center outages and reliability issues, negatively impacting user experience:

- **Connection Issues:** Outages cause pages to break, or traffic to fail open.
- **Incorrect Locale:** Search results in the incorrect language for the user, e.g. French-origin traffic gets rerouted through Germany.
- **Geographical Limitations:** Proxies are blocked by foreign countries or public Wi-Fi, causing policy enforcement loss.
- **Egress IP Reputation:** Traffic from a proxy is lower reputation and can be blocked, degraded, or subjected to more external scrutiny.

It comes down to having a solution that doesn't impact the user's day-to-day work. Ultimately, you can't band-aid a broken architecture.

"No matter what, our hotels are not near a legacy data center. Websites work *sometimes* because the data center is in another city or country."

— HOTEL CHAIN

PERFORMANCE

Redirecting all endpoint web traffic to the legacy SWG will always be slower, no matter what. Imagine taking a flight from San Francisco to Los Angeles, and stopping over in New York, wouldn't you have rather gone direct? Now consider thousands of users traveling to that stopover with you, and the congestion this creates.

Security shouldn't come at the expense of the end user's experience—and, for stopover SWGs, speed is always an afterthought. No existing SWG vendor supports HTTP/2 even though it's used on every website. You shouldn't be forced to downgrade to HTTP/1.1.

By changing priorities and architecture, end users should feel secure and unhindered by the tools protecting them.

"All my employee traffic gets severely degraded and is sent to different country where the data center resides. If we went direct, our security would be lost."

— OIL AND GAS ORGANIZATION

PRIVACY

To provide security, a proper SWG must perform Secure Sockets Layer (SSL) inspection. But, without realizing it, user traffic is often decrypted in foreign countries to perform the security/policy check at the stopover data center.

This means the risk of your sensitive data being stolen is greater. Whether it's stored-to-disk or in-memory, data should not be decrypted outside your endpoint. Flying direct with DOPE.SWG makes this risk disappear.

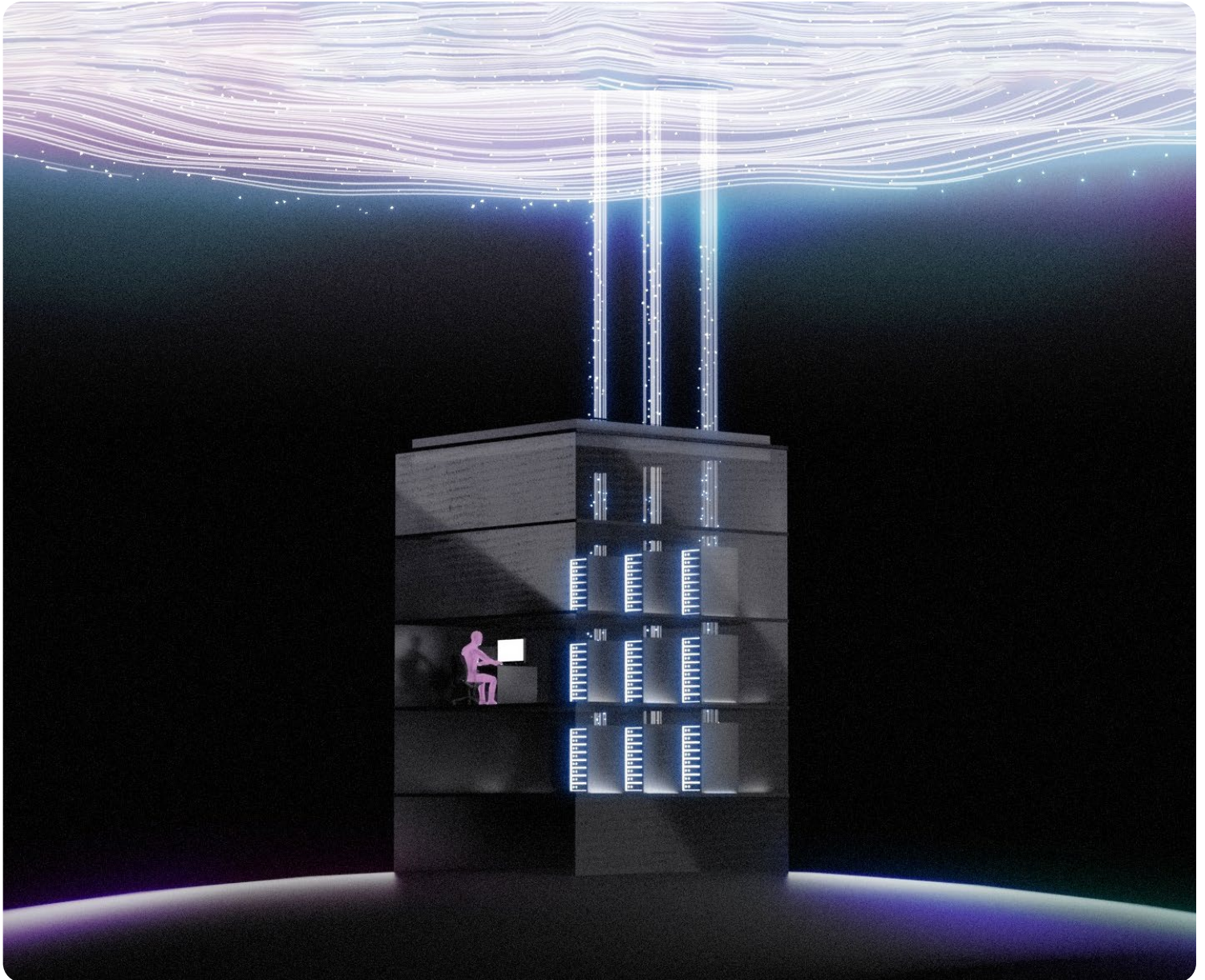
"We really do not want to break SSL in a different country, or decrypt traffic in vendor's data center. But, what option do we have?"

— INDUSTRIAL ORGANIZATION

So why stop over when you can fly direct?

To be a cloud proxy today means lifting and shifting 20-year-old technology into a data center, pumping web traffic through it, and calling it a cloud-based SWG.

The bottom line is that the response from vendors today is to maintain this architecture without solving the real issues. What the industry needs is a new direct-to-internet SWG that places reliability, performance, and privacy at the user's fingertips.



Re-Architecting the SWG

To revolutionize today's SWG, it needs to be replaced by a smarter one: a SWG that works for you, the customer, not the other way around; a SWG that places privacy first over what is already built and used today. The industry needs a SWG that does not compromise end user experience.

Welcome to your Fly-Direct Architecture.

A NEW SWG IS BORN

Stemming from our personal experiences at legacy cybersecurity companies, we heard first-hand the many issues customers faced with their legacy SWG—from reliability issues to support cases—and it was a nightmare. Above all, the company leaders didn't seem to care about fixing the problems in their security solutions. They were more focused on inventing platforms. We had to do something to help our customers and solve this 20-year old SWG problem. This inspired our team to start from the ground up.

DOPE.SWG's new architecture solves the reliability, performance, and privacy issues that customers face every day; it includes every feature you need with a first-class user experience.

YOU WERE FLYING STOPOVER, NOW LET'S FLY DIRECT

To implement this new architecture, we took advantage of new technologies that we couldn't use at those legacy companies because:

- 1 The new paradigms didn't exist
- 2 Re-architecting would short-term impact the thousands of existing customers using it daily
- 3 We knew that our SWG had to be smarter and faster—similar to what customers expect from consumer apps

So we integrated newer technologies, such as:

AT A GLANCE

DOPE.CLOUD TECHNOLOGIES

- Multi-region active-active global tables
- Multiple regions of transaction data residency (USA, Germany, Bahrain, Singapore, Brazil, Australia, and more)
- Serverless architecture
- Instant SSO via corporate email
- Instant Import of users and groups from Google and Microsoft 365

DOPE.ENDPOINT FEATURES

- HTTP/2 support
- Local enforcement, invisible to the end user
- macOS 12-13 (Intel and M1 Silicon) Native, and Windows 10-11
- Remote Troubleshooting
- Fallback Intelligently

GLOSSARY

dope.cloud
A set of security services and APIs.

dope.endpoint
The on-device proxy that manages and enforces a company-defined policy.

[SEE THE DS APPENDIX \(P. 37\) FOR MORE](#)

How to Fly Direct

The **DOPE.ENDPOINT** performs all URL filtering, cloud application controls, anti-malware, and policy enforcement on-device without any stopover data centers.

And, the best part is: our policies are user-based—each policy can be applied to users and groups after enabling instant single-sign on and user import.

You'll be ready for take-off in seconds.

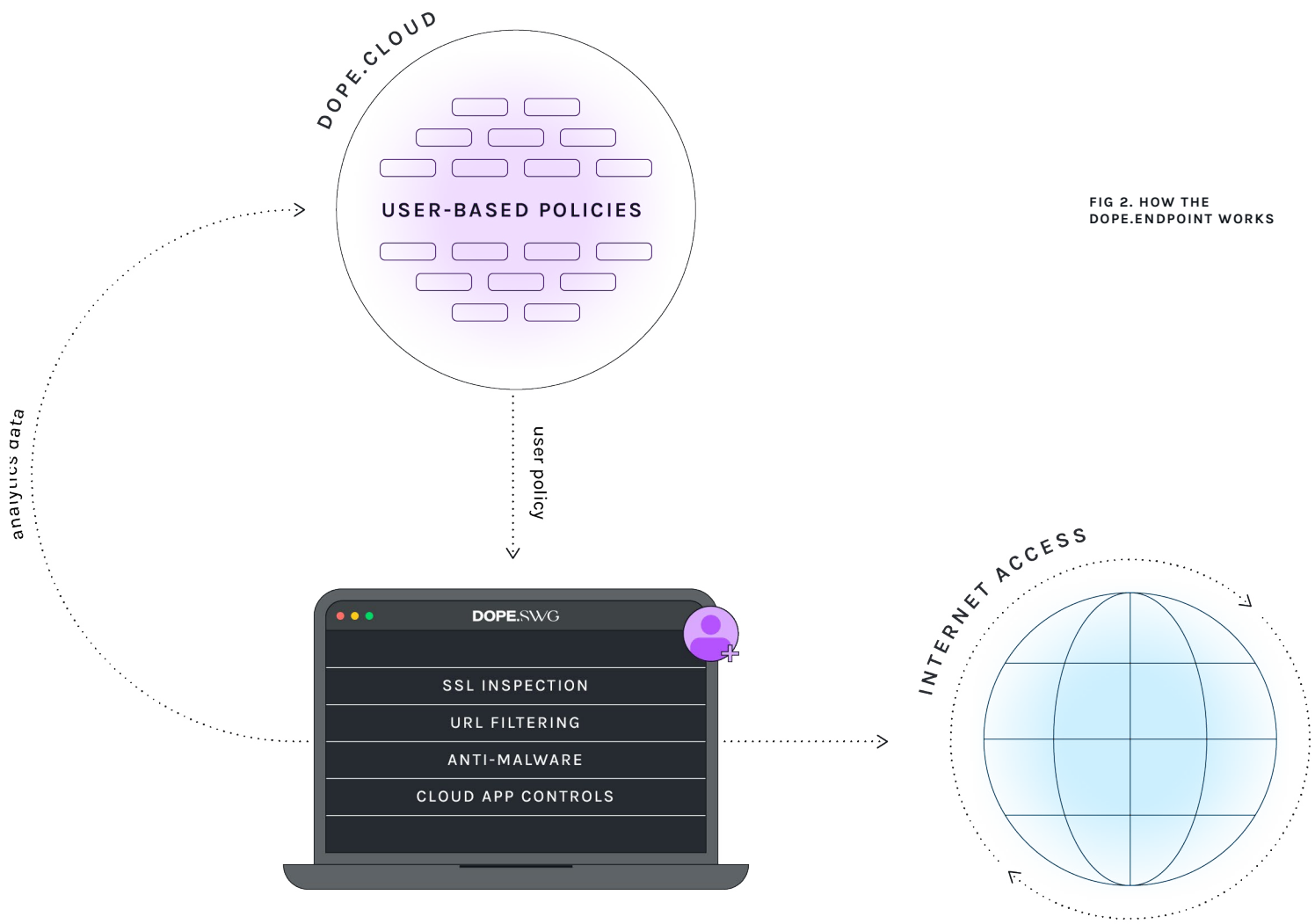


FIG 2. HOW THE DOPE.ENDPOINT WORKS

03

FEATURE BREAKDOWN

Introducing dope.swg—no stopover data centers, no performance delays, and no more privacy concerns. Your new Fly-Direct Secure Web Gateway is now on the endpoint.

Feature Breakdown

Let's take a closer look at some of the in-flight amenities on your first Fly-Direct SWG

01

SSL Inspection

02

URL Filtering

03

Single Sign-On

04

Anti-Malware

05

Cloud App
Controls

06

Cloud-Managed
Endpoint

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. Rather, all SSL Inspection is performed directly on the device in what's known as your "safezone."

What are the benefits of performing SSL Inspection in your safezone?

- 1 It keeps your data 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 safezone 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. Aside from broader compliance reasons, these legacy companies know that sending this type of sensitive data that could exist in these categories is vulnerable in a data center. So, their solution is to bypass the inspection entirely.

This bypass leads to traffic going uninspected and a loss of visibility of those web transactions—putting your data at increased risk.

THE LEGACY MAY DECRYPT... OR NOT

The legacy SWG architecture redirects and exposes sensitive data to unwanted security risks by decrypting data and breaking SSL remotely in a stopover data center.

Performing SSL Inspection the legacy way puts additional strain on the already flawed infrastructure which can lead to a degradation in performance for the end user, and is why some skip the inspection.

An administrator can choose to disable SSL inspection altogether for categories, exposing your data to increased security threats.



SSL Inspection

INSTANT SSL ERROR RESOLUTION

Sometimes SSL inspection can cause certain applications or URLs to break. This is why all SWG products, including **DOPE.SWG**, have application and URL bypass lists. With legacy providers, when SSL errors occur its up to your admins to work out what needs to be bypassed, or a support ticket needs to be logged.

We always want to provide our customers with a first-class experience so we have automated this process. When a SSL error occurs on a device the **DOPE.ENDPOINT** will report the application and the URL to the **DOPE.CLOUD**. The admins can view these errors from the notifications panel and decide if they want to bypass the application or just the effected URL across the organization.

Or, an admin may decide that they don't want to fix the problem. It really is that easy!

WHY DO SSL ERRORS OCCUR?

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

The screenshot displays the DOPE.SWG dashboard with a dark theme. The main area features a world map with colored markers indicating active, above-average, or erroneous SSL events. A 'Notifications' panel on the right lists detected SSL pinning errors, categorized by application or URL. A callout bubble highlights the 'Bypass for all policies' button for the 'osqueryd' application. Another callout points to the user icon in the top right corner, indicating that hovering over it reveals which users reported the issue. At the bottom, a summary bar shows '393 Policy Violations' for the 'Entire Organization', with 'File Storage' as the most violated category. Other metrics include 'Email' for productivity and 'Dropbox' for shadow IT.

Instantly get notified of SSL errors

Hover over the user icon to see which users have reported the issue

Notifications

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

By App 3 **By URL** 2

☐ 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 (8)
fcmconnection.googleapis.com (3)

Notifications

SSL pinning errors detected. Resolve them applications or URLs below. (?)

By App 3 **By URL** 2

☒ osqueryd (1)
osqueryd.vanta.com

Bypass for all policies

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

Policy Violations 393 Entire Organization

Violation Detail File Storage Category Most Violated

Productivity Email Most Time Spent

Shadow IT Dropbox Most Used Cloud App

Easily bypass any Apps or URLs that are identified as breaking due to SSL errors (SEE BYPASS SETTINGS P.26)

URL Filtering

Your first line of defense is **DOPE.ENDPOINT**'s URL Filtering. The redirector captures all outgoing traffic to be compared against the user's policy, in order to prevent users from accessing websites that are malicious or non-work related.

This level of content filtering increases network security and applies company policy to what can be accessed within your organization.

HOW URL FILTERING IS APPLIED

Our journey begins at the user endpoint. Once access to a website is requested, our redirector captures and sends the traffic to the on-device proxy. Next, it is analyzed and decrypted to gauge the safety of the URL. Based on the policy you have applied, the **DOPE.ENDPOINT** then makes a security decision for the URL to be "Allowed," "Blocked," or "Warned."

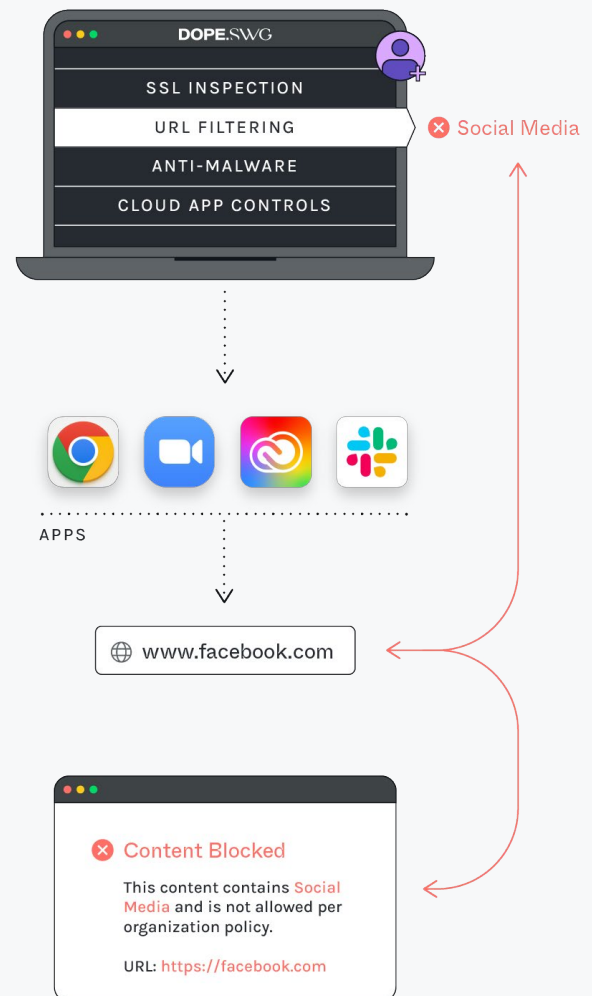
EXAMPLE

1. A user types in "facebook.com" on any browser
2. The **DOPE.ENDPOINT** redirects the request to the local proxy → decrypts it → determines the category of the URL (e.g. Social Media)
 - a. If **previously visited**, the local cache will remember the category result; the system cache is regularly refreshed
 - b. If **never visited before**, the proxy requests the category from the **DOPE.CLOUD**
3. After instant policy comparison, the result is presented to the end user depending on the setting:
 - a. Category is **Allowed**
 - b. Category is **Blocked**
 - c. Category is given a **Warning**

REMEMBER: BLOCK PAGES ARE CUSTOMIZABLE.

FIG 3. HOW DOPE.SWG APPLIES URL CATEGORIZATION

When a user attempts to visit a website, via a browser or application, it is locally inspected for threats at every stage of analysis.



Single Sign-On

We use Single Sign-On (SSO) through OpenID Connect (OIDC) with Office 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 (Azure AD, Okta, Ping, Onelogin, etc.)
- 2 Admins, end users, and their groups are automatically updated and deprovisioned

It really is one-click!

NOTE:

The DOPE.CLOUD manages the OIDC authorization between your user and the associated policy.

NOTE:

If you do not enable Endpoint Auth and import your users, only the Base Policy can be configured; additionally limits visibility, policy customizability (including exceptions), and reduces analytics.

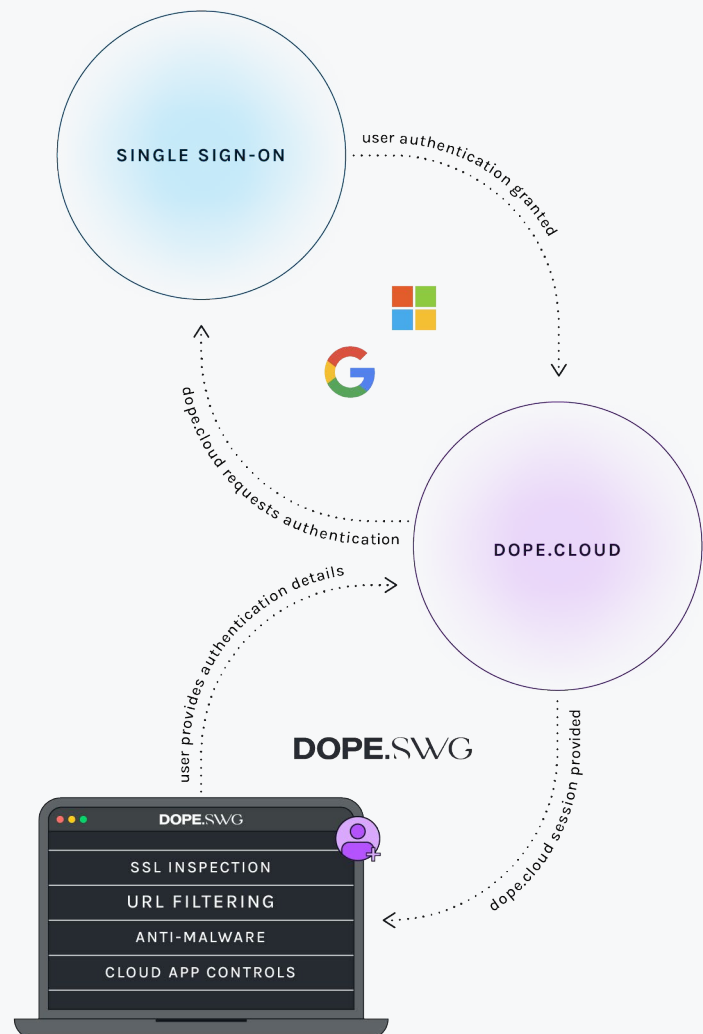
GETTING STARTED WITH SSO & IMPORTING USERS

1. **Start by enabling Endpoint Authentication**
 - a. Log in with a corporate account (Google or Microsoft 365), this unlocks full visibility across your endpoints
2. **Enter your Accepted Domains** (e.g. voyager.com) and **Save**
 - a. Certain organizations might use multiple domains
3. **Configure User Import**
 - a. This secret link can be used by the identified admin to authorize Google or Microsoft 365 read-only user privileges; we'll automatically sync your users with the DOPE.CLOUD from here
4. **Congratulations, your import was successful!**
Now you can:
 - a. See a complete list of imported users or groups
 - b. Write and assign custom policies
 - c. Act on insights ushered in the Analytics Dashboard

FIG 4. HOW SSO WORKS WITH OIDC AUTHENTICATION ENABLED

Typically, configuring SSO and user imports requires separate SAML & SCIM integrations that are complex to coordinate and manage as they require special privileges and change control. Some legacy SWGs still use active directory (AD) sync agents. With that in mind, we've removed the administrative barriers and modernized it:

- No SAML certificates or NameID/attribute mappings
- No SCIM or AD Agents



Anti-Malware

DOPE.SWG leverages multiple anti-malware services to determine file safety. The goal is simple—capture and block files that may have malware.

It is in charge of:

- 1 Capturing all file hashes from all downloads .DOCX, .PDF, .XSLX, .EXE, AND MORE
- 2 Receive the status from the Malware Service¹
- 3 Caching the result for future use
- 4 Updating the Analytics dashboard of the DOPE.CONSOLE
- 5 Serving the result to the endpoint as **ALLOWED** or **BLOCKED**

1. We use a combination of popular anti-malware services to retrieve file hash convictions.

THE DOPE ANTI-MALWARE SERVICE

EXAMPLE

1. DOPE.ENDPOINT captures and decrypts the traffic
 - a. Box.com is allowed through URL Filtering
2. We detect a file download on the endpoint
3. Before it is downloaded, we calculate the file hash and check the local cache to verify the file:
 - a. **✓ Allowed**
 - b. **✗ Blocked**
4. If we haven't seen the file before, it is hashed and checked against the DOPE.CLOUD to verify:
 - a. **✓ Allowed**
 - b. **✗ Blocked**

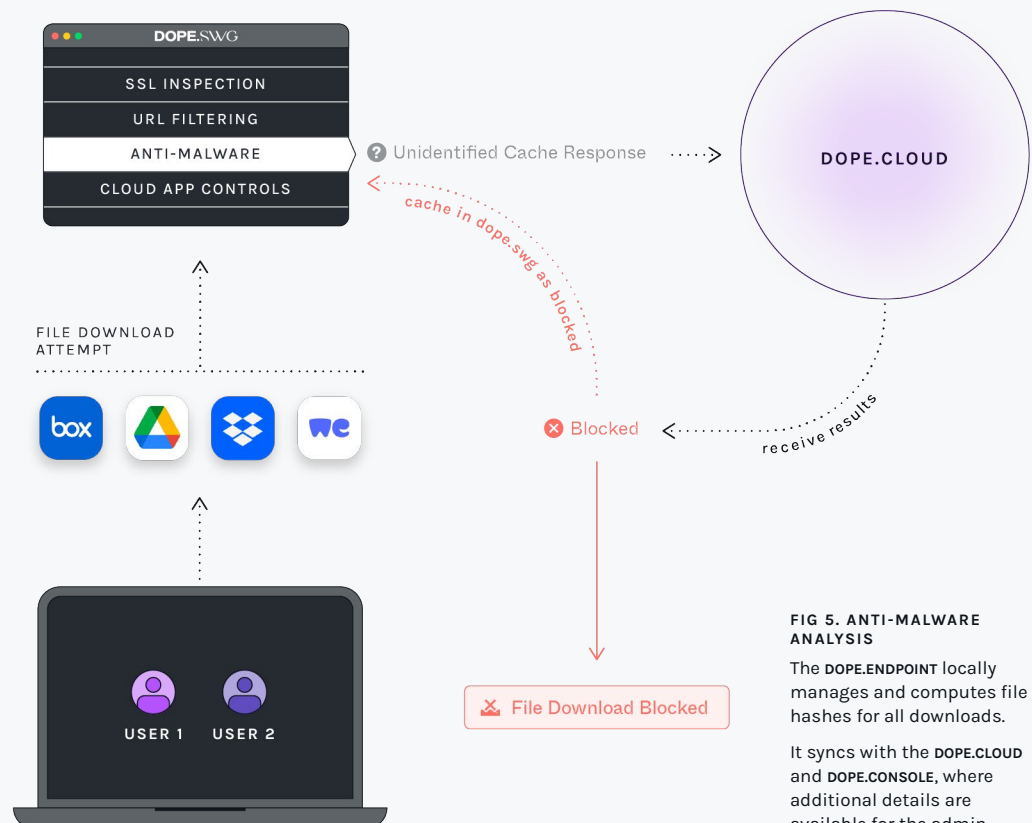


FIG 5. ANTI-MALWARE ANALYSIS

The DOPE.ENDPOINT locally manages and computes file hashes for all downloads.

It syncs with the DOPE.CLOUD and DOPE.CONSOLE, where additional details are available for the admin.

Cloud App Controls

Cloud Application Controls (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.

WE MAKE CLOUD APP CONTROLS SIMPLE

Configuring CAC on most legacy SWGs is a pain for every admin. Some offer simple allow or block capabilities on cloud apps. But if you want additional controls, you're often required to open a separate Cloud Access Security Broker (CASB) console to create a new policy for those apps. Or worse, you're required to redirect traffic from the legacy SWG to a CASB-specific proxy. The process is cumbersome, and now you have two stopovers.

WE'VE COVERED THE BASES WITH

- Simple, easy configurations via the single DOPE.CONSOLE
- Unique controls to allow/block enterprise IDs or domains, just type them in and save
- CACs are part of the same policy you customize, no separate policy required

THE BASICS OF CLOUD APP CONTROLS

CONTROL ACCESS TO ANY OF THESE APPS

Google

Microsoft 365

Salesforce

Dropbox

Slack

Box

Cisco Webex

ADD DOMAINS ASSOCIATED WITH ANY APP, e.g.

Google

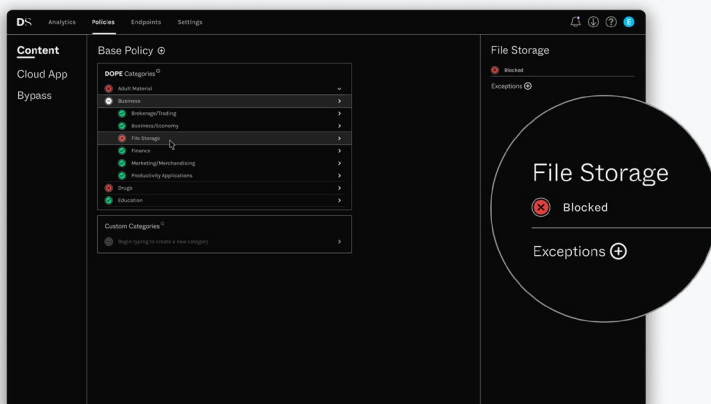
@voyager.com

@flydirect.com

→ block access to all other domains on Google

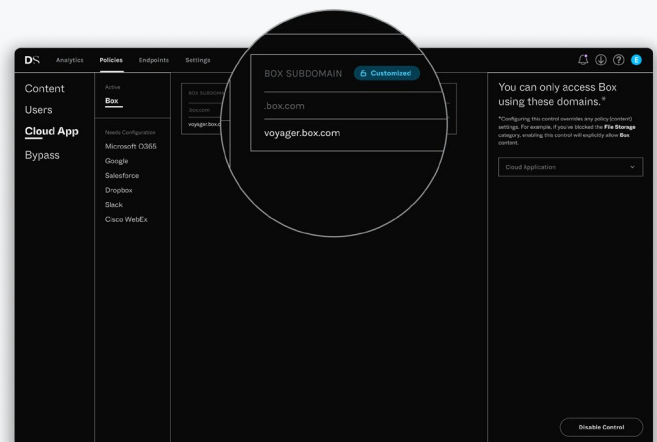
DOPE.SWG BLOCKS ANY ATTEMPT TO ACCESS A CLOUD APPLICATION WHOSE DOMAIN IS NOT IN A POLICY ALLOWED LIST.

EXAMPLE: FILE STORAGE ❌ BLOCKED



EXAMPLE 1

Under Business, "File Storage" is set to ❌ **Blocked**. As a result, websites and apps such as Dropbox and WeTransfer cannot be accessed.



EXAMPLE 2

Within the Box CAC Settings, "voyager.box.com" is set to ✅ **Allowed**. Users can only use their corporate Box account.

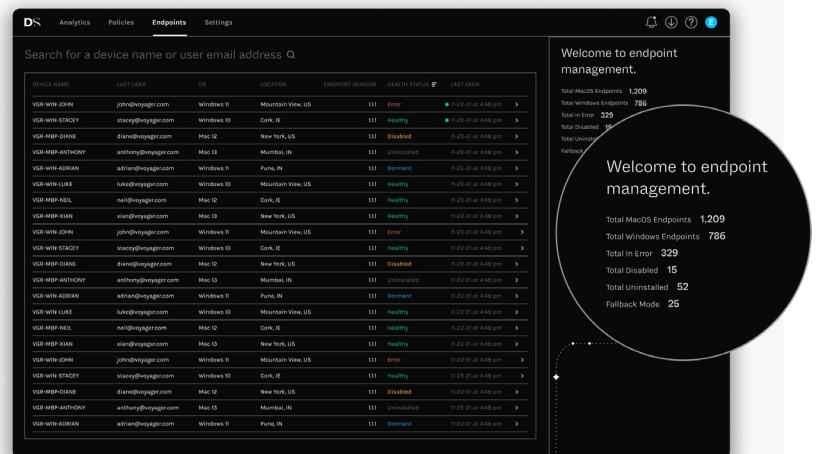
Cloud-Managed Endpoint

Endpoint Management is the administrator's cockpit. It provides visibility and troubleshooting capabilities across all endpoints.

Endpoint Management lends a helping hand between endpoints and the policies they use. We designed it so that you can quickly view the status of each endpoint connected to your network 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.

AT A GLANCE




After endpoints are installed, they are summarized in the right-hand panel.

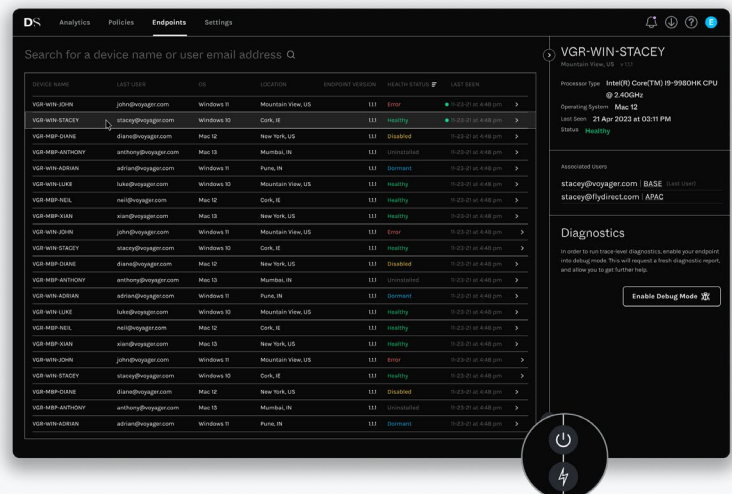


ADDITIONAL DETAILS

When you search for a device, you'll find additional details including location, endpoint version, health status, time last seen, and more.

If you are troubleshooting a user issue, we've included unique capabilities to make your life easier:

-  **Debug an endpoint:** The admin can request diagnostics and troubleshoot with one click, e.g. *an endpoint is intermittently in Fallback Mode* (SEE DEBUGGING AN ENDPOINT P.21)
-  **Disable an endpoint:** The admin can disable a user's endpoint for a period of time
-  **Double-check the policy:** The policy tester helps you to identify and test your policy in real-time



Cloud-Managed Endpoint

FALLBACK SAFELY WITHOUT LOSING PROTECTION

Each **DOPE.ENDPOINT** regularly checks its connection to the **DOPE.CLOUD**, and also sends its own health status (eg: Healthy, Fallback, Error, etc). In the event the **DOPE.CLOUD** cannot be reached, the endpoint will go into Fallback Mode.

WE OFFER TWO CONFIGURATION OPTIONS FOR THIS FEATURE

01

FAIL CLOSED ON

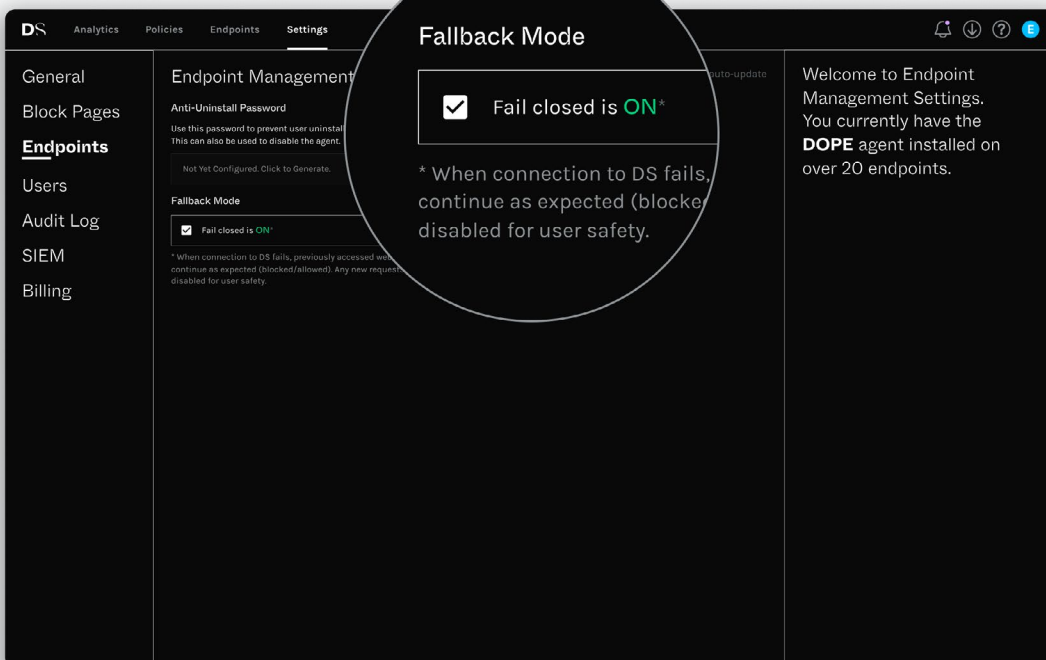
Allows previously accessed websites to continue per the policy (Allow, Block, or Warning). New requests will be **disabled for user safety**.

02

FAIL CLOSED OFF

Allows previously accessed websites to continue per the policy (Allow, Block, or Warning). New requests will be **allowed without security checks**.

CONFIGURE THESE OPTIONS UNDER SETTINGS > ENDPOINTS



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 much safer.

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

What does this mean for your organization? Uninterrupted, secure internet access for your users and effective policy enforcement at all times.

04

DIAGNOSTICS & DEBUG MODE

In our time working on legacy SWG endpoints, there were always troubleshooting issues. But, getting logs from customers was a huge hassle, and enabling trace logs was even worse.

That's why we revamped the debugging technology entirely to help our customers get flying faster. No legacy SWG offers this today.

Debugging an Endpoint

HOW TO DEBUG AN ENDPOINT

- 1 Enable Debug Mode on the endpoint
- 2 The DOPE.ENDPOINT automatically runs diagnostics
 - a. Run diagnostic tests and enable trace logging
 - b. All relevant logs are collected, e.g. endpoint and OS logs
- 3 Results are sent to the DOPE.CLOUD

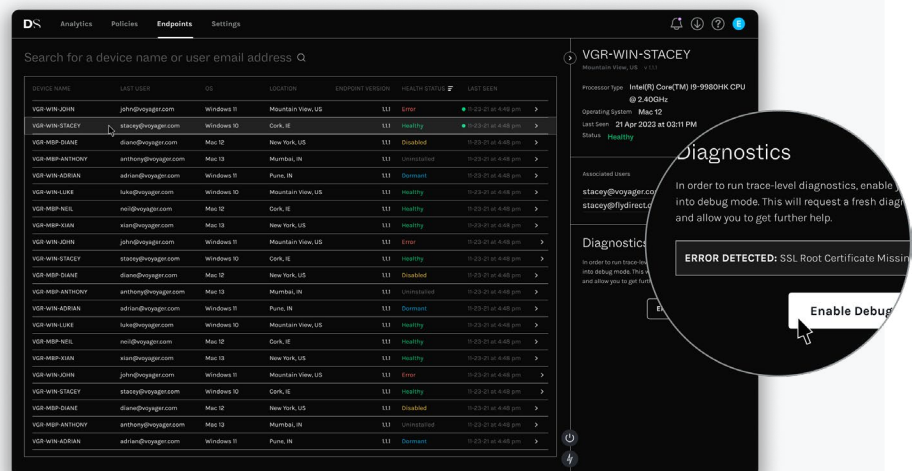
DEBUG TESTS INCLUDE

- Checking if the root Certificate Authority (CA) is Installed
- Network Connection status with and without the proxy
- Network Connection test using Redirector
- Captive Portal Test
- DOPE.CLOUD Connectivity Test

DIAGNOSTICS

We've covered why an endpoint enters Fallback Mode, but now let's understand how to troubleshoot and pull in diagnostics in order to restore an endpoint.

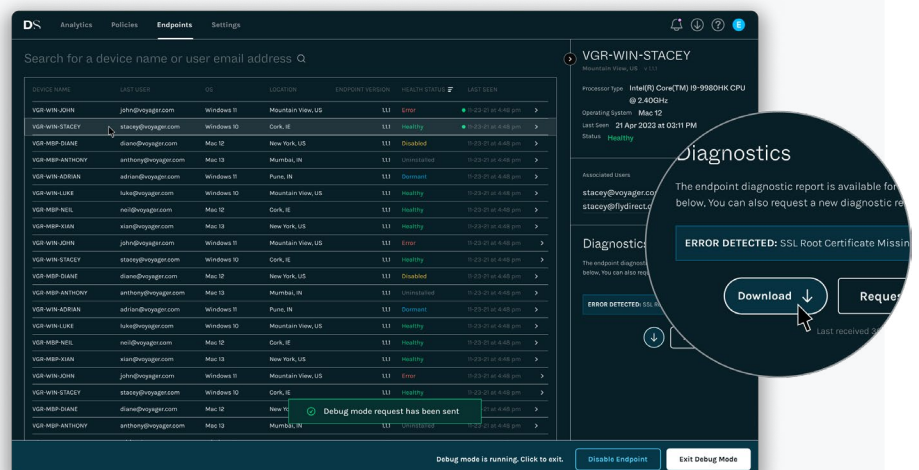
In the DOPE.CONSOLE, navigate to Endpoints for details on all endpoints in an Error or Fallback state to extract diagnostics and debugging information.



DOWNLOAD DATA

As the admin, you can remotely run diagnostic tests as required; the data gathered after each test is available for download via the DOPE.CONSOLE.

NOTE: DOWNLOAD FILE WILL BE A .ZIP CONTAINING ALL LOGS.



05

WRITING
POLICIES

Over 80 categories are ready to fly alongside your endpoints. Policy features include Cloud App Controls (CAC), custom block pages, bypass lists, and more.

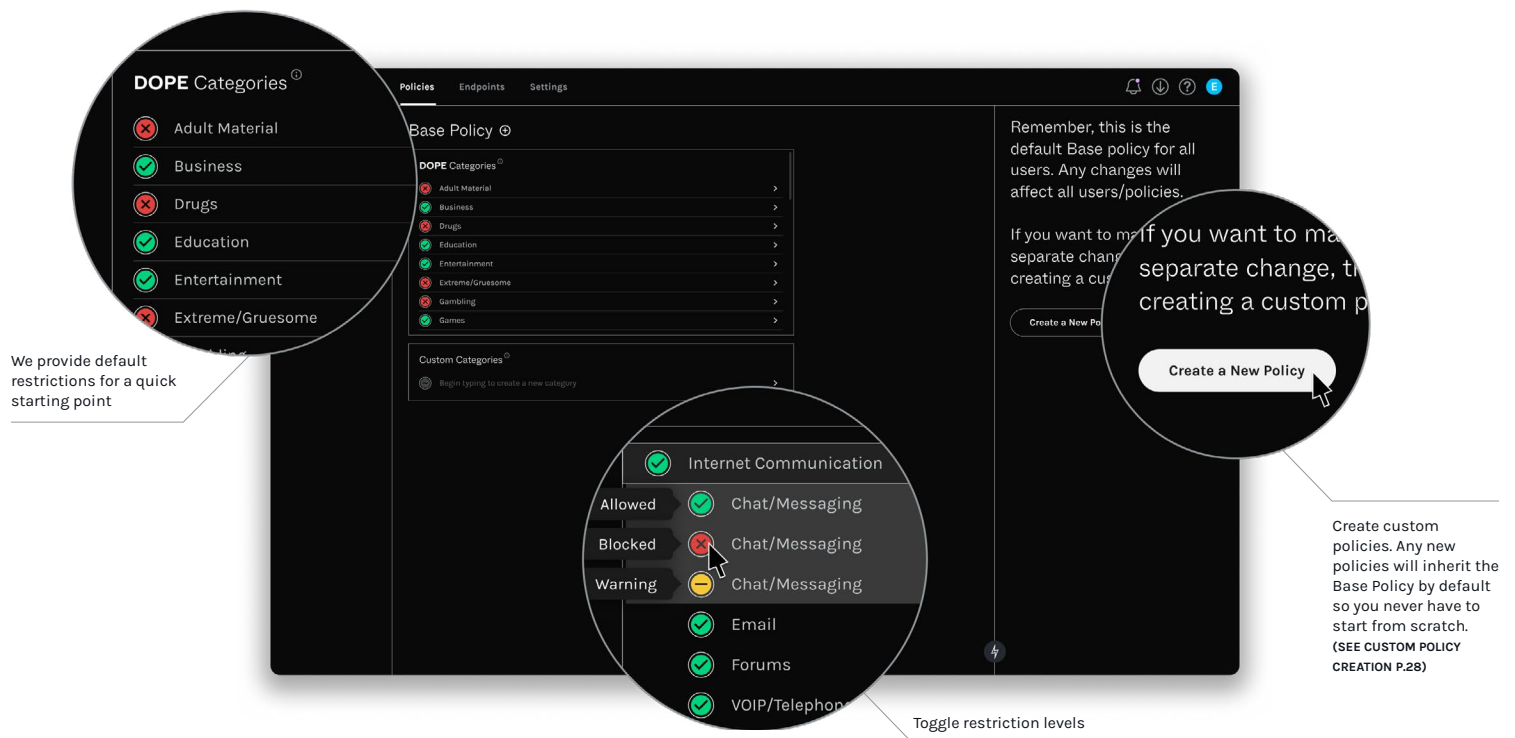
Editing the Base Policy

The base policy is configurable to suit your company's needs so you can easily adjust the out-of-the-box settings.

You can toggle the restriction level to “Allow” or “Block,” while DOPE.SWG also supports a restriction level of “Warning.”

EDITING DOPE CATEGORIES


Each of your organization's users starts with a base policy, which categorizes websites according to their purpose (e.g. Entertainment, Gambling, News). Each category has a default restriction of either “Allow” or “Block.” You can choose to allow or block any additional category you choose.



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 QUICK TOGGLE RESTRICTION LEVELS

Example: By default, the Base Policy allows “Chat/Messaging.” You can toggle to  to block this category, which will restrict the use of apps like WhatsApp and Messenger.

03 INSTANT POLICY PUSH

Once you hit save, your policy will be immediately enforced and deployed across your online devices, rather than having to wait up to 15 minutes—or even an hour.

Custom Categories

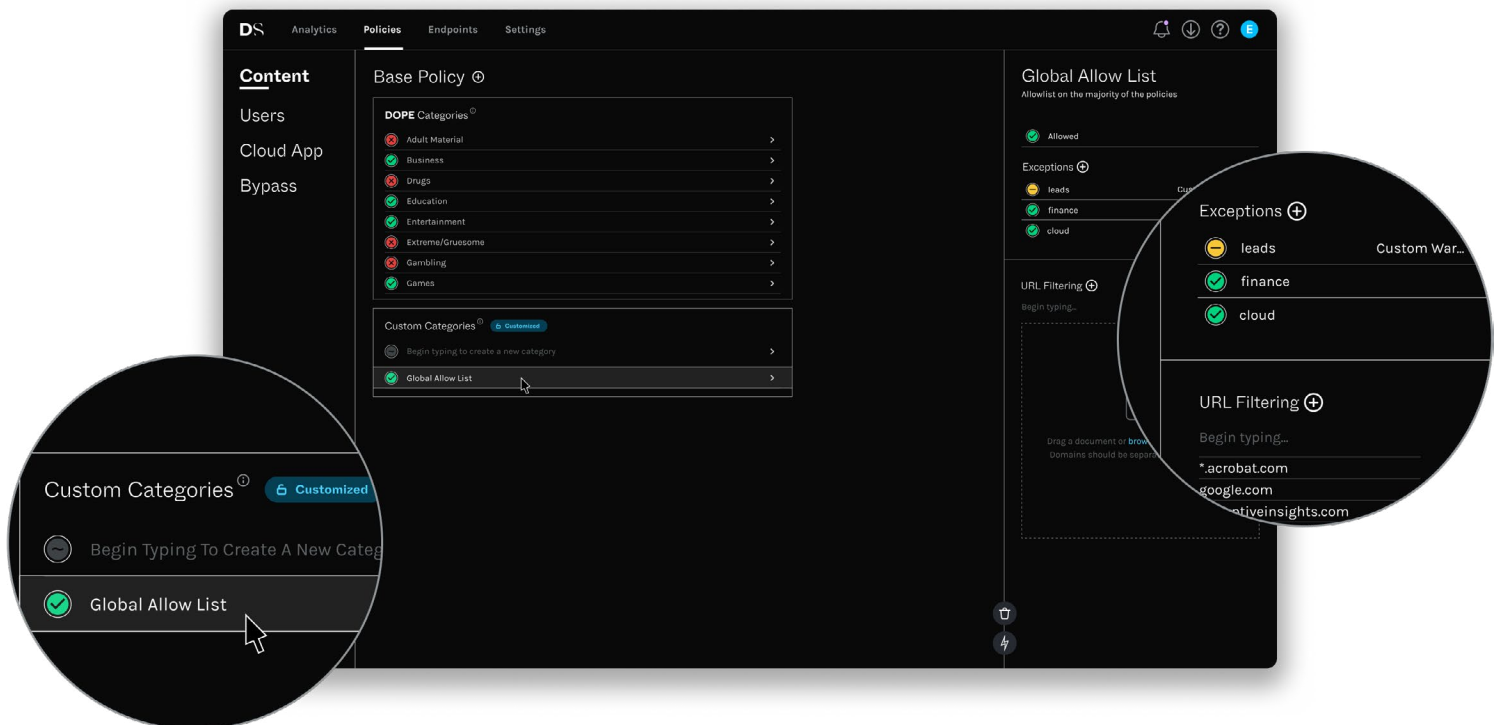
Although DOPE.SWG has over 80 categories, it's easy to create your own custom categories in addition.

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 "Warning." Custom categories are shared globally, so toggle an unwanted category to "Ignore" to keep it out of a particular policy.

Policy Exceptions

The DOPE.CONSOLE lets you make category exceptions for certain users and groups in your organization so they can visit required websites.

NOTE: YOU CANNOT CREATE USER/GROUP EXCEPTIONS WHEN USERS ARE NOT IMPORTED. ENABLE SSO AND IMPORT USERS UNDER SETTINGS TO ALLOW THIS.



Bypass Settings

Websites or apps that may break when proxied can be set to always work for your users.

DOMAIN BYPASS

There are some websites that may break when proxied that you still want people within your organization to be able to use. The URL Bypass List includes domains that typically break when proxied. Add to the bypass list by assigning your own URLs to ensure these websites will still work for your users.

APPLICATION BYPASS

The Application Bypass List is a list of apps that the **DOPE.SWG** will not apply policy to. The default list includes applications that typically break when proxied. Add to the bypass list by assigning your own application names that you'd like to allow.

Instantly get notified of SSL errors that require bypassing to function. Quickly bypass via the Notification Panel (SEE SSL INSPECTION P.13)

The screenshot displays the DOPE.SWG interface with two main sections: URL Bypass and Application Bypass. The URL Bypass section has a 'Custom' tab selected, showing a list of domain names. The Application Bypass section also has a 'Custom' tab selected, showing a list of process executable names. A notification bell icon is visible in the top right corner. A text box on the right side of the interface explains that configuring these settings will allow destinations to continue to be accessed that would otherwise break when proxied.

URL Bypass Custom Policies Endpoints Settings

Custom Default

DOMAIN NAME

Click to assign a new URL. Or, review the d

- *accounts.google.com
- *acrobat.com
- *adobe.com

URL Bypass

DOMAIN NAME
*accounts.google.com
*acrobat.com
*adobe.com
*akadns.net
*amazonaws.com
*announcerevremote.com
*anydesk.com
*apis.google.com
*apple-cloudkit.com

Application Bypass

Custom Default

PROCESS EXECUTABLE NAME

Click to assign a new application. Or, review the d

- ATASAgent.exe
- AzVpnApp.exe
- ASupSvc.exe

Application Bypass

PROCESS EXECUTABLE NAME
ATASAgent.exe
AzVpnApp.exe
ASupSvc.exe

Configuring these settings will allow destinations to continue to be accessed that would otherwise break when proxied.

[+ URL Bypass](#) [+ App Bypass](#)

A set default list of commonly broken URL and apps have been predefined. Any new URL or apps added will show up in your Custom list.

Cloud App Control

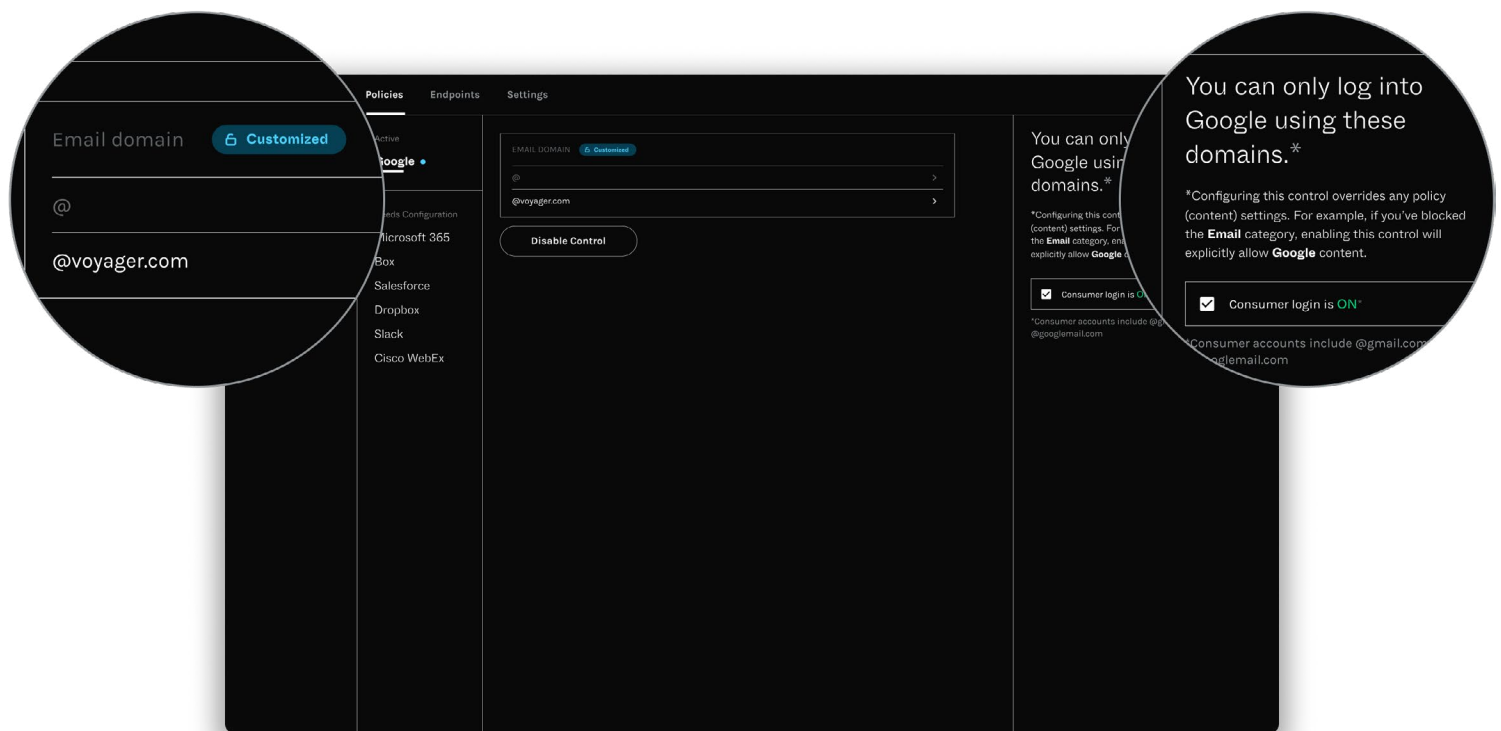
With CAC, any of your users will be blocked from accessing cloud app accounts you have not allowed. This provides an easy way to protect against data exfiltration to personal cloud application accounts, safeguarding your organization's security.

POLICY OVERRIDE

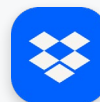
Simply enter the domains that you want your users to be allowed to access. **DOPE.SWG** will prevent logins to all domains except those entered here.

CONSUMER LOGIN

It's still possible to allow end users to access their consumer domains as gmail.com, googlemail.com, or outlook.com if so desired.



YOU CAN CONTROL ACCESS TO THESE INDUSTRY CLOUD APPLICATIONS



Custom Policy Creation

Create multiple policies to deal with your organization's needs—e.g. different geographical locations may require specific customizations. Or you can create special requirements for specific user groups.

POLICY ASSIGNMENT

Create custom policies for your needs, which can be assigned by user name or by group.

POLICY INHERITANCE

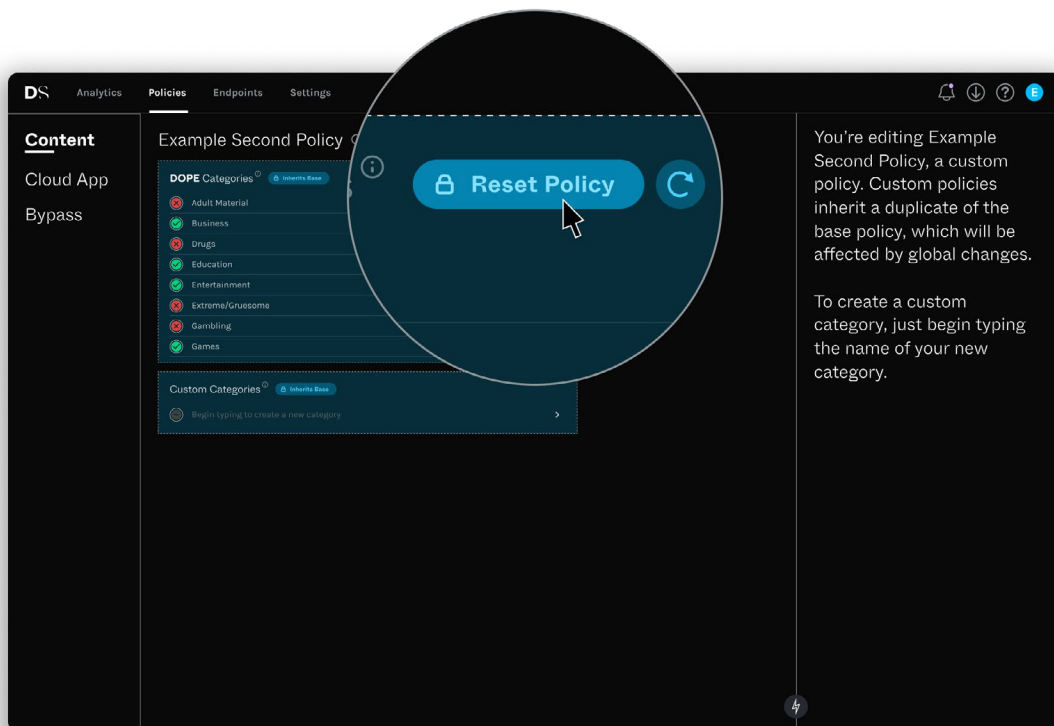
Upon creation, each new policy inherits and therefore is linked to the Base Policy. This makes maintenance of custom categories and Base Policy rules much easier. Change once, and it applies everywhere. The admin can always “unlink” or “customize” this inheritance and the additional policy becomes a new copy.

WHAT THE LEGACY SWG CANNOT OFFER

From personal experience, we know how complex creating policies can be with legacy SWGs. The dashboards are dull and convoluted, and every key element required to create a policy is scattered across a dozen tabs. It's very easy to lose track of what you've created as you're building your policy.

You'll notice our console is significantly faster than any legacy SWG, and the complex procedural policy is replaced with a simpler list. Categories are inherited from the base policy so there's no need to start from scratch.

- Create policies and assign to users and groups faster
- Customize content, CAC, and bypasses
- Understand how policies perform with actionable analytics



06

ANALYTICS, YOUR CAPTAIN'S DASHBOARD

Every data point you need under one roof. From policy violations to productivity stats to login detection, we've got you covered.

Analytics Overview

The Analytics Overview provides global visibility and a live view of all endpoint activity connected to your organization. It features immersive charts to help fine-tune your policy configurations. Other views include **POLICY**, **PRODUCTIVITY**, **SHADOW IT**, and **DETAIL**. Each view presents data with the ability to search across users, groups, and locations. Complete analytics require user configuration via Google or Microsoft 365 (set by your SSO settings).

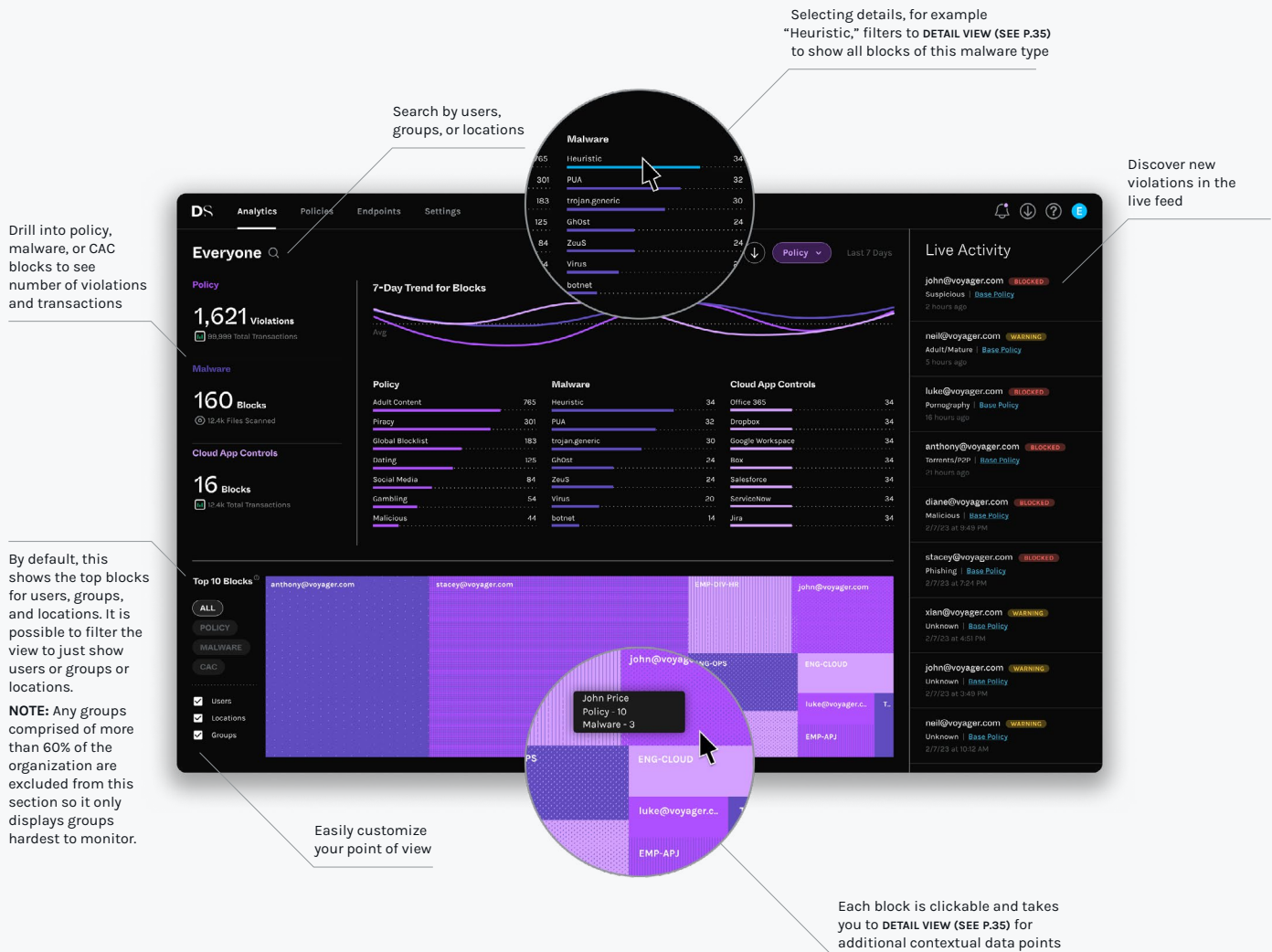


SIMPLE, INTELLIGENT, ACTIONABLE

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.

Analytics Policy View

Discover how your policies are performing with live data. Visualizations highlight policy violations, malware blocks, and CAC over a 7-day period across your organization.



DETAILED REPORTING

→ Complete analytics are available when users are imported (via Google or Microsoft 365)

→ Toggle different parameters and export into a CSV

Analytics Productivity View

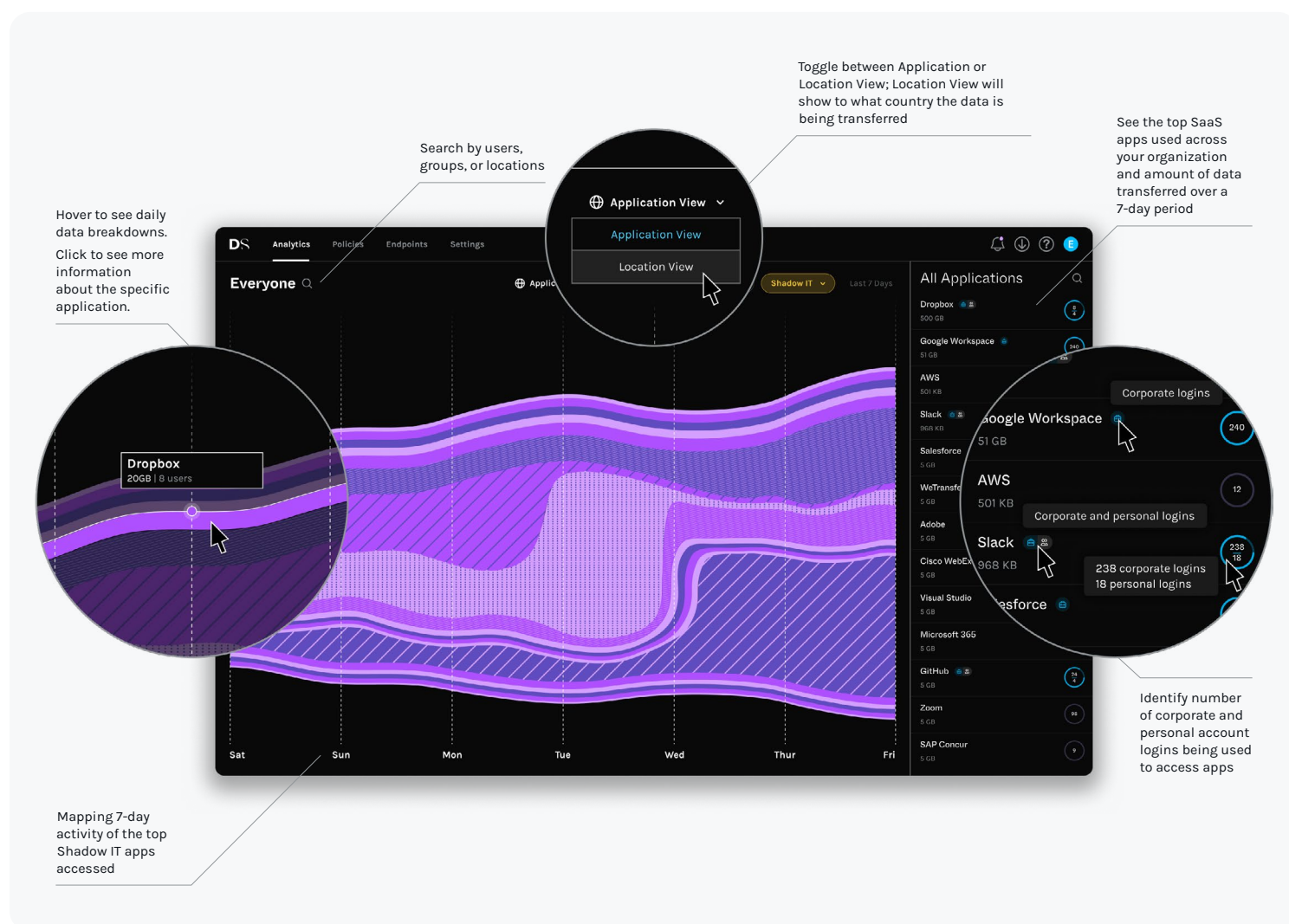
Uncover user behavior and workforce productivity through contextual and actionable features across top categories for the last 7 days, as well as user screen time and live activity.



Analytics Shadow IT View

Shadow IT can be insecure. When employees use unapproved IT resources, they're not subject to the same security controls—like Single Sign-On, or deprovisioning after employees leave. This can lead to data sprawl or other security issues.

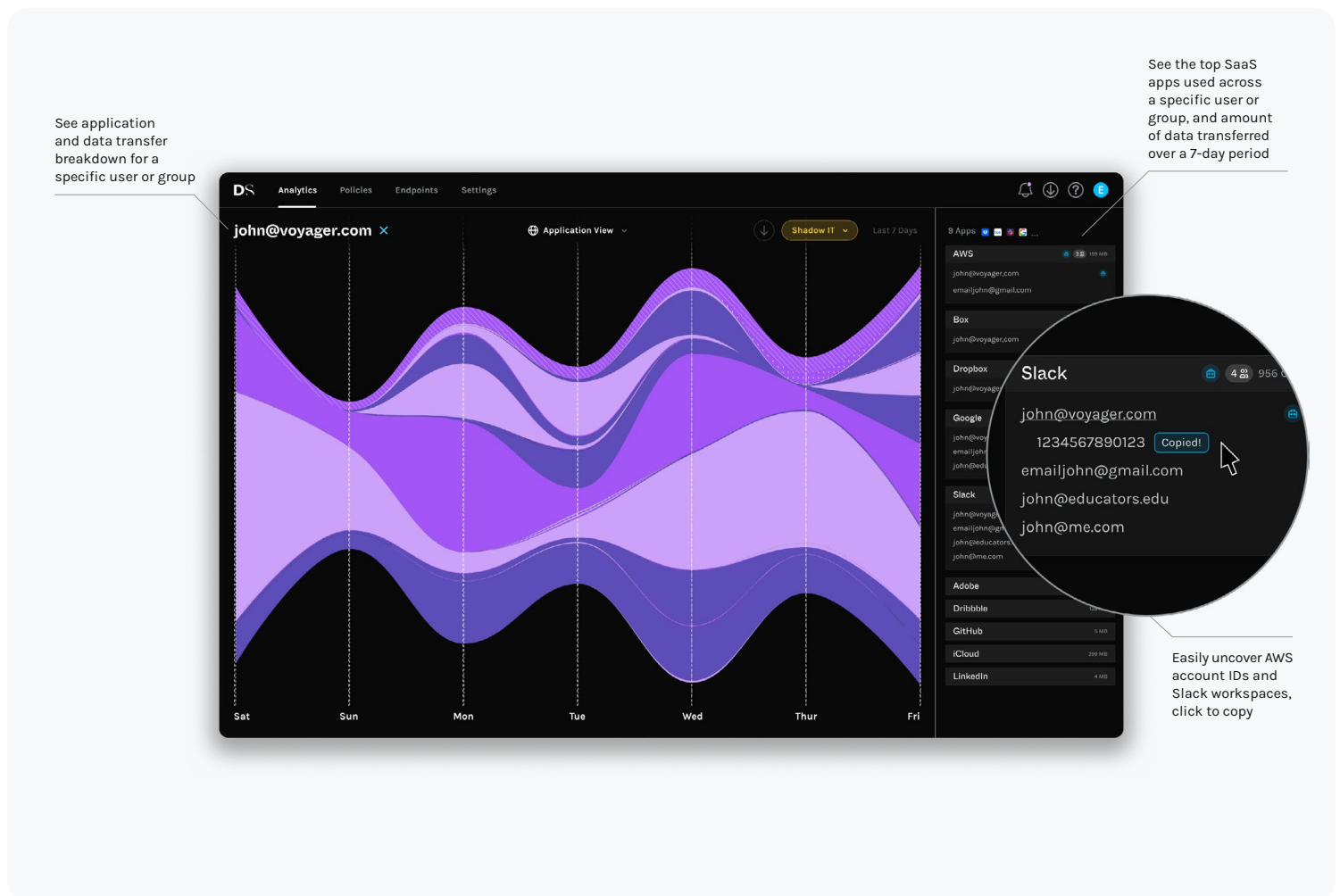
Extend your visibility to Shadow IT and uncover how users share data across your organization. Features provide application and location visibility on a per-app consumption basis, with a focus on the most data transferred.



Analytics Shadow IT View

EMAIL ACCOUNT DETECTION

See which employees are using SaaS apps by detecting specific personal and corporate account logins, and how much data they're transferring. Use this visibility to take action—inform your policy updates, and assess areas of data exfiltration and non-compliance.



Analytics Detail View

Access a complete list of all web transactions related to each policy violation or malware category, including the associated user.

Analytics

Policies

Endpoints

Settings

Everyone

Detail

Last 7 Days

DOMAIN	URL PATH	LOCATION	DESTINATION IP	CATEGORY	USER	TYPE	VERDICT	FALLBACK
piratebay.org	url/path	Cork, IE	10.0.152.180	Gambling	john@voyager.com	Policy	Blocked	
rapidshare.com	url/path	Mountain View, US	10.0.152.180	Pornography	stacey@voyager.com	Policy	Blocked	
linkedin.com	url/path	New York, US	10.0.152.180	Finance	diane@voyager.com	Policy	Blocked	
malware.com	url/path	Mumbai, IN	10.0.152.180	Productivity Applicati...	anthony@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Education	adrian@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Brokerage/Trading	luke@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Brokerage/Trading	john@voyager.com	Policy	Blocked	
github.com	url/path	Cork, Ireland	10.0.152.180	File Sharing	stacey@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Business/Economy	diane@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Productivity Applicati...	anthony@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Torrents/PPP	adrian@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Suspicious	luke@voyager.com	Policy	Blocked	
malware.com	url/path	Cork, Ireland	10.0.152.180	Suspicious	john@voyager.com	Policy	Blocked	
github.com	url/path	Cork, Ireland	10.0.152.180	Torrents/PPP	stacey@voyager.com	Policy	Blocked	

14 Results

TYPE

Filter By

☒ Policy

☐ Malware

☐ Cloud App Control

Download

Export your filtered view to a CSV.

SEARCH

Display all associated web violations for a specific user.

USER

john@voyager.com

Policy

john@voyager.com

Malware

john@voyager.com

CAC

john@voyager.com

Policy

john@voyager.com

Policy

Detail

Last 7 Days

LOCATION	DESTINATION IP	CATEGORY	USER	TYPE	VERDICT	FALLBACK MODE	TIME
Cork, IE	10.0.152.180	Gambling	john@voyager.com	Policy	Blocked	No	9-23-21 at 4:48 pm
Mountain View, US	10.0.152.180	Pornography	stacey@voyager.com	Policy	Blocked	No	9-23-21 at 4:48 pm
New York, US	10.0.152.180	Finance	diane@voyager.com	Policy	Blocked	No	9-23-21 at 4:48 pm
Mumbai, IN	10.0.152.180	Productivity Applicati...	anthony@voyager.com	Policy	Blocked	No	9-23-21 at 4:48 pm
Cork, Ireland	10.0.152.180	Education	adrian@voyager.com	Policy	Blocked	No	07 Feb 2023 at 10:24 AM
Cork, Ireland	10.0.152.180	Brokerage/Trading	luke@voyager.com	Policy	Blocked	No	07 Feb 2023 at 07:23 AM
Cork, Ireland	10.0.152.180	Brokerage/Trading	john@voyager.com	Policy	Blocked	No	07 Feb 2023 at 07:23 AM
Cork, Ireland	10.0.152.180	File Sharing	stacey@voyager.com	Policy	Blocked	No	06 Feb 2023 at 10:24 PM
Cork, Ireland	10.0.152.180	Business/Economy	diane@voyager.com	Policy	Blocked	No	06 Feb 2023 at 09:03 AM
Cork, Ireland	10.0.152.180	Productivity Applicati...	anthony@voyager.com	Policy	Blocked	No	05 Feb 2023 at 08:45 PM
Cork, Ireland	10.0.152.180	Torrents/PPP	adrian@voyager.com	Policy	Blocked	No	05 Feb 2023 at 07:23 PM
Cork, Ireland	10.0.152.180	Suspicious	luke@voyager.com	Policy	Blocked	No	05 Feb 2023 at 07:02 AM
Cork, Ireland	10.0.152.180	Suspicious	john@voyager.com	Policy	Blocked	No	05 Feb 2023 at 10:24 AM
Cork, Ireland	10.0.152.180	Torrents/PPP	stacey@voyager.com	Policy	Blocked	No	05 Feb 2023 at 09:01 AM

07

THE DS
APPENDIX

No vague buzzwords to keep you guessing. Here’s how we use language at dope.security.

The DS Appendix

C

CLOUD APP CONTROL (CAC)

CACs add a layer of security by restricting specific cloud-application domains or tenants a user can access.

D

DEBUGGING AN ENDPOINT

An endpoint-driven process for discovering and resolving bugs for an endpoint experiencing an error. It is in charge of running a series of network tests, identifying issues, and generating logs available for download.

DOPE.CLOUD

A set of security services and APIs that maintain a connection between the DOPE.ENDPOINT and DOPE.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 DOPE.ENDPOINT and the DOPE.CLOUD to keep organization-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.

E

ENDPOINT HEALTH STATUS

Healthy

A consistent heartbeat and successfully securing traffic within the DOPE.CLOUD.

Dormant

The state that is triggered when a DOPE.ENDPOINT has not connected to the internet for more than 7 days.

Fallback

If a DOPE.ENDPOINT cannot reach the DOPE.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. configuration error, service interruption, SSL Certificate not installed.

Disabled

The DOPE.ENDPOINT is disabled. DOPE.SWG will have no effect on the endpoint.

Debug Mode

Diagnostics and troubleshooting within the DOPE.CONSOLE to restore an endpoint experiencing an error.

F

FAIL CLOSE IS OFF

Allows previously accessed websites to continue as per the policy applied to that device or user. New web requests are allowed to pass without security checks.

FAIL CLOSE IS ON

Allows previously accessed websites to continue as per the policy applied to that device or user. New web requests are disabled for user safety.

FLY-DIRECT ARCHITECTURE

DOPE.SWG's cloud-based approach sitting between a user and internet access, removing the need for physical stopover data centers.

L

LEGACY

Legacy [OR LEGACY VENDOR] refers to an organization's IT infrastructure, systems, hardware, or applications that are impossible to update or improve. Also refers to an organization's approach to building a complex technology or process.

LIFT-AND-SHIFT MODEL

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

O

OpenID CONNECT (OIDC)

Allows clients to verify the identity of the end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user.

[OPENID.NET](https://openid.net)

S

SECURE WEB GATEWAY (SWG)

A SWG [PRONOUNCED "SWIG"] is designed to prevent access to harmful websites and programs by filtering and blocking them in a company-defined policy.

SHADOW IT

Shadow IT refers to IT software, applications, or services outside the approved or control of IT organizations.

STOPOVER DATA CENTER

Refers to the process of information stopping over at a data center to perform cybersecurity checks. Often conducted by many legacy SWG vendors.



It's not that we're mad at yesterday's
cybersecurity. Just disappointed.

So we made it better. We made it easier.

We made it dope.

sales@dope.security