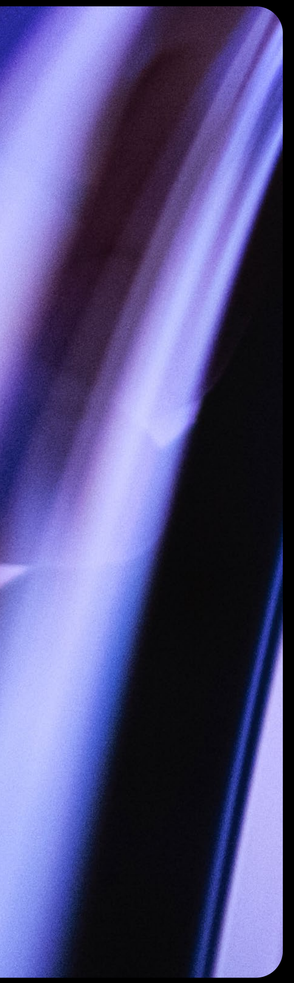
proofpoint®

Proofpoint Information Protection

Solutions Architecture

Protect people. Defend data.



Proofpoint Information Protection solution components

Proofpoint Information Protection is built on Proofpoint Nexus, which is a suite of AI-driven technologies. These technologies are designed to identify sensitive data, prevent data loss and contain insider threats across multiple channels. Nexus uses advanced language models and behavioral analysis to detect when users may be sharing sensitive data, either intentionally or inadvertently. It can also identify anomalous behaviors, such as when unauthorized users access or move data.

The solution also offers granular control through automated policies that can block or remediate risky activities in real time. By correlating data access and movement with user behaviors, Nexus helps protect sensitive data—such as personally identifiable information (PII), payment card industry (PCI) data and other classified content—across email, endpoints and cloud applications.

Moreover, Nexus enhances the capabilities of Proofpoint Data Loss Prevention (DLP) by unifying management and analytics using advanced AI. This enables security teams to monitor data access and movement, ensuring compliance with privacy regulations like GDPR and HIPAA. It also allows organizations to tailor policies to fit their specific needs. This ensures targeted protection without disrupting legitimate business operations.

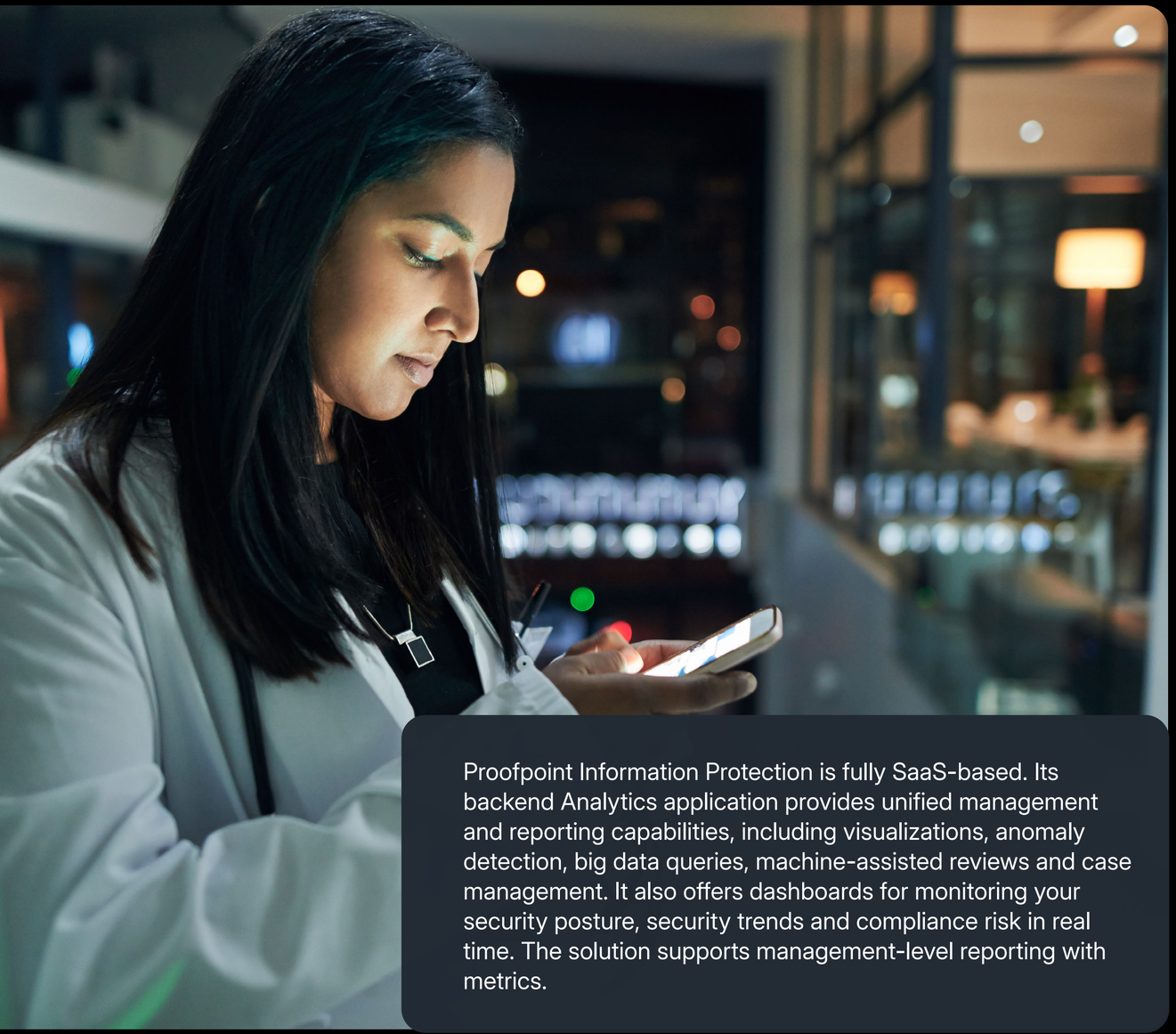
Proofpoint Information Protection is comprised of multiple products. Most of the following products integrate with this solution.

Proofpoint Insider Threat Management (ITM) and Proofpoint Endpoint DLP protect against data loss and brand damage from insiders who act maliciously, carelessly or unknowingly. Proofpoint correlates user activity and data movement. This allows you to identify user risk, detect insider-led data breaches and accelerate incident response. It also helps you to prevent data exfiltration through USB, cloud sync folders, print and more. It offers a single, lightweight endpoint agent, so you have the flexibility to monitor everyday and risky users as well as high-risk users.

Proofpoint Cloud DLP delivers human-centric data security (including inline DLP) and cloud app governance. It safeguards sensitive data and governs OAuth apps. And it helps you stay compliant with privacy and data security laws. This multimode CASB supports both API- and proxy-based deployment models, including DLP for BYOD (bring your own device).

Proofpoint Email DLP helps prevent the loss of sensitive data through email. It also helps you comply with regulatory requirements—such PCI, PII, GDPR, SOX and HIPAA—with out-of-the-box policies that align with these standards. You can also create custom dictionaries, including AI-powered classification, to identify and protect data that is unique to your organization. Proofpoint Email DLP is easy to deploy. You can set it up as part of an existing email security system. Alternatively, you can integrate it into an enterprise-wide DLP program.

Proofpoint Adaptive Email DLP uses behavioral AI to learn about your employees' normal email sending behaviors, their trusted relationships and how they communicate sensitive data. It then analyzes each email to detect anomalous behavior, notifying administrators of potential data loss incidents. It warns users in real time and prevents sensitive data loss through email. Currently, Adaptive Email DLP does not integrate with our Information Protection platform and will not be discussed further in this paper.



Proofpoint Information Protection is fully SaaS-based. Its backend Analytics application provides unified management and reporting capabilities, including visualizations, anomaly detection, big data queries, machine-assisted reviews and case management. It also offers dashboards for monitoring your security posture, security trends and compliance risk in real time. The solution supports management-level reporting with metrics.

Enterprise DLP logical architecture

The Proofpoint Enterprise DLP solution provides security administrators with tools to protect sensitive data and efficiently investigate incidents across environments. This significantly reduces an organization's risk of a data breach.

From an incident management perspective, the primary goal of the DLP solution is to provide a single pane of glass to reduce the time spent on forensic log analysis, speed up investigations and incident remediation, and generally make teams more effective with less effort.

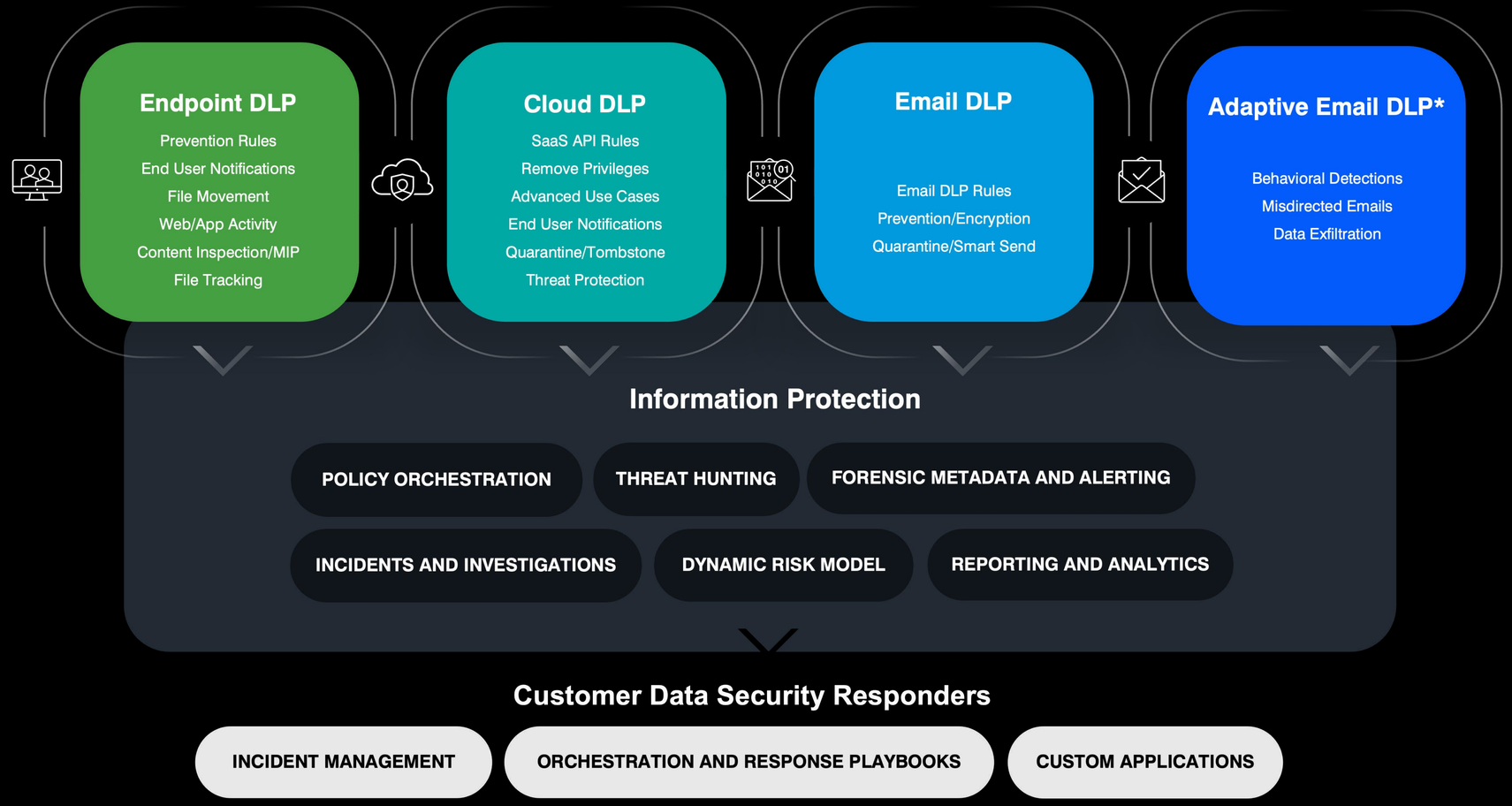
Several distinct detection components work together in an integrated solution. A solution architecture describes the configuration as well as the rules and policies for product implementation. It also clearly lays out the organizational risks and business drivers for the DLP program.

Organization-specific rules can therefore be developed to provide visibility and control to designated activities involving corporate information. DLP rules can be created for alerting a security incident analyst or orchestrating in-channel automatic remediation. Granular rules allow for flexible response capabilities so that you do not block legitimate business activities.

Additionally, important incidents and high-risk activities can easily be identified, gathered, exported and shared with responsible teams. This reduces the burden and cost of incident management and enables teams to better protect the organization and its users from the adverse impacts of data loss.

Enterprise DLP Reference Architecture

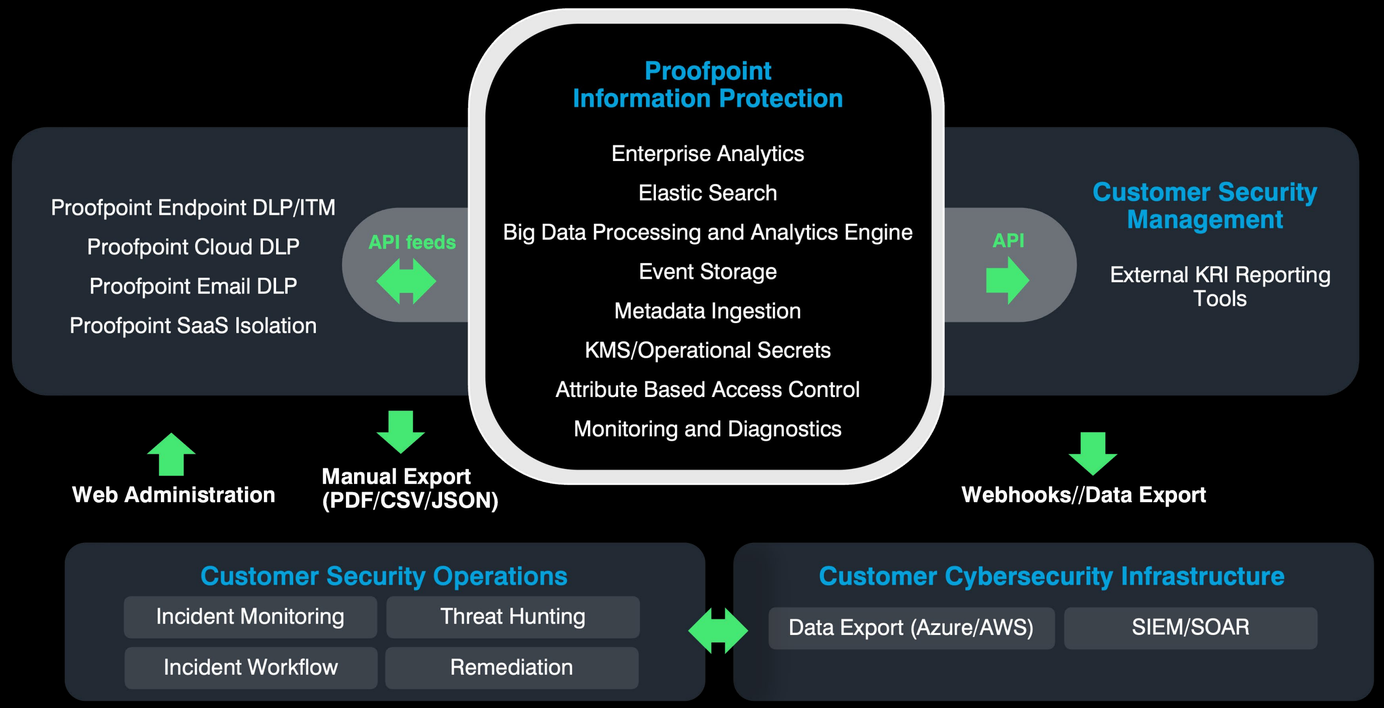
This is the flow of activity and communication between the DLP solution components:



*Future Integration

Unified Analytics for Information Protection

Unified analytics architecture for Information Protection across endpoints, cloud and email.



Unified analytics for alert management, investigations and response

The Unified Alert Manager provides data analytics and reporting for all the events that are collected by the solution. It also enables you to manage alert workflows. Many advanced use cases are delivered through this data analytics capability, such as threat hunting explorations, anomaly detection and machine assisted alerts triage.

You can develop specific detection rules in the Analytics application. These rules, in turn, generate alerts that a security incident analyst can triage. When there is a violation, an email or outbound webhook event is sent to a third-party receiver application, such as a SIEM/SOAR or instant messaging system, which contains the alert details.

Splunk and other SIEM vendors can be integrated with Proofpoint Information Protection to provide a unified look at insider threats, lateral movement and data exfiltration. This helps you to quickly pinpoint which users were involved and to correlate details against other event sources.

Via integrations, our platform can also notify ServiceNow of any data exfiltration or compliance violations. ServiceNow can then alert its customers and create new tickets or workflows based on the alerts. An integration with ServiceNow DLP speeds up investigations and response.

Document #: 1207-005-01-01

Platform access and privacy controls

Proofpoint employees never have access to your data—unless your team shares it with them. If you grant access, Proofpoint employees or your team members may use Proofpoint User Center to log into the system. Alternatively, they may be assigned access using a persona, which is essentially a user that is assumed temporarily.

Alerts should be set up around the use of a highly privileged admin account. To keep it secure, the password for this account must be changed. The password could also be held in escrow or split among responsible parties.

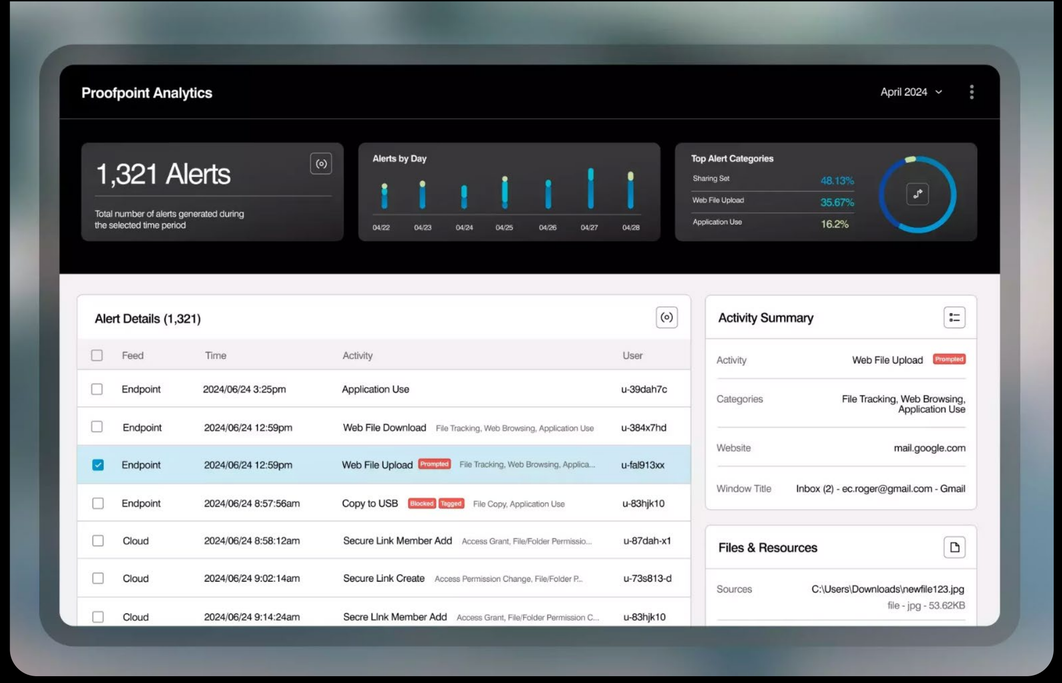
It is highly recommended that you use SAML or OAuth2.0 to integrate cloud-based authentication methods, like single sign-on (SSO) and multifactor authentication (MFA). You also have the option of connecting multiple identity providers.

You will need to go to Administration/Account Settings in the Information Protection platform to configure any identity provider according to its required settings. You will also need to configure your identity provider to connect with the Information Protection platform.

The admin account has full, deanonymized access to all settings and data in the platform. Therefore, credentials must be protected and treated as highly confidential. Additional local administrative accounts can be created during product testing under Administration/User Management. Each account can be assigned its own access policies as needed. However, in most cases, adding more admin users will require limiting their control and administrative access.

Proofpoint Information Protection is built with privacy-by-design principles. Only those with a need-to-know can access sensitive data and user-identifying information. Proofpoint uses regional data centers in the United States, Europe, Australia, Canada (end of 2024) and Japan (endpoint data only). This lets you separate data geographically. So, a U.S. realm can manage U.S. data, which is sent to the U.S. data center. Granular access policies allow your administrator to assign access so that a U.S.-based security analyst can only see U.S. data.

With Information Protection, system administrators can also configure the forensics data (PII, PHI, PCI) that they want to mask in the console and hide a user's identity to eliminate analyst bias. You can anonymize the username, host name, IP address, location information and file names. When a user's identity must be known further downstream in an investigation, the security analyst can request de-anonymization, which an administrator can grant.



Web console access

Administrators and analysts can connect to the platform using a supported browser. They can manage policies and rules, review alerts, directly remediate incidents, analyze collected data sets and review reports based on the captured user activity.

For managing separate sub-entities, many organizations can access multiple sub-tenants on the Proofpoint platform.

Platform Notifications

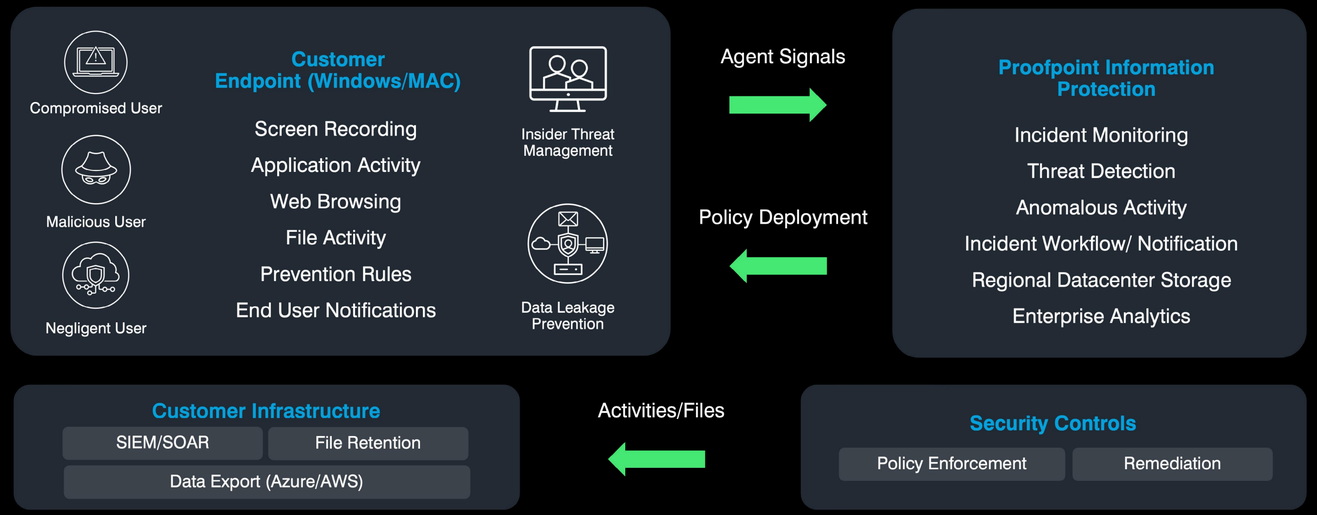
Alerts can be monitored and processed in the Proofpoint platform. Or this can be done externally in accordance with your internal incident management procedures. You will need to identify any email addresses that will receive alerts generated by the Proofpoint Information Protection platform. External systems (SIEM, SOAR, ITSM) can also be configured to receive alerts.

External Applications

External applications can access the Proofpoint platform via REST APIs.

Endpoint DLP/ITM Reference Architecture

Single agent for DLP and ITM collects and uploads data to the platform while also enforcing DLP policies.



DLP/ITM Endpoint Agent Configuration

The Endpoint DLP Agent will be installed on customer endpoints that run on supported versions of Windows or macOS. To install the agent in production, you should use unattended methods and your company-standard remote software installation tooling.

As soon as it is deployed, the agent records metadata that describes user activity. It does not need explicit rules. The metadata is securely uploaded and processed by the Information Protection platform. To administer and configure the agent, use the platform's Administration/Endpoints application.

Proofpoint endpoint agents can be silently deployed. Each one runs in user memory with minimal resource consumption and can automatically update itself. After installation or upgrade, there is no need for a system reboot. Agents will not conflict with existing endpoint security or cause other applications to break or perform poorly.

Installed agents and the ITM server communicate asynchronously via the HTTP protocol. DLP agents use TLS encryption to communicate with Proofpoint cloud services. The firewall requirements for connectivity are listed in our online documentation portal.

Agents that need to connect through a dynamic proxy will use proxy settings defined at the operating system level. The operating system must be configured to use a dynamic proxy for applications running under the system account (not the user account). Use of a static proxy is also supported. This setting is configured when agents are installed.

Some antivirus and EDR software will run on-demand, scanning executable files and hold processes or blocking them from communication by default. To ensure stable functionality, you must exclude our processes from inspection by other security tools. Proofpoint does not anticipate the need to whitelist specific applications in our own tool because our lightweight approach is unlikely to interfere with the actions of a kernel endpoint agent.

Windows endpoint agent components for safelisting
To safelist our files from being affected by EDR or antivirus systems, please refer to **this guide**.

NOTE: To display notifications or collect screenshots on macOS, you must also ensure the privacy settings are granted to our processes by deploying the mobile config file. This process is detailed in our online documentation here.

The Proofpoint endpoint agent supports two types of proxies. For a dynamic proxy, use a PAC autoconfiguration file at the operating system level. For a static proxy, supply the hostname and port at installation time. To set default credentials for the agent to use, complete the Domain, Username and/or Password fields during installation.

Agent updates
As a SaaS platform, Proofpoint can deploy new features quickly into the agent. Proofpoint also provides a long-term supported (LTS) version of the agent for customers who are unable to support our release schedule. However, we generally recommend keeping the agent on our latest supported release.

We recommend using the auto-update service to keep the agents up to date, according to a preconfigured update policy. When an administrator decides to update the agent, they simply update or create a policy defining the target release and the conditions to apply the upgrade. The agent updater processes on the endpoints and then ensures that the correct versions are downloaded and installed automatically.

Root certificate
Installed endpoints must have a valid root certificate.
Proofpoint signs the agent with a valid root certificate to ensure that the customer knows it is from Proofpoint. This certificate is dependent on a valid root certificate and has an annual expiration date.

Agent health monitoring
Agent health information, such as errors and last check-in times, are visible in the platform's Endpoint Catalogue. The Windows agent is largely self-healing and includes a watchdog service (IT cloud service) which will restart the agent if it is killed or terminates. The Mac agent logger process is similarly watched by launchd, which restarts the agent if it is killed or terminates.

Agent Hardening
The agent configuration and log files on the endpoints can be fully encrypted.
During installation, additional hardening—such as applying a security key to prevent the agent from being uninstalled or its processes from being renamed—may also be applied.

Endpoint realm configuration
Agent Realms segregate agents based on regional storage location and data retention periods.

Endpoint prevention rules are deployed through tiered Agent Policies. They enforce actions such as warning or blocking the user. Concurrently, the agent logs metadata signals about user application activity. These logs are sent to the Analytics platform for processing. Screenshots are optional.

The processed data is stored in the regional AWS data center of choice (currently US, EU, AP, JP, CAN) according to the selected Agent Realm setting.

Agent Policy settings
Agent Policies define what the Proofpoint agent captures. They are assigned to Agent Realms. This means that you can configure settings and apply them to endpoints in multiple realms simultaneously.

You can assign more than one Agent Policy to an Agent Realm. When more than one is assigned, you can prioritize their order. This enables you to further define which settings are applied to which agents. This order determines which settings will be enabled and turned on per Agent Policy.

Endpoint prevention and end user notification

A fundamental part of a successful DLP or insider risk program is shaping end user behavior to decrease the risk of a data breach. When DLP rules are deployed on managed endpoints, they can be used to block or warn end users of policy violations. This influences their behavior and thereby reduces the risk of a data breach.

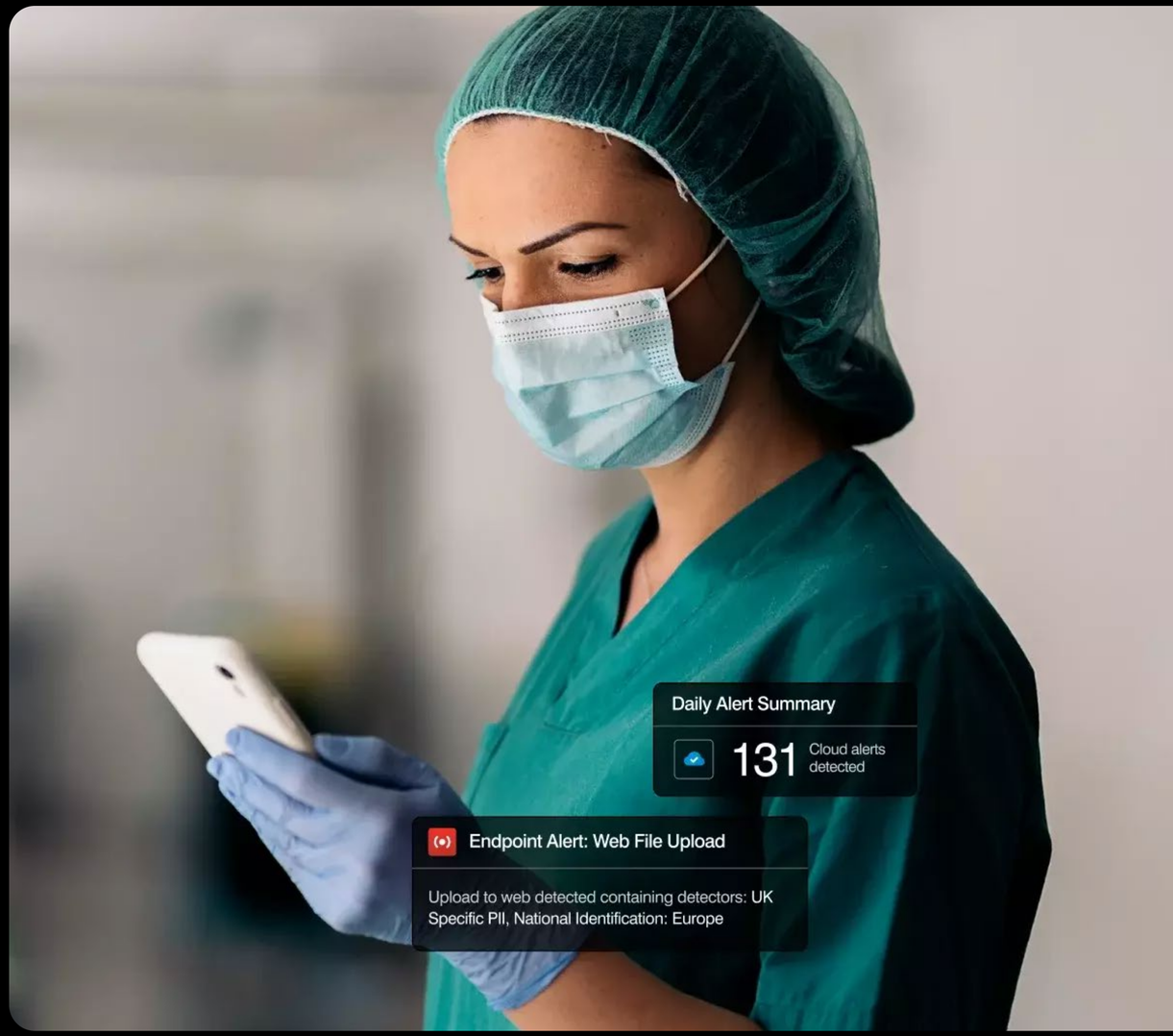
DLP rules are designed to change end user behavior when sensitive company information is being exfiltrated. Initially, a common approach is to monitor what users are doing through the activity metadata that is visible in alerts or activity explorations. As teams review alerts, they can use them to tune rules so that they align with organizational priorities and incident detection processes.

After this process is mature, rules can be deployed. At this point, when end users are not aligned with policies they will be blocked from an action and notified with a blocking message. To continue their activity, they will be asked to select from prebuilt or customized justification texts.

End user notifications are typically customized with text that describes which policy the user has violated. They also include the company's official logo and a link to a webpage that details the organization's security policies. The imported image for the company logo must be under 56K in size (MIME type image/*).

Users learn what to do when an activity is blocked or how to file a complaint about the interruption. It is also a good idea to include a link to the corporate security intranet page that explains the need for the DLP program.

Detection rules generate alerts in our Analytics application where an incident responder can manage them. They run over the collected metadata, which is generated by selected user activities on endpoint devices. The metadata is recorded by the agent according to Agent Policy settings, such as frequency and resolution of screenshots. It is managed in the administration console.



Cloud DLP configuration

Proofpoint Cloud DLP supports an agentless architecture. It uses cloud APIs to protect key cloud applications. It also offers inline DLP for BYO devices using browser isolation after a user authenticates to access a cloud application.

Cloud DLP connects to an organization's primary cloud services and sanctioned SaaS/IaaS applications via their respective APIs. This provides bidirectional capabilities—including remediation of cloud security incidents—in near real time.

Proofpoint Cloud DLP is extremely powerful, providing remediation with the same DLP detector stack that is used by Endpoint DLP.

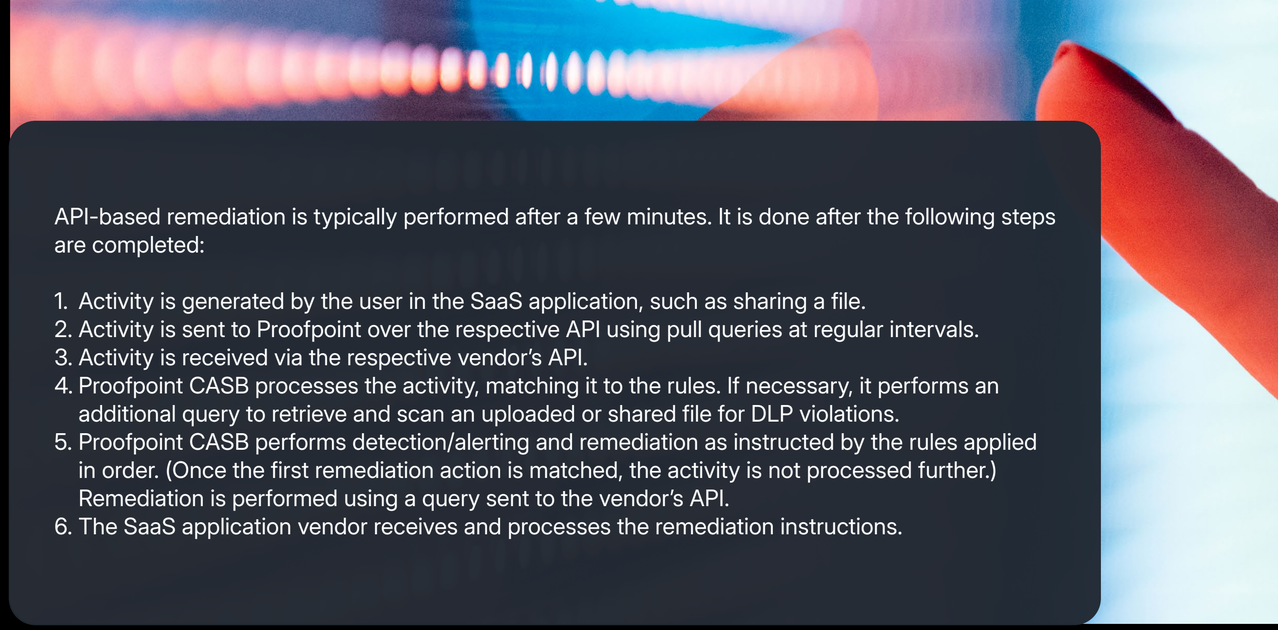
Proofpoint Adaptive Access Control extends the power of Cloud DLP to a wide variety of advanced real-time use cases. Examples include recognition and blocking of unmanaged devices as well as access from high-risk locations through our SAML/OIDC integration with cloud identity providers.

You can get even more granular DLP control over browser-based file uploads and downloads using an integration with Proofpoint SaaS Isolation. This can be achieved without an agent. Therefore, it is suitable for DLP on BYO devices. Note that Proofpoint Okta API connectors simplify SAML integrations. We can automatically apply adaptive controls for Okta-federated applications.

As an additional step, IaaS services such as Azure and AWS can be configured for DLP monitoring. Proofpoint charges for these APIs separately.

Initially, vendor APIs for your selected enterprise cloud applications will be connected to Cloud DLP for purposes of security monitoring.

You can develop specific rules in Cloud DLP to identify and remediate violations of corporate DLP policies in cloud services. You can also apply automated governance rules to third-party OAuth applications, which maintain system and data access to your primary SaaS and organizational services, such as Microsoft 365 and Google Workspace.



API-based remediation is typically performed after a few minutes. It is done after the following steps are completed:

1. Activity is generated by the user in the SaaS application, such as sharing a file.
2. Activity is sent to Proofpoint over the respective API using pull queries at regular intervals.
3. Activity is received via the respective vendor's API.
4. Proofpoint CASB processes the activity, matching it to the rules. If necessary, it performs an additional query to retrieve and scan an uploaded or shared file for DLP violations.
5. Proofpoint CASB performs detection/alerting and remediation as instructed by the rules applied in order. (Once the first remediation action is matched, the activity is not processed further.) Remediation is performed using a query sent to the vendor's API.
6. The SaaS application vendor receives and processes the remediation instructions.

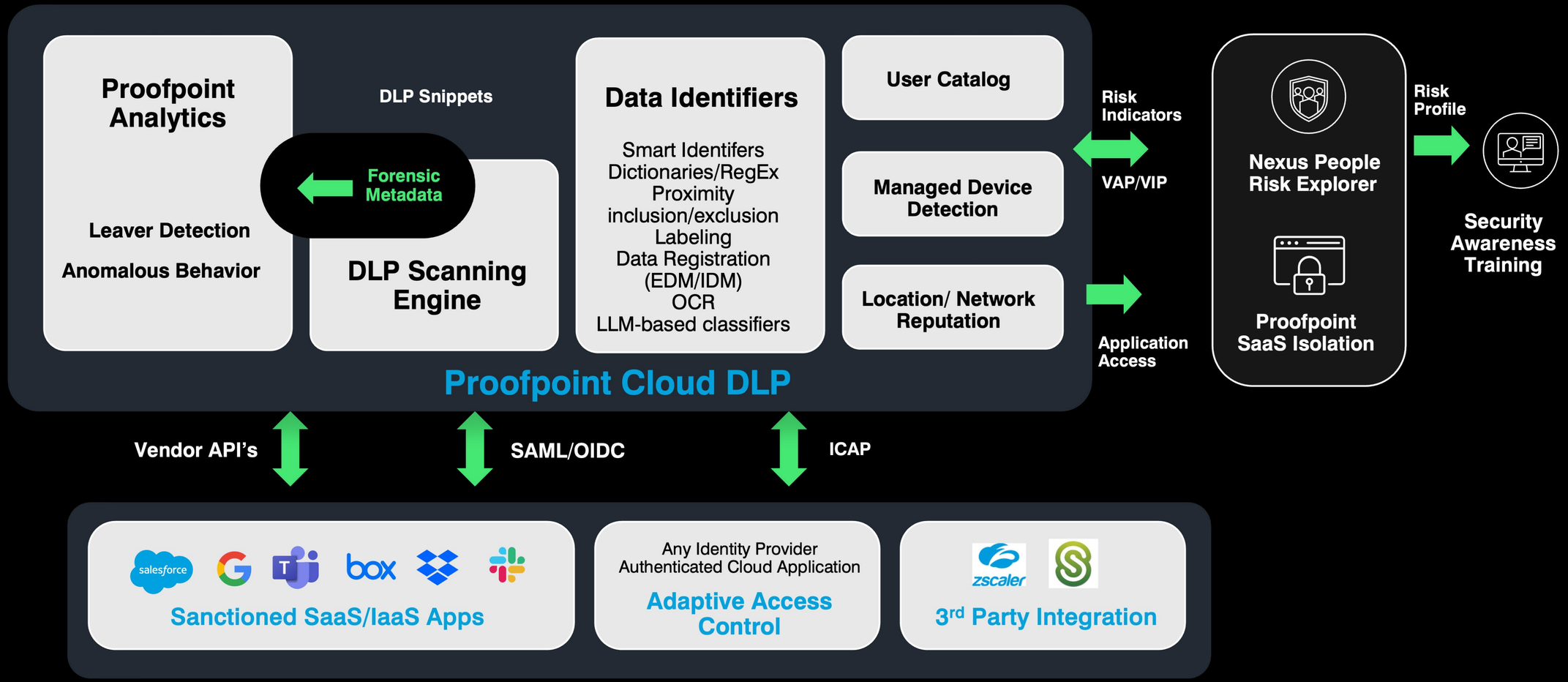
Proofpoint CSAB Adaptive Access Control allows supported applications to be controlled inline without an agent. Through SAML 2.0 or OIDC integration with your identity provider, we can apply additional protection using Proofpoint Cloud DLP to any authenticated application.

To set up Adaptive Access Control, user login requests must be rerouted through Proofpoint before they are authenticated by the identity provider. We can then apply a rule that allows access to sanctioned corporate cloud applications, but only under certain conditions.

Policies can be based on parameters such as whether a user is accessing the SaaS application from an unmanaged device, outside of an office source network egress range, from a risky location or other high-risk factors. You can get even more granular control over browser-based cloud application access using an additional integration with Proofpoint SaaS Isolation. This allows real-time integration with our DLP stack without the need for an agent.

To further unify DLP and provide cross-channel data loss visibility, Proofpoint also supports ICAP integration with Zscaler and Citrix ShareFile. To do this, configure the ICAP client of your third-party application by pointing its traffic to our DLP service after you configure your DLP detector set for this channel in our platform.

Cloud DLP Reference Architecture



Document #: 1207-005-01-01

Email DLP configuration

Email DLP uses an inline email gateway that is provided by Proofpoint to process outbound email. This gateway is integrated into your outbound email architecture.

Proofpoint will advise you on how to configure your infrastructure and systems based on your existing email architecture, whether you are testing outbound Email DLP or putting it into production.

If you already use Proofpoint for your outbound email gateway, Email DLP will simply be enabled directly on your existing Proofpoint email gateway by licensing the regulatory compliance module. No changes will be made to your email flow. There are no implications for SPF, DMARC or IP Warmup.

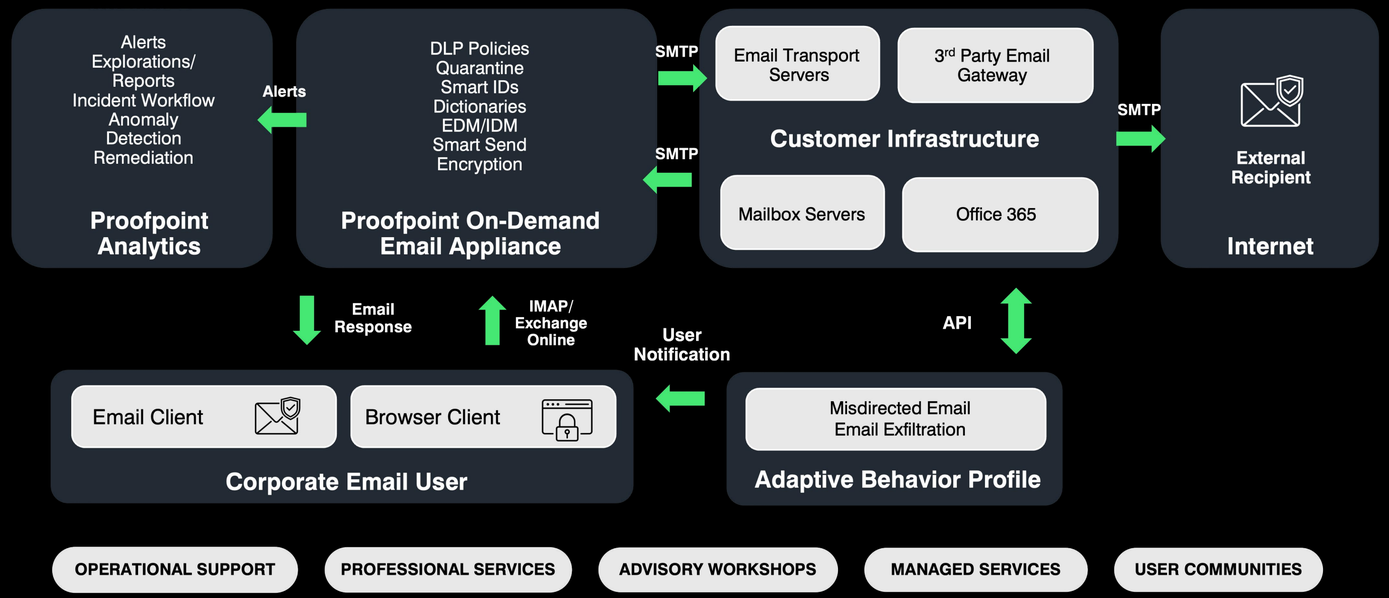
Once Email DLP is enabled, you can evaluate the full range of DLP capabilities, including reporting, enforcement, end-user notifications and interaction.

If you do not use Proofpoint as the last hop in your email processing flow, the Proofpoint cloud-based email gateway will be integrated in your outbound mail infrastructure as an extra SMTP hop. Ideally, this should be inserted before an existing email gateway to avoid additional changes in the infrastructure.

Once the outbound email service has been integrated, you can use the full range of DLP capabilities, including reporting, enforcement, end-user notifications and interaction.

Email DLP Reference Architecture

How email DLP components interrelate and communicate with a corporate email user.



Document #: 1207-005-01-01

Disaster recovery

Proofpoint fully manages and operates disaster recovery within our platform. If there is a business disruption in one of our services, Proofpoint will implement our disaster recovery plan. This includes providing regular situational update reports. These reports include a summary description of the event, the customer impact and an estimate of when normal operations will return. The documented Proofpoint business continuity program describes how business processes are restored. The plan is reviewed at least annually, and a tabletop test is performed annually. Details can be requested as part of a SOC 2 Type 1 request via Proofpoint.

Should Proofpoint cloud services become unreachable over the network, existing DLP prevention rule enforcement will not be impacted. All DLP prevention rules are applied directly to the agent through machine policies. There is no need for them to communicate with any server to be enforced.

If prevention rules are changed by the administrator during this period, machines will only receive changes once they have established connectivity to Proofpoint services. This regular heartbeat activity occurs every 10 minutes.

For detection, loss of connectivity results in the agent storing the selected events defined in the Agent Realm and Agent Policy settings, which are managed in the administration console. Once the device reestablishes communication with the application, the metadata for the selected events will be uploaded.

Data sensitivity

You can apply security controls in a consistent and holistic manner by developing DLP rules that are based on sensitive data identifiers.

Data sensitivity is defined by how much of a negative impact it will have on an organization should a group of data be disclosed. Impacts include loss of customer trust, loss of shareholder confidence, direct financial damage or fines by a regulator.

DLP detectors for Cloud and Endpoint DLP

Proofpoint DLP detectors identified here apply only to Cloud DLP and Endpoint DLP rules. If you want to use content scanning for Endpoint DLP, you need to follow these steps:

- The endpoint agent must have the content scanning component enabled during installation. Or it must be updated with this component.
- Endpoint content scanning must be enabled for the Agent Realm on these selected endpoint activities: Web File Upload, Web File Sync, copy to USB, Web File Download, Document Open, Print, Paste Text from Clipboard and Copy to Network Drive.
- If you want to use DLP detector sets for content scanning, then the detectors must be added to the Agent Realm configuration and deployed to the endpoint agents.

Once deployed, the detectors can then be used in detection or prevention rules. The prevention rule logic deployed to the agent includes endpoint enforcement (either justification or blocking) as well as the sensitive data detector.

For cloud applications connected to Proofpoint Cloud DLP, the policy engine will be able to use DLP detectors shortly after they are configured in the DLP application. Cloud DLP rules are configured to alert inside the platform. However, in write mode, they can perform remediation actions based on the type of connection for the SaaS applications (API or inline) using the rules in the Cloud DLP application. Cloud DLP rules can incorporate DLP violations into their logic. This rule property is synchronized automatically with the DLP application detectors. All cloud activity in the onboarded enterprise SaaS applications is fed into the Analytics application. Configured Cloud DLP alerts will appear in the console. Any remediation actions can be managed and viewed directly from the alerts.

Proofpoint DLP recognizes sensitive data-in-motion and data-in-use in these three ways:

1. **Files labeled with a visual sensitivity label (Microsoft Information Protection)**

   If you have a data classification program that uses Microsoft labels, we can identify Microsoft sensitivity (MIP) tenant IDs and labels. These can then be consumed in rules.

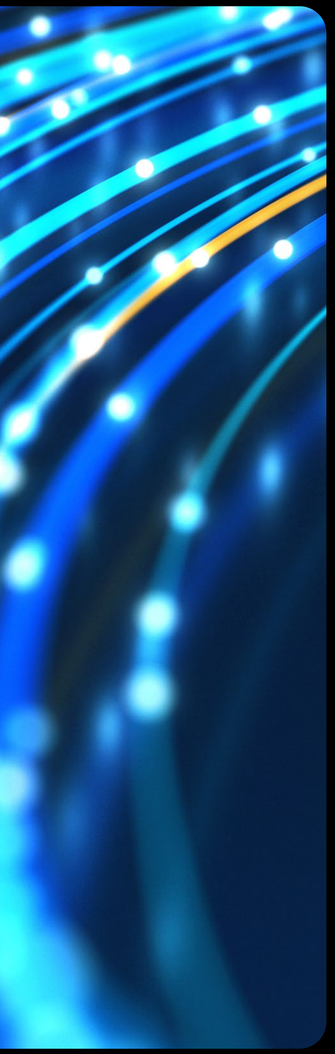
2. **Files containing content matches defined by Proofpoint DLP Detectors**

   Proofpoint DLP detectors identify sensitive content using prebuilt smart identifiers, out-of-the-box or custom dictionary keywords, classifiers, etc.

3. **Files with contextual markers such as metadata (filename, path, file extension, true file type, document properties) or files originating from tracked URLs.**

   In Endpoint DLP, a file that is downloaded to the endpoint using a supported browser is automatically tracked. All activity with the file on the device—such as copy, move, delete or rename—is tracked. Once the file leaves the machine through a specific egress channel, it is no longer tracked. All activity with tracked files is captured by the agent, and a history can be viewed on the File Timeline.

   Tracked files therefore always originate from URLs which a browser uses to locate the files, known as the tracking origin resource URL. This can be used by the endpoint agent for both detection and prevention rules to monitor and control behavior with files that originate from sensitive web services.



DLP detectors for Email DLP

DLP rules for Email DLP must be configured in the Proofpoint Email Security (PPS/PoD) solution. However, this process is outside the scope of this paper.

The Regulatory Compliance module in our Email Security solution is configured to perform the required scanning, log the required alert based on an Email DLP rule, and perform in-channel processing actions. The remediation might be to move the message to a local quarantine folder for processing, encrypt the message, respond to the end user by email and drop the message, or send the user a smart response that asks them to review their own message before approving it.

All activity that violates an Email DLP policy is then made visible in the alerts. This includes email details, which can be downloaded and reviewed directly by an administrator..

DLP identifiers, detectors and sets

Our detector expressions are written in a proprietary syntax. Expressions include any Boolean combinations for five condition types: smart IDs, dictionaries, proximity inclusion/exclusion, and EDM and IDM data sets. Their order of processing is indicated by parentheses (). Tracked URLs will be (lists of) specific URLs that are visible to the agent when a file is downloaded with a browser from the designated location.

Custom dictionaries are lists of customer-specific terms used by DLP detectors to locate potentially sensitive data in files. When a file is scanned, a detector compares all words and phrases in the file against all terms in the enabled dictionaries.

Custom smart IDs are more deeply integrated into the platform and are managed by Proofpoint engineering. In some cases, they may need to be created to perform checksums on values—for example, a customer-specific loyalty card number or an algorithm that uses regular expressions and code.

A large part of the initial deployment is spent on refining and tuning sensitive data markers. This helps to ensure a low rate of false positive alerts and high rate of accuracy. Content scanning detectors indicate the match conditions for sensitive data based on the included dictionaries and smart IDs.

Detector sets contain the DLP detectors used by the endpoint agent. They must be included in the Agent Realm configuration settings and deployed.

Other advanced capabilities for inspecting content include:

- Optical character recognition for processing images into extracted text for DLP analysis.
- Exact data matching for delivering highly accurate detection through multicolumnar matches of structured tabular data.
- Indexed data matching (document fingerprinting) for uploading unstructured files and performing similarity analysis on files that are transmitted via an egress channel.

Currently, advanced functions are not available on the endpoint agent due to resource constraints. However, these constraints are eliminated when the scanning process is done in the cloud. As such, these features are available for Cloud DLP and Email DLP only.

Offline archive/data export

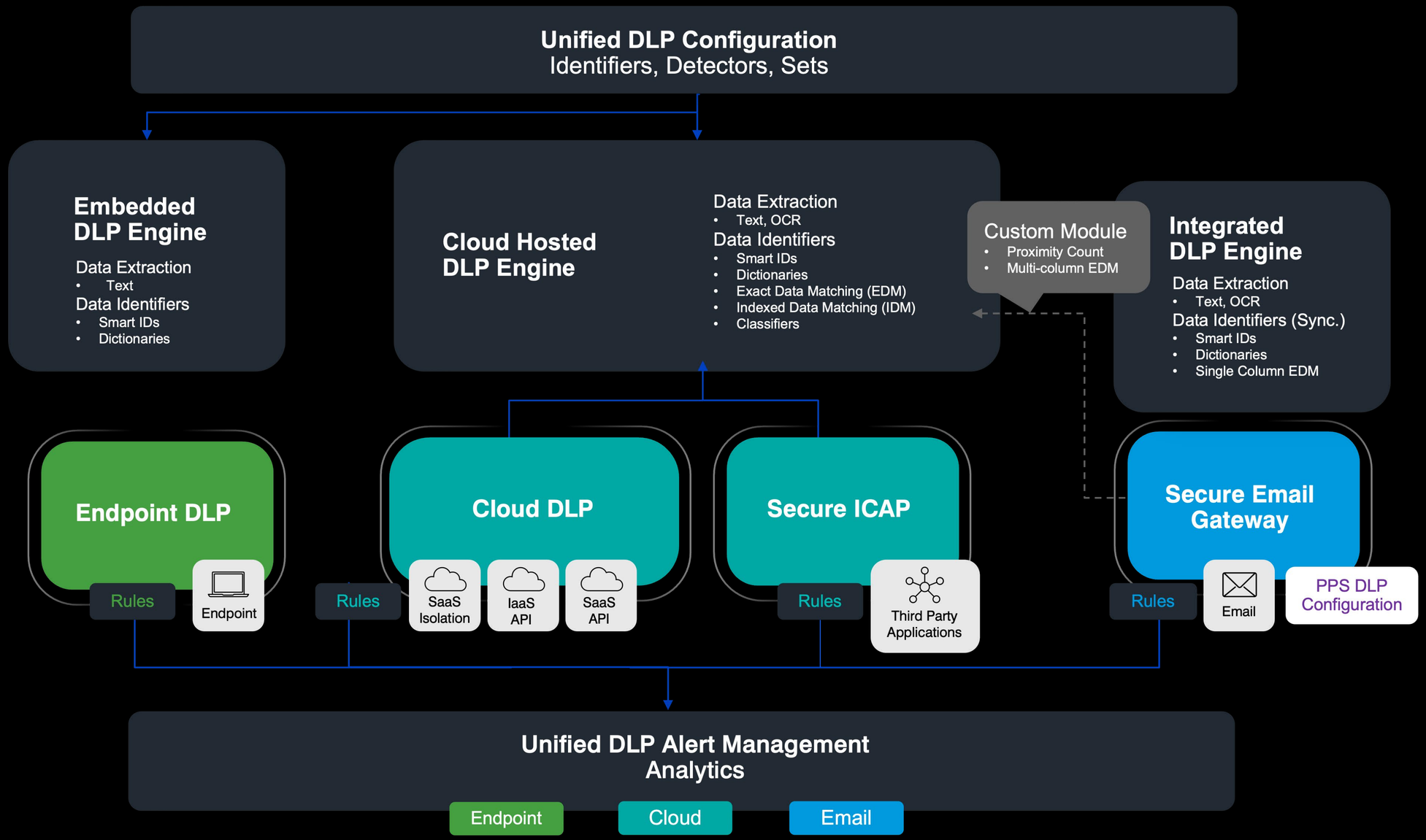
Our data export feature lets you securely replicate your data outside Proofpoint. You specify which data you want to export. This includes activity data, alerts and events. There is no retention limit on the exported data. Once it is exported, you can manipulate the data to analyze and correlate it.

Data can be replicated to a customer-owned AWS S3/Azure bucket, which is independent of the Proofpoint application. Once it's there, you can pull it into other analytic tools such as SIEMs and data lakes.

Exported data is from 15 minutes prior to the point that you triggered the export. It runs every 15 minutes.

.

Data extraction and identifiers by DLP channel



Document #: 1207-005-01-01

proofpoint.

Learn more at proofpoint.com

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.