netskope

White Paper

Why You Should and How You Can Move Away from Existing DLP Programs

1. DATA PROTECTION NEED IS GREATER THAN EVER

Data breaches continue to expose personally identifiable information (PII), intellectual property (IP), and other sensitive data at an alarming scale. Human error and credential theft are often involved; 82% of data breaches involve the human element and 61% involve credentials,[1] meaning that intentional and unintentional data loss by both malicious and well-meaning employees is a predominant cause of a breach in addition to the malicious data exfiltration conducted by external cybercriminals. All of these trends must be tactically addressed as part of an overall data protection strategy.

> 82% of data breaches involve the human element

Data breaches are costly events that carry lingering consequences. The average cost of a data breach increased 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.[2] The consequences of a breach affecting PII and IP can be very serious, and include direct loss of revenue, diminished reputation and effect on customer trust, noncompliance fines, class action lawsuits, loss of competitive advantage, operational downtime, and employee turnover, especially at the executive level. Many companies underestimate the effect a breach can have on reputation, but their customers' perception can be severely impacted by a business' data breach, with 69% of respondents in a 2019 survey claiming they would avoid a company that had suffered a data breach, and 29% of them claiming would never visit that business again.[3]

Data Breaches

- Data exfiltration
- Outsider attacks

Regulatory Non-Compliance

- GDPR, CCPA—privacy
- PCI-DSS, HIPAA, GLBA

Insider Behavior

- Malicious insiders
- Negligent insiders

Data protection solutions are therefore, more than ever, vital security controls to protect the reputation and the business continuity of every organization. Recent forecasts on information security estimate the growth rate for enterprise data loss prevention at 6.6% in 2022 with cloud data protection growing at a higher double-digit rate, as the number doesn't even include the massive adoption of DLP capabilities from integrated DLP services or cloud-native service providers.

2. MODERN BUSINESS TRENDS EXPOSE DATA IN NEW WAYS

The emergence of the hybrid workforce—where employees have the flexibility to work freely between corporate offices, branch offices, home, or on the road—has rapidly changed the way business is done. In order to sustain this highly distributed enterprise model, which accelerated rapidly during the onset of the COVID-19 pandemic, organizations have increasingly embraced a large number of cloud-based tools. In fact, cloud apps have become an instrumental means to keep all employees easily connected, foster business collaborations, and conveniently share data. The worldwide end-user spending on public cloud services is forecast to grow 20.4% in 2022.

Hybrid Work
Data outside of the
corporate premises

Apps Hyper-Growth
Data spread across
many cloud services

Evolution of Data
Growing in volume,
variety, velocity

In this scenario, organizations are facing new and unexpected data protection challenges as their sensitive data, such as personally identifiable information (PII) and intellectual property (IP), is moving outside of the traditional corporate premises, and is more exposed in the cloud and across the mobile workforce to newer threat vectors.

Over the years, data has also evolved significantly, growing in volume, variety, and velocity. Sensitive information can be embedded in structured files and data types, unstructured formats like images and screenshots, and even flow through asynchronous communications on email messages and collaboration apps like Slack and Teams. As a result, sensitive data is harder to identify, and therefore, to protect.

Data is harder to track and protect, more vulnerable to theft, and prone to both intentional and unintentional exposure. Data protection technologies have tried to evolve accordingly but it is hard for most DLP vendors to keep up with the rapid changes of our modern times.

3. TRADITIONAL DLP SOLUTIONS

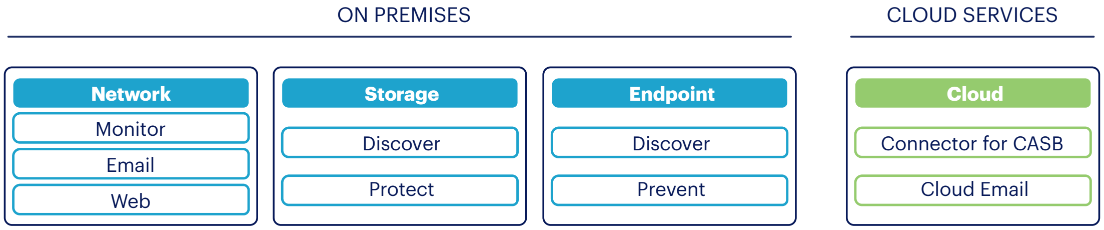
Traditional DLP solutions have protected organizations from the risks of data loss successfully for over 10 years. Originally designed to solve for a small variety of conventional data loss use cases, their fundamental mission was to discover sensitive data and prevent them from leaving the organization's boundaries: an employee's device, a physical file repository like a file server or NAS, a data center's network, etc.

Some DLP solutions have been able to expand gradually, with update after update over the years, to cover newer compelling use cases and new network environments, including endpoint off networks, larger and larger storage repositories, server clustering for high availability, and more network egress points via proxy and email MTA.

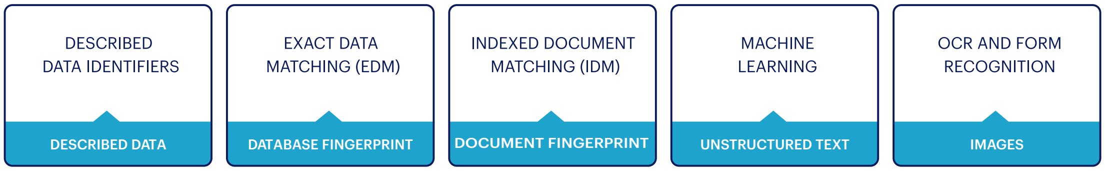
> One problem is that most DLP solutions—particularly legacy DLP solutions—weren't designed to meet the cloud-first characteristics of a hybrid workforce.

Before the cloud era, those solutions reached a high level of sophistication monitoring data egress points on-premises and still today not many alternative solutions can claim the same comprehensive coverage of data channels and the maturity of the traditional DLP's controls.

Legacy coverage of DLP channels



Traditional sensitive data detection techniques



But the cloud has changed everything. Back when DLP solutions were initially conceived, their architecture was conveniently layered on-premises on the network infrastructure of that time. DLPs are traditionally software-based solutions that need server machines, hardware proxies, ICAP connections, local agents, on-premises databases, on-premises management interfaces, and other components in order to work.

Their **complexity** has intensified over time, requiring multiple detection servers to solve for data at-rest, in-use, in-motion, larger databases, increased computing scale, and a costly bolt-on approach to expand to new environments. And such on-premises architecture was likely to be replicated for each branch office.

In cloud-enabled environments, the protection perimeter is fundamentally the data itself. The “perimeter” now extends beyond legacy network constructs and legacy modes of approaching data protection. Data travels everywhere and can be accessed from seemingly anywhere a user or a device wishes to connect to it.

With legacy DLP deployments, many organizations have invested great amounts of time and money. They have gone through several growth stages, have spent years setting up and fine-tuning their data protection policies and configurations, have extended their policies to newer channels, added new compliance requirements, created complex network configurations, and their practitioners have become technology experts. Now these organizations are realizing that years ago what might have been an architectural masterpiece is no longer sustainable. Moreover, it’s becoming too obvious that traditional DLP cannot solve most of today’s use cases, as data is massively used and stored across cloud services and shared across devices outside the managed premises. But because these technologies are too anchored by their on-premises deployments, they are very sticky. It is not easy to replace them with something modern that would possibly work better, at least not without security downtime and a lot of work by already-stretched teams.

The reputation of traditional DLP has drastically diminished. Legacy DLP solutions are now seen as extremely complex to deploy and maintain, requiring complicated programs and no longer effective as the needs have evolved. It’s known that with complexity comes liability, high operational costs, maintenance, and training expenses. Another perception is that DLPs can only be used by very large enterprises, because only large organizations have the bandwidth and the budgets to afford their total cost of ownership (TCO). This is a challenging paradox for most enterprises: Data protection is increasingly needed, and the DLP adoption is growing at a fast pace, but traditional DLP is no longer loved.

4. SHORTCOMINGS OF EXISTING DLP SOLUTIONS

Digital transformation and increased cloud adoption have created several challenges for traditional DLP solutions that have become bigger and bigger until reaching a failpoint. Besides the architectural and operational complexity of traditional DLP, practitioners also realize that there are use cases that cannot be obviously solved and environments that cannot be covered by the existing tools. In fact, with an overwhelming number of devices today being mobile and unequipped with any DLP, with an ever-increasing number of cloud apps (35% increase in number of apps in use in 2022), and with data no longer sitting in an on-premises data center, the paradigm has shifted, making old DLP go blind fast.

There are three main reasons for these shortcomings:

1. **Cloud and hybrid work, including SaaS, IaaS, and PaaS.** Architected as on-premises solutions and anchored by their on-premises infrastructure (i.e., proxy appliances, multiple detection servers, on-premises databases, etc.), traditional DLPs don't really extend to cloud channels. A way around for data discovery in the cloud initially was partially solved by the DLP vendors through ICAP integration with CASB solutions creating the first big architectural limitations: disjointed environments, hard-to-reconcile policies, different enforcements, separate consoles, and considerable latency to enforce protections. Another approach was tried via cloud detection services and REST API connectors, as a way to connect the on-premises DLP enforcement and CASB, but this method only patched some of the problems and did not provide a real long-term solution. Cloud adoption has increased exponentially, and so have the use cases and risks to data.

   Complex
   On-prem deployments rely on servers, ICAP and integrations

   Costly
   High TCO and maintenance costs for the hybrid infrastructure

   Resource Intensive
   Manual software upgrades and disjointed policies across environments

   Hybrid work has left organizations with this huge burden of having to deal with a DLP infrastructure that has become massive, extensive, and sticky, tight to on-premises dependencies and hardware components like proxies, databases, servers, etc.

   Coverage for highly distributed enterprises has become a nightmare because most likely the on-premises architecture must be replicated for each branch office. Most importantly, the legacy approach lacks coverage for remote employees connecting to corporate resources and risky cloud apps, for the unmanaged personal BYO devices that must also connect to corporate assets, and even for IoT devices accessing sensitive data from anywhere.

2. **Big data and increased computational requirements for DLP.** Over the years, data has evolved significantly, booming not just in volume but also in variety and velocity. Sensitive information can be embedded in more unstructured formats like images and screenshots, stored and shared in the cloud, and even flow through asynchronous communications on email messages and collaboration apps like Slack and Teams. As a result, sensitive data is increasingly harder to identify, and therefore, to protect.

   These solutions don't scale at cloud speed and they can hardly keep up with newer use cases, data privacy laws, and newer regulatory requirements. They can't ingest and process larger and larger amounts of information or leverage sophisticated machine learning and AI models, not without adding more detection servers, larger databases and voluminous endpoint agents, and slowing down other computational processes of the organization. Therefore many use cases will stay unsolved such as: advanced image recognition, correlation of context-based information from many risk vectors, advanced endpoint-based detection, fingerprinting of large files and datasets, etc. In addition, software updates for traditional DLP solutions are a complete nightmare because they notoriously take months or even years and a lot of manual work to go from one version to the next, not taking into account possible system errors and irremediable loss of data and configurations. Organizations are typically behind DLP version upgrades and therefore are not using newer protections (newer data identifiers, newer detection methods, newer compliance policies, etc.) because of the lengthy and resource-intensive updates that they have to go through.

3. **Too many false positives and no zero trust design.** With data residing and moving to more environments outside the managed data center network and with the amount of data constantly growing, the number of incidents has grown to a point that it is now nearly impossible for the incident response team to triage and remediate every incident with the right level of analysis and understanding. A massive number of false positives flood incident response teams—thousands or hundreds of thousands of alerts per day that would demand direct attention, but that have to be overlooked for lack of time and bandwidth. Incident response teams have expanded accordingly at a high cost.

   Automation and orchestration tools like UEBA have come to assist, ingest alerts, and figure out a more optimized way to remediate them in bulk. UEBA is an effective tool in symbiosis with DLP, but the UEBA model is not sustainable if DLP becomes more and more inaccurate and its gaps larger.

   DLP must shift into a fully integrated zero trust data protection platform, able to ingest and use information from any security source and translate them into actionable policy recommendations and intelligent incident response rules.

5. THE NEED FOR CHANGE

Digital transformation has fundamentally shifted the ways organizations deliver value and drive revenue. It has forced them to rethink and redesign customer experience delivery and to reconceive products and services. Today, in a cloud-enabled world, we must align data security initiatives to these changes and innovate continuously at cloud speed. Corporate business initiatives suffer when security teams fail to adapt to these changes and adopt the modern architectural and operational models to facilitate them.

It's a no-brainer that the DLP architecture must change in order to adapt to the modern hybrid work world and be future-proof. DLP has to be delivered from the cloud to ensure broad coverage, high efficiency, great scalability, and unlimited computing power. It also needs to provide a high degree of efficacy to guarantee accurate data protection against every data loss risk.

For example, SaaS applications have replaced many on-premises applications because they are able to deliver great advantages to organizations as they go through the modern digital transformation and embrace hybrid operational models. SaaS apps keep their users always connected, help store more data, make resources available anytime and from everywhere, make business transactions and customer services efficient, easier and faster, and they scale rapidly to cover additional branches and employees. They fundamentally solve complicated problems more easily. In the same way, data protection offers great advantages when it's delivered from the cloud.

The most relevant benefits include:

- **Comprehensiveness of coverage beyond networks—**cloud-delivered data protection means that data protection can easily extend beyond the corporate boundaries, to cloud services and users anywhere. It can discover and protect data across every channel, on-premises and in the cloud, everywhere data flows and anywhere it's stored. This model doesn't require additional infrastructure but can leverage existing control points such as SaaS APIs, cloud security gateways, endpoint clients, etc.
- **Infinite computational scale to anticipate new needs** and unlimited levels of sophistication—data scanning and detection algorithms can run in the cloud, eliminating the burden on the network computing infrastructure and voluminous endpoint agents. They can ingest and process large amounts of information and context to make smart decisions automatically based on rich risk context. They can finally deploy sophisticated machine learning and AI data identification models to detect sensitive data with a high degree of accuracy and solve for more challenging use cases. This provides a higher degree of detection accuracy, minimizes false positives, and automates incident remediation workflows.
- **Risk and context awareness for high data protection efficacy—**A cloud-delivered data protection platform can be easily integrated across the security and networking infrastructure and within cloud services, sharing intelligence and continuously gathering risk context. It has the ability to collect great amounts of logs and information available from other security and infrastructure sources like cloud security tools, SaaS security posture management, cloud security posture management, network security, endpoint security and posture, identity, user behavior analytics, security orchestration, etc. Such a vast pool of information can be leveraged to identify sensitive data accurately and, most importantly, to determine the best type of response to data security incidents and violations based on risks, situations, instances, locations, behavior, reputation, and other factors. **Security context makes DLP risk aware with continuous and adaptive assessments**.
- **Lower cost of ownership, ease of deployment, and maintenance and scale—**A cloud-delivered architecture is not tight to an infrastructure. It can be modeled to the cloud, meaning always staying up to date, with always-on protections and latest updates available in real time everywhere the service is deployed.

6. NEW CLOUD DLP PLATFORMS SOLVE MODERN USE CASES BUT NOT ALL OF THEM ARE MATURE YET

Today a few security vendors have taken the opportunity to drive the change and fill the modern data protection needs that are left unresolved by legacy solutions.

Maturity

Coverage

Effectiveness

New cloud-delivered DLP solutions provide more visibility in the cloud and beyond the corporate premises, and they scale with less friction. The old bolt-on DLP approach made of multiple detection servers used to cover different environments (web, email, at-rest discover, cloud CASB, etc.) has been finally replaced by a single data protection brain in the cloud for consistency of policy enforcement everywhere data is and for better system manageability. ML and AI can now be finally delivered at full capacity leveraging the highly scalable computational power of the cloud. Cloud DLP solutions also have the capacity to ingest and triangulate more information from different sources, including application risks, network risks, device postures, user behaviors, etc. This is transformative.

But not all the new DLP solutions out there are the same, and indeed most of them have not reached the right level of maturity, the detection accuracy, and the sophistication of controls required to take on the heritage of legacy DLP solutions and to be practical. In fact, some vendors only recently have started offering integrated DLP capabilities in their core products, hoping that aggressive marketing would be enough to convince buyers on products that actually lack breadth and depth.

Two dominant models have emerged:

- **Integrated DLP solutions,** which include DLP capabilities as part of a web gateway, CASB, or NGFW, and broadly described as being part of SASE platforms, delivered from the cloud and integrated within a network security appliance or a service.
  - Cautions: They usually lack endpoint and email use case coverage and may offer inadequate detection capabilities compared to legacy DLP. For most of these solutions, advanced detection engines are absent or too basic, while their ML and AI are no more than marketing buzzwords.
- **Cloud-native DLP solutions.** Today many cloud service providers (CSPs) and SaaS vendors offer native DLP capabilities. These are cloud-focused solutions, readily available that are increasingly chosen by organizations pursuing a cloud-first strategy or those that are beginning their data protection journey.
  - Cautions: They basically address the cloud data protection use cases for specific environments and may lack broad coverage. Their capabilities are typically not adequate to match those of legacy DLP solutions. Some enterprises legitimately start here, but it is important to understand that this approach may eventually lead an organization to adopt multiple siloed DLP options for subsequent use cases.

Data protection must be undoubtedly delivered from the cloud to be practical in modern times. In addition, practitioners know very well that a data protection program also needs feature maturity and a vendor's full dedication and expertise in order to succeed. In fact, "good enough" capabilities can produce inaccuracy, partial detection, and most importantly, a lot more false positives than an organization is capable of handling. The fact that they are integrated solutions most of the time means they are just bundled services, "included" but not architected to actually consume logs and contextual information from other controls. Therefore, their incident response actions stay inaccurate because they lack awareness of business context and risks. This is a data protection strategy destined to fail.

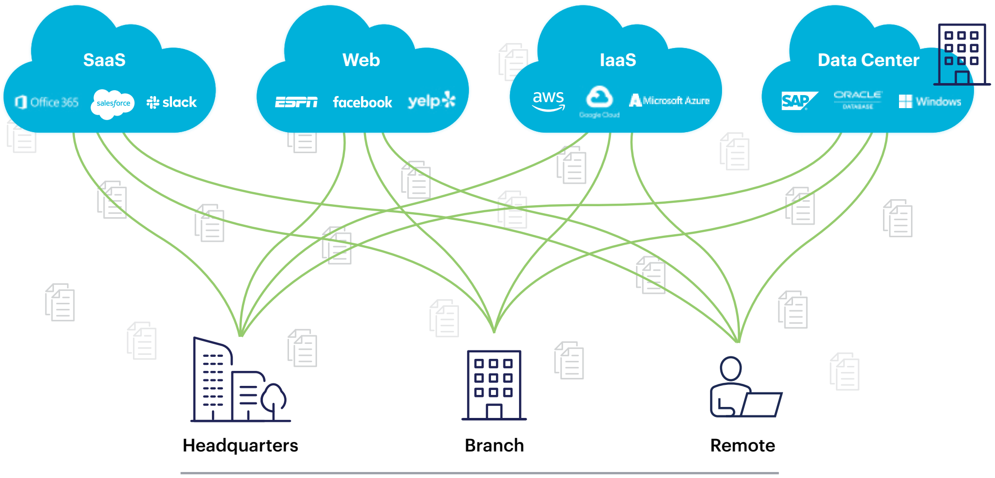
In the next section of this paper we will explore the reasons why only Netskope DLP provides a high level of sophistication and a superior solution needed for a data protection program to succeed, thanks to the vendor's full dedication to data protection and its continuous innovations over the past decade. Netskope is not just another SWG/NGFW/CASB vendor adding a DLP capability to their core product. Netskope is the data protection vendor of choice in modern times.

To start a new journey, enterprises need to look for a number of additional specifics in cloud DLP. Gartner's recommendations for DLP include the following:

1. Define a DLP strategy based on data risk and the needs of the business. Select DLP products and execute proofs of concept with the objective of supporting this strategy, rather than finding solutions to address limited use cases.
2. Invest in a DLP solution that not only provides content inspection capabilities but also offers extra features such as data lineage for visibility and classification, user and entity behavior analytics (UEBA), and rich context for incident response.
3. Overcome the challenges presented by a cloud-first strategy by implementing a solution to map and secure sensitive data across the hybrid environment.

7. THINGS TO LOOK FOR WHEN SWITCHING TO A CLOUD-DELIVERED DATA PROTECTION SOLUTION

Every organization has specific data protection needs and some unique use cases. Data protection programs are never the same from one another. That's the reason why a DLP technology needs to be adaptive, rich in functionalities, and broad in coverage and depth in order to be shaped around each specific data protection program.



There are, though, a few common architectural guidelines and technology aspects that should always be considered in order to move from an existing DLP deployment to one that meets modern requirements:

Comprehensiveness of coverage
You can't protect what you cannot see. Traditional DLPs provide extensive coverage of data channels, mostly on-premises, including web transmissions, email SMTP and endpoint. It is reasonable to expect a replacement solution to provide a similar coverage in addition to cloud repositories SaaS and IaaS. It's always recommended to start with complete enterprise coverage for both the cloud and the traditional on-premises channels. In that sense, it's also important to know that most cloud DLP solutions are architected in the cloud to solve only for the cloud use cases and don't cover certain on-premises channels such as endpoints.

There are many modern use cases that are fundamental, should not be overlooked, and must be properly addressed, such as transfer of sensitive data across thousands of unsanctioned risky SaaS apps or to personal instances of sanctioned SaaS apps like a personal Gmail account or a personal cloud storage instance of Onedrive versus the corporate Onedrive, and private applications in the public cloud or in the data center. For the modern highly distributed enterprise made of multiple branches and the hybrid remote workforce, DLP must protect all web transmissions of data from any location and any device, including managed devices, unmanaged devices, and even IoT. Collaboration apps like Slack and Teams need granular DLP coverage as well as email use cases including outbound email, SMTP, and webmail.

Core data detection capabilities

Data visibility is a tactical necessity to assess the entire operating environment and implement the optimal protection strategy. It all starts from data discovery and classification. Because manual data classification by the data owner could be an unreliable process, this task needs to be automated in DLP by means of a complete set of detection engines. Such engines define the organization's predefined detection policies or data profiles.

- **Data identifiers** have been and still are the must-have of any DLP solution. They are used to identify certain types of sensitive data based on described matching criteria that generally characterize objects like SSN, payment card information, or passport numbers, such as number of digits, text patterns, sequences, separations, and proximity words. Having regular expression (regex) capabilities is fundamental but this can't be a check-the-box feature. More types of sensitive data types, newer use cases have emerged and newer compliance requirements demanding to protect the privacy of individuals in a broader fashion. In fact, a large number of predefined data identifiers is the first element of consideration, but also the granularity of the rule customizations like boolean logic, severity levels, the extent of proximity checks, etc., must also be taken into account.
- But don't just look for the data identifiers you need now; look for several thousands of predefined data identifiers, as your future needs will most likely expand along with your organization's size and data protection maturity. Look for the presence of regulatory compliance templates that you need to support to verify that the latest are all there—GDPR, CCPA, PII, PCI, PHI, and source code, to name a few of the better known regulations.)—to understand the level of commitment of the vendor to keep up with the most recent compliance requirements, knowing that the vendor most likely will expand them in the future. The ability to edit existing regexes or identifiers or to create custom data identifiers with granular controls is critical as every organization has different needs such as specific type of information that is sensitive just for that particular organization.
- The number of **file types** supported is another key element. There are over 1,500 file types that may contain sensitive information. Text, Presentation, Email, Images and Screenshots, Spreadsheet, Cad, Social Posts, Online Forms, Slack Messages and other Chat channels, Encapsulation, Attachments, Graphics and Pictures like JPEG and PDF, etc.
- **AI/ML data classifiers** to aid data discovery and identification. Manually defined rules are the foundation of data detection, but in the modern world, automated engines can supply invaluable assistance and make sensitive data detection and categorization more accurate.
- **Exact data matching (EDM)** is a traditional, yet almost infallible, method designed to detect specific information that is sourced from structured data sources such as spreadsheets and databases. With EDM, a DLP solution can fingerprint and index databases of confidential customer and employee records, information that, when combined, can identify an individual such as full names, Social Security numbers, addresses, identification numbers, etc., or financial records that identify an individual's financial assets like credit card numbers or bank account numbers associated with customers. Even healthcare information or product identification and pricing databases. Such indexed information can then be found anywhere the data flows are expected to happen.

- For EDM to be effective and accurate, it has to be capable of leveraging granular conditions to match various pieces of the indexed data and match combinations of data fields from a particular record, the ones that matter. EDM scale is a very important factor, especially for large enterprises and for organizations looking for future growth. Hundreds of thousands or even millions of records must be supported.

Advanced data detection capabilities

The introduction of newer data types and newer ways of sharing and transmitting data, the massive growth of data volumes, and new compliance requirements require advanced ways of detecting sensitive information.

Legacy DLP solutions have introduced advanced detection capabilities in the past but have started failing to produce accurate detection results for lack of computing power and scale. Therefore, they generate more and more false positives that hinder business flows and overwhelm incident response teams.

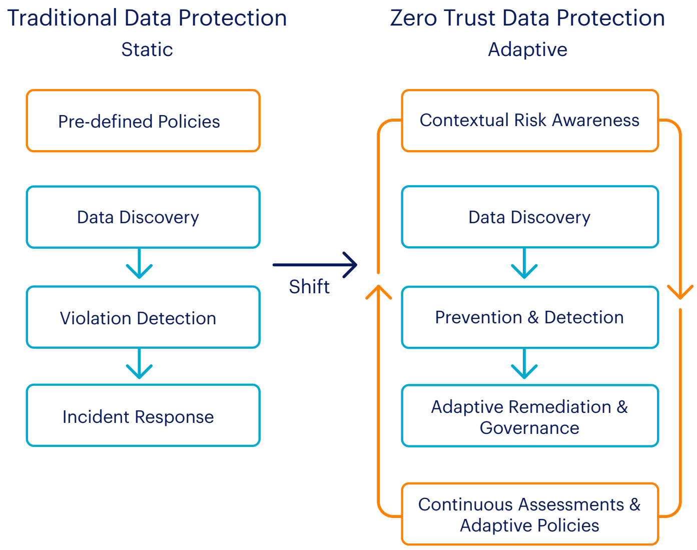
On the other hand, the vast majority of recent cloud DLP solutions are immature and unproven in terms of efficacy. It's important to verify the presence and the level of sophistication of the following advanced detection capabilities:

- In the present world, users find it very convenient to snap photos of documents, forms, ID cards, whiteboards, and even pictures of other pictures. For example, screenshots are a very common vehicle to quickly capture information and immediately share it with a colleague. As a consequence, **optical character recognition (OCR)** and AI-based image recognition are becoming more and more instrumental for a modern and future-looking data protection strategy. With OCR, a DLP solution can extract textual information from an image and can then apply data classification based on the detection policies that are in place.
- **AI and ML image classification** is even able to recognize common file and document types like SSN cards, patents and M&A documents, tax forms, source code, desktop screenshots, passports, and other IDs, etc., without necessarily extracting the content that such assets contain.
- Such detection methods must provide a high level of sophistication to be able to detect blurry, crumbled, and damaged pieces of content, with information that may be hard to read clearly. This is because pictures and screenshots may be taken quickly and with poor or too strong light conditions or because a document may be damaged and aged.
- **File and document fingerprinting** is another advanced capability that many organizations find vital for their own ways of conducting business. Certain mission-critical documents and highly confidential files must be protected at all cost from complete or partial exfiltration and duplicate copies. File fingerprinting can index entire documents and then detect exact or even partial copies of the information that they contain with certain degrees of similarity, when this content is found across environments and transmission channels that are considered risky, such as an upload to a private instance of an email application.

A zero trust-ready model

Digital transformation and evolving collaborative business models have changed our operating security paradigms.

From Implicit Trust to Adaptive Zero Trust Data Protection


Traditional Data Protection
Static
Pre-defined Policies
Data Discovery
Violation Detection
Incident Response
Shift
Zero Trust Data Protection
Adaptive
Contextual Risk Awareness
Data Discovery
Prevention & Detection
Adaptive Remediation & Governance
Continuous Assessments & Adaptive Policies

Zero trust is a modern strategy that brings security controls to the data itself as a new perimeter, and replaces implicit trust with continuous and adaptive risk assessment in order to constantly adapt to changing risk conditions. Data controls have proven to cause operational friction and hinder value creation because they lack context. This is why traditional DLP has failed to be effective: There was not enough business context and risk awareness to provide confidence for stopping data movement. Most of the incident remediation decisions in DLP had to be manually made by the incident response team, which also lacked enough risk and behavioral context. Because of that, traditional DLP is today perceived as a business inhibitor especially when blocking mode is turned on, rather than an effective data protection solution. In fact, most organizations are using it as a data discovery and compliance tool, working rather in monitoring mode in order to avoid problems.

With zero trust applied, these challenges are solved. Data protection technology is required to shift from a static model made of predefined fixed policies, lacking context and unaware of risks and changing behaviors, to a dynamic and adaptive zero trust approach that can leverage security context and continually enable the proper protection automatically based on changing conditions.

Automated data protection response requires defined processes and granular policies along with clear rules of engagement, what actions to take under what conditions with what degree of confidence. DLP must integrate with the most number of security control points, continually ingest their logs, and leverage them dynamically. A zero trust-ready DLP must take into account organizational risks from users, devices, data, networks, and applications in order to gain rich risk awareness and always provide the right remediation action. For example, behavioral monitoring for users, devices, and applications gives valuable insight into anomalous user activity, potentially malicious actions, risky apps, unsafe connecting locations, unsecure postures, and indicators of compromise.

To be truly effective, a zero trust data protection solution needs to monitor what's taking place and who's doing what across the entire corporate infrastructure, including clouds, remote users, and unmanaged devices.

8. NETSKOPE DLP IS THE WHOLE PACKAGE

Comprehensive Coverage

For all sensitive data across every network, cloud, endpoint, email, user

Precise Detection

The highest degree of data protection efficacy to address real risks, not false positives!

Effortless and Affordable

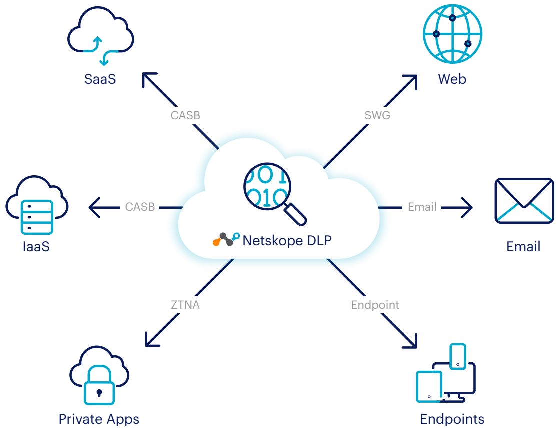
The simplest and most cost effective enterprise DLP deployment

CISOs and information security teams today are faced with a hard dilemma:
Is it better to rely on mature legacy DLP solutions that are however complex and costly or is it time to adopt easy-to-deploy, cloud-delivered data protection solutions that lack breadth and depth?

Netskope DLP is the answer. In fact, it is the industry's most comprehensive, most precise, and effortless cloud DLP solution that secures sensitive data across clouds, networks, emails, endpoints, and users consistently everywhere. Netskope DLP is also architected to enable zero trust data protection and is natively integrated into the Netskope's market-leading Security Service Edge (SSE) solution.

Netskope cloud-delivered DLP offers major advantages, including:

1. **Comprehensive protection coverage** of every location where data is stored, used, or transferred. Netskope DLP cloud service is natively integrated into the broad Netskope SSE solution and delivered across network in-line, SaaS at-rest, SaaS in-line, IaaS, private applications in the data center and in the cloud, branch offices, the remote workforce, email, and on users' endpoints. It provides comprehensive coverage and unified data protection policies for every location where data is stored, used, or transferred and delivered from a centralized cloud service.

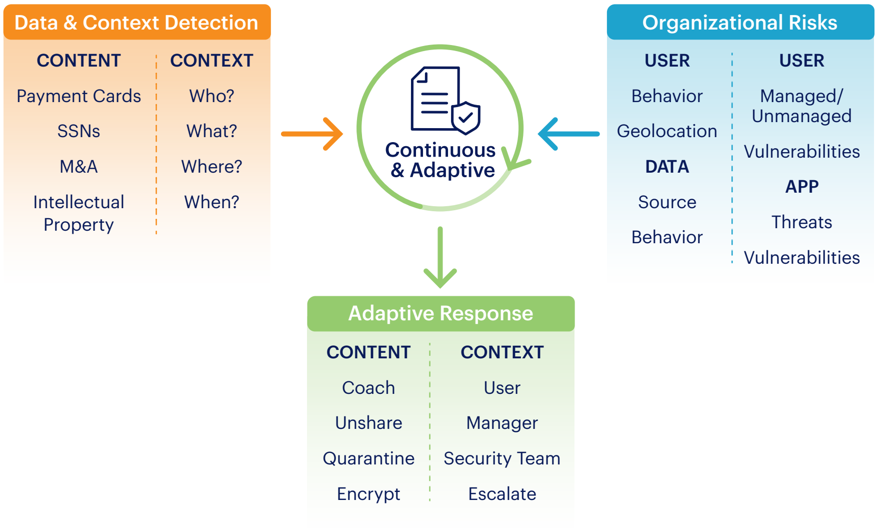


2. **Accurate and reliable detection** of all sensitive data in any form with the lowest degree of error possible. This is achieved through a broad set of detection technologies and advanced classification tools like several thousands of data identifiers and file types with contextual detection policies, highly scalable exact data matching (EDM), fingerprinting of structured and unstructured documents, ML-based image classification, advanced optical character recognition (OCR), and AI/ML data classifiers to aid data discovery and identification.

3. **Ease of deployment and maintenance** as well as **low total cost of ownership (TCO)** thanks to its cloud-delivered architecture that doesn't require on-premises components. Centralized policies are delivered consistently everywhere the service is enforced. Always-on and up-to-date protections replace the need for lengthy manual software updates typical of legacy DLP.

9. ZERO TRUST DATA PROTECTION

At Netskope we believe that the implementation of a data protection program should not hinder user experience or be an obstacle to business productivity. Data protection should be at the core of an organization's zero trust initiatives. Judiciously applying **zero trust** means that we must go beyond merely discovering sensitive information and controlling who has access to it, and factor in the continuous, real-time access and policy controls that adapt on an ongoing basis based on a number of factors, including the users themselves, the devices they're operating, the apps they're accessing, the threats that are present, their changing behavior and reputation, and the context with which they're attempting to access data such as geolocation and type of endpoint machine. Data protection is ultimately about context. By monitoring traffic between users and applications, we can exert granular control. We can both allow and prevent data access based on a deep understanding of who the user is, what the user is trying to do, and why the user is trying to do it. This data-centric approach is the only effective way to manage risk in the modern hybrid and highly distributed enterprise.



Data & Context Detection

CONTENT	CONTEXT
Payment Cards	Who?
SSNs	What?
M&A	Where?
Intellectual Property	When?

Continuous & Adaptive

Organizational Risks

USER
Behavior
Geolocation
DATA
Source
Behavior

USER
Managed/ Unmanaged
Vulnerabilities
APP
Threats
Vulnerabilities

Adaptive Response

CONTENT	CONTEXT
Coach	User
Unshare	Manager
Quarantine	Security Team
Encrypt	Escalate

Netskope DLP is the only solution that not only can take on the heritage of legacy DLP solutions, but move the technology to the next level, a Zero Trust Data Protection solution, with innovative technologies like machine learning and UEBA.

Netskope DLP is natively integrated to the comprehensive Netskope Security Service Edge (SSE) solution and delivered as a core element of SASE, enabling organizations to take advantage of a fully converged cloud-native security platform that consolidates the most vital security technologies onto a unified, integrated cloud-native platform. This approach eliminates security blind spots, provides consistency, enhances performance, and dramatically reduces the costs and complexity typical of a multi-vendor ecosystem.

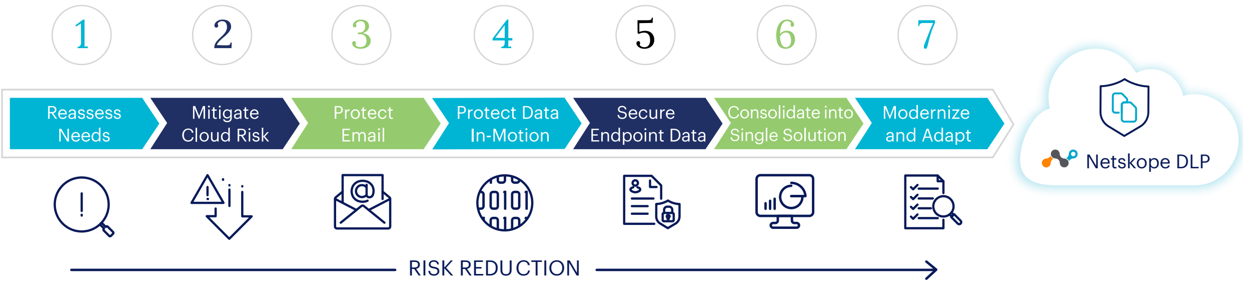
Customers can:

- Attain greater visibility and risk mitigation across all key vectors from a single converged SSE data protection solution based on zero trust principles and state-of-the-art data protection controls.
- Simplify data classification, policy definition, and incident management with a converged platform enriched by machine learning, rich reporting, and advanced analytics.
- Boost end-user agility and reduce friction with flexible context-driven policies and a lightweight agent.

Ultimately, a successful data protection program must coach employees and encourage safe data behavior while preserving the freedom of business decisions. User coaching must produce real-time alerts to the users about their data security violations in order to be immediately effective, not in retrospect as the users may have no memory of past events.

With 10 years of investments in data protection and a long tale of industry's first innovations, Netskope is a technology leader that is fully committed to data protection, with DLP at the core of its approach to helping businesses everywhere.

10. STEPS TO TAKE TO TRANSITION TO NETSKOPE DLP



Traditional security implementations like DLP often carry the legacy of accumulated compositions from years of deployment, maintenance, patching, and expansions, like giant tumbling block towers, where all the pieces are meant to stick together.

Switching from such composite infrastructures is never an easy task or an aspiration, but knowing that the value of the innovation will be substantially greater should drive the change, as organizations seek agility and scalability through their digital transformation.

The transition doesn't have to be radical and can be executed step by step. It's also beneficial to leverage current investments that are working and build upon them. Replacing a legacy enterprise DLP in its entirety and protecting all sensitive data across every on-premises and cloud environment by means of a single data protection solution should be the end goal.

To get there, it's important to make the business case and produce security metrics for all audiences (strategic metrics for the senior leadership, operational metrics to guide the interaction with the internal security teams, and tactical metrics to direct the activities of the frontline staff). Netskope support teams can help provide guidelines to produce leading indicators, and generate compelling data points and reports.

There is no "right way" to migrate to modern Netskope cloud-delivered DLP. Most organizations adopt the entire solution from the very beginning; others instead move slowly from a legacy deployment adapting and adopting the components that make sense for them first, as they move through their maturity stages. Every organization is different but generally the migration journey follows this logical course of action:

1. **Reassess your data protection needs.** The first stage is to conduct a thorough assessment of the current technology environment, to identify and understand what data must be protected, which services and repositories are being used by the organization to store and process sensitive information, how these services are being used by departments and individuals, etc. Here the security team needs to specifically identify and assess all corporate applications, the email services adopted and other collaboration tools, network locations, the users' hybrid work practices, the connecting devices, and the organization's business processes of today, such as how data is being shared among employees or with external parties. It's important to identify and assess data-at-rest and data-in-motion activity and possibly identify the categories and the many types of data stored or processed within the scope of business. This stage can represent a "quick win" for organizations, because it can support regulatory compliance efforts, and most importantly, because it may unveil that certain portions of legacy DLP deployment are perhaps less effective now and no longer needed. For example, traditional on-premises storage discovery may not be worth the investment as before because more data is stored on emerging cloud repositories.

2. **Many organizations start with the cloud apps.** The second stage is to determine where the highest risks are and make it a priority to mitigate those risks. Solving for new cloud data protection use cases is usually the motive and first step that leads information security organizations to transition to a modern cloud-delivered data protection solution. After all, more and more data is living across corporate SaaS applications, cloud email and IaaS today, exposed to unintentional data sharing, malicious exfiltration, and other cloud-based cyber threats. Netskope's market-leading CASB solution embeds DLP as its core component. This approach solves for both data security for corporate sanctioned cloud applications and for protection of data in-motion, especially when sensitive data is moving across unsanctioned and possibly risky apps.

   Choosing the right data protection vendor at this point is the most important step, because eventually organizations need to expand the solution to every environment they have for consistency. Netskope DLP is the only cloud vendor that provides that necessary hybrid coverage for all cloud channels and beyond, including on-premises data movements, because the solution includes endpoint DLP, email DLP, network DLP for web and for email, DLP for SaaS and IaaS, for private apps, etc.

3. **Cloud email is another starting point.** The corporate migration to cloud-based email service is another opportunity to kickstart the change. Netskope provides a very extensive DLP protection for email including Microsoft 365 and Gmail via APIs, real-time email protection inline, and even data protection through personal email instances.

4. **Protect data in-motion through every connection.** With more sensitive data now stored in the cloud and flowing everywhere, connections to corporate assets can be established directly from home and other networks without a VPN connection, from branch offices, from corporate devices as well as from personal devices and from IoT peripherals. This way, data can be accessed, uploaded, and downloaded beyond the oversight of enterprise security controls. In this scenario, a traditional "proxy-connected" DLP solution sitting in the data center partially covers data in-motion to corporate apps and to the web only when the connection happens from the main HQ offices. Netskope's intelligent SSE natively embeds the unified Netskope DLP service to secure sensitive data transactions from anywhere people work when accessing the web, the cloud, and the private applications with zero trust principles and without any hardware constrictions.

5. **Protect data on employees' endpoints.** For most organizations utilizing legacy DLP solutions, endpoint DLP is fundamental. Yes, data today is stored more and more on cloud services; however, it is obvious that much sensitive data is still created on or downloaded to a corporate provisioned machine. Once the data is on the machine, it could be easily exfiltrated through USB, for example.

   Netskope DLP cloud service is integrated to the Netskope client and will not require deploying a separate agent on the endpoint. It is a lightweight endpoint DLP that is designed to minimize resource utilization while featuring the full suite of advanced DLP capabilities, including ML-based classifiers, OCR, File Fingerprinting, Exact Data Match, etc. It enables detection of data in-use via USB, USB device protection, and other device control policies to ensure that sensitive data is not lost or stolen whether the device is online or offline, on the corporate network, or connected from anywhere else.

6. **Build upon a solution that is working now.** Another important consideration is that, if a recent investment was made toward native DLP capabilities on the cloud service provider (CSP) or from a specific SaaS vendor and this solution is solving present needs, a wise approach is probably to live with it in the short or medium term. But as the organization is planning to extend data protection to additional environments like multiple clouds and SaaS apps, you should consider that these environments could turn into too many consoles and disjointed sets of policies. Netskope DLP consistently protects all environments with uniform policies and via a single console.

7. **Evaluate and take advantage of newer capabilities offered by Netskope.** Modern use cases require an updated approach to data protection. Netskope DLP expands the scope of data protection by delivering advanced data detection technologies driven by ML, superior performance and computing scale, and more accurate risk mitigation. For example, DLP is no longer a composite solution made of different components and third-party integrations (such as with a CASB), but a comprehensive service with unified policies and a single console. Certain resource-intensive detection methods like EDM, image recognition, and ML are now present even on a lightweight endpoint DLP agent, thanks to the cloud, as they were not possible in the past for endpoint DLP. Netskope today has enormously expanded the DLP computing capabilities in the cloud and can, for example, scan and fingerprint very large datasets. Most importantly, with Netskope, DLP is no longer an autonomous solution disjointed from the company security stack and unaware of business risks, but today it's integrated into SSE and aware of business risks, behaviors, and security vulnerabilities across the entire organization. By ingesting information about users, devices, networks, clouds, and behaviors, Netskope DLP adapts its decisions to changing conditions, minimizes false positives, and produces more accurate results.

The experience built by the internal DLP practitioners (the policy admins, the incident response team, etc.) over the years with the existing legacy DLP solution is an extremely valuable asset that should be leveraged to replicate best practices and to ensure that all the technological expectations are met, including producing compliance policy profiles and establishing the proper remediation workflows. As the Netskope DLP minimizes the program's efforts, security teams can spend less time on management and frustrating incident triage, and more on substantive security activities and proactive initiatives.

[1] Verizon's 2022 Data Breach Report

[2] IBM Cost of a Data Breach 2022 Report

[3] 2019 Verizon Survey

[4] Gartner

[5] 2022 Market Guide for Data Loss Prevention (July 2022)

[6] Netskope Cloud and Threat Report: Cloud Data Sprawl

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

To learn more visit: https://www.netskope.com/products/data-loss-prevention.