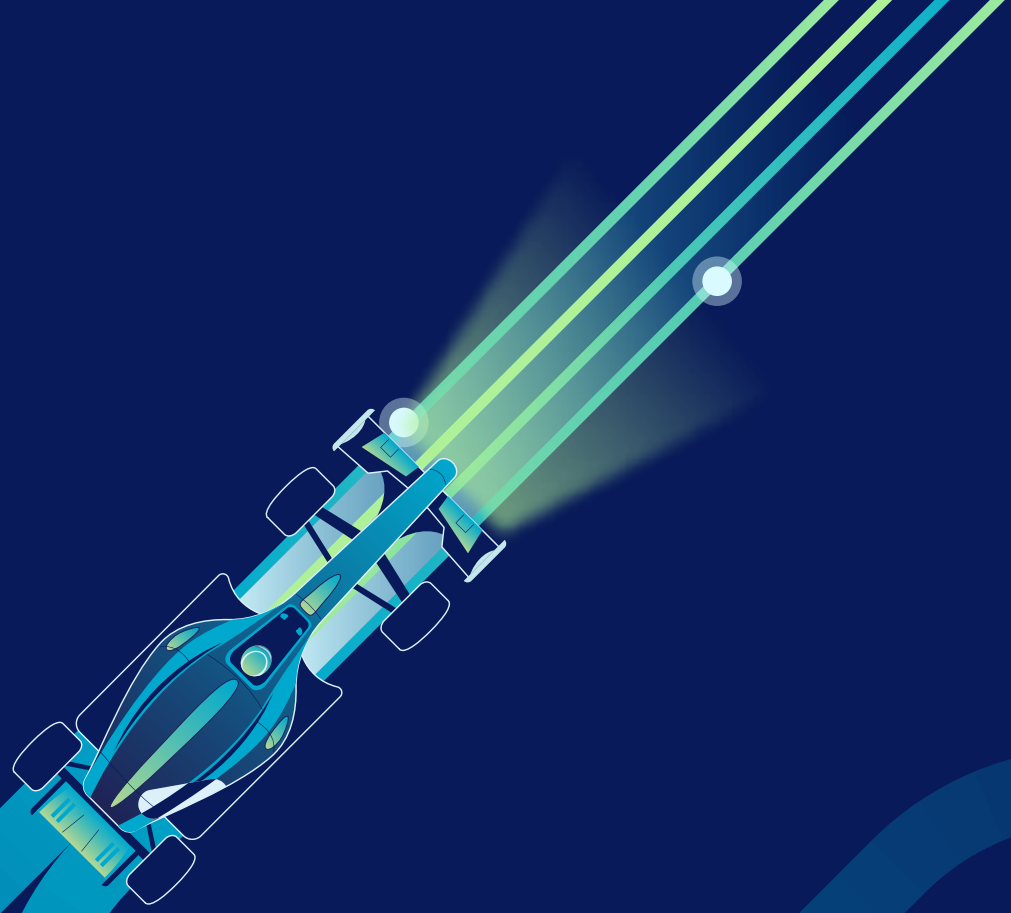
netskope

The Unified Data Security Playbook

Turbo-charging data protection by combining DSPM and DLP in one solution



The

Unified Data Security Playbook

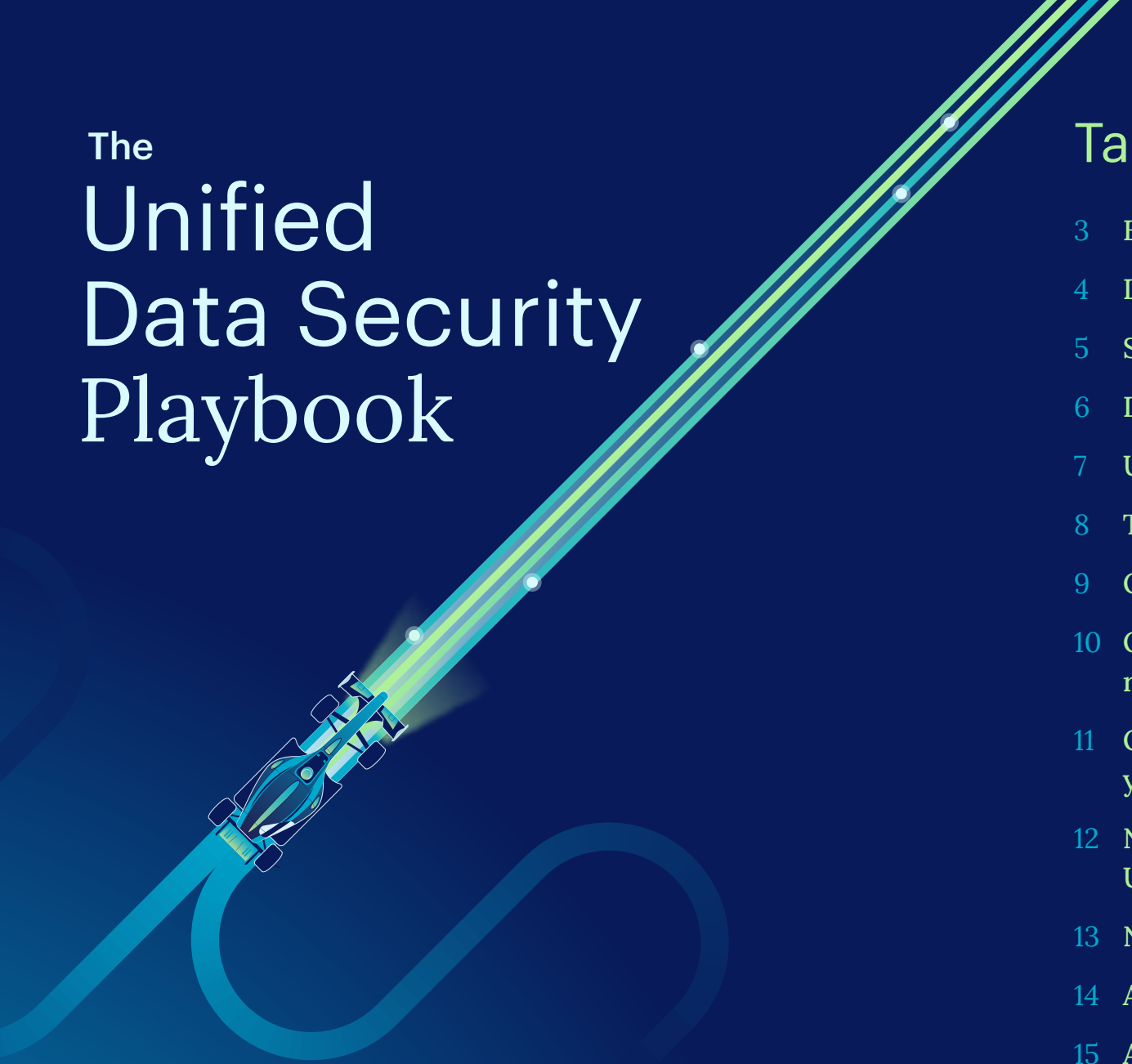


Table of Contents

Executive Summary

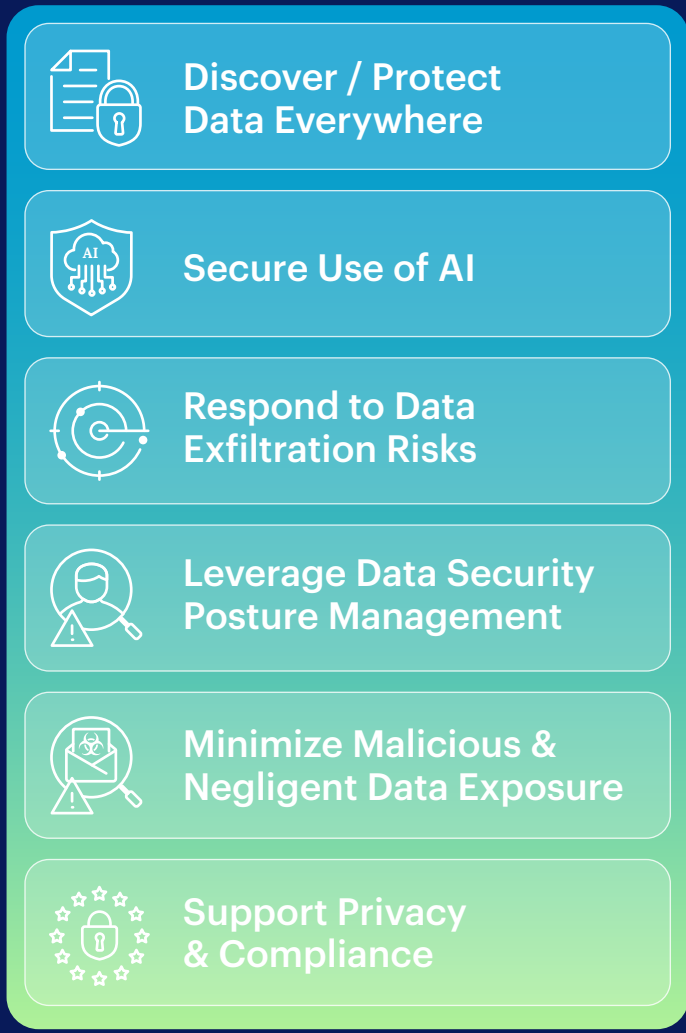
Corporate security, risk management, and compliance teams may feel they're in a never-ending race, trying to stay ahead of a lineup of threat actors. They are not wrong. Data breaches become increasingly common every year, and no organization is immune. The problem affects companies of all sizes, in all industries, across all geographies.

Consumers may have some awareness of the risk, but they expect the companies they do business with to protect their information. Few events are more impactful to a company's brand reputation than a large-scale cyberattack.

The threat landscape has led regulators to raise expectations for corporate data privacy. Breaches often follow organizations' failure to comply with rules designed to keep sensitive data safe. Regulators who discover that a targeted company was not compliant with mandatory regulations tend to react strongly, imposing punitive fines.

Ensuring security and compliance was already challenging when a company's valuable information all lived within its own corporate perimeter. Today, it's even more difficult because 60% of the average company's customer data is in the cloud.[1] This highly valuable information lies outside of the IT team's traditional sphere of control.

Securing digital assets in the modern enterprise requires a new way of thinking. Unified data security combines data discovery, classification, access governance, and risk assessment capabilities (those found within data security posture management [DSPM] tools), with the real-time protections of data loss prevention (DLP) technologies. Fully integrated, these solutions lock down a company's data—even data stored in the cloud and in shadow applications unmanaged by corporate IT—through six key capabilities.



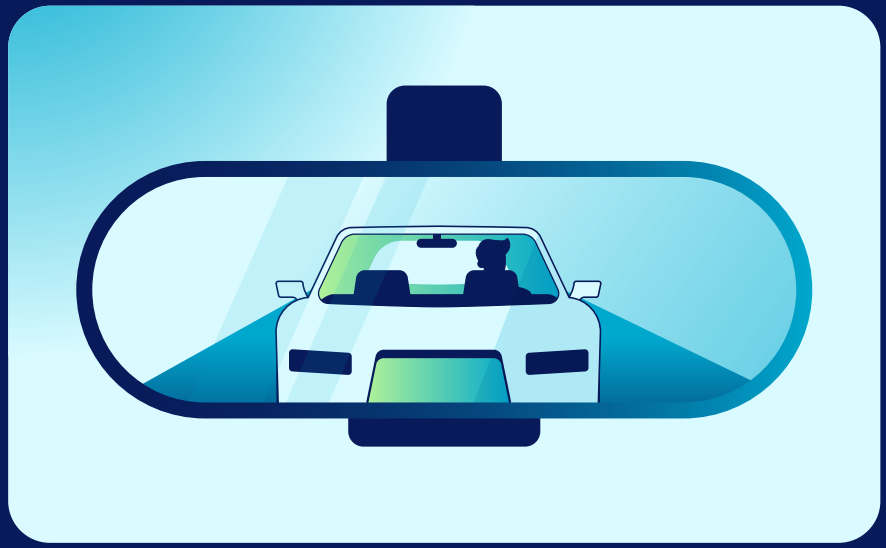
[1] Source: Statista. "Share of corporate data stored in the cloud in organizations worldwide," March 2022.

Data Security Fundamentals in the AI Era

Companies need to recognize their security blind spots in order to effectively block cyberattackers' attempts to get past safeguards. To ensure they have a clear line of sight to all the applications and data that users are accessing, IT teams must ask themselves several key questions:

- Where is all our data?
- What is the nature of this data?
- Who has access to the sensitive data?
- How risky are our data interactions?

The purpose of this exercise is simple: If a cloud-based solution or database contains customers' personally identifiable information (PII), such as addresses or Social Security numbers, or any other sensitive corporate information, the organization needs to understand what guardrails it has in place to keep data risk on track.



Pro Tip

If a cloud-based solution contains customers' PII, or other sensitive corporate information, the organization needs to understand what guardrails it has in place to keep data risk on track.

Steering Through Data Risk

The challenge in identifying data blind spots is that companies need to secure a lot of different information, and it isn't always moving around the track in an orderly manner. Security teams may need to manage data across a wide swath of endpoints, websites, and email systems. Sensitive information may also reside in databases, data lakes, and/or data warehouses, as well as a range of cloud-based systems—not only Software-as-a-Service (SaaS), but also Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Some of this data is on premises; some exists in the cloud. All must be secured while it's in motion, while it's in use, and while it's at rest.

Further complicating the challenge, approximately 90% of corporate data is unstructured,[2] existing in files like Word documents, PDFs and images. Compounding this challenge, sensitive files often mutate—renamed, compressed (ZIPs), or converted (e.g., Excel to PDF)— evading controls. Without visibility into lineage, these changes are invisible to standard sensors, yet this data requires protection equal to structured database information.

Finally, although business-critical data should reside in applications managed by corporate IT, shadow IT is an ongoing issue. Business units frequently deploy unmanaged technologies for a specific purpose without getting IT's buy-in. 97% of the cloud applications that the typical company's employees use exist outside of IT's awareness.[3]

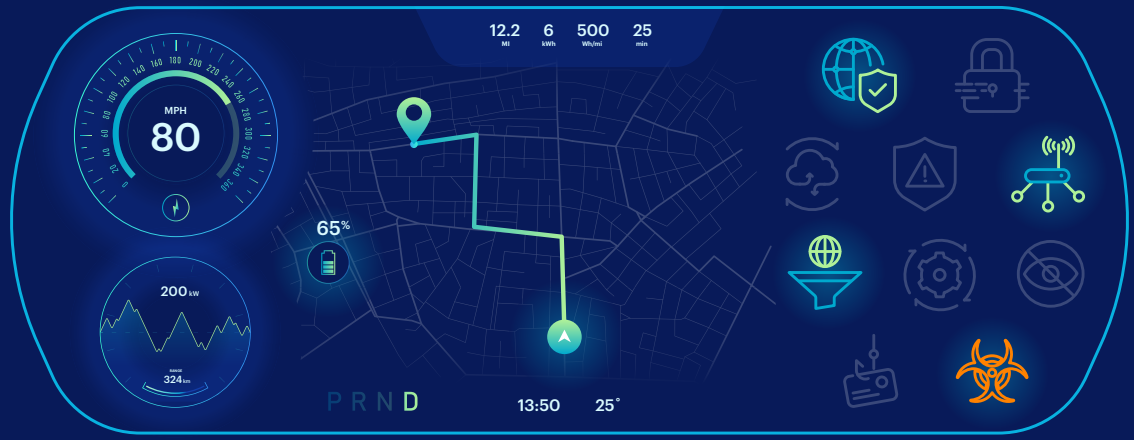
Approximately

90%

of corporate data is unstructured.

88%

of users interacting with personal cloud apps - Shadow IT[4]



[2] IDC. "Untapped Value: What Every Executive Needs to Know About Unstructured Data," August 2023.

[3] Netskope Threat Labs Cloud and Threat Report: 2025.

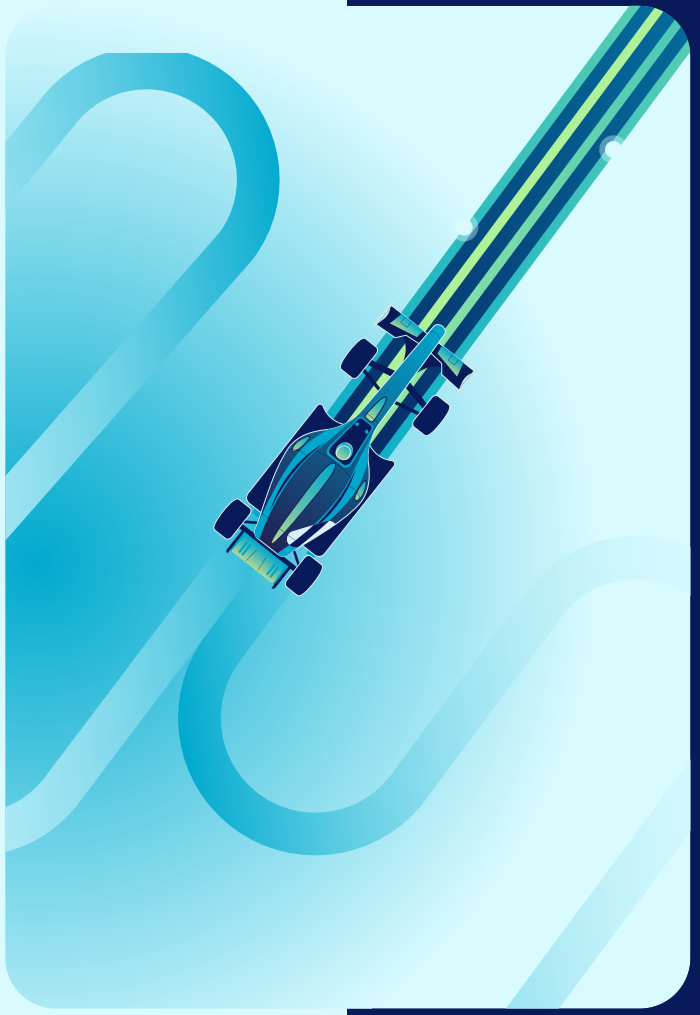
[4] Netskope Threat Labs Cloud and Threat Report: Generative AI, 2025.

Disparate Technologies Fail to Meet the Challenge

Companies do not lack options for protecting individual data types, but usually they need an assortment of solutions to cover all their data. Security teams have had to increase coverage over the years, and this trend is expected to continue as new technologies and vulnerabilities surface.

Endpoint DLP systems do a good job of securing data on corporate endpoints. However, to protect sensitive information in emails, a company needs either email DLP or another solution. Some organizations have a separate solution to secure the usage of AI within their environment. The functionality of this solution might include preventing accidental leakage of corporate data in the public domain, but it might not cover the company's regulatory compliance needs. For insider threats, the organization might have a behavior analytics tool to prevent sabotage. And for discovery and classification of sensitive data, DSPM is the best choice.

The problem is that deploying all these different solutions creates a complex landscape of disparate technologies that strain IT resources and can make corporate data less secure.



"It's time to reimagine data security if you have been treating DSPM and DLP as separate silos. They can work together to form the backbone of a comprehensive approach that not only secures your data but competitively positions your organization to lead in today's data-driven economy."

Ankur Chadda

Marketing Leader for Data Security
Netskope

Unified Data Security

IT teams need a security platform that can protect all types of data while offering single-pane-of-glass visibility. That is the goal of unified data security platforms, which join DSPM and DLP capabilities in a single solution.

Bringing all of a company's data onto the same solution has several major benefits:

- **Improved visibility.** IT staff can look at a single dashboard to understand data security concerns that may exist on premises or in the cloud, across managed and unmanaged data that is in motion, in use, or at rest.
- **Better security.** Disparate systems typically result in a disjointed response to any threat. Conversely, a tightly integrated platform ensures that information about risks or threats gathered by one solution will be shared with the other solutions, enabling a coordinated response everywhere the company stores data.
- **Ease of management.** Administration of the security infrastructure takes less staff time, shifting the security team from constant reactive firefighting to vulnerability remediation, long-term planning, and other strategic initiatives.

"I understand what my policy set looks like across multiple features and applications, versus some of our legacy applications where I had four different places to manage a single application and its features."

VP of Infrastructure

Technology

The Netskope One Approach to Unified Data Security

Netskope One helps organizations shift into a high gear by providing a unified platform for comprehensive data security. It joins together DSPM and DLP with the goal of bringing precision and accuracy to risk detection and threat mitigation.

A key differentiator from alternative solutions is the Netskope One Platform's ability to secure data at rest, in motion, and in use across all key threat vectors. By consolidating these capabilities, it enables all the tools protecting sensitive information to share context across users, applications, and actions.

This approach strengthens security in five key ways:

1. Reducing the company's risk surface: Netskope One controls access to all the web, SaaS, and private applications where data resides
2. Accelerating data discovery
3. Visualizing data lineage: Going beyond static logs to map the entire journey of a file—from origin to mutation to destination—providing a visual evidence trail that connects the dots instantly
4. Enabling automated, real-time control of data risk
5. Supporting scalability: Data policies and profiles can be built once, then leveraged everywhere

Netskope One provides best-in-class breadth and depth of coverage everywhere a company's data resides. Now let's look at the three questions that will help you to assess your organization's environment:

Question 1: How much risk does your surface area pose?

Question 2: How quickly do your security solutions respond to risky behavior?

Question 3: How are you applying DLP policies to your remaining traffic?

"Netskope enables us to quantify data exfiltration and link risky behaviors to individuals, allowing us to take timely action."

Senior Director

Global Insider Risk Program, Major Financial Services Company

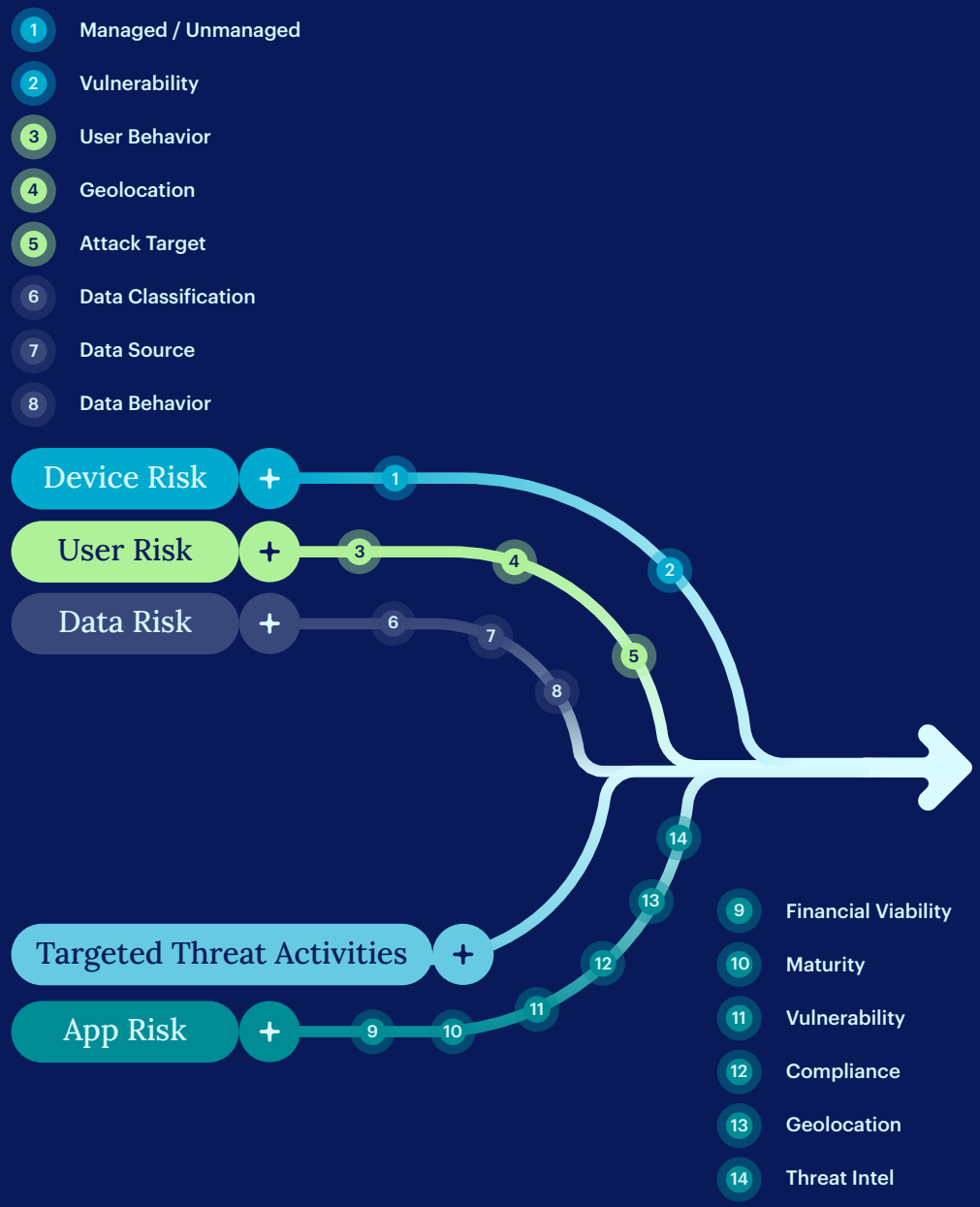
Question 1: How much risk does your surface area pose?

Netskope One makes continuous, adaptive, trust-based policy decisions in real time. Anytime a user attempts to store, move, or manipulate data, the platform evaluates the risk across four vectors:

- **User risk:** Is your data secure from impersonators? Are you able to verify that users are who they claim to be?
- **Device risk:** Is the individual on a managed device, at a known and trusted location?
- **Application risk:** Is the software involved in an IT-managed application? And is this a company or personal instance of the software?
- **Data risk:** Is the data confidential or sensitive corporate information?

Netskope has analyzed and rated more than 80,000 applications and developed 130 categories for URLs. The Netskope One platform sorts traffic accordingly, to accelerate management of any threats. The platform can also differentiate among thousands of SaaS instances.

Netskope One pulls together all this information, then leverages user and entity behavior analytics (UEBA), along with real-time threat intelligence, to rate the user's attempted activity on a scale of risky behaviors.



Question 2: How quickly do your security solutions respond to risky behavior?

After completing the risk analysis, Netskope One Data Security policy enforcement pauses suspect traffic while the user re-authenticates or provides a justification for their behavior. Alternatively, it can automatically block the traffic—in the worst-case scenario, isolating the user and/or the device until a human can evaluate the activity.

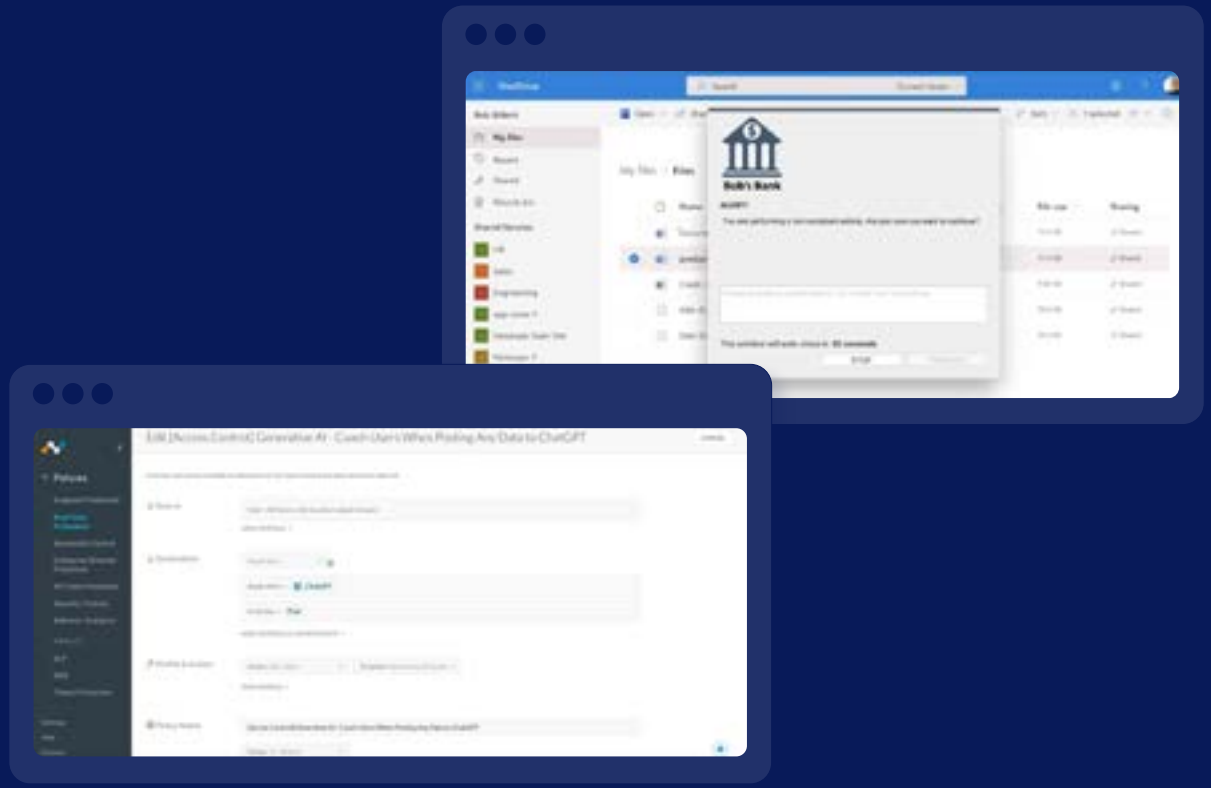
Companies can use Netskope One Data Security to introduce granular controls that, among other things:

- Block malware and content that violates acceptable use policy (AUP)
- Stop cloud-based activities and/or applications known to be risky
- Prevent uploads to any cloud application, or app instance, that IT does not manage

When an incident occurs, speed is critical. Instead of spending days parsing logs manually, data lineage allows analysts to instantly visualize the root cause, slashing MTTR and forensic costs.

One unique feature of Netskope One Data Security is that it can be configured to provide real-time coaching to educate users whose behavior violates corporate data policy.

> "We're getting very concerned about the aggression of [advanced persistent threat actors] going after our data. The Netskope SSE solution helps us really get a handle on that much, much more effectively."
>
> **VP of Infrastructure,**
> Technology Company



Question 3: How are you applying DLP policies to your remaining traffic?

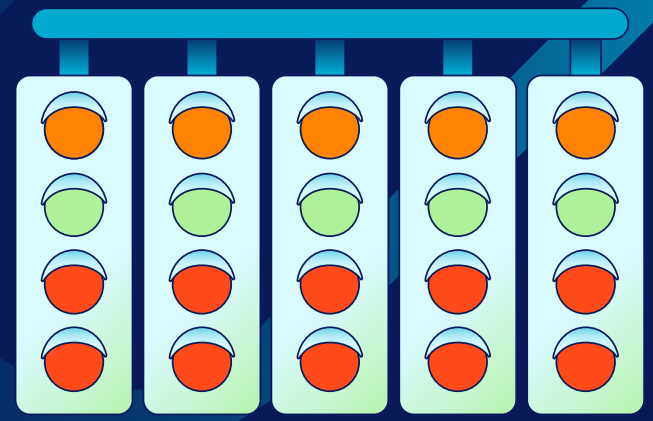
For traffic that gets past DSPM analysis, Netskope One Data Security applies DLP techniques to ensure that users do not exfiltrate any data. The platform's capabilities examine data across emails, endpoints, websites, and various data storage formats, both on premises and in the cloud.

Like earlier iterations of DLP, Netskope One Data Security uses custom regular expressions, keywords, dictionaries, and exact data matching (EDM) and indexed document matching (IDM) to identify data. It gathers context clues from both the platform—factors such as user risk or information from the cloud access security broker (CASB) or SaaS security posture management (SSPM) features—and external sources, such as single sign-on (SSO) or secure email gateway (SEG) integrations. Like the DSPM, Netskope One DLP leverages content inspection using ML models to find PII, PHI, and other types of data.

For the 84% of organizations that must abide by some kind of external compliance framework,[5] these capabilities are crucial. Netskope One comes with 38 predefined legal and regulatory compliance templates, supporting business units around the world in meeting local requirements. Best of all, even as the platform improves compliance, it reduces security friction for users so that it doesn't impede the business's productivity.

"Netskope provides us with the tools and capabilities to securely embrace cloud technologies while maintaining control and compliance."

Security Lead
Apex Group



[5] Source: Coalfire. "Securealities Report: Compliance 2023," May 2023.

Netskope One ML Interprets Both Structured and Unstructured Data

Netskope One uses machine learning (ML) both to determine the content of unstructured data and to categorize data. For example, the platform's image classification process uses a trained ML algorithm to identify sensitive documents such as passports or driver's licenses without examining the text. Meanwhile, optical character recognition (OCR) technology within the platform can extract text from images for analysis.

The ML capabilities built into Netskope One use attributes of both structured and unstructured data to label it as PII, personal health information (PHI), subject to the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA), etc. The platform comes with more than 3,000 data-risk classifiers built in, and companies can develop their own ML-based classifiers as well.

Netskope One can also be trained to look for combinations of identifiers, such as Social Security numbers in tax documents, or to perform a privilege analysis comparing data and user characteristics. Leveraging machine learning in these ways reduces security's operational overhead by minimizing human involvement in routine decision-making, while improving the efficacy of the decisions by eliminating the chance of human error.

Pro Tip

Machine learning reduces security's operational overhead by minimizing human involvement in routine decision-making, while improving the efficacy of the decisions.

Netskope One: The Right Choice for Unified Data Security

Netskope One races ahead of would-be attackers. We combine DLP, DSPM, and data lineage to ensure you see the data, stop the threat, and have the chain of evidence to understand exactly how the breach was attempted.

Our unified platform handles all data sources—both on premises and in the cloud—providing a single-pane dashboard showing concerns, controls, and threat response across the full data life cycle. A Forrester Total Economic Impact study found that the typical Netskope customer achieves these business outcomes:[6]

> "I would definitely say that the risk has been lowered [by deploying Netskope SSE] because we're not fighting fires all the time and we can concentrate on vulnerabilities and actual work instead."
>
> **VP of Digital Experience**
> Financial Services Firm

Business Outcomes

- ✓ **80% reduction in the risk of a severe data breach by external attack**
- ✓ **60% reduction in mean time to resolution (MTTR), driven by single-console visibility and visual data lineage forensics**
- ✓ **10% reduction in infrastructure costs**
- ✓ **80% reduction in help desk ticket volumes**
- ✓ **15% reduction in unplanned downtime**
- ✓ **30% increase in network and security operations effectiveness**
- ✓ **Improved intellectual property (IP) protection from DLP**
- ✓ **Improved regulatory compliance readiness and responsiveness**
- ✓ **Greater alignment with environmental, social, and governance (ESG) goals**

6. Forrester. "The Total Economic Impact of Netskope SSE," October 2024.

A Victory Lap with Netskope One

Winning the race against cyberattackers requires strategy, preparation, and execution. When the pedal hits the metal, it's all or nothing.

Unified data security with Netskope One offers all the capabilities security mechanics need to protect their highly valuable machines:

- **Automate discovery and classification of corporate data wherever it lives and moves**
- **Respond to data exfiltration risks quickly**
- **Achieve compliance and data privacy efficiently**
- **Reduce malicious insider risk significantly**
- **Minimize negligent data exposure**
- **Deliver a frictionless end user experience**
- **Ensure safe organizational AI usage**
- **Manage data lifecycle comprehensively**
- **Satisfy regulators with audit-ready accountability**

"Cybersecurity is a competitive differentiator for us, helping us to attract new clients, particularly from industries that value robust data protection."

CISO
Global Service Company

"Netskope SSE showed us all these issues that we didn't really know we had. We found systems on the internet that weren't going through our security controls … We were shocked [and] we fixed [the issues]."

VP of Digital Experience
Financial Services Firm[7]

Netskope One

Buckle up your data with Netskope One Data Security.

Learn more ⟶

[7] Forrester. "The Total Economic Impact of Netskope SSE," October 2024.

About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

Interested in learning more?

Request a demo

Resources

- The Value of Unified Data Security
- The State of Data Risk Management Report
- Introduction to Netskope One SSE Hands-on Lab
- Introduction to Netskope One Data Loss Prevention (DLP) Hands-on Lab

netskope