netskope

Cloud and Threat Report: 2022 Year In Review

Back to Work: Users and Attackers Across Cloud and Web

BROUGHT TO YOU BY

netskope

THREAT LABS

EXECUTIVE SUMMARY

This edition of the Cloud and Threat Report takes a look back at 2022 and highlights the most significant trends relating to cloud adoption and threats on the web and in the cloud. Compared to 2021, Microsoft OneDrive, Teams, and Sharepoint–all components of the Microsoft 365 App Suite–remained the most popular apps in the enterprise. The most significant change in app use in 2022 was a marked increase in the percentage of users uploading content in these and a variety of other cloud apps.

Collaboration apps, like Microsoft Teams, saw a huge increase in popularity at the beginning of the COVID-19 pandemic, when many companies shifted to remote and hybrid work. While remote work decreased slightly during 2022, led by the Asia region and retail industry, it has not yet dropped below its April 2020 levels and the popularity of collaboration apps continues. This continuing trend of remote and hybrid work underscores the importance of providing remote workers secure access to private and cloud organization resources and to the web.

Cloud malware delivery increased in 2022 after having remained constant in 2021, caused by an increase in the total number of apps abused to deliver malware and the quantity of malware downloads coming from the most popular apps. Microsoft OneDrive's position as the most popular cloud storage app in the enterprise also meant that it continued to lead the charts in 2022 as the origin of the plurality of cloud malware downloads.

Phishing, scams, credit card skimmers, exploit kits, and other malicious web content also continued to rise in 2022. Compromised sites, sites created using free hosting services, and fake websites hosting seemingly legitimate content have helped attackers disguise malicious web content, making it difficult to filter malicious content using URL categorization alone. The rise in cloud malware delivery and malicious web content underscores the importance of inspecting all content, from all destinations, for both web and cloud.

REPORT HIGHLIGHTS

- OneDrive is the most popular cloud app in the enterprise, with more than **40%** of people using it daily and more than **25%** uploading content to it daily.
- While remote work decreased in 2022, it has yet to recede below its April 2020 levels at the start of the COVID-19 pandemic.
- Cloud malware delivery increased, with malware downloads from **401** different cloud apps, led by Microsoft OneDrive.
- Cloud malware delivery is a global challenge, common in all industry verticals and geographies, led by the North America region and the telecom industry.
- **94.4%** of malicious web content was accessed from compromised sites, free hosting services, and fake websites used to spread malicious content, with only **5.6%** coming from so-called uncategorized sites.

ABOUT THIS REPORT

Netskope provides threat and data protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization. This report contains information about detections raised by Netskope's Next Generation Secure Web Gateway (SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the period starting January 1, 2021 through December 9, 2022. Stats are reflection of attacker tactics, user behavior, and organization policy.

Netskope Threat Labs

Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DEF CON, Black Hat, and RSA.

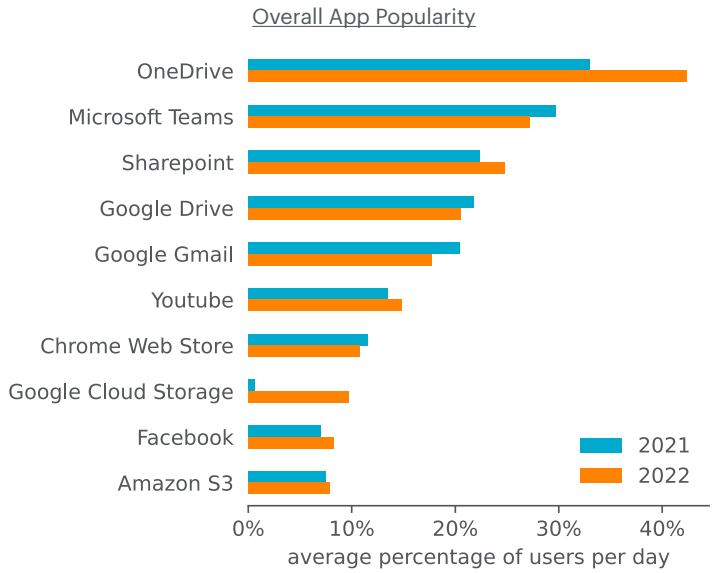
Microsoft 365 Dominates the Enterprise

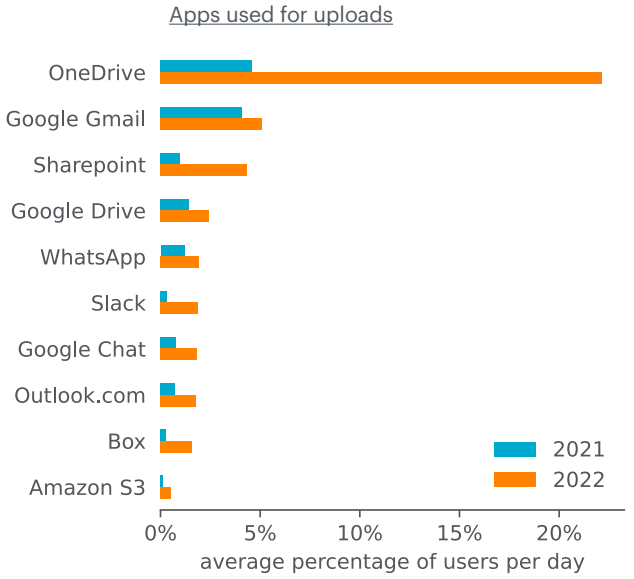
In both 2021 and 2022, Microsoft OneDrive, Teams, and Sharepoint were the three most popular apps overall. On an average day in 2022, more than 40% of users on the Netskope Security Cloud platform used OneDrive, more than 25% used Teams, and more than 20% used Sharepoint. By comparison, Google Drive, part of the Google Workspaces suite, was used by nearly half as many users as Microsoft OneDrive. In the top ten, the popularity of each app remained largely unchanged with one exception: Google Cloud Storage saw significant increase in usage as it gained popularity for object hosting across the web.

Where more drastic changes were observed was in how many users uploaded data to cloud apps, with increases across the board. Microsoft OneDrive saw the largest increase, from 5% of users uploading data to OneDrive on the average day in 2021, to more than 20% uploading data daily in 2022. All other apps in the top ten also experienced increases, including webmail apps Gmail and Outlook.com, messaging app WhatsApp, and chat app Slack.

By industry vertical, OneDrive consistently showed up as a top app, although the popularity varied by industry. It was highest in financial services, at 51%, and lowest in healthcare at 27%. Its popularity increased in all reported industry verticals compared to 2021. OneDrive also consistently showed up as a top app regionally. It was most popular in Australia, at 52%, and least popular in Europe, at 33%.

Widespread cloud app usage in the enterprise presents multiple challenges. First, the apps listed here are used to conduct internal business, to interact with customers and partners, and for personal reasons. Controlling the flow of data into these multiple instances (company and personal) can help prevent sensitive data ending up in the wrong place. Restricting apps that do not serve any business purpose can also reduce the risk surface for data loss and data exposure. Cloud apps also present a risk for the infiltration of malware and other malicious content, which will be discussed in detail in subsequent sections.





Remote Work Continues for Most Knowledge Workers

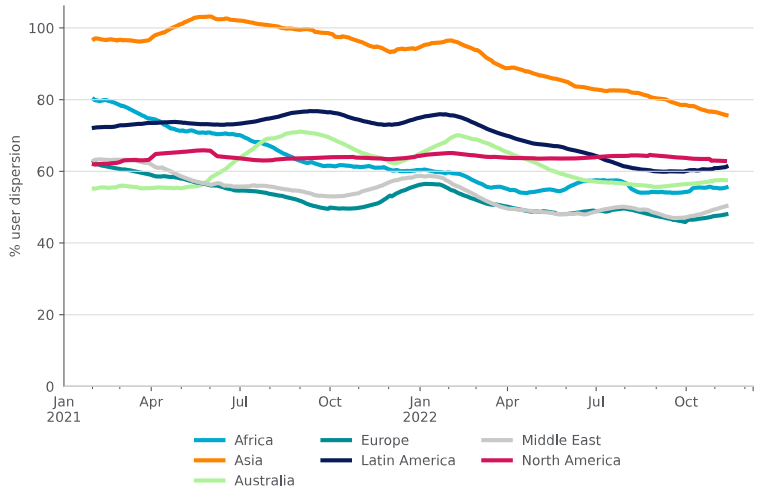
At the beginning of the COVID-19 pandemic, Netskope Threat Labs tracked a significant increase in remote work. User dispersion, the ratio of the number of users on the Netskope platform to the number of network locations from which their traffic originates, increased from 26% to 66% in early 2020 at the start of the pandemic. User dispersion continued to increase, topping out at 78% and then gradually decreasing back to 66% at the end of 2022.

Regionally, Asia has the highest user dispersion and also had the biggest drop in 2022. User dispersion stayed near 100% for most of 2021 and is currently on a downward trajectory. Meanwhile, the other six regions reported remained relatively close to each other throughout the past two years, closing out 2022 between 55% and 65%.

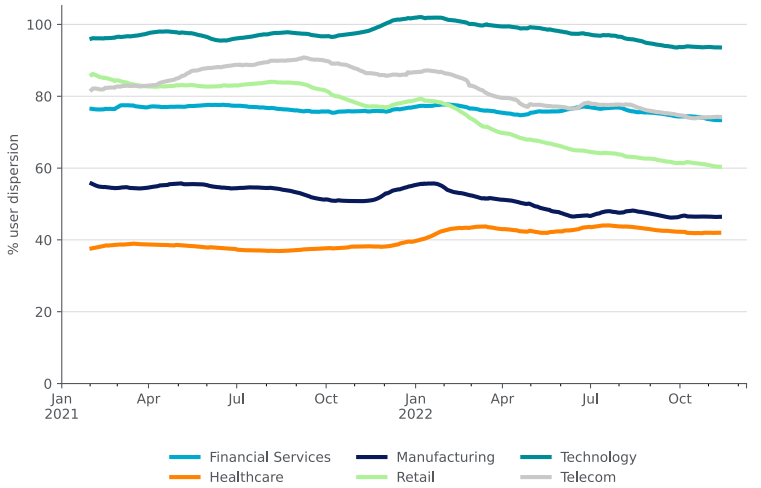
By industry vertical, there is much more variation. Healthcare remained the vertical with the lowest dispersion throughout the past two years, despite modest increases. At the other end of the spectrum was technology, which remained the industry with the highest percentage over the past two years, despite modest decreases. The vertical with the largest decrease was retail, which began 2021 at over 85% and finished 2022 at 60%. All other verticals experienced some fluctuation throughout the past two years, and ended 2022 below where they started in 2021.

Remote and hybrid work poses multiple cybersecurity challenges, including how to securely provide users access to the company resources they need to do their jobs and how to securely provide users access to the internet at scale. A zero trust network access (ZTNA) solution can help obviate the need for a traditional VPN while also ensuring that users are only granted access to the resources they need to perform their jobs. A cloud-delivered secure web gateway (SWG) and firewall can also obviate the need for a traditional VPN by enabling users to connect directly to the internet.

Remote work by region



Remote work by industry



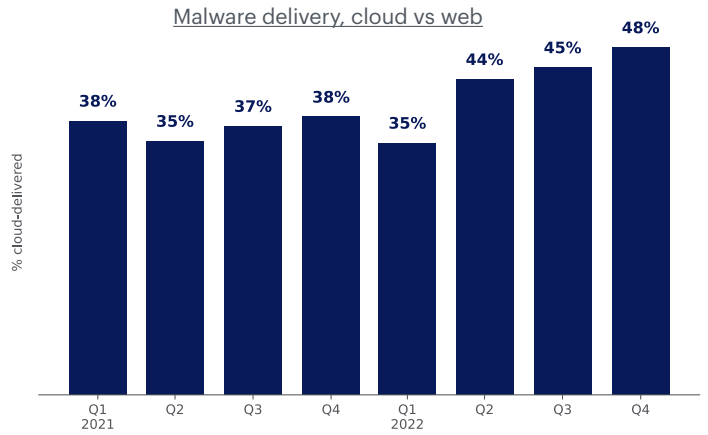
Cloud-delivered Malware Resumes its Rise

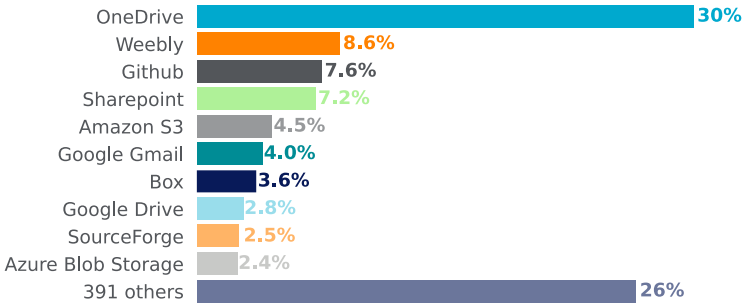
In 2022, the percentage of malware downloads increased, ending the year ten points higher than in 2021. Cloud malware downloads had plateaued in 2021 and remained largely unchanged throughout the year. In Q4 2022, 48% of HTTP/HTTPS malware downloads originated from cloud apps, such as Microsoft OneDrive, while the remaining 52% of malware downloads originated from traditional websites. Overall, Netskope detected malware downloads from 401 distinct cloud apps in 2022, a 2.9x increase from 2021.

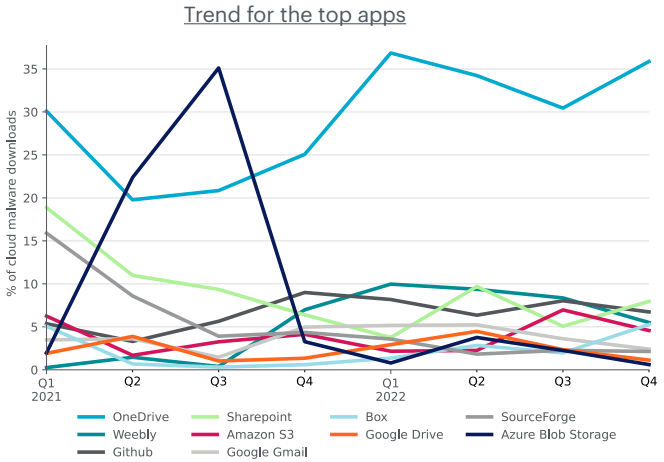
In 2022, 30% of all cloud malware downloads originated from Microsoft OneDrive. This is a reflection of attacker tactics, user behavior, and company policy. For a cloud malware download to occur, the malware must have been successfully uploaded to and shared from the cloud app, the user must have been tricked into downloading the malware, and company policy must have allowed the user access to file. One of the main contributing factors here is the popularity of OneDrive, both making it a target for abuse and increasing probability of user exposure. OneDrive held the top spot in 2021 as well, but by a smaller margin, as malware downloads from Sharepoint, SourceForge, and Azure Blob Storage were higher in 2021.

Generally, all of the top apps for malware downloads made the list because of their popularity in the enterprise. The apps included free hosting services (Weebly), free software hosting services (GitHub and SourceForge), free webmail services (Google Gmail), and free cloud storage apps (Google Drive, Box). Not only are these apps popular in the enterprise, they are also free and therefore inexpensive for attackers to abuse.

To protect themselves against the rise in cloud-delivered malware, organizations should ensure that all HTTP and HTTPS traffic, including traffic for popular cloud apps (both company and personal instances), is inspected for malicious content. Second, organizations can reduce their risk surface by restricting downloads from apps that serve no valid business purpose. Restricting or applying extra scrutiny to file types commonly abused by attackers, like EXE, DLL, BAT, REG, ISO, and LNK, can also reduce malware risk.







Cloud Malware Delivery is a Global Challenge

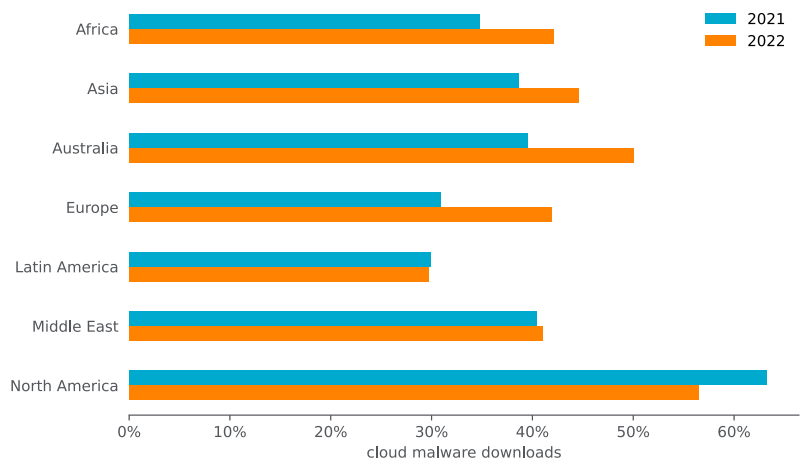
While cloud malware downloads increased on average in 2022, the greatest regional increases occurred in Australia and Europe, while North America saw the largest decrease. Despite the decrease, the percentage of cloud malware downloads still remains highest in North America. In all seven regions, the plurality of cloud malware downloads originated from Microsoft OneDrive, a reflection of the global popularity of OneDrive.

By industry vertical, the largest increases in cloud malware downloads occurred in healthcare, manufacturing, and telecom. Despite the large increase, manufacturing still has the lowest percentage of cloud malware downloads of any of the reported verticals. The plurality of cloud malware downloads originated from Microsoft OneDrive in most verticals, with Google Drive taking the top spot in retail and Azure Blob Storage leading in healthcare. The rankings are a reflection of both attacker activity (where attackers host malware), user activity (where users are likely to download files), and company policy (which apps users are allowed to access).

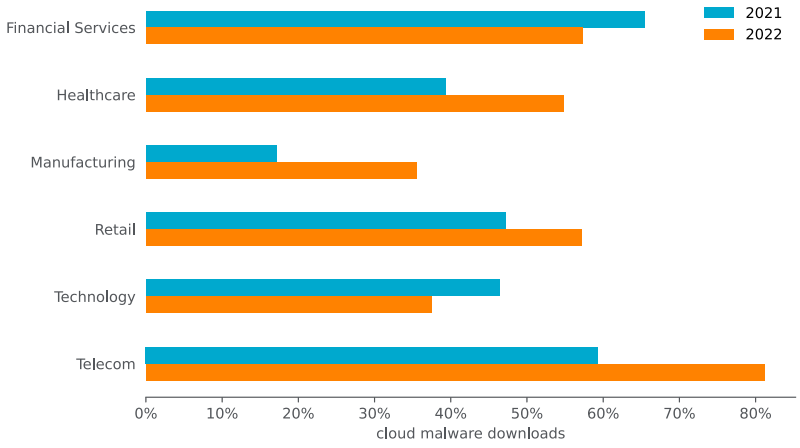
Top Apps for Malware Downloads By Vertical

Financial Services	Microsoft OneDrive
Telecom	Microsoft OneDrive
Healthcare	Azure Blob Storage
Technology	Microsoft OneDrive
Manufacturing	Microsoft OneDrive
Retail	Google Drive

Cloud Malware Downloads by Region



Cloud Malware Downloads by Industry Vertical

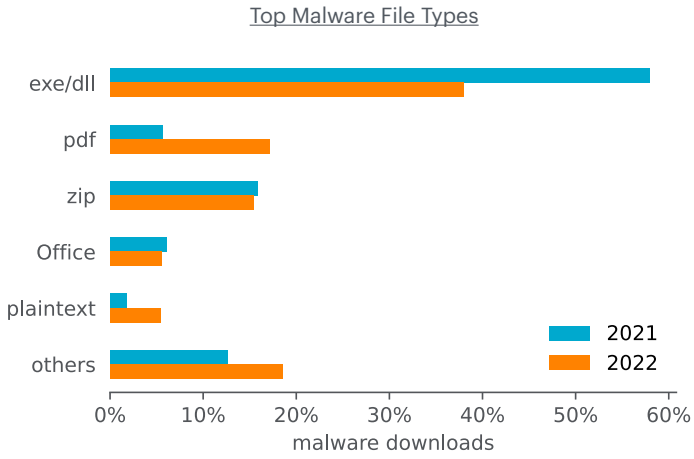


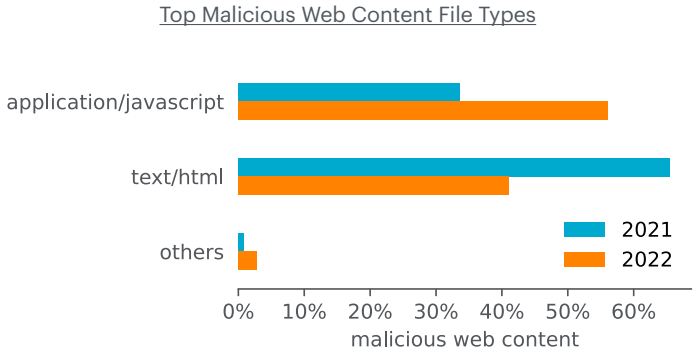
Malicious Content Lurks All Over the Web

The preceding section focused on malware downloads, where portable executable files (EXE and DLL files) accounted for the plurality of the malware downloads in 2022, down 20 points from 2021. Malicious PDF files saw the biggest increase in 2022, followed by plaintext files (including Powershell, Python, and other scripts).

This section focuses on malicious web content: phishing pages, scams, credit card skimmers, bitcoin miners, drive-by-downloads, HTML smuggling, exploit kits, and more. Malicious web content is typically JavaScript content that is executed by the web browser. The JavaScript is typically either a standalone file or is embedded in an HTML file. Other, less common file types include CSS, SVG, or XML files, all containing embedded JavaScript.

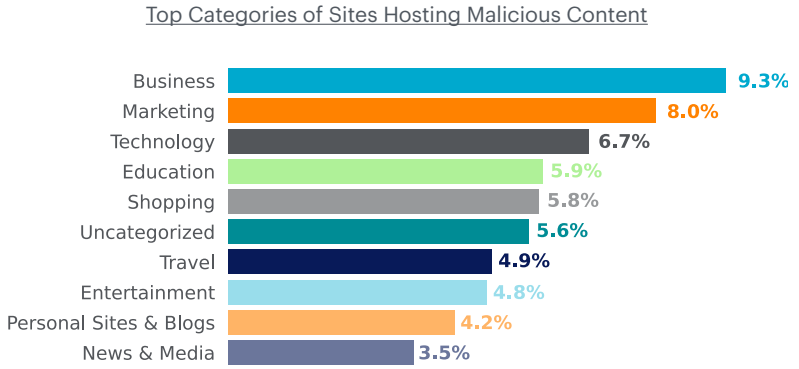
Where is all of that malicious web content hosted? This section examines what types of sites were hosting malicious content when it was first detected by Netskope. In the top ten are two categories that one might have expected to see: uncategorized sites and marketing sites. Uncategorized sites are sites that have not been seen frequently enough or do not host enough content to have been categorized. Malicious sites often fall into this category when they are first created. Marketing includes online ads, which are often abused by attackers for malvertising.





Uncategorized and marketing sites account for only 13.6% of the total malicious web content access, with the majority of the malicious content being spread over a variety of other categories, with no single dominant category. Attackers have been populating their websites with enough content to make them seem legitimate, and only using them to host malicious content after they have been around long enough to blend in. They have also been abusing free hosting services and compromising existing websites to deliver malicious content.

Organizations can protect themselves against malicious web content that is spread all over the web by blocking risky content like ads, uncategorized sites, newly registered domains, and newly observed domains. Remote browser isolation (RBI) can also reduce the risk surface for a wider variety of categories. But the majority of malicious content users encounter is hosted elsewhere on the web. Using a secure web gateway that can inspect and block malicious content from any source can greatly reduce this risk against both known and unknown malicious content. Script blockers can also protect users from running malicious JavaScript. Ultimately, using a combination of all of these technologies can greatly reduce the risk of malicious web content.



RECOMMENDATIONS

To protect against evolving threats and cloud risks, Netskope recommends taking the following steps:

1. Deploy multi-layered, inline threat protection for all cloud and web traffic to block inbound malware and outbound malware communications. Cloud security platforms remove the tradeoff of performance versus security, enabling you to scan all content and deliver a fast user experience.

2. Enforce granular policy controls to limit data flow, including flow to and from apps, between company and personal instances, among users, to and from the web, adapting the policies based on device, location, and risk.

3. Deploy cloud data protection to limit the movement of sensitive data, including preventing its movement to unauthorized devices, apps, and instances.

4. Invoke real-time coaching to users to use safer app alternatives to protect data, justify unusual data activity, and provide step-up authentication for risky conditions within business transactions.

5. Reduce browsing risk for newly registered domains, newly observed domains, uncategorized websites, and other security risk categories by using remote browser isolation (RBI).

6. Mitigate the risk of stolen credentials by enabling multi-factor authentication (MFA) and extend MFA to unmanaged apps via your identity service provider or SSE platform.

7. Use behavioral analytics to detect compromised accounts, compromised devices, and insider threats.

8. Enable zero trust principles for least privilege access to data with continuous monitoring and reporting to uncover unknown risks using a closed loop to then further refine access policies.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on how to mitigate risk, contact us today:
WWW.NETSKOPE.COM/REQUEST-DEMO

BROUGHT TO YOU BY

netskope
THREAT LABS