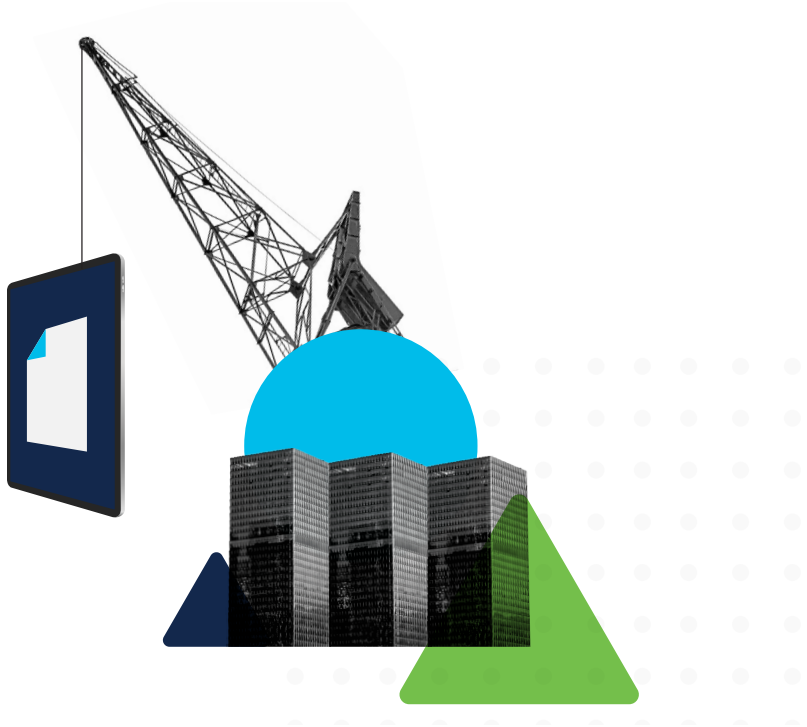
Cisco Umbrella

2021 cloud application security

The current landscape, risks, and solutions



About this report

This report features data drawn from Cisco Umbrella's DNS resolution and application discovery capabilities. The data is from paying Cisco Umbrella customers and has been de-identified, aggregated into categories, and anonymized. The data consists of IP addresses, the owners of IP addresses, locations, the types of services accessed via IP, and whether applications and services were blocked by customers of our software. (Customers may block specific services or software based on threat intelligence and their own security policies and controls.) In some cases, outliers were removed to focus on the primary applications and trends.

Most of the data was collected on a daily basis between November 1, 2020, and March 29, 2021. In some instances, where stated, data was collected during the 2020 calendar year or from other time periods as disclosed.

Cisco Umbrella's global cloud architecture processes 620 billion internet requests every day at the moment a request is made. This real-time DNS data is further enriched with diverse public and private data feeds. Our application discovery service discovers tens of thousands of applications annually, controlling more than 3,000 applications and counting.

With such a massive and diverse data set, we have a unique perspective on global DNS and cloud application traffic. Our threat analysis – based on aggregated DNS query logs paired with scrubbed and anonymized customer demographic information – is ideally suited for uncovering patterns that signal malicious behavior.

All analyses, statements, and claims made in this report, unless otherwise cited and sourced, are derived from Cisco Umbrella's DNS resolution and application discovery capabilities. As such, the findings discussed in this report will reflect the perspectives limited by Cisco Umbrella capabilities.

SaaS is the way we work now – but are we working the way we want?

Occasionally, we have one of these rare moments where the world splits into a "before" and an "after" – a major turning point when nothing will ever be quite the same.

March 2020 feels like one of those moments.

Suddenly, our work lives and home lives are blending in ways we never could have imagined. And we're finding that the key to making it work – to striking a new balance, to building our way toward a better tomorrow – is in cloud-based applications and services (also known as software-as-a-service [SaaS]).

But, in this new world of work, we find ourselves wrestling with new questions and challenges and boundaries. When it comes to using cloud apps, where does work stop and personal use begin? Is streaming a little music while working on a project a misuse of company resources? Are we opening ourselves up to unacceptable risks using unapproved teleconferencing or collaboration or storage tools?

This report explores the world of these cloud-based apps – their current usage, the risks and the opportunities, and what we can do to move forward with them the right way.

Key cloud application insights

1 Cloud apps on the rise

Internet traffic from cloud-based applications grew 33% in 2020. Tracking along with that, Cisco Umbrella's app discovery service experienced 20% growth in the number of applications controllable by our service – i.e., apps we can see, assess the risk of, andblock if necessary.

2 Businesses block what they don't use

The cloud apps that get blocked by your employer greatly depend on the office productivity applications your team primarily uses. For instance, Microsoft Office 365 generates 22X more internet traffic than its next closest competitor – Google. So, if your business is Team Microsoft, you may find Google apps like Gmail are more frequently blocked in your organization.

3 Shadow IT still limits visibility

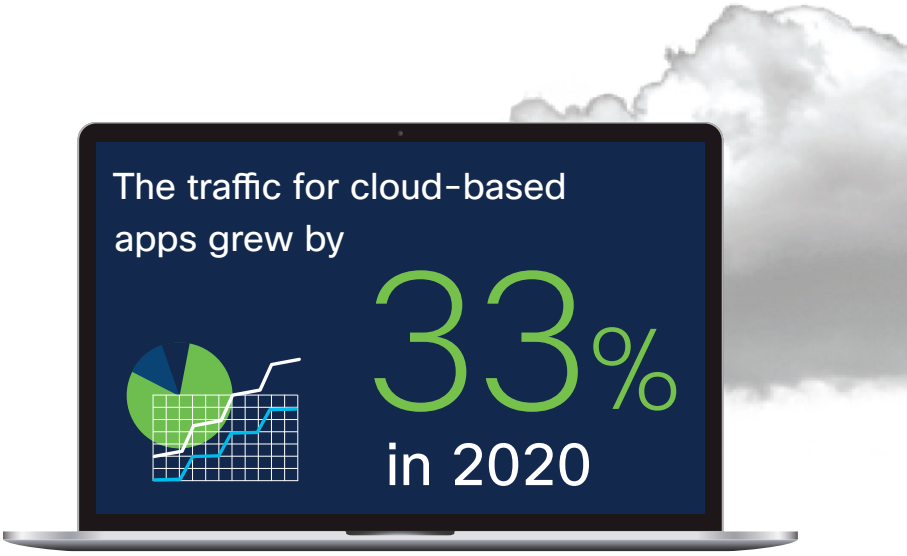
The move to remote work and an increase in bring-your-own-device (BYOD) policies are making it more difficult for IT teams to maintain oversight over cloud apps – particularly in areas like DIY tech support and streaming media players.

4 More social, more media

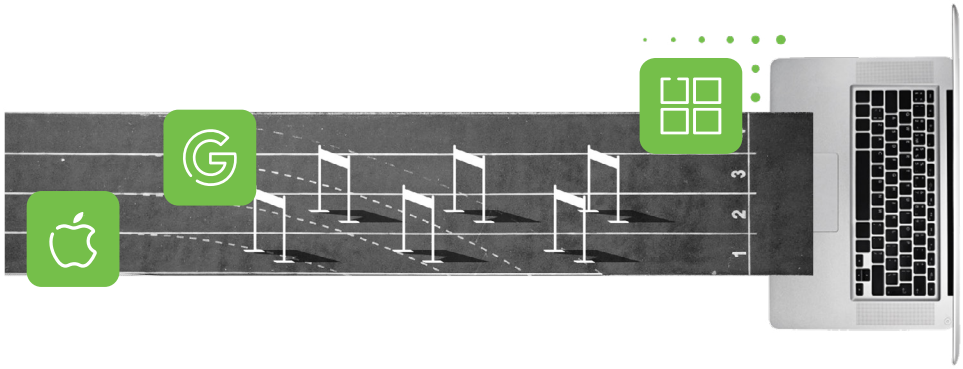
As work-from-home (WFH) practices continue, our work and personal lives blur together, leading to a significant rise in the use of social and media applications on the job.

5 Data loss a risk with cloud storage

As users continue to embrace cloud storage services unapproved by IT, data protection remains a major issue, leading to a considerable number of blocked queries to those services. So, which storage did customers of our app discovery service block the most? Apple iCloud and Dropbox are blocked at 20X and 16X the rate of other cloud storage providers.



Productivity apps: One person's gain is another one's loss



IT sprawl and complexity are dragons that corporate IT departments are constantly trying to tame. The number of cloud-based apps that an organization maintains varies widely – small-to-medium businesses may utilize dozens of apps; with larger enterprises, that number can be in the thousands.

So, it's no surprise that IT would want to consolidate and standardize the cloud applications approved for use. However, creating a short list of approved applications typically means that many other apps are blocked – however safe or legitimate they might be.

For instance, for the most part, the business world is divided across three major office productivity platforms: Microsoft Office 365, Google Workspace, and, to a lesser extent, Apple iWork.

Based on Cisco Umbrella's measurement of app queries, Microsoft leads the office productivity category by far. Cisco Umbrella sees this in terms of the DNS activity associated with Microsoft Office applications, which run at 18X the activity of its closest competitor, Google. Based solely on the DNS queries that Cisco Umbrella tracks, Team Microsoft is also growing faster than the other productivity platforms – at a rate of about 58% (compared to roughly 30% for Google).

What this means, then, is that, because IT departments focus exclusively on this platform, applications "outside the circle" of Microsoft products tend to be restricted at higher rates. So, for example, Gmail, Google Hangouts, and Apple iCloud are blocked on Cisco Umbrella's app discovery service at 10X the rate of Microsoft apps.

This can be challenging if certain departments within your organization depend on "outsider" apps for particular aspects of their work. Consider adopting a solution that allows you to selectively block or allow the use of specific applications, rather than a blanket ban on everything outside of your productivity suite.

Apps at a Glance

Office Productivity

Challenge: Most organizations have an approved productivity suite, but some employees and partners may use outside tools instead or in addition. These unsanctioned tools can be a drain on productivity or a way for bad actors to exfiltrate sensitive files and data from the organization.

Solution: Cisco Umbrella's application and category blocking empowers organizations to restrict unapproved or higher-risk productivity apps. And with approved tools, IT can allow the corporate instance to run, but block all other instances, helping sidestep distractions and the risk of data loss.

New needs, new tools, new risks

Centralizing IT onto just a few cloud-based tools and platforms has been facing some stiff headwinds since the COVID-19 pandemic first struck in early 2020. As WFH and BYOD policies quickly took hold, there came with them a rise in the use of tools that had previously been sideshows or shadow IT – in particular:

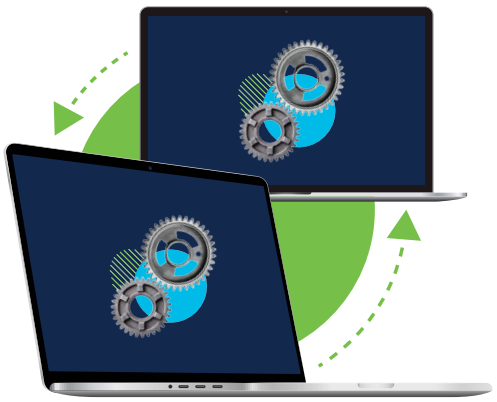
Cloud storage services - like iCloud and Dropbox

Remote desktop software – like TeamViewer

Media streaming software and websites – like TikTok

Aside from the obvious inefficiencies of a fragmented IT footprint, there are significant risks that arise as employees and associates introduce unapproved apps or shadow IT into the work environment. By far the greatest is the loss of visibility into what's happening on users' endpoint devices. This in turn leads to the risk of data exfiltration, as we'll see later on.

Remote tools with far-from-remote risks



47–55%

of recent ransomware attacks used Remote Desktop Protocol as the attack vector.

Another major challenge for IT teams is a rise in the use of unauthorized remote desktop, remote monitoring, and virtual PC software. There are a variety of reasons for this growth, but the simplest is that working from a remote office generally means getting remote support.

But, if workers can't get the technical support they need when they need it – an increasing likelihood with the anytime, anywhere nature of pandemic work – they may turn to their personal support network and use whatever tools are at their disposal, whether they're approved or not. And this can leave them open to attacks.

Two independent analyses of the vectors used in successful ransomware attacks indicate that the most exploited vector is Remote Desktop Protocol (RDP), which was used in 47 to 55% of attacks.[1]

A look at top blocked applications, as documented by Cisco Umbrella's app discovery service, reveals that TeamViewer, a free remote desktop application, amassed more blocks than any other software – averaging over 3 billion blocked DNS requests every day. And it's little wonder, considering the potential risks it holds. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently published an advisory concerning an intrusion into a Florida water treatment facility by an attacker who used TeamViewer in an attempt to change the water supply's chemical composition.

Mitigating the security risks of these remote tools will be an ongoing, two-pronged effort – improving awareness and training among workers about this software, while also implementing cloud access security broker (CASB) controls (like those found in Cisco Umbrella Shadow IT Discovery and App Blocking).

Apps at a Glance

Remote Desktop Protocol (RDP)

Challenge: Outside of official help desk services, RDP has the greatest potential for abuse and has become a major vector for ransomware attacks.

Solution: Cisco Umbrella's application discovery and blocking capabilities can streamline and automate the task of identifying and blocking rogue RDP queries.

A social and streaming free-for-all

Finally, we come to the area that is truly the Wild West for IT teams – social media and entertainment streaming. While a few platforms (like LinkedIn) are seen as having some role in workplace life, most are viewed as strictly personal services that have no place during work hours – until now.

As remote work and personal life blur together, drawing clear lines between the apps used in those once-separate spheres becomes more and more difficult. If streaming music helps a worker focus on the work at hand, is banning streaming actually impairing productivity? If collaboration is key to innovation, should we be preventing colleagues from messaging on social networking sites?

Unsurprisingly, as these lines blur, social media and entertainment services register some of the highest daily internet query rates of all cloud-based applications. Facebook and YouTube remain as popular as ever, having grown 40% (as measured in query volume by Cisco Umbrella) over our reporting period; they now drive more than 10 billion queries daily – about 30X more than others in their category. TikTok, the new kid on the block, grew by an astonishing 102%, overtaking Netflix for third place.

Obviously, some of this activity can be seen simply as wasted time for the employer. But, as separating approved and blocked behavior grows more challenging – and as businesses discover some of these activities may actually hold some workplace benefits – IT teams will have to learn to strike the right balance to keep control of their bandwidth. Here again, increasing awareness of the risks of these apps, clarifying company policies, and clearly defining approved apps will help organizations tame this new digital frontier.

Apps at a Glance

Social and Streaming Media

Challenge: Streaming media and social sites can improve employee productivity and be a source of valuable information in some situations. But, without limits, they can also be a distraction, a drain on corporate resources, and even a path to data exfiltration.

Solution: Cisco Umbrella's application discovery, risk rating, and category and app blocking can all help your organization manage these apps. Granular app controls go even deeper, allowing IT to block specific actions like uploading files, posting, or sharing attachments.

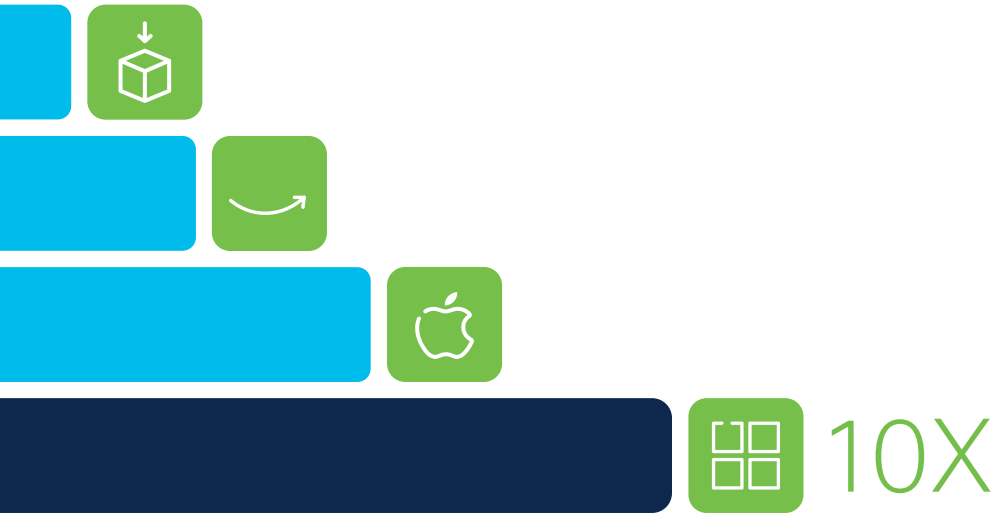
More cloud data storage, more potential data loss

In this new world of work, perhaps the greatest challenge is also the most overlooked: protecting valuable data from being lost or stolen. This is particularly true when it comes to cloud storage services.

Today, there are more cloud storage applications than ever. And, unfortunately, many organizations have an "anything goes" mentality when it comes to these services – use the apps you want, how, where, and when you want. Obviously this comes with some complications – not only in the increased potential for malware infections, but also in the heightened risk of malicious or inadvertent data loss.

Cloud storage services produce some of the highest rates of DNS activity that we track at Cisco. And, much like we discussed with productivity apps, most organizations have one preferred platform, blocking any alternatives. For instance, Microsoft Azure runs 50 to 60 billion daily internet transactions – 3X as much as the next largest storage provider, Apple iCloud. However, users don't always use the platform that IT prefers. We can see this in the way that Apple iCloud and Dropbox are being blocked at 20X and 16X rate of other cloud storage providers.

It's time to put an end to this fragmented system of storage services. Today's organizations must develop a thoughtful cloud storage adoption strategy, along with appropriate data loss prevention (DLP) controls and the capability to monitor and alert on data loss incidents and cloud malware infections. This in turn requires a carefully considered approach with the right balance of technology, process controls, IT knowledge, and employee awareness.

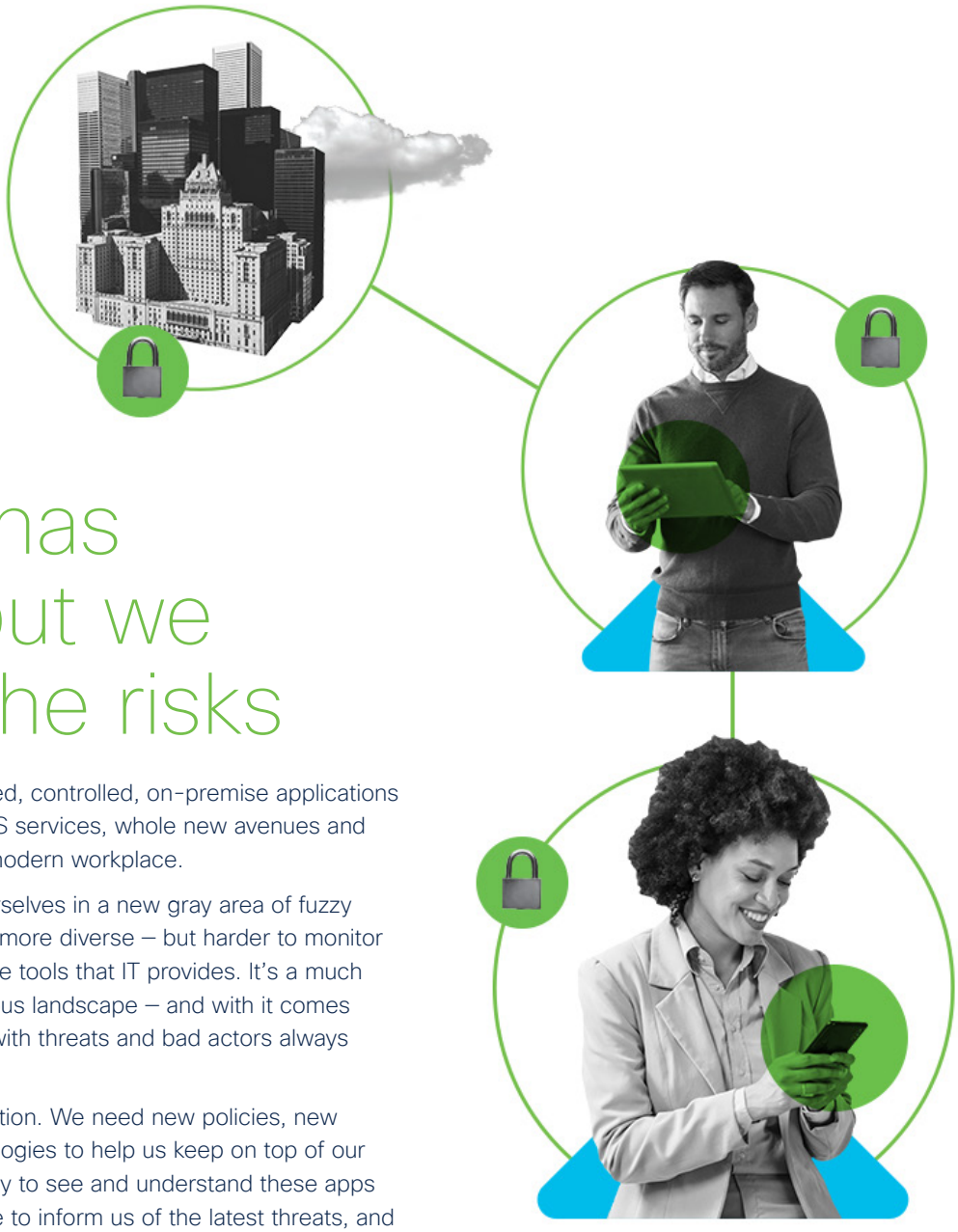


Apps at a Glance

Cloud Storage Services

Challenge: Cloud storage usage is on the rise – and with it comes greater risk. IT needs to monitor the use of these apps and protect data assets from being exfiltrated. Cloud malware is a particular risk.

Solution: Cisco Umbrella's cloud malware detection functionality automatically sends new, existing, and recently modified files in cloud-based storage services for malware scanning and enforcement.



The cloud has no limit – but we must limit the risks

As we've made the leap from centralized, controlled, on-premise applications to the wider world of cloud-based SaaS services, whole new avenues and opportunities have opened up for the modern workplace.

But, in taking this leap, we've found ourselves in a new gray area of fuzzy borders and hidden risks. Services are more diverse – but harder to monitor and manage. Users don't feel tied to the tools that IT provides. It's a much more distributed, fragmented, amorphous landscape – and with it comes greater risk of data loss and malware, with threats and bad actors always hovering just out of sight.

In this new world, we can't rely on tradition. We need new policies, new procedures, and above all, new technologies to help us keep on top of our cloud applications. We need the visibility to see and understand these apps and the risks they pose, the intelligence to inform us of the latest threats, and the functionality to enforce the right policies, to respond to issues as they arise, and to control and block apps, wherever they're being used.

Now that you know the trends and the risks, it's time to start looking for the solutions. Together, we can reap the benefits of cloud-based applications, while also ensuring our data, our users, and our organizations have the protection they need, both today and tomorrow.

Cisco Umbrella

About Cisco, Cisco Secure, and Cisco Umbrella

For 36 years, Cisco has worked with hundreds of thousands of companies to secure users, devices, applications, and data from a growing number of cyber threats. The world's largest security vendor,we protect 100% of the Fortune 100.

Cisco Secure is built on the principle of better security, not more security. Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use – and that it all works together. We understand that customers want to cut through the complexity and noise and feel confident in their security, and Cisco Secure delivers.

We empower the security community with the confidence that they're safe from threats now and in the future with the Cisco SecureX platform. Together with Cisco Umbrella – our multi-function, cloud-native security service – we enable the world to connect to the internet on any device with confidence. We provide a secure, reliable, and fast internet experience to more than 24,000 customers globally.

Cisco Umbrella protects against more than 3 million malicious domains and IPs, while discovering over 60,000 new malicious destinations (domains, IPs, and URLs) every day. Each node of attack infrastructure is an opportunity to identify and neutralize before it can be used for new attacks.

Learn more about how to protect yourself from threats:

Join a demo

1. "Want to Avoid Ransomware Attacks? Start by Fighting Your Shadow IT," Information Security Buzz, November 12, 2020