REPORT

McAfee

Cloud Adoption and Risk Report

Work from Home Edition

Cloud Adoption and Risk Report

Work from Home Edition

The recent work from home mandate has dramatically changed how we live and work. Organizations are getting creative about how they can continue to operate productively when most of their employees are working from home. In normal times, most employees would be expected to work in the office, on the internal network. For anyone working remotely, a VPN could be used to access internal applications. At any given time, only a small percentage of employees would be working from home.[1] COVID-19 has turned this reality completely upside down as most corporate offices, cinemas, streets, and stores have been left eerily empty and our desks and conference rooms are gathering dust.

So how does this affect cloud service usage? In March 2020, around the same time most large companies imposed travel restrictions, large industry events were canceled, some countries and states imposed a shelter-in-place order, and more people worked remotely, Microsoft shared that its cloud services were seeing growth as high as 775%.[2] While some of this growth may normalize, a fundamental shift has occurred in business. Remote working is the new normal. Even after the pandemic, how we work may never be the same.

To bring more insight into the impact of working from home on the adoption and use of cloud services, McAfee aggregated and anonymized cloud usage data from more than 30 million McAfee® MVISION Cloud users worldwide between January and April 2020. This data set represents companies in all major industries across the globe, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

Key Findings

- Overall enterprise use of cloud services spiked by 50% with manufacturing and financial services companies increasing the most.
- Collaboration services saw an increase of up to 600% in usage. Not surprisingly, education is driving this increase, while government and financial services closely follow.
- External attacks on cloud accounts increased 630%, with the transportation, government, and manufacturing verticals most affected.

Connect With Us

Overall Cloud Service Usage Increases

Our data shows a 50% increase overall in enterprise cloud use across all industries. Most notably, manufacturing experienced the largest increase of 144%, followed by education with 114%. Our analysis showed an increase across all cloud categories. For example, the financial services sector increased usage of collaboration services such as Microsoft 365 by 123%, while also seeing an increase in use of business services such as Salesforce by 61%.

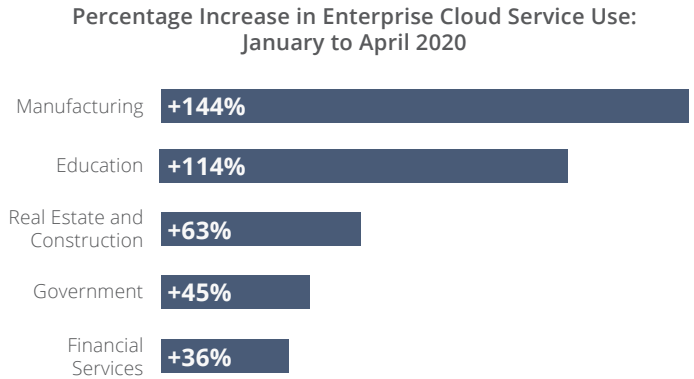


Figure 1. Increase in cloud service use by vertical.

Collaboration Services Experience Largest Increase in Usage

Enterprise use of collaboration cloud services has more than doubled since the beginning of the year with Zoom (+350%), Microsoft Teams (+300%), and Slack (+200%) seeing some of the largest gains. While Zoom has received the most press recently, we have seen an even larger increase in use of Cisco Webex, with a 600% increase in usage during the same period. Cross-referenced with industry segmentation, the largest increases in the use of collaboration services were in manufacturing and education. While nearly all industries have an increased need for remote collaboration tools, education has seen one of the most dramatic shifts, with classes going online for students at all levels.

Figure 2. Increase in collaboration cloud service usage measured week 11 of 2020.

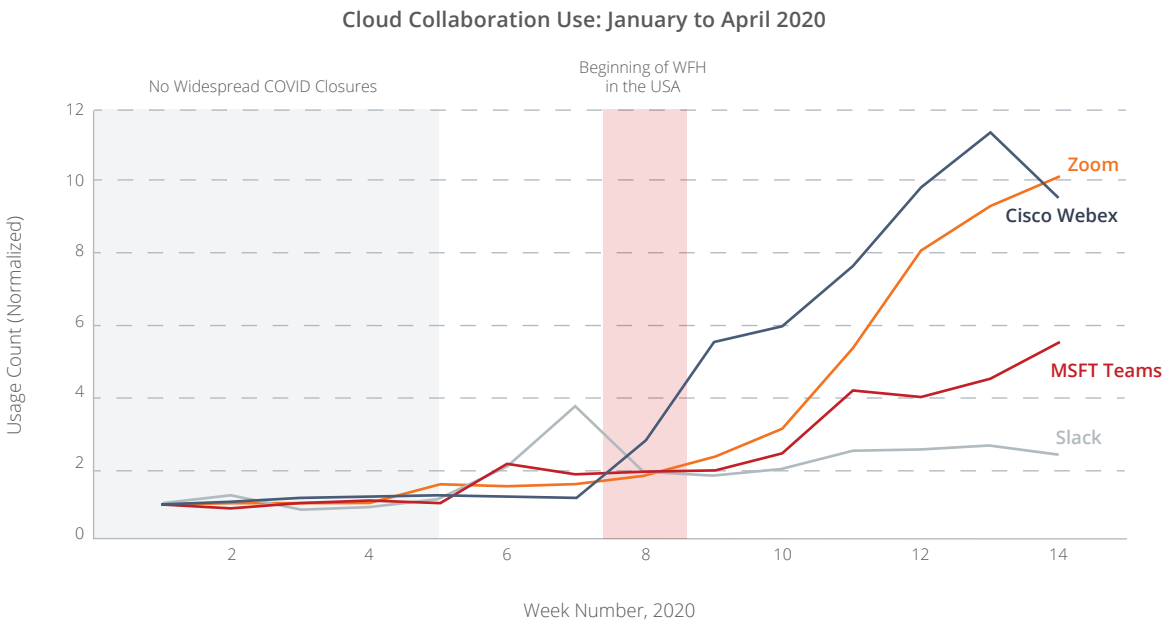


Figure 3. Collaboration cloud service usage by week.

Enterprise Cloud Usage From Unmanaged Devices Doubles

We also saw cloud traffic from unmanaged devices double across all verticals, which presents an increased source of risk stemming from these devices accessing cloud services while outside corporate managed networks. There's no way to recover sensitive data from an unmanaged device, so this increased access could result in data loss events if security teams aren't controlling cloud access by device type.

Threat Actors Target the Cloud

The amount of threats from external actors targeting cloud services increased 630%, with the greatest concentration on collaboration services like Microsoft 365. For the purpose of this analysis, we've placed these external threats into two categories: Excessive Usage from Anomalous Location, and Suspicious Superhuman. Both typically involve the use of stolen credentials:

- **Excessive Usage from Anomalous Location.** This begins with a login from a location that has not been previously detected and is anomalous to the user's organization. The threat actor then initiates high-volume data access and/or privileged access activity.
- **Suspicious Superhuman.** This is a login attempt from more than one geographically distant location, impossible to travel to within a given period of time. We track this across multiple cloud services, for example, if a user attempts to log into Microsoft 365 in Singapore, then logs into Slack in California five minutes later.

Internal or insider threat categories have remained the same. This indicates that employees don't go rogue and attempt to steal more data because they are working from home. Most of the attacks we see are external, cloud-native threats targeting cloud accounts directly.

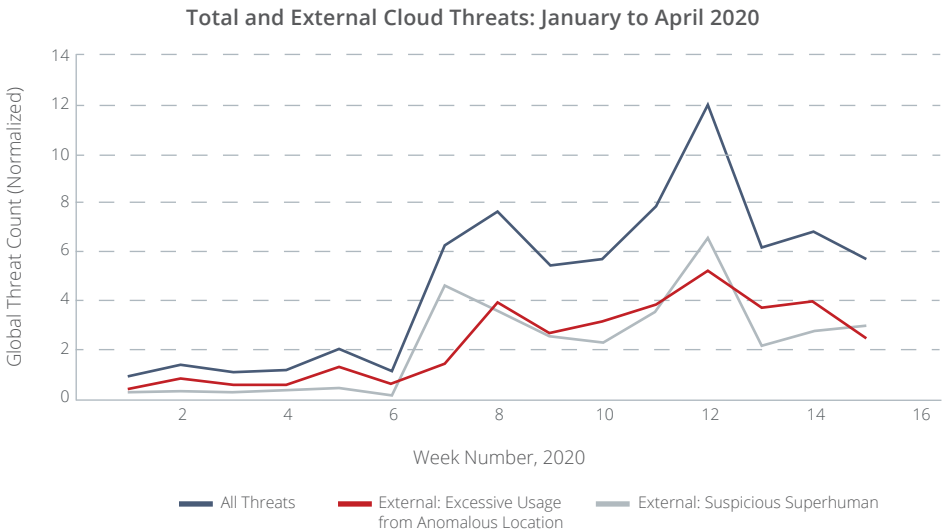


Figure 4. Cloud threat events across all industries.

Vertical Focus: Cloud Threats

By vertical, we can see that Transportation and Logistics, Education, and Government saw the largest increases in the amount of threat events in their cloud accounts, here shown for both internal and external threats. Naturally, as these industries increasingly lean on cloud services for productivity, attackers are following in-step with attempts to access their accounts and exfiltrate data.

Percentage Increase In Cloud Threats by Vertical: January to April 2020

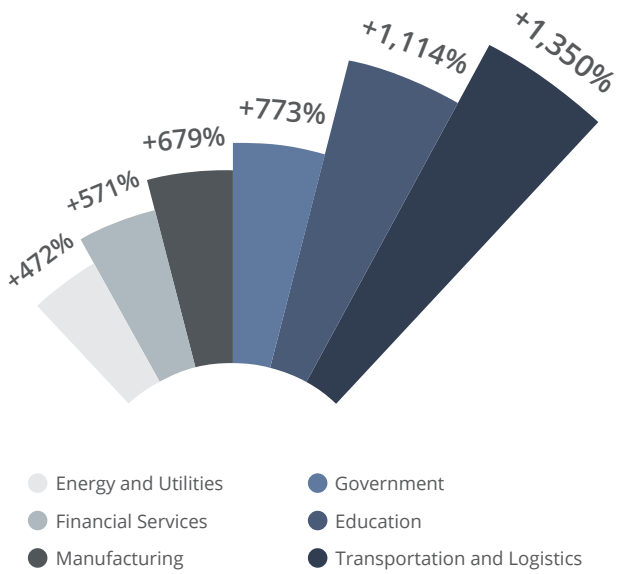


Figure 5. Increase in cloud threat events by industry.

Shifting back to threats from external actors alone, we ran an analysis of the source IP addresses used in these attacks to see the locations they were sourced from.

While source IP can't be used to determine attribution for an attack, it still provides us a useful view of the data that can assist with the implementation of security controls. The IPs we monitored were not only used to attack cloud accounts, but also other malicious activity, pointing to the reuse of criminal infrastructure for multiple attacks.

First, let's take a global view of the data. In the following chart, the size of the circle indicates the number of IP addresses used to launch attacks, and the depth of color indicates the peak number of threat events targeting an individual organization from these IPs.

Source IP Geolocation for External Cloud Threats: January to April 2020

Figure 6. Global view of external attack sources on cloud accounts by source IP geolocation.

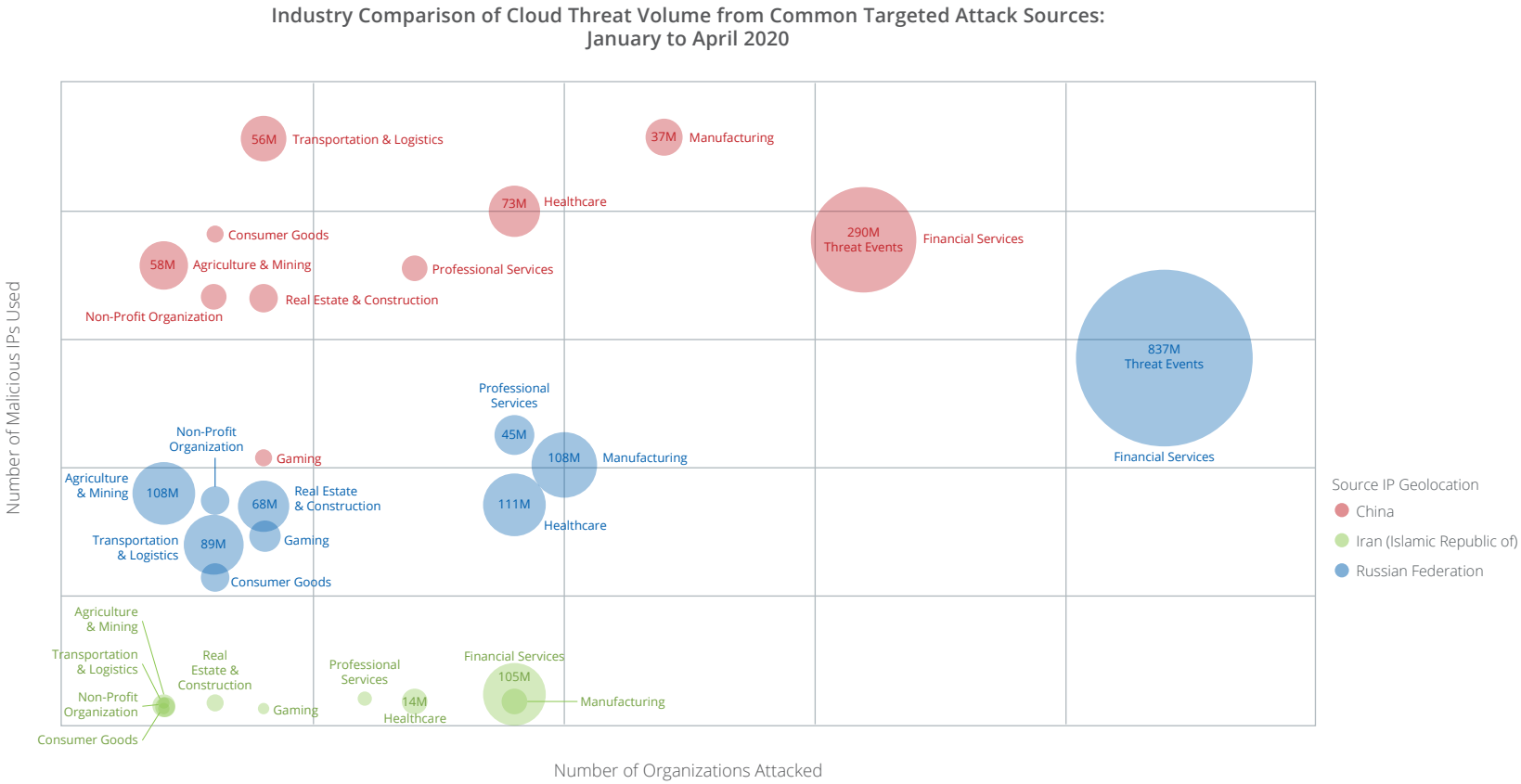
The top 10 source IP geolocations for external attacks on cloud accounts from January to April 2020 (sorted by number of IPs used) are:

1. Thailand
2. USA
3. China
4. India
5. Brazil
6. Russian Federation
7. Laos
8. Mexico
9. New Caledonia
10. Vietnam

Interestingly, none of the countries in our top 10 are in Europe, home to some of the most stringent data protection regulations in the world. The majority come from countries historically active in cybercrime and others lacking resources to enforce cybercrime regulations.[3]

Many of these attacks are likely opportunistic, essentially "spraying" cloud accounts with access attempts using stolen credentials. However, several prominent industries are often targeted by external threat actors, in particular Financial Services. These targeted attacks are often found to have a source in either China, Iran, or Russia.[4]

We can use the IP geolocation of these three countries to give us a deeper view into how industries are being targeted by external cloud attacks. In the following chart, the vertical axis shows the number of IPs used against each industry, with more IPs typically indicating more infrastructure and funding behind the attacks. The horizontal axis shows the number of organizations in a given industry being attacked, giving us a sense of the allocation attack infrastructure across verticals. Bubble size similarly shows us the volume of threat events targeting a specific industry, with color representing either Russia, China, or Iran.



In our first look at the vertical impact of external cloud threats, Financial Services had the fifth highest increase in attack volume. Looking here at a view of common source locations for targeted attacks, we see Financial Services experiencing the highest attack volume of any industry, and also the most organizations affected.

Healthcare is the second most targeted industry, followed by manufacturing. All organizations, but those in highly targeted industries in particular, need to continuously monitor their cloud activity to detect and block malicious access to their sensitive data.

Summary

These dramatic shifts in enterprise cloud use are breaking the efficacy of legacy security and networking solutions deployed by many organizations. VPN infrastructure is struggling to handle the surge in remote employees.[5] Modern applications like Microsoft 365 are delivered directly through the cloud, yet many organizations still use a hub-and-spoke network architecture to route cloud traffic through security appliances in their data center. In reality, employees will do whatever is easiest and fastest. They will turn off their VPN and access applications in the cloud directly.

The work-from-home guidelines and collaboration initiatives across many industries are putting to rest archaic models of connecting into a corporate network through a VPN before going to SaaS, PaaS, or IaaS. The new VPN-liberated models will require conditional access controls for corporate-issued and personal devices, comprehensive data protection, strengthened user behavior analytics, and cloud-native threat prevention with automated policy responses to remediate risks.

Threat actors have redoubled their efforts to exploit the distractedness and sudden changes wrought by the world's response to the pandemic. There are important changes needed to implement new delivery models for security in a distributed, work-from-home environment. However, the data shows that the increased risk of cloud-native threats brought by threat actors targeting cloud services far exceeds the risk brought by changes in behavior by employees simply working in a new, remote location.

Recommendations

Securing a remote workforce shifts the major security control points to the device and cloud. A cloud-native approach to delivering security will provide the most complete coverage, capable of reaching devices off-network and connecting to cloud services directly. Enterprises can establish a cloud-native security posture by:

1. Implementing a cloud-based secure web gateway so corporate devices can be protected against web-based threats without routing through VPN.
2. Allowing employees to connect to sanctioned cloud services from their corporate devices without using their VPN, protecting data with a cloud access security broker (CASB).
3. Setting policy in your CASB so that cloud services have device checks, data controls, and are protected against attackers who can access SaaS accounts over the internet.
4. Implementing multi-factor authentication for sanctioned cloud services where applicable to reduce the risk of stolen credentials being used to access accounts.
5. Letting employees use their personal devices to access corporate SaaS applications to maintain productivity, with conditional access to sensitive data in the cloud.

Learn More

For more information on cloud security technology, please visit the following links:

- McAfee® Cloud Security Solutions
- Security For Working From Home
- McAfee® Unified Cloud Edge (Secure Access Service Edge)

Interested in learning more? Contact McAfee for a custom briefing with more in-depth detail into this data, and how the trends discussed here may impact your organization.

Methodology

McAfee MVISION Cloud is a platform that provides cloud-native security for services across SaaS, PaaS, and IaaS.

To bring you these findings, we aggregated, anonymized cloud usage data for more than 30 million McAfee MVISION Cloud users worldwide who collectively generate billions of unique transactions and policy events in the cloud each day. This data set, collected between January and April, 2020, represent companies across all major industries across the globe, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

1. https://www.owllabs.com/blog/remote-work-statistics
2. https://azure.microsoft.com/en-us/blog/update-2-on-microsoft-cloud-services-continuity/
3. https://www.researchgate.net/publication/308775653_The_Current_State_of_Cybercrime_in_Thailand_Legal_Technological_and_Economic_Barriers_to_Effective_Law_Enforcement
4. https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20180221005206
5. https://www.theregister.co.uk/2020/03/11/corporate_vpn_coronavirus_crunch/

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com