WHITE PAPER

BrightCloud®
Threat Intelligence

The View from the Cloud:

Managing Security, Visibility and Access Control with Cloud Applications

Introduction

The number of enterprises and small-to-medium businesses using cloud-based applications for file sharing, data storage, project collaboration, and more keeps growing. While moving to the cloud offers undeniable benefits in terms of efficiency and flexibility, it can also bring significant security risks. Not only do the applications themselves pose potential security vulnerabilities, but it's also hard to prevent employees from using other, unsanctioned applications (aka "shadow IT").

63% of web-borne malware and 15% of phishing attacks are delivered over cloud applications.

When you consider today's cyber threat statistics and factor in the number of cloud services enterprises use (over 2,000, on average[1]), it becomes even more complex for businesses to assess their security risks. How can businesses get an accurate picture of which cloud applications are being used in their environments and for what purposes?

Cloud Applications and their Adoption

Broadly speaking, cloud services and applications are those that are delivered on-demand to companies and customers using a cloud architecture instead of internal infrastructure or on-premises hardware. There are three main types of cloud services: Infrastructure as a Service (IaaS); Platform-as-a-Service (PaaS); and Software-as-a-Service (SaaS). By using cloud services, businesses can gain easier access to applications and functions at a relatively low price with minimal time to implementation.

Up to 94% of enterprises already use cloud services.

The majority of today's enterprises already use cloud services, and adoption within small and medium-sized businesses (SMBs) is now outpacing their larger counterparts, with 70% of SMB workloads and data set to reside in a public cloud within the next 12 months.[2] Additionally, the average enterprise uses over 2,000 cloud applications throughout its operations.[1]

Thanks to the efficiency and collaboration benefits they provide, often at a cost savings over on-prem software and storage solutions, cloud services are here to stay. However, there are some important considerations in terms of security.

Cloud Applications and their Security

Although 84% of organizations report using SaaS services at their company, more than 93% of those said they still deal with unsanctioned cloud app usage. Additionally, 83% of enterprises indicate that cloud application security is a challenge.[2] As adoption continues to grow, it's critical for SMBs and enterprises alike to balance their cloud application use with security and access control; otherwise, the benefits they see may quickly turn into regulatory compliance issues, data loss disasters and security breaches.

92% of enterprises admit their organizations have a gap between current and planned cloud usage and the maturity of their cloud security program.

While cloud transformation is a strategic imperative, often receiving priority funding and resources, CISOs and IT teams are often left out of the discussion around adoption. Teams and business units across an organization may quickly adopt cloud services ad hoc to address perceived service needs without consulting centralized IT and cybersecurity teams. Then, as different areas of the business realize the rapid time to value, adoption and use grows. With a focus on speed, collaborating with cybersecurity teams (which are often understaffed) is seen as a threat to that speed due to increased evaluation and adoption requirements.[4]

Given the increased security risks that come with cloud adoption, treating security as an afterthought is a dangerous oversight. As cloud services and applications become ubiquitous, so should the effort to protect the data stored within them.

Common Security Risks

Although some enterprises still cite security as a cause for concern when using cloud services, especially those that are hosted in public clouds, the real security and data loss risk from using these cloud services comes more often from the customers themselves, though targeted attacks by cybercriminals do happen. These user-generated risks are typically due to common missteps, such as improper or unapproved deployment leading to shadow IT, uploading infected files, lenient access control, and lack of adequate data loss prevention.

Cloud Service Models

Infrastructure as a Service (IaaS)

Provides basic infrastructure of IT systems including servers, network devices, data storage options and more. Minimizes the need for hardware in a physical location.

Platform-as-a-Service (PaaS)

Provides software framework for businesses to create and run their own applications.

Software-as-a-Service (SaaS)

Provides software solutions on a subscription or pay-per-use model. SaaS applications are typically managed in a central location by the provider, so businesses don't have to worry about maintenance and management.

- ***Malware and Phishing Threats***

  In part because of user-generated risks, it's not just small, lesser known applications that present security concerns. Even major, trusted cloud service providers bear some risk from user missteps and targeted attacks. On average, one in three corporate instances of SaaS apps contained malware. Of the four major SaaS applications – OneDrive, Google Drive, Box, and Dropbox – Microsoft OneDrive had the highest rate of infection at 55%. Google Drive had the second highest rate of infection with 43% of instances being impacted, followed by Dropbox and Box with 33% each.[5]

  In November 2020, phishing attacks on the following cloud apps saw the biggest growth :

  - LinkedIn: + 306%
  - Twitter: +232%
  - Facebook: +177%
  - Dropbox: +129%

***63% of web-borne malware** and **15% of phishing attacks** are delivered over cloud applications.*[1]

***44% of scanned organizations** had some form of malware in at least one cloud application.*[5]

- *Shadow IT*

  Shadow IT is the use of any IT technology connected to an organization's network without the knowledge and approval of the IT department. This category can include hardware, software (including SaaS applications), and web and cloud services.

  While shadow IT is nothing new, the issue it presents is exacerbated by both the ease of cloud service models and the growth of remote work. The risks are fairly straightforward; if IT doesn't know about an unsanctioned application or device, then they don't know to protect it or the data it accesses and stores. The application then becomes a potential entry point for malicious actors to exploit.

  In addition to cybersecurity risks, there are data privacy regulations to consider, such as PCI or GDPR. The user of a given shadow IT application may not properly adhere to these regulations, thereby unwittingly violating privacy or data storage regulations.

***50% of enterprises** report the use of shadow IT apps has led to unauthorized access to data.*[3]

- *Access Control and Visibility*

  As with any IT system, managing which users can access which applications, network locations, and data is critical. As employees onboard, offboard or change positions within an organization, their access levels should be changed accordingly, preferably by a centralized IT group.

  In the absence of centralized management, enterprises and SMBs still need some kind of insight into who can access the cloud applications. While some may deploy cloud identity governance (CIG) solutions to help security and IT teams automatically and continuously discover identities, fully map them out, and control them and their access rights in multiple cloud environments, other organizations may not have the resources, time or expertise to implement such a service.

When infrastructure that hosts and delivers cloud services is managed by a third party, it can create a visibility gap existing network-based security controls can't or don't address.[3]

- *Data loss*

  Data is the lifeblood of an organization; losing access to it or having it land in the wrong hands can cause serious damage. While cloud services are often positioned as a solution to ease data access challenges, there are risks that can lead to data loss ranging from accidental deletion and human error to malicious activity and outright data theft.

***71% of organizations** report the majority of their cloud-data is sensitive. That's a 42% increase vs. the year before.*[3]

Cloud Access Security Brokers (CASBs)

To improve visibility into the cloud applications being accessed, create usage policies, and address security risks, many businesses are turning to Cloud Access Security Brokers. CASB services are typically placed between cloud service consumers and providers, safeguarding the gateway between a company's on-premises IT infrastructure and a cloud service provider's infrastructure. As such, CASBs can provide a central location for policy and governance concurrently across multiple cloud services — for users and devices — and granular visibility into and control over user activities and sensitive data. They typically help to enforce data-centric security policies based on data classification, data discovery and user activity surrounding data.

CASBs often use threat intelligence, network sandboxing, and malware identification and remediation, but they tend to rely on OEM versions of existing enterprise-grade antimalware and sandbox tools, rather than building their own. In some cases, CASB vendors may have their own analyst teams researching cloud-specific and cloud-native attacks.

How Threat Intelligence Improves Security, Visibility and Control

Faced with a continually growing and changing number of cloud applications and services, it's critical to have accurate, up-to-date cloud-specific intelligence, not only for CASBs but also other security tool providers who provide support and policy control capabilities around cloud applications. This list includes identity and access management providers, secure web gateways, firewalls and firewall as a service (FWaaS), SD-WAN, zero trust network access (ZTNA) and remote browser isolation, among others. In addition to the inherent value up-to-date, cloud-specific intelligence offers, it can also be tailored to help CASBs and other providers enhance their services, help their customers comply with regulations and policies and decrease security risks.

Cloud-Specific Threat Intelligence Benefits

Actionable threat intelligence can provide data around three majors areas of concern within a cloud application or service: which services are being used within an organization; how the applications are being used; and what the security reputations of these applications or services may be.

- *Identify which applications are being used*

  Being able to help to identify in-use cloud services and applications within a given organization's infrastructure helps combat shadow IT and decrease risks from unauthorized or un-vetted cloud applications.

  By classifying each URL associated with a cloud application into a relevant category — such as "cloud file sharing", "social networking", "office doc and productivity", etc. — intelligence helps enforce access or usage policies for specific applications based on security or compliance risks.

- *Better understand how someone is using a specific application*

  When you can see how applications are being used within an organization's environment, you can track abnormal activities (such as excessive data downloads) and prevent misuse or inappropriate access control.

  By categorizing each URL accessed in the operation of specific function within a cloud application, such as "upload" and "download" — intelligence helps to enforce policies pertaining to usage of cloud applications with general functions based on security or compliance risks.

- *Gain insight into the service or application's reputation*

  Having a better understanding of the cloud service in use helps an IT department evaluate which services are reputable and which ones may need further evaluation due to compliance or security risks. Technology providers themselves can better address application risks and set up and enforce policies that pertain to usage of cloud applications, therefore strengthening the overall value of their offering.

BrightCloud® Cloud Service Intelligence

BrightCloud® Cloud Service Intelligence enables CASB providers and other technology vendors to enforce data-centric security policies to prevent unwanted interactions with cloud services and associated applications. Through a suite of three services – Cloud Application Classification, Cloud Application Function, and Cloud Application Reputation – partners can identify, classify, and block or allow access based on the application's classification, functions, and reputation score.

Users of BrightCloud Cloud Service Intelligence can also use these components to supplement their data on which cloud applications pose security or compliance risks, as well as identify user actions within these applications, allowing the partner to better address risks as well as identify and stop shadow IT behavior in order to better control data.

Cloud Service Intelligence Components

Cloud Application Classification

Each URL associated with a cloud application is assigned a related category.

Cloud Application Function

Each URL accessed in the operation of specific function within our most widely used business applications will be categorized by that function.

Cloud Application Reputation

Each cloud application will be assigned a heuristic-based reputation score ranging from 0-100.

Conclusion

The use of cloud services and applications is only going to continue to grow, as will demand for cloud-based utilities that facilitate remote work. As more organizations store data, perform business functions and support remote work in the cloud, the demand for solutions that can provide security, visibility and control over cloud applications will also increase.

With more CASBs and other providers stepping in to fulfill these needs, it's critical that such services use cloud-specific application and service intelligence to enforce acceptable risk and access policies and protect organizations from data loss, compliance issues and security threats.

Partners can embed these components into their solutions via the BrightCloud® Threat Intelligence API. The API uses many of the same access conventions as other BrightCloud APIs, including a unified authentication method, to streamline adoption for existing customers.

Next Steps

To discover more about how BrightCloud® Cloud Service Intelligence can strengthen your solutions, click here.

---

1 Netskope. “Cloud and Threat Report – August 2020 Edition.” (August 2020)

2 Flexera. “2020 State of the Cloud Report.” (April 2020)

3 Oracle and KPMG. “Cloud Threat Report 2019.” (February 2019)

4 Oracle and KPMG. “Cloud Threat Report 2020.” (May 2020)

5 Bitglass. “Malware, P.I.: Tracking Cloud Infections.” (February 2018)

6 Figures derived from real-world observations of threat activity by BrightCloud Cloud Services and the BrightCloud Platform.

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry’s most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.