netskope

WHITEPAPER

ALLOW IS THE NEW BLOCK

10 REQUIREMENTS TO SAFELY SAY “YES” TO SHADOW IT

OVERVIEW

Cloud adoption in the enterprise continues to gain momentum with more than 1,000 cloud services used by employees in a variety of environments from retail to healthcare and everything in between. It turns out that fewer than 5% of these cloud services are sanctioned with IT having administrative access and the ability to manage or secure the deployment. Sanctioned cloud services often include suites like Office 365 and Google G Suite and apps like Salesforce, Box, ServiceNow, and dozens of others. While sanctioned cloud services often garner most of the enterprise focus, more than 95% of cloud services used by enterprises are unsanctioned, shadow IT services and are either shepherded in by lines of business or brought in by individual users that sign up for them because they are easy to access and use. Unsanctioned cloud services often fly under the radar of IT and security personnel. Many of these unsanctioned services are IaaS (think Amazon Web Services, Microsoft Azure, and Google Cloud Platform) solutions being used by DevOps teams building apps that access critical systems and contain sensitive resources to support the business. When misconfigured, IaaS resources like S3 buckets in AWS may expose sensitive data out in the open, leaving it easy for malicious actors to take advantage of the data or introduce threats.

Given the lack of visibility and control, what does the security team do about shadow IT? Do they take extreme security measures and try to block them using legacy security tools or do they allow their use and hope users stay secure from threats and don't leak sensitive data? This is a difficult decision and presents a catch-22 between extracting value from the cloud and being secure. Let's take a look at the potential impact resulting from an allow or block decision only versus a layered approach of multiple security policies and rules.

BLOCK

What is the risk if you try to block all these cloud services with legacy tools?

- **You will be blind to more than 50% of cloud usage.** Legacy security tools like firewalls and secure web gateways were not architected to adequately cover the way people work today. More than 50% of cloud usage takes place with users that are mobile and remote, outside of the perimeter that these tools are protecting. The other issue is that many cloud services often fly under the detection abilities of legacy tools, even VPNs that hairpin traffic back to on-premises systems (which are both expensive and create a heavy operational burden) and users learn to go around these tools. If you block Dropbox, they use lesser-known alternatives like FreakShare and these services are often riskier than the ones being blocked as sensitive corporate data being transferred in them are more open to leaks.
- **For the apps and services you can block, firewall exception sprawl runs rampant.** Even if you do an adequate job blocking cloud services with your firewall, there will likely be users and departments that demand access to certain services in order to get their job done. Perhaps they need to access that Google Drive shared by a partner or they need to test out a marketing app to support an important campaign. Or another team wants to test out a new app on Microsoft Azure. Before you know it, there are hundreds of exceptions in place on the firewall, creating complexity and management overhead.

- **Gaps in security policies.** Legacy tools such as on-premises data loss prevention and firewalls can only understand allowing or blocking. This places security and IT professionals in an impossible situation. How does one restrict the sharing of data to an approved corporate instance of a SaaS application or IaaS instance when there are unapproved services running in the same clouds? Legacy tools, which lack the context to understand the difference between personal and corporate managed instances must either allow or block all forms of usage as they cannot distinguish across the thousands of clouds where data may be sent.

- **Impact to your company's ability to move fast.** Legacy tools cannot enforce policies across thousands of cloud services. Legacy technologies such as firewalls, and layer 3 and 4 web proxies even when coupled with API-only cloud access security brokers cannot enforce data loss prevention controls across the entirety of cloud service providers. Cloud services users will gravitate towards the services that provide the greatest functionality and return for their services. Attempting to limit their choices to a handful of services, due to the limitations of the API-only approach is a sure-fire way to accelerate the adoption of unapproved services, for which API-only approaches cannot protect the enterprise against. In addition to the technical challenges faced by trying to block the cloud with legacy security tools, there are the business implications. Taking a heavy- handed approach to blocking the cloud could have a negative impact on productivity, ability to innovate, and employee morale. The cloud enables your employees and teams to move fast, collaborate, and be more innovative. Block the cloud and you can stifle innovation.

ALLOW

What is the risk if you don't secure these cloud services?

- **Loss of sensitive data via unsanctioned cloud services.** Many of the thousands of unsanctioned cloud services are used by employees to house and transfer sensitive data. Top categories for DLP violations include webmail, cloud storage, and collaboration and this represents more than 100 unsanctioned cloud services alone. And with IaaS use on the rise, storage like S3 buckets exposed to the internet and improperly configured present huge opportunities for hackers. If your data loss prevention focus only covers on-premises and cloud-based, sanctioned services then you are leaving a big hole. Data loss does not discriminate between whether a cloud service is managed and secured by IT teams. A devops engineer using an unsanctioned Microsoft Azure instance with misconfigured settings can just as easily allow for data leaks as while using an IT-sanctioned Box account. A common data loss scenario is when users download sensitive data from a sanctioned cloud service like Office 365 or Salesforce and upload that sensitive data to their personal cloud service. This is a blind spot and obviously presents risk tied to another form of data loss – as data exfiltration taking place from a sanctioned to unsanctioned cloud service.

- **Out-of-compliance.** Whether your concern is PCI, HIPAA, GLBA, SOX, FINRA, GDPR, or any other regimen that aligns with your business, compliance considerations should be extended to shadow IT as well.

- **Malware and ransomware infection via unsanctioned cloud services.** Unsanctioned cloud services presents a perfect opportunity for various strains of malware like ransomware to hide and spread to unsuspecting victims. One example is the cloud malware fan-out effect that takes place with the combination of shared folders and local sync clients. When malware makes its way into that environment it often goes undetected and spreads quickly to the users that are connected to the share and have a sync client installed. More than 50% of malware in the cloud is shared – with an increasing number of malware targeting resources in public clouds like AWS, Microsoft Azure, and GCP.

THE SOLUTION - SAFELY ENABLE UNSANCTIONED, BUT PERMITTED CLOUD SERVICES

Fortunately there is a better option. The Netskope Security Cloud is the only cloud access security broker (CASB) that was architected to safely enable unsanctioned cloud services instead of forcing you into difficult allow or block decisions at the perimeter. Netskope advocates a granular and comprehensive approach to securing shadow IT by preventing risky actions while still allowing the cloud service to be used and covering all methods of access to these services. If you are evaluating a CASB, here is a look at the 10 requirements to make safe enablement possible.

10 CASB REQUIREMENTS TO SAFELY ENABLE SHADOW IT

Requirement #1: Ability to discover cloud services in use and assess risk

Discovery and risk assessment is often the first step as part of any cloud security strategy. This is table stakes for several CASB vendors, but it involves the ability to collect cloud usage details from log data or an inline method and match that against a database of cloud services that have been researched and scored. One of the first steps before safe enablement might actually be to block the most risky cloud services based on their score.

Requirement #2: Forward proxy deployment options to cover on-premises, mobile, and remote users

Getting access to unsanctioned cloud traffic originating from where users are is an important requirement. An agentless forward proxy option for on-premises users can be combined with a forward proxy client deployment for mobile and remote users.

Requirement #3: Coverage for all access methods including browsers, desktop apps, sync clients, and mobile apps

Covering all ways users access the cloud is also important. More than 50% of cloud usage takes place in native applications, so supporting browser-only traffic presents a big blind spot.

Requirement #4: Granular activity-level visibility and control for thousands of shadow IT services

Getting access to where users are and how they are accessing the cloud is an important first step, but understanding that traffic is a critical next step. Simply adding a forward proxy isn't sufficient and neither is supporting only dozens of user-led cloud services, given that there are nearly 1,000 of them per enterprise. You need a CASB that understands activity-level details and can perform granular control for the thousands of user-led cloud services that are being proxied by the forward proxy.

Requirement #5: DLP inspection coverage for thousands of shadow IT services

Having the ability to inspect thousands of shadow IT cloud services with DLP is another key requirement for safely enabling these cloud services. Advanced DLP functionality like fingerprinting, exact match, and optical character recognition (OCR) are important, but if your DLP only supports dozens of cloud services, you are vulnerable to sensitive data loss across the thousands of unsanctioned cloud services that are missed.

Requirement #6: Encryption support for sensitive data going to shadow IT services

There may be scenarios where you allow certain data to go to unsanctioned cloud services, but you first want to secure that data with encryption to ensure it does not get into the wrong hands. A CASB should support the ability to encrypt certain data going to unsanctioned cloud services and only allow that data to be viewed by users going through the CASB.

Requirement #7: Malware protection for shadow IT services

Supporting real-time malware inspection on traffic going to and from user-led cloud services is a key requirement to help protect against various strains of malware like ransomware. There are two sides to ransomware protection. One is both static and dynamic analysis to help prevent ransomware infection, and the other is post-infection remediation with the ability to introduce a remediation workflow enabling you to seamlessly roll back your files to the last known "good" version.

Requirement #8: Category-level policies

Given that there are, on average, nearly 1,000 cloud services in the enterprise, having a policy infrastructure that enables you to easily triage your cloud services is important. This starts with support for category-level policies, where you can choose categories such as 'cloud storage', 'collaboration', and social media' and be able to secure potentially hundreds of cloud services with one policy entry. Without this capability, you would have to perform policy one-by-one for nearly 1,000 cloud services. That is unrealistic.

Requirement #9: Layered policies with allow / block actions

In addition to category-level policies, triaging shadow IT via policy also requires layered policies that support both allow and block actions. For example, if you want to block PCI data going to all unsanctioned cloud storage services, but allow PCI data to go to the IT-sanctioned Microsoft Office 365, you would create two policies—the first would be tied to an 'allow' action of PCI uploads to Office 365 and the second policy would be a 'block' action of PCI uploads to 'cloud storage' at the category level (while still allowing use of services in that category).

Requirement #10: Instance awareness

The final requirement is tied to the previous one. In order to thread the needle and perform policy on unsanctioned versus sanctioned cloud services and vice-versa, your CASB needs to understand the difference between instances of a cloud service. Which is the sanctioned OneDrive vs. the shadow IT OneDrive? Which instance of Google Cloud Platform is the production one and which one is just being tested by a line of business? Which version of Box is the Marketing version? The CASB needs to understand this and be able to bring that instance awareness into policy.

SUMMARY

The cloud presents a tremendous opportunity to make your users more agile and collaborative, giving your company a competitive edge. There is an opportunity to embrace both cloud services, but do it safely. **Allow is the new block.**

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.