OVERCOMING ADVERSARIAL ADVANTAGE IN ENTERPRISE CLOUD ADOPTION

Key Issue:

Adversarial advantage in the cloud poses certain disadvantages for enterprise cloud adoption

Enterprises that have committed to migrate to cloud to provide scalability, flexibility and efficiency should not be surprised by reports that show threat actors have moved their infrastructures to cloud for similar advantage. Netskope recently reported on a handful of incidents in which the effects of ransomware were amplified across cloud environments to affect multiple users and endpoints. [1]

In one incident, a user fell prey to a ransomware attack and subsequently had files encrypted. The user reportedly stored another set of files in a popular cloud application. The files in the repository were set to sync on a prescribed schedule. The synching of the locally encrypted files triggered synchronization of the cloud-based file versions, maliciously encrypting those files as well. Subsequent users accessing files in the infected repository suffered infections of their devices by the original ransomware attack. Netskope dubs this phenomenon, "fan out" which allows bad actors to amplify attacks across enterprises with increased scale and velocity, utilizing essential business tools such as cloud storage as the mechanism for spreading. Cloud services of this type enable users to synch and share files easily, which unwittingly contributes to the propagation of malware via malware delivery platforms (MDP).[2]

This adversarial advantage is a boon to attackers bent on committing voluminous infections. Organizations unfortunately are at a significant disadvantage, given the climbing adoption rates of cloud services and the transference of poor cyber hygiene habits into cloud environments. This makes them more susceptible to attacker advantage within cloud contexts.

Challenges and Opportunities:

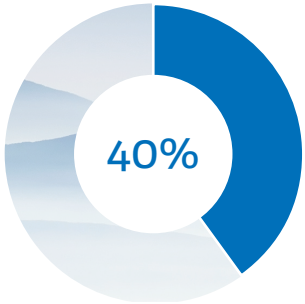
Challenges

In 2009, only a handful of cloud applications were on the minds of early adopters – typically sales enablement, collaboration, cloud messaging and cloud storage platforms.[3] Nearly a decade later, **the average number of cloud applications detected in typical organizations is between 800 and 900, a 33 percent increase from reported levels in 2015**. Of this number, **a mere 5 percent are sanctioned applications. About 20 percent of organizations have more than 1,000 cloud applications in use at any given time**.[4] The scale of applications is foreboding for those tasked to manage and secure cloud environments of this size. Predictably, the number of endpoints in Internet of Things (IoT) centric environments are soaring and will rise exponentially in the short term.[5] Adversaries are leveraging this scale not only to amplify attacks but also cloak their activity under the cover of this increased attack surface.

Malware spreaders are additionally aided by poor information technology habits replicated into the cloud, also at scale. Skyhigh reported in its Q4 2015 Cloud Adoption Risk Report a noticeable uptick in the storage of sensitive documents in the cloud.[6] Password documents occur with the third highest prevalence in the cloud, underscoring the issue of "poor" on premise cyber hygiene penetrating cloud environments. This statistic is disconcerting for cloud adopters yet a boon for threat actors. Other sensitive data types including salary, files marked "confidential," and budget information are ubiquitous in cloud environments without adequate controls.

Opportunities

A large percentage of cloud adoption disadvantage can be attributed to the accelerated growth of shadow IT and a new emergent and empowered class of users called "citizen IT." Citizen IT is defined as the unsanctioned and often unfettered ability of users, or citizens, to access cloud applications. Both shadow IT and citizen IT pose a formidable challenge for organizations attempting to throttle down cloud service usage as threat actors evolve their cloud tactics, techniques and procedures. Further, the proliferation of mobile devices and the exponential rise of IoT devices further compounds the challenge, effectively enlarging attack surfaces and increasing the occurrence of sensitive data in the cloud. According to a recent SANS cloud adoption report, 40 percent of all organizations have reported unauthorized access to sensitive data stored in the cloud. Thirty percent of all organizations are unaware of cloud applications.



Forty percent of all organizations have reported unauthorized access to sensitive data stored in the cloud.

Because cloud application adoption rates are not slowing, follow these programmatic steps for successful and secure SaaS adoption given the threat landscape.

1. Inventory and manage cloud services used by business units to minimize unknowns that could pose a risk to the business.
2. Securely enable business units to use cloud services quickly.
3. Centralize cloud security strategy that is spread across many tech departments and potentially uncoordinated.

Thirty percent of all organizations are unaware of cloud applications. [6]

The Path Forward:

Many of the challenges posed by adversarial advantage can be overcome by well-defined maturity models. Planning, building and running strong programs that are well-defined and measurable means developing the following capabilities within the program framework:

- Governance
- Visibility
- Identity and access management
- Threat protection
- Compliance
- Data security

The capability to discover cloud services in use is paramount for any SaaS initiative, and companies should curate a list of sanctioned and unsanctioned applications. A cloud risk assessment by means of cloud access security broker (CASB) can facilitate discovery. The resulting enumerated cloud services list generates the needed awareness to spearhead a planned SaaS adoption. Further, identity and access, emerging threats and data security controls should be identified to enhance an organization's security posture in the cloud and ensure compliance to policy. Cloud data loss prevention (DLP), cloud-encryption and cloud monitoring are important controls to secure the cloud.

Modeling Outcomes

With Optiv's maturity model, stakeholders of cloud adoption programs can confidently build and measure progress. There are a five phases on the path to a mature cloud program, namely maturity, awareness, reactive, adaptive, purposeful and strategic. Program outcomes derive from the program framework. The key outcomes that support Optiv's programmatic strategy for cloud adoption and maturity model are the following:

- Policy
- Understanding
- Execution

Certain program capabilities, along with the expected key outcomes, provide organizations the ability to mature and measure every aspect of a SaaS cloud strategy. For example, in the area of cloud SaaS policy, organizations can publish an "acceptable use policy" or AUP statement or review existing ones. Disseminate the policy to a wide audience so users are made **aware** of the business stance regarding usage. At the **reactive stage**, organization should possess the ability to track compliance to the AUP, applying governance process on a per incident basis. At the **adaptive stage**, organizations review policy statements regarding data security of sanctioned cloud applications in accordance with a regular review cycle. Organizations extend policy to define multiple tiers of cloud application at the **purposeful stage**. At the **strategic stage** of the maturity cycle, companies publish and adopt a multi-tiered enforcement policy that provides guidelines and a review process for ongoing process improvement. Similar maturity paths for understanding and execution support an organization's tactical and strategic migration of systems, data and business processes to the cloud.

Call to Action

It is imperative that information technology leaders plan SaaS adoption carefully. This starts with awareness and visibility of current cloud usage and often directly correlates with other "XaaS" initiatives going on within any given organization. Review current security processes and remediate any gaps prior to cloud migration to reduce the potential spread of poor cyber hygiene to cloud environments. Sanction business applications and rigorously govern and monitor usage to assure compliance. Periodically perform assessments of SaaS providers to track risk as part of a third-party risk program. Last, organizations can overcome adversarial advantage threatening security and privacy through the adoption of structured maturity models.

References:

1. "Gartner Research Spotlight: How to Evaluate and Operate a Cloud Access Security Broker," Netskope, last modified December 18, 2015, https://resources.netskope.com/h/i/181824636-gartner-research-spotlight-how-to-evaluate-and-operate-a-cloud-access-security-broker/169105

2. "Cloud Security Brokers Play a Key Role," SaaS in the Enterprise, last modified July 11, 2014, http://www.saasintheenterprise.com/author.asp?section_id=3154&doc_id=274035

3. "Google's 'Gov Cloud' Wins $7.2 Million Los Angeles Contract," InformationWeek, last modified October 28, 2009, http://www.informationweek.com/cloud/software-as-a-service/googles-gov-cloud-wins-$72-million-los-angeles-contract/d/d-id/1084397?

4. "Cloud Computing Trends 2016," Skyhigh, 2015, https://www.skyhighnetworks.com/cloud-computing-adoption-trends/

5. Dave Shackleford, "Orchestrating Security in the Cloud," A SANS Survey (2015), https://www.sans.org/reading-room/whitepapers/analyst/orchestrating-security-cloud-36272

Mark Arnold

Senior Research Analyst
Solutions Research and Development Optiv

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

 1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com