Shadow IT Security Checklists

The cloud (SaaS, PaaS, and IaaS) is changing business for the better, making employees more productive and businesses more innovative.

Companies across all industries have begun to embrace the cloud as they migrate to popular enterprise cloud services such as Office 365, Salesforce and Box.

However, this enthusiasm for cloud adoption is tempered by security, compliance and governance concerns. Employees aren’t slowing down and are adopting cloud services on their own. Cloud services procured and managed outside of IT’s purview, often referred to as “Shadow IT”, complicate the situation for IT and IT security teams.

In fact, as of Q4 2017, the average company uses 3,154 cloud services, an increase of 38.9% from this time last year. This number shouldn’t come as a surprise if you consider that cloud services are incredibly easy to adopt, with most requiring only an email or a credit card to sign-up. The result is that individual users and business units often begin using cloud services without any involvement from IT.

Even if a company takes a measured approach to cloud adoption while implementing the required security, compliance and governance controls around them, employees are likely not acting with the same discretion when they sign-up for new cloud services on their own; which can be problematic.

Across over 17,500 cloud services in use today, only 8.1% meet the strict data security and privacy requirements of enterprises as defined by Skyhighs CloudTrust Program.



**Key Shadow IT Stats**

* 72% of companies don’t know the scope of Shadow IT at their organizations but want to
* 30 the number of cloud services used by the average employee
* 1,154 the average number of cloud services in use at enterprises
* 8.1% of the over 21,500 cloud services in use at enterprises meet strict data security and privacy requirements

**Key Questions It Security Should Be Able To Answer Related To Shadow It Visibility & Control**:

1. Which services are employees and business units using overall and in each category (e.g. file sharing, social media, collaboration)?
2. Which services are gaining in popularity and should be evaluated for enterprise-wide adoption?
3. What is the risk-level of each service in use?
4. How effective are my firewalls and proxies at identifying cloud services and enforcing acceptable cloud use policies?
5. Which redundant services are employees using, and are they introducing additional cost, risk or inhibiting collaboration?
6. How do I quantify the risk from the use of cloud services and compare it to peers in my industry?
7. Which services house sensitive or confidential data today?
8. What are the security capabilities of the services storing sensitive data?
9. Which partners’ cloud services are employees accessing and what’s the risk of these partners?

**Key Requirements for Enabling Secure Shadow IT Usage**

1. Log-based visibility into all users, services (SaaS, PaaS, IaaS), and data transfers
2. On-premises tokenization of log data for security and privacy
3. Comprehensive cloud registry covering a minimum of 17,500 cloud services
4. Detailed risk assessments provided for all cloud services
5. Usage analytics to identify redundant services and popular and growing services primed for enterprise-wide adoption
6. Ability to audit the effectiveness of firewall and proxies at enforcing policies
7. Closed-loop remediation with firewalls and proxies
8. Ability to coach employees using a chained forward proxy or integration with existing firewalls and proxies
9. Ability to enforce fine-grained access control policies for application functionality (e.g. upload) based on application, user, device, geography
10. Customizable reporting with automatic periodic reporting capabilities
11. Vertical-specific, pre-built DLP policy templates
12. Ability to leverage policies from on-premises DLP systems and extend them to cloud services
13. Ability to quantify cloud risk, compare it to benchmarks from peers in the industry and track it over time
14. Anomaly detection across all services to identify insider threats or security breaches
15. Adaptive authentication to force additional authentication steps when a threat is detected using identity and access management solutions
16. Ability to identify unmatched uploads for further investigations
17. Integration with SIEMS for incident response remediation
18. Darknet intelligence to identify stolen employee credentials
19. User reputation analysis based on correlated activities across cloud services
20. Frictionless deployment that doesn’t impact end user

This rapid adoption brings with it the benefit of increased productivity and agility, but the downside is that IT often has little to no visibility into the full scope of IT services employees are using. Without visibility, it becomes very difficult for IT to manage both cost expenditure and risk in the cloud.

The average organization experiences 19.6 cloud-related security incidents each month. These events include insider threats (both accidental and malicious), privileged-user threats, compromised accounts and attacks that leverage the cloud as a vector for data exfiltration.

Many of the services used in the number and variety of cloud services available to enterprises is growing at a staggering workplace are consumer-grade and do not meet the strict security and governance needs of an enterprise; so understanding the services employees are using, what type of data that is uploaded and shared, and the security capabilities of these services is critical.