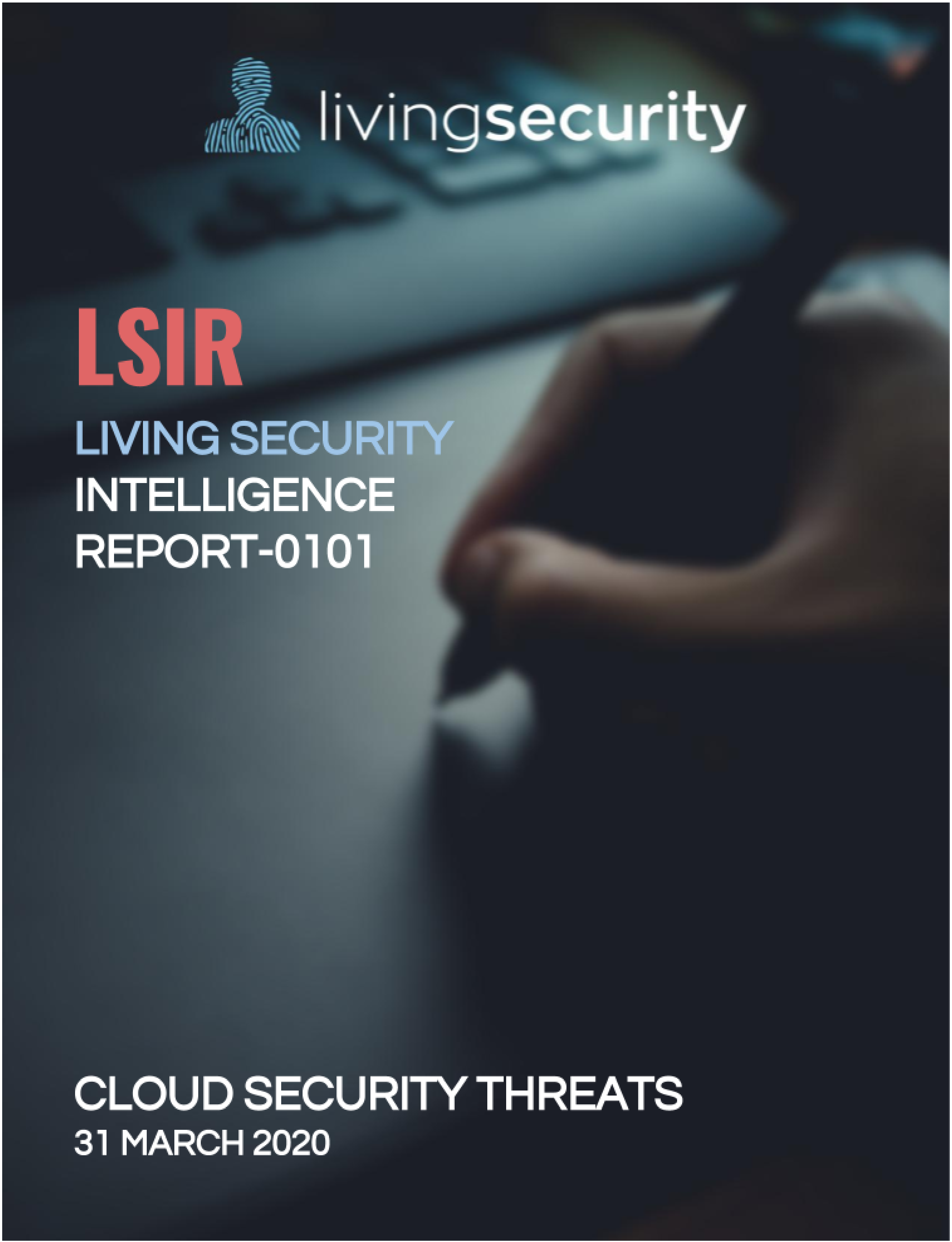


LSIR

LIVING SECURITY INTELLIGENCE REPORT-0101

CLOUD SECURITY THREATS

31 MARCH 2020

Cloud Service Introduction

The ability to obtain a seemingly unlimited amount of computer resources and storage can be achieved using cloud services. Cloud services are any service made available to an organization or user on demand over the internet from a cloud computing or storage provider. This allows users to access resources or their information anywhere due to the service being run on the service provider's hardware and accessible over the internet. Also, it greatly reduces the organization or user's responsibility for maintenance and purchasing of hardware because it is all controlled by the service provider. Cloud services increase efficiency and accessibility of work and information, but it also produces security threats that are vital to understand in order to mitigate them.

Cloud Security Threats

As more companies and individuals increase their use of cloud services it inevitably becomes a gold mine for cyber criminals. Organizations often utilize cloud services to store confidential data, personally identifiable information, proprietary products, among other important information. When using public cloud services this information does not always have the same firewalls and security checks a private network or private cloud provides. However, the convenience of not needing to purchase and maintain the hardware that is needed to store massive amounts of information and being able to access it anywhere outweighs the risk involved for most users. Therefore, in order to take advantage of cloud services it is vital to understand the threats and risks in order to better protect from becoming a victim of an attack.

Data Breach:

A security issue where sensitive information is released, stolen, or accessed by an unauthorized individual. This is a break in the confidentiality of the information which can result in loss of intellectual property, loss of trust or reputation, monetary loss, market value decrease, legal liabilities, as well as incident response costs. It is necessary organizations take precautions such as policies that enforce complex passwords and make users setup multifactor authentication (MFA) so that issues, such as these, are less likely to occur.

Misconfiguration and Inadequate Change Control:

This occurs when computer systems are set up incorrectly which leaves them vulnerable to malicious activity. These misconfigurations include unsecured data storage, excessive permissions, default credentials, default configuration setting, and the standard security controls being disabled. Misconfiguration is the leading cause of data breaches which leads to confidentiality integrity, and potentially the availability of information being compromised.

Lack of Cloud Security and Architecture and Strategy:

Organizations are moving their Information Technology (IT) infrastructure to public cloud services. The biggest challenge that comes with this is properly implementing security architectures to withstand cyberattacks. Organizations are more inclined to choose speed of the migration over security which leaves the organization vulnerable to attacks during and after the migration process. Therefore, it is necessary for organizations to develop a robust security strategy and implement a security infrastructure in order to build a foundation to conduct themselves securely in the cloud.

Insufficient Identity, Credential, Access and Key Management:

Cloud services introduce changes to the traditional practices of identity access management (IAM). The cloud service user is required to manage a large portion of their IAM in the attempt to increase security. It is vital to ensure adequate protection of credentials, regular automated rotations of cryptographic keys and certificates, a scalable IAM system for users, use of MFA, and a password policy that ensures strong passwords.

Account Hijacking:

This is the practice of gaining access to highly privileged accounts by cyber criminals. The accounts at the highest risk are cloud service accounts or subscriptions because they are accessible online to anyone with the correct privileges or credentials. These can fall victim to phishing attacks, exploitation of cloud-based systems, and stolen credentials. The impact of account hijacking can result in a breach in confidentiality, integrity, and availability of information and resources.

Insider Threat:

Insider negligence or malicious intent is responsible for 58 percent of security breaches. 64 percent of these breaches are due to employee negligence, 23 percent are related to criminal intent, and 13 percent are due to credential theft. This is a threat that is difficult to mitigate but requires educating employees about the prevention systems in place, such as logs of the system, and common scenarios of negligence and credential theft. This will help deter employees from misusing their privileges because they know their actions are recorded as well as inform others on dangerous scenarios where they are putting the company at risk.

Insecure interfaces and APIs:

Generally, APIs and user interfaces (UI) are the most accessible and exposed portion of a system. This results in them consistently being attacked with the intent to gain greater access than was intended. Therefore, it is necessary to make sure the design of a UI and API are secure and do not allow for accidental or malicious attempts to circumvent security policies. This is accomplished through sanitizing any possible input as well as minimalizing what a person accessing the UI and API is capable of doing. Also, ensure that a select few administrative accounts are granted access to the systems API.

Weak Control Plane:

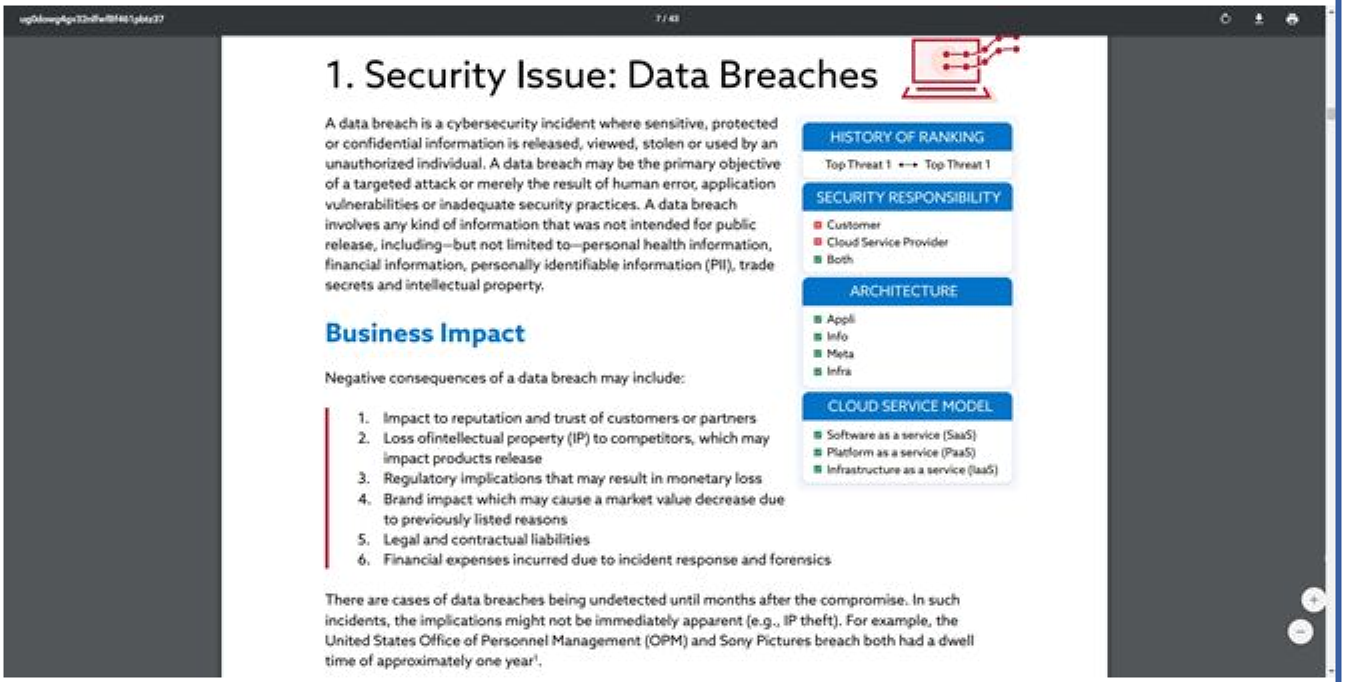
When an organization starts using more cloud services and resources, it results in an increasing variety of cloud administrative consoles and interfaces known as the cloud control plane. It is vital to properly lock down this control plane in order to protect the organization from cyber-attacks. This can be accomplished through account inventory which involves meticulously defining users and accounts that need administrative access. Ensure that all administrative accounts are using MFA by strictly enforcing its use. Also, enable logging of the entire system to ensure the ability to determine if an account is hijacked. Restrict API access to a small set of administrative users who are responsible for controlling and making changes to the API.

Limited Cloud Usage Visibility:

The issue of limited cloud usage visibility arises when an organization does not possess the ability to visualize and determine whether cloud service use within their organization is safe or malicious. Organizations often provide sanctioned applications that their employees are permitted to use however they are unable to determine how their applications are being leveraged by insiders. While these applications are sanctioned, they may still be vulnerable to SQL injections, Domain Name System (DNS) attacks, credential theft, among other vulnerabilities. However, the bigger risk comes from shadow IT. This is the use of IT systems, devices, software, applications, and services without approval from the IT department. This is often done by employees to increase their productivity and efficiency. In doing this, employees find themselves working around security policies in the attempt to get their job done. This can result in data leaks, unauthorized access, among other more serious attacks. The limited cloud usage visibility makes it difficult for organizations to prevent occurrences such as this from happening.

Abuse and Nefarious Use of Cloud Services:

The responsibility to mitigate this threat rests on the shoulders of the cloud service provider (CSP). Cyber criminals can leverage cloud services to be a platform for malicious actions. They are able to host malware on cloud services which appear to be legitimate due to the use of the CSP's domain. Cyber criminals are also able to use cloud-sharing tools as an attack vector to improve upon their reach and propagate themselves deeper into organizations. In order to mitigate the misuse of cloud services CSPs must include detection of payment fraud and misuse of cloud services. An incident response framework where customers are given the ability to report possible abuse of services. CSPs should also include controls that monitor the health of a customer's cloud workload along with file-sharing and storage applications.



1. Security Issue: Data Breaches

A data breach is a cybersecurity incident where sensitive, protected or confidential information is released, viewed, stolen or used by an unauthorized individual. A data breach may be the primary objective of a targeted attack or merely the result of human error, application vulnerabilities or inadequate security practices. A data breach involves any kind of information that was not intended for public release, including—but not limited to—personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

HISTORY OF RANKING

Top Threat 1 ←→ Top Threat 1

SECURITY RESPONSIBILITY

- 🟥 Customer
- 🟥 Cloud Service Provider
- 🟩 Both

ARCHITECTURE

- 🟩 Appli
- 🟩 Info
- 🟩 Meta
- 🟩 Infra

CLOUD SERVICE MODEL

- 🟩 Software as a service (SaaS)
- 🟩 Platform as a service (PaaS)
- 🟩 Infrastructure as a service (IaaS)

Business Impact

Negative consequences of a data breach may include:

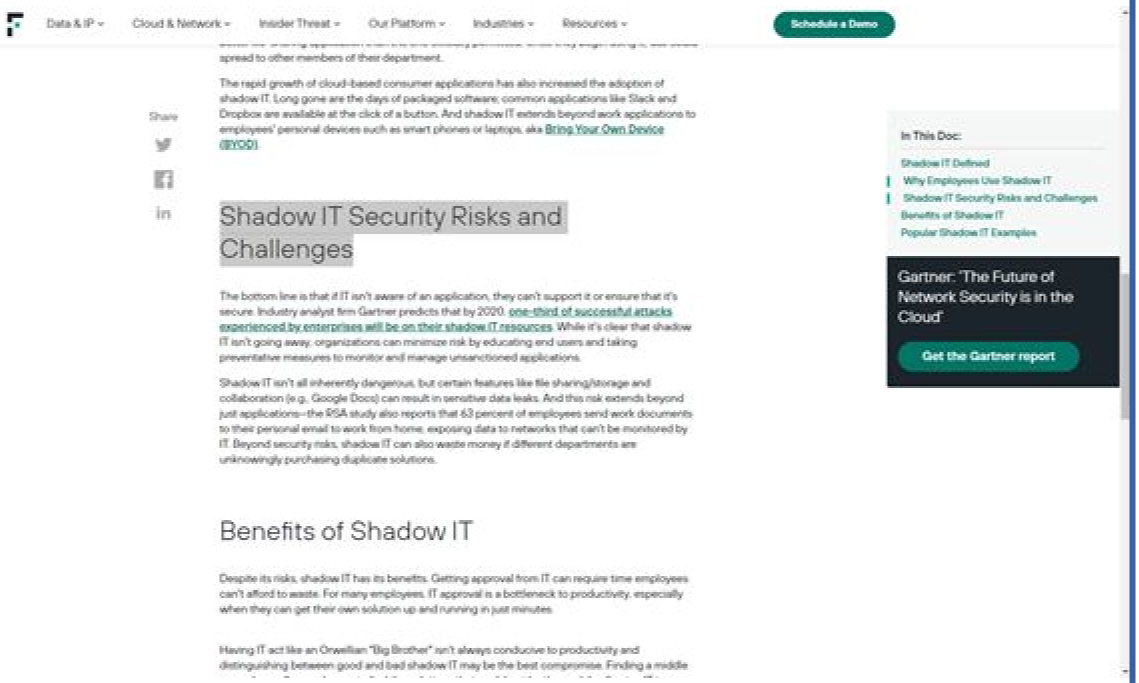
1. Impact to reputation and trust of customers or partners
2. Loss ofintellectual property (IP) to competitors, which may impact products release
3. Regulatory implications that may result in monetary loss
4. Brand impact which may cause a market value decrease due to previously listed reasons
5. Legal and contractual liabilities
6. Financial expenses incurred due to incident response and forensics

There are cases of data breaches being undetected until months after the compromise. In such incidents, the implications might not be immediately apparent (e.g., IP theft). For example, the United States Office of Personnel Management (OPM) and Sony Pictures breach both had a dwell time of approximately one year[1].

Outstanding source! great detail and easy to read.

Capture Date	Mar 27, 2020 2:07PM GMT -0400
Page Hash	b8f8bddc9e2c6a2c853357c242c46cc0fbe61ca66d683b8255f789290e2c5579

URL	https://s3.amazonaws.com/content-production.cloudsecurityalliance/ug0dowg4gv32nlfwf8f461pbtz37?response-content-disposition=inline%3B%20filename%3D%22The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf%22%3B%20filename%2A%3DUTF-8%27%27The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20200327%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200327T143115Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=a8b8826928c16509ed1f71e4907699f48a66db2b0573ff6d5df7d6dfa92ad162



spread to other members of their department.

The rapid growth of cloud-based consumer applications has also increased the adoption of shadow IT. Long gone are the days of packaged software; common applications like Slack and Dropbox are available at the click of a button. And shadow IT extends beyond work applications to employees' personal devices such as smart phones or laptops, aka Bring Your Own Device (BYOD).

Shadow IT Security Risks and Challenges

The bottom line is that if IT isn't aware of an application, they can't support it or ensure that it's secure. Industry analyst firm Gartner predicts that by 2020, one-third of successful attacks experienced by enterprises will be on their shadow IT resources. While it's clear that shadow IT isn't going away, organizations can minimize risk by educating end users and taking preventative measures to monitor and manage unsanctioned applications.

Shadow IT isn't all inherently dangerous, but certain features like file sharing/storage and collaboration (e.g., Google Docs) can result in sensitive data leaks. And this risk extends beyond just applications—the RSA study also reports that 63 percent of employees send work documents to their personal email to work from home, exposing data to networks that can't be monitored by IT. Beyond security risks, shadow IT can also waste money if different departments are unknowingly purchasing duplicate solutions.

Benefits of Shadow IT

Despite its risks, shadow IT has its benefits. Getting approval from IT can require time employees can't afford to waste. For many employees, IT approval is a bottleneck to productivity, especially when they can get their own solution up and running in just minutes.

Having IT act like an Orwellian "Big Brother" isn't always conducive to productivity and distinguishing between good and bad shadow IT may be the best compromise. Finding a middle

In This Doc:

- Shadow IT Defined
- Why Employees Use Shadow IT
- Shadow IT Security Risks and Challenges
- Benefits of Shadow IT
- Popular Shadow IT Examples

Gartner: 'The Future of Network Security is in the Cloud'

Get the Gartner report

Interesting threat concept

Capture Date	Mar 27, 2020 3:30PM GMT -0400
Page Hash	149f3ae74fa011414149e78efb47bf5b4baef4bf97b46070368788f103b6c0ec
URL	https://www.forcepoint.com/cyber-edu/shadow-it

Conclusion

Overall, cloud services are increasing connectivity and efficiency for organizations. While it is impossible to mitigate all risk, it is necessary to educate in order to understand the threats that exist on public cloud services. Through this, organizations and users are better prepared to mitigate the risks that accompany cloud services and continue to take advantage of the remarkable advantages that they provide.

Full Page History

Page ID	Page Title / URL	Date Visited	Date Updated
1	**cloud security threat - Google Search** https://www.google.com/search?q=cloud+security+threat&rlz=1C1CHBF_enUS894US894&oq=cloud+security+threat&aqs=chrome..69i57.3010j0j7&sourceid=chrome&ie=UTF-8	Mar 26, 2020 3:59PM GMT -0400	Mar 26, 2020 3:59PM GMT -0400
2	**The Top Cloud Security Threats for Your Business in 2019 and How to Avoid Them | Eastern Pe ak - Technology Consulting & Development Company : Eastern Peak – Technology Consulting & Development Company** https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/	Mar 26, 2020 3:59PM GMT -0400	Mar 26, 2020 3:59PM GMT -0400

3	**cloud storage and computing data breach - Google Search** https://www.google.com/search?q=cloud+storage+and+computing+data+breach&rlz=1C1CHBF_enUS894US894&oq=cloud+storage+and+computing+data+breach&aqs=chrome..69i57j0l7.32168j1j7&sourceid=chrome&ie=UTF-8	Mar 26, 2020 4:19PM GMT -0400	Mar 26, 2020 4:19PM GMT -0400
4	**7 Most Infamous Cloud Security Breaches - StorageCraft** https://blog.storagecraft.com/7-infamous-cloud-security-breaches/	Mar 26, 2020 4:19PM GMT -0400	Mar 26, 2020 4:19PM GMT -0400
5	**Massive WWE Leak Exposes 3 Million Wrestling Fans' Addresses, Ethnicities And More** https://www.forbes.com/sites/thomasbrewster/2017/07/06/massive-wwe-leak-exposes-3-million-wrestling-fans-addresses-ethnicities-and-more/#7241d1f375dd	Mar 26, 2020 4:21PM GMT -0400	Mar 26, 2020 4:21PM GMT -0400
6	**how do cloud services get hacked - Google Search** https://www.google.com/search?q=how+do+cloud+services+get+hacked&rlz=1C1CHBF_enUS894US894&oq=how+do+cloud+services+get+hacked&aqs=chrome..69i57.10923j0j7&sourceid=chrome&ie=UTF-8	Mar 26, 2020 4:23PM GMT -0400	Mar 26, 2020 4:23PM GMT -0400
7	**5 Safety Concerns with Cloud Data Storage, Answered.** https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/	Mar 26, 2020 4:23PM GMT -0400	Mar 26, 2020 4:25PM GMT -0400

8	**5 Safety Concerns with Cloud Data Storage, Answered.** https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/	Mar 26, 2020 4:31PM GMT -0400	Mar 26, 2020 4:31PM GMT -0400
9	**10 critical cloud security threats in 2018 and beyond | Synopsys** https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/	Mar 27, 2020 9:06AM GMT -0400	Mar 27, 2020 9:06AM GMT -0400
10	**can your put cloud servers behind a private network - Google Search** https://www.google.com/search?q=can+your+put+cloud+servers+behind+a+private+network&rlz=1C1CHBF_enUS894US894&oq=can+your+put+cloud+servers+behind+a+private+network&aqs=chrome..69i57.40430j0j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 9:07AM GMT -0400	Mar 27, 2020 9:07AM GMT -0400
11	**What Is a Private Cloud, the Benefits, and Who Should Use It?** https://www.liquidweb.com/blog/private-cloud/	Mar 27, 2020 9:08AM GMT -0400	Mar 27, 2020 9:08AM GMT -0400
12	**difference between private cloud and public cloud - Google Search** https://www.google.com/search?q=difference+between+private+cloud+and+public+cloud&rlz=1C1CHBF_enUS894US894&oq=difference+between+private+cloud+and+public+cloud&aqs=chrome.0.0l8.10883j0j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 9:12AM GMT -0400	Mar 27, 2020 9:12AM GMT -0400
13	**Private vs. Public Cloud: What’s the Differ ence20-=20Expedient?=** https://www.expedient.com/knowledgebase/blog/2014-06-05-private-vs-public-cloud	Mar 27, 2020 9:12AM GMT -0400	Mar 27, 2020 9:12AM GMT -0400

	-whats-difference/		
14	**Cloud Computing and Data Center Infrastructure as a Service - Expedient** https://www.expedient.com/services/cloud/	Mar 27, 2020 9:15AM GMT -0400	Mar 27, 2020 9:15AM GMT -0400
15	**Active directory in cloud services - Google Search** https://www.google.com/search?q=Active+directory+in+cloud+services&rlz=1C1CHBF_enUS894US894&oq=Active+directory+in+cloud+services&aqs=chrome..69i57.8260j0j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 9:19AM GMT -0400	Mar 27, 2020 9:19AM GMT -0400
16	**Define cloud services - Google Search** https://www.google.com/search?q=Define+cloud+services&rlz=1C1CHBF_enUS894US894&oq=Define+cloud+services&aqs=chrome..69i57j0l7.3990j1j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 9:23AM GMT -0400	Mar 27, 2020 9:23AM GMT -0400
17	**Home | Cloud Security Alliance** https://cloudsecurityalliance.org/	Mar 27, 2020 10:30AM GMT -0400	Mar 27, 2020 10:30AM GMT -0400
18	**Top Threats to Cloud Computing: Egregious | Cloud Security Alliance** https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven	Mar 27, 2020 10:30AM GMT -0400	Mar 27, 2020 10:30AM GMT -0400
19	**Top Threats to Cloud Computing: Egregious Eleven filetype:pdf - Google Search** https://www.google.com/search?q=Active+directory+in+cloud+services&rlz=1C1CH	Mar 27, 2020 10:31AM GMT -0400	Mar 27, 2020 10:31AM GMT -0400

	BF_enUS894US894&oq=Active+directory+in+cloud+services&aqs=chrome..69i57.8260j0j7&sourceid=chrome&ie=UTF-8		
20	**Top Threats to Cloud Computing: Egregious Eleven filetype:pdf - Google Search** https://www.google.com/search?rlz=1C1CHBF_enUS894US894&sxsrf=ALeKk01h4TJBxcnnBW3531UXBF75LR6WGA%3A1585315172511&ei=ZP19XpDlHqKC9PwP29eR8Ao&q=Top+Threats+to+Cloud+Computing%3A+Egregious+Eleven+filetype%3Apdf&oq=Top+Threats+to+Cloud+Computing%3A+Egregious+Eleven+filetype%3Apdf&gs_lcp=CgZwc3ktYWIQAzoECAAQRzoCCAA6BggAEBYQHjoFCAAQzQI6BQghEKABOgUIIRCrAlDJjoYCWN6xhgJg-bKGAmgAcAR4AIABvgGIAcsPkgEEMC4xNJgBAKABAqABAaoBB2d3cy13aXo&sclient=psy-ab&ved=0ahUKEwiQp9ud37roAhUiAZ0JHdtrBK4Q4dUDCAs&uact=5	Mar 27, 2020 10:31AM GMT -0400	Mar 27, 2020 10:31AM GMT -0400
21	**ug0dowg4gv32nlfwf8f461pbtz37?response-content-disposition=inline%3B%20filename%3D%22The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf%22%3B%20filename%2A%3DUTF-8%27%27The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20200327%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200327T143115Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=a8b8826928c16509ed1f71e4907699f48a66db2b0573ff6d5df7d6dfa92ad162** https://s3.amazonaws.com/content-production.cloudsecurityalliance/ug0dowg4gv32nlfwf8f461pbtz37?response-content-dispositi	Mar 27, 2020 10:31AM GMT -0400	Mar 27, 2020 10:31AM GMT -0400

	on=inline%3B%20filename%3D%22The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf%22%3B%20filename%2A%3DUTF-8%27%27The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20200327%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200327T143115Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=a8b8826928c16509ed1f71e4907699f48a66db2b0573ff6d5df7d6dfa92ad162		
23	**Netwrix 2018 Cloud Security Report - Google Search** https://www.google.com/search?q=Netwrix+2018+Cloud+Security+Report&rlz=1C1CHBF_enUS894US894&oq=Netwrix+2018+Cloud+Security+Report&aqs=chrome..69i57.1632j0j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 11:12AM GMT -0400	Mar 27, 2020 11:12AM GMT -0400
24	**Netwrix Research | 2018 Cloud Security Report** https://www.netwrix.com/2018cloudsecurityreport.html	Mar 27, 2020 11:12AM GMT -0400	Mar 27, 2020 11:12AM GMT -0400
26	**unsanctioned app use - Google Search** https://www.google.com/search?q=unsanctioned+app+use&rlz=1C1CHBF_enUS894US894&oq=unsanctioned+app+use&aqs=chrome..69i57j0l7.6527j0j7&sourceid=chrome&ie=UTF-8	Mar 27, 2020 12:13PM GMT -0400	Mar 27, 2020 12:20PM GMT -0400

27	**Get to Know About Sanctioned & Unsanctioned Apps With Associated Concepts - cloudsecurity.over-blog.com** http://cloudsecurity.over-blog.com/sanctioned-unsanctioned-apps.html	Mar 27, 2020 12:22PM GMT -0400	Mar 27, 2020 12:23PM GMT -0400
28	**What is Shadow IT? Defined, Explained, and Explored | Forcepoint** https://www.forcepoint.com/cyber-edu/shadow-it	Mar 27, 2020 12:30PM GMT -0400	Mar 27, 2020 12:30PM GMT -0400
29	**ug0dowg4gv32nlfwf8f461pbtz37** https://s3.amazonaws.com/content-production.cloudsecurityalliance/ug0dowg4gv32nlfwf8f461pbtz37?response-content-disposition=inline%3B%20filename%3D%22The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf%22%3B%20filename%2A%3DUTF-8%27%27The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb2020.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20200327%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200327T143115Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=a8b8826928c16509ed1f71e4907699f48a66db2b0573ff6d5df7d6dfa92ad162	Mar 27, 2020 2:07PM GMT -0400	Mar 27, 2020 2:07PM GMT -0400
30	**What is Shadow IT? Defined, Explained, and Explored | Forcepoint** https://www.forcepoint.com/cyber-edu/shadow-it	Mar 27, 2020 3:30PM GMT -0400	Mar 27, 2020 3:30PM GMT -0400