Secureworks®

GUIDE

The 2019 Cloud Security Guide: Platforms, Threats, and Solutions

Cloud security is a pivotal concern for any modern business. Learn how the cloud works and the biggest threats to your cloud software and network.

Today, nearly every enterprise relies on digital data and services to operate their business. Many organizations must abide by government regulations, such as **GDPR**, to store and access data when processing customer information. Consequently, businesses need a safe and secure way to house their information. Most organizations can't afford to do it all in house.

The cloud is instrumental for most businesses; **public cloud adoption is at 91%, and the private sector adoption is at 72%** for at least one application and its related data. As **cybercrime continues to rise** across the globe, businesses cannot risk storing critical data on unsecured servers. The result is heavy investment in cloud security protocols to make sure enterprise data is protected from hackers and breaches. **The Ponemon Institute demonstrated in a 2018 study** that that every key metric relating to the damage resulting from data breaches, from average total cost of a breach to cost per stolen record is increasing year over year, and the price tag for global damage is measured in tens of billions.

The vast majorities of American enterprises cannot afford the excessive costs and penalties from a data breach, so we must learn exactly how data is processed and stored to understand how to protect it. Let's first examine exactly what is the cloud.

What is the Cloud?

The "cloud" is not a physical location, but rather a mesh of computing resources, including networks, servers, and applications. The term **"cloud computing"** originated in the 1960s when early tech innovators used a cloud symbol to represent what would eventually become known as the internet. Data storage and software application usage are completely reliant upon this connected ecosystem.

Whether it's a place to store data or software, organizations use cloud facilities for a variety of reasons. For instance, many designers subscribe to **Adobe Creative Cloud services** to create visual content. Users access the software through a cloud service provider to create visual information like pictures and video without having to store copious amounts of data and software on their personal machine. This model benefits the software providers, because users do not have to install any software on their local computer. All they need is a web browser.

On a larger scale, corporations use cloud servers to store customer data. For example, Apple uses the Google Cloud Platform for **iCloud storage**. Although data is held in the cloud, information is still physically stored in servers and, depending on the provider, the type of data, and required access to the data, may be located internationally.

How does the Cloud Work?

In very simple terms, imagine the cloud as something similar to a local storage service. In order to keep your belongings safe and avoid a cluttered home or building an addition on your house, you opt to store things you don't need immediate access to in an outside facility for a usage-based fee. Now you've freed up space in your home, stored your belongings securely, and you can get to them anytime you like.

The cloud is similar when it comes to data storage. For example, storing all of the Netflix movies you watch physically on your device would quickly cause numerous issues from your bogged down hard drive. The cloud provides swift access to Netflix services, where users stream content without having to download the program or shows directly to their devices.

Cloud Service Providers (CSPs) take the storage and computing power burden off of large enterprises that pay to store and process their data and application processes in the public cloud. This type of structure is also known as "Infrastructure as a Service" (IaaS). Enterprises also pay for ready access to their data and for a multitude of CSP services which can include additional security "below the hypervisor". But, for many enterprises, the security control provided by their CSP's is a pivotal concern, especially when working with lesser known brands outside of the triumvirate of Amazon, Microsoft, and Google.

What is Cloud Security?

Cloud security includes the ecosystem of people, processes, policies, and technology that protect data and applications that operate in the cloud. **Cloud security consultants** examine how an enterprise processes and stores data and then craft a custom data-governance protocol for comprehensive protection. Professional cloud security assessments and penetration testing are instrumental to helping ensure cloud-service providers meet **government compliance** to responsibly protect your valuable data.

The previous sentence is the crux of cloud computing; cloud service providers are storing other people's data, some of which is personally identifiable information (PII). The cloud has created great opportunity, but also great responsibility for those providers to secure their customers' data.

Incidents such as the **Equifax data breach in the fall of 2017**, from which more than 143 million individuals' data may now be at risk, not only cost companies untold millions to return to compliance, but also compromise the confidence of their subscribers and shareholders. Businesses can rarely afford such a monumental hit to their reputation, so employing the **best cloud security** practices is critical for any modern enterprise.

In the unfortunate event of a company experiencing such a breach, having a **cloud incident response plan** in place is crucial to mitigate the impact of suspicious activity and minimize damage. Enduring any catastrophic enterprise event is traumatic enough, but how the enterprise reacts after such an event will often determine the fate of that organization. The organization's response plan will often determine the cost of a cyber breach.

Protecting critical data in the cloud is a shared responsibility.

Cloud Computing Services: SaaS vs PaaS vs IaaS

There are three different types of cloud computing services:

1. Software as a Service (SaaS)

Software as a Service (SaaS) allows a software company to publish their software and let their users access the software via a web browser. Suite servers like Microsoft Office 365 or applications like Salesforce provide users with instant access to documents and files without the hassle of installing, managing, and storing applications and data on their personal devices.

Users and organizations utilize SaaS applications for additional computer space, added cloud security, ease of updating software, and the ability to synchronize data across many devices. SaaS applications help users avoid software ownership and costly, time-consuming updates and typically operate on a monthly or annual subscription-based model.

2. Platform as a Service (PaaS)

Platform as a Service (PaaS) means that an enterprise uses software and hardware provided by a **Cloud Solution Provider** (CSP) to build and deploy their own suite of services. For instance, Amazon Web Services (AWS) and Heroku are popular PaaS providers that act as the platform or host to many other **popular software programs** such as **QuickBooks Online, Expedia, and Adobe. Enterprises** can utilize PaaS providers to develop and launch simple cloud-based apps to cloud-enabled enterprise applications.

Businesses can store their clients' data in the platform provider's cloud service without having to invest in hardware, software, and connectivity. They can also use testing and compiling **functions from PaaS** to efficiently communicate and deliver new production

developments with an extended national or international network. Avoid expensive investments for managing software licenses and utilize tools to inspect data and improve your cloud-based services.

3. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS), also referred to as utility computing, allows users to obtain access to servers, storage, and hardware through the cloud. The pay-as-you-go method allows users to pay a single monthly subscription fee based on how many gigabytes or megabytes of data they have hosted by the provider.

IaaS is the most flexible cloud computing service and allows users to customize their product mix. Direct access to outside servers requires no internal capital investment in expensive hardware. IaaS enables its organizational users to have the most control over their cloud infrastructure. Gain the cloud security your enterprise needs without upfront capital investments.

What are the Risks and Challenges of Cloud Computing?

Although cloud computing services are a great option for many businesses, there are some risks that come with the territory. Since the introduction of cloud computing, more and more companies have been steadily switching to third-party cloud computing providers. This influx of valuable data in single locations makes cloud providers a prime target for malicious activity.

As an illustration of this issue, imagine that everyone stores their savings in a personal safe at their respective homes. That means each homeowner is directly responsible for their own money. However, most people prefer to store the majority of their money in a third-party bank. Although this means that the bank will provide added security and have more secure safety regulations, it also means the bank is a prime target for professional robbers to attack.

Just like the bank scenario, businesses have to trust cloud vendors to secure their critical data. Although there are many security and government regulations in place, no data center is 100% safe from hackers and malware. Also, **insider threats** are becoming a prevalent concern for many cloud service providers.

CISOs should work closely with their cloud providers, treating the relationship as a partnership rather than just a hardware or software vendor. When treated as a partnership, you can vet out the details of the services that the cloud service provider is offering and you can choose the right partner for your needs.

Top Cloud Security Threats

Cloud providers are a prime target for malevolent hackers. Experts at the **Cloud Security Alliance** have identified the following 12 critical issues to cloud security (ranked in order of severity per survey results) referred to as the **"Treacherous 12"**:

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure Application Programming Interfaces (APIs)
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

The rise of enterprise cloud computing has created tremendous opportunity not only for cloud service providers, but also for cloud security specialists. Preventing any of these twelve vulnerabilities has become an industry unto itself. Small and medium-sized businesses are ridiculed for attempting to maintain their own data servers. Thus, every business that utilizes SaaS becomes dependent upon secure PaaS and IaaS providers, and vulnerable to any of these 12 threats.

Cloud Security Solutions

A protected cloud infrastructure is now a commodity that every modern business must have to remain competitive. Learn more about our **cloud security solutions** and how we can create a security strategy that fits your business' needs. From **cloud incident response** to resources for selecting a **cloud managed security services provider (MSSP)**, it is critical to learn how to protect your valuable data.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp