Cloud Computing Security

David Munyaka
Burman Noviansyah
Vibhor Goel
Andrew Yenchik
Steve Durham
# Table of Contents

Introduction .................................................................................. 3  
Infrastructure as a Service ............................................................... 4  
  Overview .................................................................................. 4  
  Products and Services .................................................................. 5  
  Future of IaaS ........................................................................... 5  
Platform as a Service ..................................................................... 6  
  Overview .................................................................................. 6  
  Products and Services .................................................................. 6  
  Future of PaaS ........................................................................... 7  
Software as a Service .................................................................... 7  
  Overview .................................................................................. 7  
  Products and Services .................................................................. 7  
  Future of SaaS ........................................................................... 8  
Security as a Service ..................................................................... 9  
  Overview .................................................................................. 9  
  Categories and Key Players .......................................................... 10  
  Deterrent Factors ...................................................................... 11  
  Future ....................................................................................... 12  
Cloud Stack Security Concerns ....................................................... 12  
  IaaS Security ........................................................................... 12  
  PaaS Security ........................................................................... 12  
  SaaS Security ........................................................................... 13  
  SECaaS Security ....................................................................... 13  
Cloud Computing Security Market Outlook .................................... 14  
  What is driving the growth in the Cloud Computing Security market? ........................................................................................................... 14  
  What does the Cloud Security Market look like today? .................. 16  
  Where Will the Market Go? .......................................................... 16  
Works Cited .................................................................................. 18
Introduction

Cloud computing has more to offer businesses and individuals than ever before. Many are moving to the cloud to take advantage of the on-demand nature of documents, applications and services. An area of cloud computing that is starting to garner more attention is cloud security, as well as Security-as-a-Service (SECaaS). These security areas are increasing in attention in response to businesses move to the cloud – cyber thieves follow data and confidential information. Similar to on-premise computer and server security, cloud security adoption has lagged behind cloud service adoption.

However, the SECaaS area is beginning to growing rapidly, and will continue to grow. Many individuals move to the cloud without considering what possible security pitfalls may be present, and who could be reading their sensitive information. Services like email (Gmail, Hotmail, etc.) and social networks have always been housed in the cloud, and have long been a personal security threat.

Conversely, many organizations are paralyzed with regard to cloud services, not realizing that there are security solutions that can protect confidential information as it passes through the cloud stack (Penn). These organizations have robust security options, as many familiar names in IT security have products for cloud security. SECaaS products include Identity and Access Management, Data Loss Prevention, Web Security, and Intrusion Management, and more (Orans, MacDonald).

The cloud is going to continue to grow for the foreseeable future. Mobile access to company assets is a trend that will continue to grow at a fast rate. Governments are moving their data to the cloud, and purchasing cloud security solutions to protect themselves and their agents all over the world; about 30% of cloud security solutions are purchased by government entities at this point.
Although SECaaS currently accounts for only 2-3% ($463MM) of the overall security market, we forecast that it will continue to grow to ~5-6% ($1.5B) of the security market by 2015, and possibly as much as ~20%($9B) by 2021 (Technavio Insights, Penn).

Cloud computing is a hot trend. Going to the cloud is not only fashionable, but it saves time, money, and resources. The move to the cloud shows no signs of slowing down, and cloud security products will need to continue to keep up with demand. SECaaS has the potential for exponential growth and expansion in the ever-evolving cloud computing market.

**Infrastructure as a Service**

**Overview**

Infrastructure-as-a-Service (IaaS) as a concept is easier to grasp because of some similarity it shares with the traditional infrastructure that was used and is still used in many organizations today. With the traditional infrastructure an organization needed to purchase servers, all networking components and storage devices. A lot of capital is required to start up a business and more funds may be required for a company that wants to change its business model to adapt to changes in the market. Even though the concept of cloud computing dates back to the 1960’s, Cloud Computing Services were not widely offered until mid 2008, at least in the way it is discussed in this paper (eyeOS Blog)—“cloud computing” may have different meanings depending on how the term is used. It was during 2008 when services such as IaaS began to be offered by companies such as Amazon.

The ability for a business to acquire IaaS began to make it easier for Startups and other businesses, especially those who could not afford infrastructure they needed, to meet their technology requirements. Advancements in computer technology in areas such as networking, the Internet, virtualization technology, clustering and load balancing capabilities have enabled IaaS providers to offer scalable, shared and manageable environments (Dawoud). Other companies that provide cloud computing services specifically IaaS are Amazon, AT&T, HP, Verizon, CA Technologies, Cloud Scaling, DATA PIP and Eucalyptus Systems among others (Cloud360).
However, even with the advantages that are mentioned above, IaaS has significant security challenges. The security challenges of providing this service become increasingly complex as the number of users increases. Also, customers of IaaS must share resources, which has security implications as well. The IaaS delivery model consists of components such as service level agreement, utility computing, cloud software, platform virtualization, network connectivity, and computer hardware (Dawoud). All of these components face different security and privacy issues. The challenges of cloud computing from a user's (i.e. company that pays for the service) point of view are: knowing exactly where the data is located, whether others are accessing the data, and whether the data is being compromised.

**Products and Services**

Products and services that are offered by IaaS providers are:

Servers: Most business may require similar servers but depending on the nature and size of a business the number and type of servers required may differ. Examples of servers that are commonly used are Database servers, Application servers, and Mail servers, among many others. Security products used in traditional way of securing servers and storage are still relevant, e.g. use of firewall and Intrusion Detection Systems. An IaaS provider can provide a firewall for a fee to filter mail received by a startup business.

Storage Devices: High Capacity hard drives are also made available for lease to companies that need these services. The IaaS providers are able to do this as they have data centers with hard drives that are able to store large-scale data, and with use of virtualization this capability is significantly improved.

**Future of IaaS**

Currently there are security concerns that are holding businesses back from acquiring services such as IaaS. However, with more studies concerning these addressing these issues, we can expect that more companies/businesses will feel confident migrating to the cloud. Also by applying Moore’s Law there can be an expected increase in processing power and memory (Ushman). Based on Moore’s law we can then predict that virtualization capacity will also increase. With increased virtualized capacity, we
can expect increased efficiency and scalability. This may cause more companies to migrate to the cloud in the future.

**Platform as a Service**

**Overview**

In the cloud stack, Platform-as-a-Service (PaaS) sits in the middle, between Infrastructure-as-a-Service and Software-as-a-Service. Customers who make use of PaaS do not want to deal with the hassle of purchasing a physical computer, installing the operating system, and all other steps that go into integrating a computer into the company’s workflow (Keene). PaaS is often used in instances of application development, which allows for a developer start programming without having to install an Operating System, a Database server, or a Web server. This frees organizations from significant overhead in terms of money and resources in supporting their hardware.

PaaS offers the ability to make the computer into a service, freeing the user from maintenance on the machine – and truly – even caring about the operating system that they are using. PaaS deployments can be public – like Google App Engine and Windows Azure – allowing anyone to sign up and use the platform. They can also be private, set up and monitored by an organization, used only by internal members of that organization. Private clouds offer two distinct advantages: 1) sensitive information need not be transmitted over the public internet, 2) if the internet connection in the building is down, local network resources that are still available can serve data from the private cloud (Bhadauria).

**Products and Services**

High-Assurance Hypervisor is an idea that is on the rise, and very close to corporate acceptance. This would greatly improve the confidence in public PaaS in the commercial world. If a Hypervisor is High-Assurance, users can be confident that their data and deployments are safe from outside tampering. Many companies are beginning to support this capability (MacDonald).

Along with the rise of High-Assurance Hypervisors, the private cloud is an idea that is also gaining traction. This is due to the natural progression from server virtualization to server virtualization in the
cloud. Many companies have found the virtualization reduces capital costs, and will soon find that a private cloud can speed the delivery of services (Penn).

Google App Engine, along with other offerings such as Engine Yard and Microsoft Azure allow for the complete development, deployment, and hosting of mission critical web applications. Customers only have to pay for the bandwidth they use, with the provider scaling network resources to fit the demand for the application (appengine.google.com).

**Future of PaaS**

We believe that PaaS will continue to grow along with demand for SaaS. As consumers care less about what platform they need to run their software (as a service), they will care less about what, if any, platform they have. PaaS by way of Google’s Chrome OS will continue to make itself relevant through its use in schools, due to low cost hardware (Lardinois).

Having PaaS tool as a startup can drastically lower barriers of entry. Companies will take advantage of the ability to run their whole operation without buying a single server.

**Software as a Service**

**Overview**

In the Cloud Computing Stack, Software-as-a-Service (SaaS) sits on top of Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). SaaS is simply software that is delivered from a server in a remote location to your desktop, and is used primarily online. Typically, it is accessed using a thin client via a web browser, although some SaaS software uses its own interface, designed to provide special characteristics for its application or its users. Initially, SaaS software existed only in real time – within an online connection. But, as SaaS evolved, applications that live on an appliance (a server managed by the SaaS vendor) on the user organization’s premises became prevalent (Simon 97-112).

**Products and Services**

SaaS applications are available more or less for all business segments. As part of their SaaS product line, Google provides Google Apps for Business, which includes solutions like business email,
calendar, documents and more. These products are bundled with features such as multiple platform integration and 99.9% uptime SLA (Google Apps for Business).

SaaS startup desk.com (previously known as Assistly) helps companies collect and organize all of their customer conversations into a prioritized actionable list and equips support staff with the tools to respond to customers. The application allows businesses to filter conversations, access customer histories, automate processes and even tap into social media conversations on Facebook, Twitter and other sites (Rao). Demandforce’s SaaS application automates Internet marketing and communications so customers can focus on running their day-to-day operations (Rao). Cloud financial management company Intacct sells cloud-based software for financial functions — including applications for accounting, contract management, revenue management, inventory management, purchasing, vendor management, financial consolidation and reporting (Lomas). Education technology company EverFi has created a SaaS application for schools to help educate young adults on financial literacy, student loan default prevention, filing taxes, credit card debt and other critical life skills. The application’s curriculum incorporates virtual worlds, social media and videos to help teach children these life skills (Rao).

**Future of SaaS**

Investment in cloud computing is increasing more rapidly than investment in IT in general. One of the most promising trends in SaaS-applications is the mutual integration of various SaaS-services, including those developed by different vendors. As software offered by different vendors is developed to remove compatibility issues, dependency on SaaS applications will increase. We believe the future of SaaS is the elimination of servers being hosted at user location, with all applications being hosted on cloud. The future is looking bright for SaaS as clients move beyond early experimental implementations. Moreover, SaaS providers are coming up with solutions to problems like data security, application uptime and more. These problems have played a major role in preventing users from adopting SaaS services and applications. Gartner projects global spending on SaaS to remain strong through 2015 when it is estimated to reach $22.1 billion. Market researcher IDC maintains that SaaS delivery will significantly outpace traditional software product delivery, growing nearly five times faster than the software market as a whole. Specifically, IDC says that by 2015, nearly $1 of every $6
spent on packaged software and $1 of every $5 spent on applications will be consumed via the SaaS model. Moreover, SaaS delivery will constitute about 13.1% of worldwide software spending across all primary markets and 14.4% of application spending during the same time frame, IDC says (Stackpole). The chart below displays predicted distribution of workload processing.

Security as a Service

Overview

After understanding the basics of the cloud stack, the next challenge is to protect these services from security threats. Securing conventional assets for infrastructure, platform, and software can be done by, but is not limited to, implementing physical access limitations. But for the cloud, where physical assets are seemingly intangible, various ways of providing security solutions are inevitably needed. In general, Security-as-a-Service (SECaaS) is outsourcing security management to a third party. Before the cloud era, a conventional company would host their own infrastructure at a physical location. That company would then allocate further expenses to secure their IT assets. These security expenses could vary from implementing network security appliances (e.g. IDS/IPS appliance, Firewall appliance) to hiring experts who evaluate security operations and procedures. When a company moves their IT services from their own internal network to the cloud (to a cloud provider, such as AmazonWS), the company can cut down the physical maintenance and data security expenses to the cloud provider.
This allows the company to focus on their business, concentrating on what they do best and leaving IT security to cloud experts.

For each cloud service that has been discussed, the cloud service provider provides some security measures. For example, that IaaS service provider only allows connectivity from specific IP addresses in their Access Control List (ACL). PaaS service providers only allow certain usernames and passwords. SaaS service providers also limit their service to those who already have the security token before utilizing the software.

SECaaS does not refer only to securing cloud infrastructure. SECaaS also has the ability to secure the entire enterprise network that may be hosted physically on-premise. The security tools and main appliances are hosted by a SECaaS company in the cloud. For users who want this level of service, the SECaaS company can put a small appliance in the user’s or company's network so that their network can be reached by the SECaaS provider. Usually, an enterprise already maintains network security policies that only permit specific protocols and port numbers to enter the network. With this SECaaS appliance, a company can allow the incoming and outgoing traffic to the SECaaS provider confidently.

But, the question still lingers: should the enterprise trust a third party to secure their digital and data assets? Before we can come to a conclusion, we should delve into the types of services as well as the providers of SECaaS.

**Categories and Key Players**

The Cloud Security Alliance (CSA) identified the categories of services that define the major security concerns for cloud computing. These categories originate from research, studies, and surveys collected from experienced customers of cloud services (SECaaS Working Group). The categories are:

**Identity and Access Management (IAM)** - provides protective and preventative controls for assured identity and access management. Key players include SailPoint, Aveksa, Oracle, Courion, and CA Technologies (Perkins, Carpenter 3).

**Data Loss Prevention (DLP)** - provides preventative controls by monitoring, protecting and verifying the security of data at rest and in motion. Key providers include Symantec, McAfee, Sophos, Trend Micro, and Kaspersky Lab (Firstbrook, MacDonald, and Girard).
**Web Security** - provides real-time protective, detective, and reactive control by protecting software and appliance installations. This may occur on-premise or via cloud by proxying or redirecting web traffic to the cloud provider. This may include the ability to perform URL filtering and Malware detection. Key players include Cisco, BlueCoat Systems, Websense, Zscaler, and McAfee (Orans, and Firstbrook 2).

**Email Security** - provides protective and reactive control over inbound and outbound email from threats such as phishing, malicious attachments, and spam. Key players include Cisco, Symantec, Proofpoint, Microsoft, Google, and McAfee.

**Security Assessment** - provides detective control by auditing cloud services or assessing systems located on company premises based on industry standards.

**Intrusion Management** - provides detective, protective, reactive control by using predefined signatures to prevent unusual events. Key players include McAfee, Sourcefire, and HP (Young, and Pescatore 2).

**Security Information & Event Management (SIEM)** - provides detective control by performing correlation analysis between logs and event information and then analyzes the system behavior to enable real-time alerting and reporting. The key SIEM players are HP ArcSight, IBM Q1 Labs, McAfee Nitro Security, NetIQ (Novell), and LogRyhtm (Nicolett, and Kavanagh 2).

**Encryption** - provides protective control by scrambling data (i.e. plain text) using certain cryptographic algorithms to produce a ciphertext, which is only understandable by the intended party.

**Business Continuity and Disaster Recovery** - provides reactive, protective, and detective control by measuring the design and implementation of a certain system so that operational resiliency still exists when a service disruption occurs.

**Network Security** - provides detective, protective, and reactive control by allocating access, distributing, monitoring, and protecting the network resources that provide a total service. Certain services, protocols, or ports can be explicitly allowed or denied.

**Deterrent Factors**

Enterprises might be reluctant to use SECaaS to secure their network. SECaaS providers are not cheap, and allowing a third party to access their network or to store an appliance within their network is additionally concerning. This is similar to allowing a stranger to enter your house and inspect it for
security against thieves. Moreover, many companies and enterprises have proprietary policies, software, and operations that they don’t want to reveal to anyone, even their security provider. There will always be a trade-off between security, speed, and secrecy.

Future

Over the next five years, we believe that the number of players in the SECaaS game will grow along with the security needs on the cloud. Several factors that deter many enterprises from going to the cloud will be diminished as the price of SECaaS services decrease but the offerings grow more robust. The competition in the SECaaS market will drive products to be robust, secure, and cost-effective. Additionally, SECaaS provider’s credibility will grow as more enterprises successfully implement and prove their services.

Cloud Stack Security Concerns

IaaS Security

Storage hardware or servers can be physically accessed and compromised (Dawoud). This can lead to denial of service attack and, depending on the nature of the attack, this could lead to loss of important data availability. Confidentiality could be an issue if the attacker is able to view data at a datacenter—a problem that is handled by use of encryption and access controls, but attackers can always find their way around these barriers.

Cloud software can have bugs and vulnerabilities that can be exploited. Virtual machines are mobile and the hypervisor stores the virtual machines as files, making the virtual machines vulnerable to copying to another device. The ability of an attacker to copy a virtual machine provides the attacker the advantage of trying to break into the system without detection since these attacks are being performed on a copy of the virtual machine (Dawoud).

PaaS Security

Some of the threats that PaaS administrators face include the fact that since PaaS instances operate as virtual machines, it can be possible for users to “break out” of their virtual machine. By doing so they
may be able to bring down the hypervisor, which may be running many other customers’ PaaS instances, effectively causing a denial of service (Schultz).

Like any other cloud service, the user is removed from the machine they are working with, and the upkeep and maintenance is performed by others. A hypervisor administrator without scruples would have the ability to look at private data, possibly stealing intellectual property. Care must be taken in what data to store in such situations, as well as how to store the data.

A concern that is ever present when dealing with public cloud services is the transmission of sensitive data over the public Internet, and especially through the hardware of a hypervisor that has other tenants. Another virtual machine may intercept traffic coming over the shared network connection, exposing sensitive information to unintended parties (Dawoud).

**SaaS Security**

The biggest security concern in the SaaS environment is immature identity management. Google has a “Secure Data Connector” that forms an encrypted connection between a customer’s data and Google’s business applications. This allows the customer to control which employees may access Google Apps resources. But users who use multiple SaaS applications will end up using different security and identity systems. At times it is required by a client that sensitive data should remain within certain geographical locations. But, with SaaS, users cannot be sure about the location of data storage. Moreover, currently there are no robust standards to evaluate SaaS security or Cloud Security in general. Some service providers claim to be SAS 70 and ISO 27001 compliant, but these standards are relevant to information and systems security. Moving forward, policy makers should come up with specific standards so that users can evaluate the SaaS application from security perspective before using it (Brodkin).

**SECaaS Security**

Enterprise users should not simply allow a SECaaS provider to put equipment on their premises without understanding what information may be passed through said hardware; security is still the enterprise users’ responsibility, even if it is delivered by a SECaaS provider. The company can assume that all
traffic passing through a SECaaS appliance will travel securely to the provider. However, sensitive data should be filtered by an IDS or IPS before travel to the cloud. A stateful packet inspector can also be used to monitor data passing through the appliance.

Security in IaaS, Paas, and SaaS is mainly concerned with limiting connectivity to and from certain networks. In SECaaS, permissions can be implemented to control access to specific resources.

SECaaS assists in bridging the gap between the security that Cloud Service Providers (CSPs) offer and the security that should be in effect on company premises. SECaaS will not maintain the security layers for each cloud service. It is the responsibility of the CSP to provide security solutions for IaaS, PaaS, and SaaS. CSPs typically only provide limited security features like username and password, Access Control List, or possibly a session token ID. Those security features can only guarantee which usernames access the cloud.

SECaaS offers the capability to manage how enterprise networks should be configured, so that a secure state can be achieved. SECaaS also can be used to secure other cloud services. For enterprises that have higher risk than others, having a secure way to connect to the cloud is a must. Hence, enterprises can have a layer of security between their assets and equipment that connects them to the cloud. Enterprise can install and deploy IPS on the cloud along with a DLP solution, so that data that is transmitted from Enterprise premises can be inspected before being sent to the cloud. This also can prevent sensitive data from transmission to another cloud without being detected.

Cloud Computing Security Market Outlook

What is driving the growth in the Cloud Computing Security market?

The use of cloud services is growing rapidly in a broad range of areas as more companies start using the cloud. Employees are on the go with mobile devices with VPN connections and huge amounts of data being stored and analyzed in the cloud. The use of cloud-based solutions is growing at a rapid pace, and we predict that this growth will not slow down. It is important to understand what is moving this market forward in order to observe and understand the aligned security concerns. See Global
Cloud Computing Security

Cloud Security Software Market for a more detailed breakdown of these growth drivers, as the following is a summary of their findings mixed with additional research (Technavio Insights).

**Mobile Employees:** The majority of employees are continually on the move. The rise of global firms and geographically dispersed operations require companies to provide employees with access to critical information through the cloud. Providing access to email, databases, documents, and records from anywhere at anytime is alarming and opens extra risks to a firm's digital holdings. With mobility and travel for employees moving ever forward, cloud security is a growing and inevitable concern (McKendrick).

**Specific Attacks on the Cloud:** The cloud has been the Wild West of technology for the past few years. Until recently, cloud specific attacks were sparse due to the unknown and varying nature of cloud technologies. As these technologies mature and become more common, honed, cloud-specific attacks are now real and dangerous. Companies and users put critical data in the cloud – this entices specific attacks on the cloud. A growing number of specific attacks on the cloud are forcing companies to find and implement robust cloud security solutions (Strauss).

**Government Adoption:** Large portions of government departments are adopting cloud-based services. Currently, government agencies account for 30% of cloud based security solution purchases (Technavio Insights). Government employees are on the go at the highest rate ever. Defense and Intelligence agencies rely on cutting edge technologies to stay abreast of threats and ahead of would-be data thieves. Government has a mammoth amount of sensitive data to store, secure, and analyze. Moreover, the government is the focal point of a large number of attacks. These reasons constitute the fact that cloud security solutions are needed to ensure the safety and continual use of the cloud by government.

**Non-Traditional Adoption:** Commonly, cloud based solutions are thought of as solutions for government or Fortune firms with big data problems. This common thought does not take into account the benefits that any firm finds by moving to the cloud. Social networks, file sharing networks, online gaming or gambling, streaming video, and other non-traditional cloud consumers are all moving to the cloud and are seeing huge advantages. Most email solutions (Gmail), social networks (Facebook),
personal file storage (Dropbox), and online archive services use the cloud. These high adoption rates make the cloud a prime target for hackers to steal sensitive personal and company data.

**Business Continuity and Disaster Recovery Solutions:** An advantage of cloud based storage is its ability to store large amounts of data in secure locations in real-time (Crandell). Seamless integration and backups make the cloud a prime location to store, backup, and archive data. Websites and firms, large to small, all value the safety and security of redundancy and off-site backups. The cloud is a critical storage solution, whether the cloud is public or private. Companies are adopting cloud security solutions at a rapid pace; placing critical recovery data at great risk (“Onsite and Offsite Cloud Backups”).

**What does the Cloud Security Market look like today?**

The Cloud Security market is a growing market, and is relatively small when compared to the overall computer security market worldwide. In 2010, cloud security accounted for only 2-3% of the overall global computer security software market (Technavio Insights, McKendrick). Predictions estimate that cloud security, including SaaS, is outpacing the overall security market and will increase in size proportional to the whole. A Technavio Analysis estimates that the cloud security market will account for 4% of the overall global security market in 2014 (Technavio Insights). Furthermore, Forrester forecasts that the cloud security market will reach 1.5 billion, 5-6% of the overall security market, in 2015 (Penn).

These insights and forecasts by top research institutions show the rapid growth of cloud security compared to the overall market. Based on the analysis of cloud computing, the rapid acceptance of its use, and the continuing improvement of security concerns, it is possible that the cloud computing security market will reach 12% by 2018 and 20% by 2021.

**Where Will the Market Go?**

Predictions about the growth of the cloud security solutions market are based on estimates made by leading research firms, such as Forbes, Forrester, and Gartner. The graph below is an amalgamation
of their predictions, showing how much companies will spend on cloud security solutions each year until 2021. Note that all values are in millions of dollars.

Growth in this market has remained steady since 2010, averaging between 35 and 45% growth each year. This same growth is projected to continue until 2015. Projecting past 2015, growth is expected to increase to around 50% each year until 2020. At that time, it is expected that the growth in the cloud security market will slow substantially. This will occur due to a few factors. First, most companies that want to be in the cloud will be there, in some way, by 2020. Second, SECaaS will be providing sufficient security products to deal with the majority of security concerns by 2020. Next, cloud security is the focus of much professional and academic research, speeding the maturity of the security market. Finally, the overall cloud market will begin to mature around 2020, contributing to a plateau in the cloud security market at around the same time.
Works Cited


