Security-as-a-Service from Clouds: A Comprehensive Analysis

Deepak H. Sharma
Department of Computer Engineering,
K. J. Somaiya College of Engineering,
Mumbai, India

C A Dhote, PhD.
Department of Computer Science & Engineering,
P. R. M. I. T & R,
Amravati, India

Manish M. Potey
Department of Computer Engineering,
K. J. Somaiya College of Engineering,
Mumbai, India

ABSTRACT
In Security-as-a-service model the focus is on security provided as cloud services; i.e. security delivered through the cloud instead of on-premise security solutions. The security-as-a-service model can also enhance functionality of existing on-premise implementations by working as a hybrid solution. The paper provides the comprehensive analysis of security-as-a-service delivery model from various perspectives. The paper addresses various issues regarding security delivered as cloud service. This paper addresses various questions that may arise regarding security-as-a-service viz. definition of security-as-a-service, its need, different security services currently available, different providers of same, different users and likely users of this service, various evaluation criterions for security-as-a-service solutions and implementation methods of such solutions.

General Terms
Cloud Computing, Security issues, Hosted Security model.

Keywords
Security-as-a-service

1. INTRODUCTION
Security-as-a-service model focuses on security provided as cloud services; i.e. security delivered through the cloud instead of on-premise security solutions. The security-as-a-service model can also enhance functionality of existing on-premise implementations by working as a hybrid solution. The paper provides the comprehensive analysis of security-as-a-service delivery model by discussing various aspects about it. The paper addresses various issues regarding security delivered as cloud service. This paper addresses the following issues in separate sections. Section 2 defines security-as-a-service. Section 3 discusses its needs and its various advantages over on-premise platform based security solutions. Section 4 then covers the different security services presently available. A survey of various providers is done in Section 5 to enlist who are the different types of providers of security as a cloud service. This type of cloud security service can be used by a number of different organizations; this paper then presents in Section 6 the different types of organizations who can use such type of cloud service effectively. Section 7 discusses how such services are being implemented by various providers. With various vendors offering such kind of managed security service it is very important to understand how to evaluate effectiveness of such security services. Section 8 enlists these various criteria. This paper then concludes in Section 9 by discussion on the future of security-as-a-service delivery model.

SECURITY-AS-A-SERVICE

The focus here is on security provided as cloud services; i.e. security delivered through the cloud. The information security vendors are changing their delivery methods to include services delivered through the cloud. Some information security companies are emerging as pure cloud service providers to provide security only as a cloud service [6]. The main areas of focus today are email security, end point protection, web protection, anti-malware and anti-spam being provided by various vendors [6]. Security-as-a-service is likely to continue to grow in future not only in terms of security capabilities but also in terms of different options, services being offered and their depth.

2. NEED OF SECURITY-AS-A-SERVICE
Hosted security model is emerging as convincing alternative to on-premise platform based security solutions. There is considerable reduction in the total cost of ownership as compared to on premise security solutions as reported by [14] because there is no upfront capital expenditure involved in these types of services. When anti-virus and anti-spam filtering services are hosted on cloud, it will eliminate around 75% of the email that would normally come into the organizations' network as spam, only to be quarantined and eventually discarded by end users. This will reduce the on-premise bandwidth and storage requirements, and their related costs. Many security solutions for remote and mobile users will now become available. With proliferation of more endpoints (mobile and otherwise) and moving antimalware also to the cloud, the overall detection rate will be better and effective as compared to results of single engine running on an endpoint. Security-as-a-service model when implemented for organizations will put an end to expensive security appliances and complex security software deployments. The hosted security model can be used in a hybrid manner to enhance functionality of existing on-premise implementations. Thus, allowing organizations more flexibility in choosing desired security options for different remote premises or headquarters. For example an organization can deploy on-premise security for a headquarters operation, while using hosted security for remote offices. The services and solutions will be more efficient and easy for administration with services moving to the cloud as service. Hosted security solutions provide a better security as they use multiple malware-scanning systems as compared to single malware scanning in on-premise solutions. They update new signatures and other defenses faster as compared to direct updates at various customer endpoints in on premise solutions. Easy, highly scalable and fast deployable security solutions can be made available as cloud services.

3. SECURITY SERVICES PRESENTLY AVAILABLE

The Cloud Security Alliance (CSA) [2] has identified various categories of security-as-a-service offerings in 2011 [16]:

- Identity and Access Management: It includes managing access to enterprise resources by verifying the identity of an entity and granting it correct level of access based on its authorized level.
- Data Loss Prevention: Data Loss Prevention is protecting and securing the data at various stages in the cloud viz. data at rest, in motion and in use both in the cloud and on-premises.
- Web Security: Web Security is real-time protection offered via the cloud by redirecting web traffic to the cloud provider and then forwarding clean traffic to the customer's organization.
- Email Security: Email Security provides control over inbound and outbound emails, thereby protecting the organization from phishing, malicious attachments, and enforcing corporate polices as desired by the customer organization.
- Security Assessments: These are audits done by third party for cloud services or assessments of on-premises systems via cloud-provided solutions based on some industry standards.
- Intrusion Management: Intrusion Management is the process of intrusion detection / prevention using signature or anomaly based approach to respond to unusual events.
- Security Information and Event Management (SIEM): SIEM analyses and correlates logs and event information related to security issues to provide real-time reporting and alerts on security incidents / events that may require attention.
- Encryption: It is the process of providing private and public key cryptographic algorithms for security of data at rest, in motion and in use both in the cloud and on premises.
- Business Continuity and Disaster Recovery: These are the processes and measures to ensure operational resiliency in the event of any failures and service interruptions.
- Network Security: Network Security consists of security provisions that allocate access, distribute, monitor, and protect the underlying network resource services.

The main areas of focus today are email security, end point protection, web/ Internet protection, Vulnerability Assessment and management, Identity management, anti-malware and anti-spam being provided by various vendors. Other emerging hosted security services include Managed firewalls, IDS and IPS, instant messaging security, authentication, e-mail archiving and Cloud based vulnerability management etc. Security-as-a-service is likely to continue to grow in future not only in terms of security capabilities but also in terms of different options, services being offered and their intensity.

4. DIFFERENT TYPES OF PROVIDERS OF SECURITY AS A CLOUD SERVICE

The Security-as-a-service is currently being provided by two types of security providers. The first types of vendors are existing information security providers who are changing their delivery methods to include services delivered through the cloud. The second types are information security companies who are emerging as pure cloud service providers which provide security only as a cloud service. The current services being focused are anti-malware vendors and services especially with regard to email filtering. Current security-as-a-service being provided by different vendors improves information security: email filtering including backup, archival, and e-discovery; web content filtering including IDS / IPS; vulnerability management and identity-as-a-service. Functionality of existing on-premise implementations are being enhanced by using security-as-a-service as a hybrid solution.

5. DIFFERENT USERS/ LIKELY USERS OF THESE SOLUTIONS

These solutions can work best with existing on premise platform based solutions in a hybrid manner to enhance their security capabilities. Many companies have security needs for remote and mobile users for all which will now become available. With proliferation of more endpoints (mobile and otherwise) these solutions will be needed for all these corporate, Small and Medium-sized Business (SMB) companies. The SMB sector who want to reduce the initial Capital Expenditure (CAPEX) and want fast deployable and easily administrable security solutions. In addition to business travelers, smart phone users, many employees are now working from home or from remote locations, this means that the existing security solutions will have be extended to cover all above types of users. In these types of cases security delivered as cloud service can be very effective, manageable and scalable as well.

6. IMPLEMENTING SUCH SECURITY SOLUTIONS

In this type of security model the entire traffic viz. email, web, etc. going inbound and outbound from an organization is diverted to the security service providers' cloud as shown in Figure 1 [6] and Figure 2 [13], where all security enforcement policies are applied and only clean, filtered traffic is delivered to the organizations network [6][13]. This in fact also reduces the bandwidth requirement on the organizations' network as all spam, malware; etc. is already filtered out even before it reaches the organizations network. Various security policies like anti-malware, anti-spam, data analysis, URL filtering, compliance reporting, data leakage protection, encryption etc. can all be applied at service providers level and for all types of users mobile and otherwise. The right security-as-a-service solutions can perform effectively and at a lower cost as compared to on premise solutions.

Figure 1 from Ref [13]

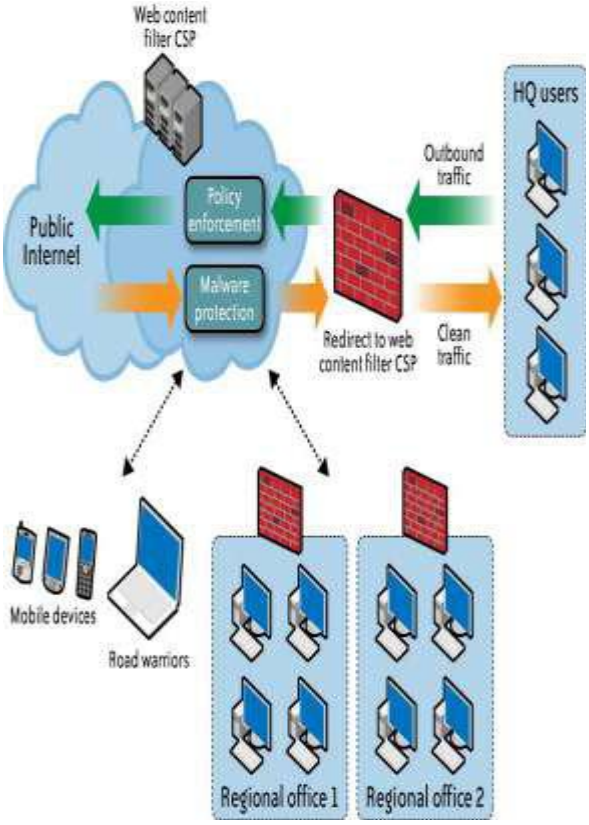

Figure 2 from Ref [6

8. EVALUATION CRITIRION FOR SECURITY-AS-A-SERVICE SOLUTIONS

It is very important to understand and evaluate a security-as-a-service solutions' effectiveness. It must truly provide a better alternative to on-premise security solution without compromising on the overall security effectiveness. The following are the some of the evaluation criterion as suggested by white paper from Websense [14].

- Reliability: highly reliable and fully available services as downtime would mean an organization assets will be exposed to attacks which would defeat all its advantages. Hence service providers have to guarantee highly reliable and always available services.
- Effectiveness: the solutions available should be as effective as legacy solutions for handling known threats and should also be able to handle unknown threats effectively.
- Performance: moving the security on the cloud will actually improve performance and can scale a security solution on demand. As routing all traffic through security service will ensure that all spam, malware and unwanted web traffic never reaches a customer's local network and never impacts its bandwidth and network integrity. The service providers have to ensure that service on the cloud is efficient and does not become a bottleneck.
- Flexibility: a security-as-a-service solution can work together with existing on-premise solutions in hybrid manner and can result in benefits like off-loading of processing, reducing bandwidth, and protection against traffic spikes etc. The service providers have to make this hybrid option available so that such solutions can work with legacy on-premise solutions.
- Control: the service provider has to guarantee meaningful service level agreement (SLA). This will ensure the effectiveness of such solutions give a level of uptime assurance that is available for an on-premise solution. The customer organization uses a web browser to manage system in same way they manage an appliance on their network.
- Privacy and security: another primary concern a customer organization might have is privacy and security of their sensitive data which might get exposed to unauthorized users. One of the ways to ensure this is to assess the service provider's / vendor's privacy and security measures through the use of some third-party certification procedures and compliance periodically.
- Total cost of ownership: the core benefit of such security services is reduced total cost of ownership. The costs of distribution, deployment, and ongoing upgrade of on-premise hardware are eliminated. Bandwidth costs reduce, labor costs reduce and built-in fault tolerance on the cloud further eliminates the need for additional redundancy hardware / software measures.

The above mentioned evaluation criterions are sufficient for the services being provided currently. But with likely increase in number of services some more criterions will be needed and will have to be explored further viz. ease of use, seamless

integration of all services together, ensuring 100 % availability etc.

9. CONCLUSION

The cloud service delivery model is being extended to provide security delivered as cloud service. Various options today exist and Security-as-a-service is likely to continue to grow in terms of security services and in terms of different options, capabilities and their depth. The security-as-a-service is performing reliably and effectively to deliver security services better than on premise solutions. The advantages that are being offered by providing security as service from clouds are lowered costs for enterprises without compromising privacy and security. There is no upfront investment needed, no maintenance of hardware and software, the security solutions are resource-friendly, the updates take place automatically and transparently, the services are easy to use, easy to maintain and the services are available through Web based management anywhere, anytime. The services can be provided in a hybrid manner together with legacy solutions to improve overall effectiveness and provide more flexibility in choosing what goes where according to the individual customer needs. The evaluation of such services and service providers is essential so as to ensure that these services are effective and does not lose out to on-premise platform based solutions. With new services being added some more additional evaluation criterions will be needed and will have to be explored to judge the effectiveness of such services. Various security services are currently not available, so the provisions of such services will have to be made in future and other important issue is seamless integration of all such services. The integration issue is also to be addressed by all services providers/ researchers.

10. REFERENCES

[1] Vaquero, Luis M., Luis Rodero-Merino, Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, ACM SIGCOMM Computer Communication Review, Volume 39, Number 1, January 2009

[2] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009.

[3] C. Wang, Forrester: A close look at cloud computing security issues. http://www.forrester.com/securityforum2009, 2009

[4] Marios D, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali, Cloud Computing: Distributed Internet Computing for IT and Scientific Research, IEEE Internet Computing 2009 IEEE.

[5] Rich Maggini, Solari, Cloud Computing is changing how we communicate, IEEE 2009

[6] Tim Mather, Subra Kumaraswamy, and Shahed Latif, 2009, Cloud Security and Privacy. An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 336.

[7] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues, IEEE 2010.

[8] Tharam Dillon, Chen Wu, Elizabeth Chang, 2010, 24 th IEEE International Conference on Advanced Information Networking and Applications, Cloud Computing: Issues and Challenges

[9] Bernd Grobauer, Thomas Schreck, Towards Incident Handling in the Cloud: Challenges and Approaches CCSW'10 ACM 2010

[10] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, Security and Privacy in Cloud Computing: A Survey, 2010 Sixth International Conference on Semantics, Knowledge and Grids IEEE 2010

[11] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, Cloud Computing Research and Development Trend, 2010 Second International Conference on Future Networks, IEEE 2010

[12] Kresimir Popovic, Zeljko Hocenski, Cloud Computing security issues and Chanllenges, MIPRO 2010

[13] Security-as-a-service white papers from isheriff. Web page http://www.isheriff.com

[14] Websense white paper, Seven Criteria for Evaluating Security-as-a- Service Solutions, 2010

[15] Osterman Research whitepaper, The Advantages of a Hosted Security Model, July 2009

[16] Cloud Security Alliance, Secaas Defined categories of service 2011

[17] Forrester Research, Inc., Saas Valuation Criteria, 2010