Integrating Security Services in Cloud Service Stores

Joshua Daniel, Fadi El-Moussa, Géry Ducatel, Pramod Pawar, Ali Sajjad, Robert Rowlingson, Theo Dimitrakos

Integrating Security Services in Cloud Service Stores

Joshua Daniel[1], Fadi El-Moussa[1], Géry Ducatel[1], Pramod Pawar[2], Ali Sajjad[2], Robert Rowlingson[1], Theo Dimitrakos[1,2]

[1]BT Research & Innovation, Ipswich, UK

{joshua.daniel, fadiali.el-moussa, gery.ducatel, robert.rowlingson, theo.dimitrakos}@bt.com

[2]School of Computing, University of Kent, Canterbury, UK

{pramod.pawar, ali.sajjad}@bt.com

Abstract. Protecting systems, applications and data hosted on a Cloud environment against cyber-threats, and accounting for security incidents across the Cloud estate are prerequisites to Cloud adoption by business, and a fundamental element of both national and corporate cyber-security and Cloud strategies. Yet, Cloud IaaS and PaaS providers typically hold Cloud consumers accountable for protecting their applications, while Cloud users often find that protecting their proprietary system, application and data stacks on public or hybrid Cloud environments can be complex, expensive and time-consuming. In this paper we describe a novel Cloud-based security management solution that empowers Cloud consumers to protect their systems, applications and data in the Cloud, whilst also improving the control and visibility of their Cloud security operations. This is achieved by enhancing the security policy management of commercial technologies, and via their integration with multiple Cloud-based hosts and applications. The result of this integration is then offered as a re-usable service across multiple Cloud platforms through a Cloud service store.

Keywords: Security as a Service, Cloud Security, Cloud services provisioning and management, Service stores

1 Introduction

In the last decade there has been an expanding body of work in academia and industry about protecting data and applications on large-scale virtualized IT and network platforms, and Cloud infrastructures. Publications range from surveys, such as 1 and 2, to security landscaping, such as 3 and 4, to analyses of security risks 5 and security control recommendations 6. Yet, the security mechanisms offered by Cloud infrastructure and platform providers in practice typically consider application protection to be beyond the provider's concerns and thus they fail to protect comprehensively against attacks exploiting application vulnerabilities. Cloud users often find it complicated and expensive to deploy integrity and protection mechanisms on 3rd party public, or

on hybrid Cloud environments, and lack the required security expertise or the security operations capability that can scale accordingly to the Cloud use. The constant change in security perimeter due to the elastic boundaries in Cloud services further complicates the security management problems. Cloud adoption will always be limited until these gaps are filled. Lack of transparency, loss of confidentiality, as well as legal and regulatory context is widely recognized as a barrier to Cloud adoption by public authorities, companies and individuals 7. Recent studies have provided further evidence to ground these concerns: for example the "Cloud Adoption & Risk Report" [8] evidences that "only 9% of Cloud services used by enterprise customers in Europe today offer enterprise-grade security" and "beyond that, only 1% of Cloud services in use in Europe offer both enterprise-grade security and meet the EU data protection requirements".

The Cloud-based security services market will be worth $2.1 billion in 2013, rising to $3.1 billion in 2015 27, and the top three most sought-after Cloud services moving forward will remain email security, web security services and identity and access management (IAM), according to a report from Gartner. In 2013 and 2014, the most growth is forecast to occur in Cloud-based encryption, security information and event management (SIEM), vulnerability assessment and web application firewalls. For Cloud adoption for enterprise use to materialize at a scale, there is a growing demand for innovations that enable businesses to maintain high levels of visibility and governance of their ICT assets, data and business applications in the Cloud and to enforce the controls required for operating high-assurance applications in the Cloud.

This paper presents BT Intelligent Protection [12], [13] - a Cloud-based security service prototype (currently in beta testing) designed in collaboration with security and service management technology vendors, to address these problems. The core technology behind Intelligent Protection is based on available commercial technologies but extends them by further automating their governance, their security policy management, and their integration with multiple Cloud-based hosts and applications. The result of this integration is offered as a re-usable Cloud based service across multiple Cloud platforms from different Cloud providers.

Section II reviews the background work in this area particularly in the context of Cloud security and Cloud marketplaces (or Cloud service stores). In section III we describe the rationale and approach to the design of Intelligent Protection. We also examine the challenges associated with the introduction of common capabilities for security into Cloud service stores. In section IV we present the high-level architecture of the Cloud-based security service (Intelligent Protection) and the fundamental concepts underpinning security integration with a Cloud Service Store. Section V describes two examples of the use of Intelligent Protection in representative scenarios. Firstly in the case of the security administration and user experience of assembling, deploying and managing a protected Cloud application. And secondly, in the novel case of establishing a managed Cloud re-seller service, in effect allowing a reseller to access and manage the necessary tools to run a Cloud service in which they can customize security to the needs of their customers.

2 Background & Related Work

Protecting hosts and applications in the Cloud has been the focus of recent academic research, such as 14, 15, 16, 17, [28] and some emerging commercial products, such as 29, 30 and 31. However research and industry alike still lack a fully managed and comprehensive solution to the problem, and especially one that can scale to protecting complex distributed applications on multi-cloud environments.

If Cloud providers have paid less attention to supporting the security of customer applications they have paid much more attention to providing software marketplaces, or what we might call Cloud Service Stores. Cloud providers such as Amazon WS have launched their own service stores while innovative solution providers such as Appcara AppStack 18 , Jamcracker Service Delivery Network 19, Canopy 20, Parallels Automation 21, SixSQ SlipStream 22, Cloudsoft AMP 23, and the open-source projects Brooklyn 24 and Juju 25 are developing solutions that integrate with the programmatic interfaces of several Cloud platforms in order to automatically assemble complex applications, deploy them on one or multiple 3rd party Cloud infrastructure chosen by the user and in some cases manage their life-cycle. Any advanced security for cloud based applications will need to integrate with such cloud service stores [38].

With respect to security one approach, recently taken by the UK government CloudStore Service [26], is to focus on compliance and accreditation to assure the quality of available solutions and enable them to be used both in the public and private sector without repeated compliance measures. The European Commission too has been highly active in describing accreditation and compliance regimes for cloud users. Currently however compliance is a relatively static and manual process. It is not a good fit to the dynamic nature of cloud deployments where loss of visibility and control is a significant risk. The constant change in security perimeter due to the elastic boundaries in Cloud usage also necessitates a more dynamic security approach.

Examples of commercial Cloud-based security solutions that can enable a cloud-based security service include, among others, Trend Micro Deep Security 29, McAfee 30 and Symantec 31 , for application and host protection, Trend Micro Secure Cloud 32, Vormetric 33 and SafeNet Protect V 34 for Cloud data volume encryption as a service, Z-Scaler 35 for web threat protection, CA CloudMinder 36 and SailPoint 37 for corporate identity as a service. Beyond their proprietary and function specific technological advancements, the common novelty of these services is mainly about offering security & protection of hosted systems, application and data as a value-added service (multi-tenant security SaaS), while enforcement is delivered via the Cloud infrastructure, with minimal integration overhead. This approach enhances Cloud user experience by offering more secure, flexible, automated security management for applications deployed or on-boarded to Cloud Infrastructures (IaaS).

3 Approach

In this paper we present an example of a Cloud-based security service that has been integrated into a Cloud Service Store as a “horizontal” service, i.e. a reusable com-

mon capability offered via a subscription-based service delivery model. This involves using conceptually similar security service design and service management automation patterns in order to enhance the same service store with capabilities for data protection, secure communications and identity management. For example, the data protection capability offers encryption as a service for volume (block storage), data-base and object-storage protection while keeping critical information such as encryption keys and algorithms under the Cloud consumers control and out of the Cloud provider's reach. The main goals in offering "horizontal" security services in PaaS are:

1. To offer Cloud consumers a choice of which security capabilities to use for a system and on what Cloud environment.
2. To offer corporate security operations teams - to extend their corporate policy to the Cloud and offer comparable- if not better- levels of assurance for Cloud-hosted applications as for any other enterprise application
3. To create a new scalable and cost-efficient channel to market for managed security service providers and re-sellers by automating the purchasing and integration of the managed service into PaaS.

A common issue in providing such security capability as Cloud services and platforms is that service assemblies are simple, mission specific, and generally do not cater for combining Cloud platforms and applications with security services in a mutitenant environment. Through our experimentation and trials with customers and partners we identified the following as common characteristics of the security operations experience that corporations deploying and managing their applications in the Cloud aspire to:

- A choice of which security functions to apply on any application stack they deploy into the Cloud.
- Security controls automatically integrated into the system and application stack they deploy in a Cloud environment with minimal intervention
- A security management dashboard that allows the security operation teams to interact with
  - Tools for defining application or data specific security policy once and automatically applying this homogeneously across multiple Cloud environments that may host instances of the same application stack
  - Tools for automatically detecting the vulnerabilities of their applications and automatically deploying security patches to fix them in the Cloud.
  - Tools for detecting and preventing intrusion attempts in any Cloud environment their IT assets reside in.
  - Tools for analyzing security risks for their applications in terms of criticality and define how to manage these risks.
  - Tools to help analyze security events associated with their IT assets across their whole (multi-)Cloud estate.

The overall environment needs to be truly multi-tenant, isolating security policies, security events, security controls, security control communications between tenants (i.e. corporations using the capability) and restricting access and visibility only to the Cloud environments parts and to the systems and applications that correspond to the tenant.

Intelligent Protection addresses the problems described above by enabling the protection of systems, applications and data processing on a mix of public and private Cloud environments through a collection of security functions that can be offered as managed or self-service Cloud-based integrity and security services. Controls to enforce the integrity and security functions can also be integrated in a Cloud Application and Service store as "horizontal" common capabilities at the Cloud service management automation layer thereby enabling the application and data protection functions to become selectable properties of any application stack that the user choses to assemble on any Cloud platform or infrastructure. Cloud users can therefore maintain the visibility and control of their applications in the Cloud. With a few clicks, users can deploy protected applications in several Cloud infrastructures or Cloud platforms and to manage their security and integrity through a single unifying multi-Cloud security operations management layer. Through this integration, we offer a new customer experience to seamlessly manage security in the Cloud, focusing on the following traits:

1. Fusion: security management becomes an integral part of Cloud application assembly
2. Uniformity and Customization: the integrity and security functions become management parameters of any application in the service store, while the form and coverage of the functions automatically adjust to user selection.
3. Automation: "click-to-buy" security services and "click-to-build" secure applications with a few mouse clicks.
4. Versatility: automatic generation of security policy based on vulnerability analysis of the application stack, Cloud characteristics, user preferences and desired business impact levels.
5. Universality: one Cloud-based service securing applications and data on multiple private and public Cloud infrastructures and platforms.
6. Visibility: a customizable security dashboard is automatically created for each customer offering a unifying view of the security state of user's applications on any Cloud platform.
7. Control: enables enforcing a common security policy to all instances of an application on multiple Cloud environments.

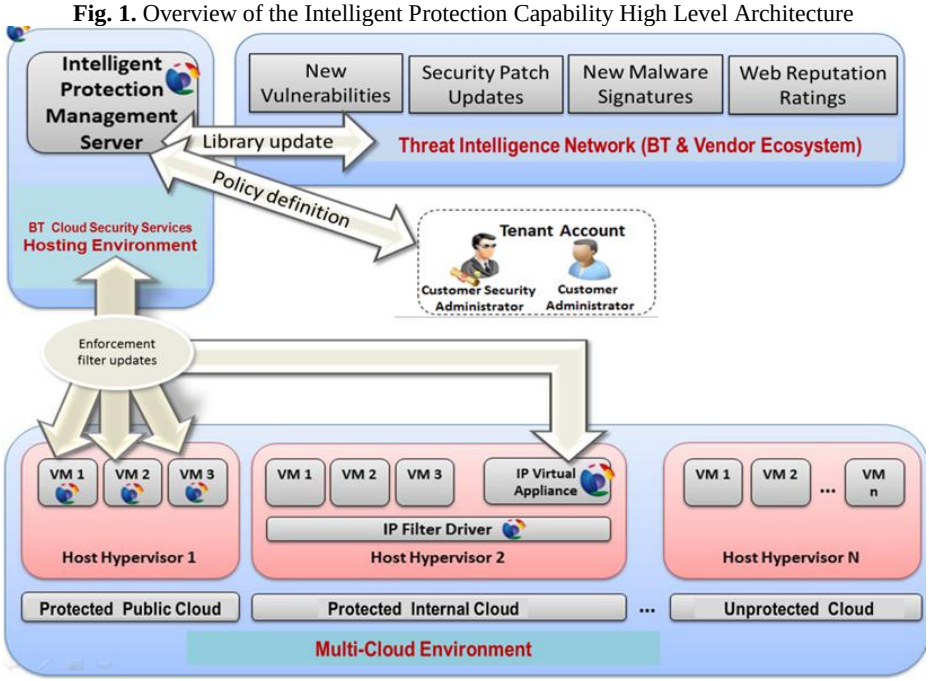
4 Architectural Overview

4.1 General architecture: Cloud-based security capability

An architectural overview of the Cloud-based Intelligent Protection solution offered to each tenant can be divided in three dimensions as depicted in figure 1:

- *Policy enforcement*: this is the mechanism used to manage the protection of a system; it can be an agent installed on a Virtual Machine (typically on an external Cloud) or a physical server or a virtual appliance that together with a hypervisor plugin installed on the physical nodes of an internal Cloud.
- *Policy administration*: this is the management mechanisms at the Intelligent Protection server used for defining security policies based on a library of rules that include virtual patches for a very large number of systems and applications, firewall and protocol rules, etc., and for updating the configuration and enforcement rules of the agents or hypervisor-level virtual appliances.
- *Threat intelligence*: this is the mechanism for enhancing the data-base of primitive rules, attacks or virus signatures, vulnerabilities, etc., via a network that includes a large number of security and application vendors, as well as contributions from BT's security ecosystem.

Fig. 1. Overview of the Intelligent Protection Capability High Level Architecture



Using an agent-based on-boarding model, Virtual Machines (VMs) running on any 3rd party Clouds or physical servers can be connected to the Intelligent Protection service and enable their administrators to remotely monitor and manage the protection of their environment.

In addition to the Cloud Service Store integration, there are three further ways of making a VM manageable by Intelligent Protection, depending on the level of integration of the corresponding Cloud environment with the Intelligent Protection service:

- The user specifies their VM architecture and operating system, and downloads from the service a light-weight agent installer. The installer will then automatically contact the BT Intelligent Protection service and automatically download, register and activate the appropriate agent software. The same process also works for any physical server that is connected to the internet.
- The Cloud provider offers a template with a pre-installed agent installer that is then activated by the user by providing their Intelligent Protection service credentials for verification.
- The Cloud provider includes the Intelligent Protection agent and appropriate configuration in a VM template or a contextualized image 43,45,[45] creation process.

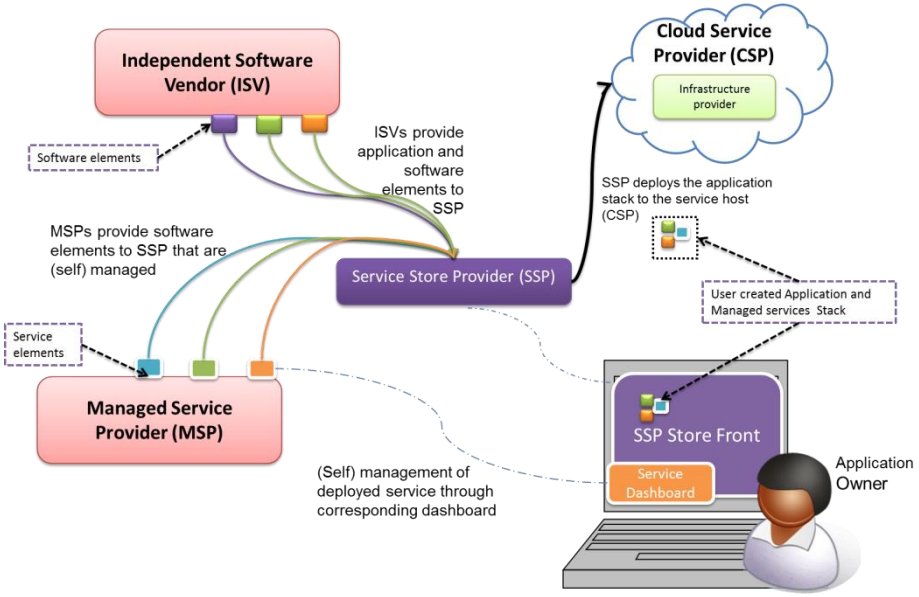
The Intelligent Protection service has a plug-in for the management APIs of the corresponding Cloud provider. The users simply use their Intelligent Protection service account and their Cloud account credentials in order to execute an installation script on the targeted VMs that will automatically obtain all the VM architecture and operating system details, establish a secure connection between the VMs and the Intelligent Protection service, download, install, register and activate the corresponding Intelligent Protection agents on the managed VMs.

4.2 General architecture: Cloud service store integration

A high-level architectural overview is provided in **Error! Reference source not found.** where we identify the following types of actors:

- Cloud Service Provider (CSP): A Cloud provider and service host, which acts as the IaaS or PaaS provider.
- Service Store Provider (SSP): A (Cloud) service store provider that offers the ability to assemble vertical application stacks from software components offered by ISVs and deploy, configure and manage the application stacks on different CSPs.
- Independent Software Vendor (ISV): Their role is to provide applications or software elements (e.g. operating systems, web servers, data-bases, web applications, etc.) which will be published in catalogues by the SSP and will be assembled by application owners in order to be hosted by the CSPs that the application owner selects.

Fig. 2. Overview of the architectural pattern of Intelligent Protection Pattern with a Cloud Service Store



- (Self-)Managed Service Providers (MSPs): These are offering hosted or Cloud-based services that allow the governance of features (e.g. network performance, encryption, security, federation, data protection, system and application protection, etc.) that are integrated into the SSP and via the SSP on the CSPs.
- Application Owner: Finally, we refer to the entity that exploits or consumes compound services as the application owner. These application owners need to create complex services and integrate cross services features that fulfil their regulatory and compliance requirements (e.g. security policies, data retention, etc.).

CSPs may use an SSP in order to offer access to application catalogues that are specific to a range of vertical sectors and have been populated by themselves or ISVs. This can include application elements ranging from operating systems, database servers, ERP application and web servers to web store front-ends.

The application owner selects a pre-defined application assembly from application catalogues. The application assembly defines basic configurations and policy templates for vertical application stacks that cover the Cloud life-cycle of the whole stack from network connectivity to an operating system, to core components such as databases and web servers to business applications and processes. System intelligence encoded in policies, dependencies and constraints guide the selection of a consistent assembly. The resulting application may be single or multi-tiered and be contained in a single server or distributed over a group of networked nodes, and even across Cloud regions.

The integration architecture of MSP services such as Intelligent Protection into a Cloud-based SSP is based on:

- Using clear meta-data models in order to describe dependences, configuration, installation and service management requirements for each application element in the service store catalogues.
- Using clear meta-data models in order to describe how the elements of an application stack (e.g. operating system, server, data-base, application, etc.) are assembled, how their dependences are managed and associate installation and post-installation configuration scripts that ensure the proper set-up and operation of all application stack elements.
- Using clear meta-data models in order to describe the dependences, configuration, installation and service management requirements of the security control implementations; these are typically software elements that are jointly installed and integrated with a virtual machine, server, operating system or application element during the deployment of an application and connect to the Cloud-based security management service via a secure channel establishing a continual "heart-beat" though which security policy updates propagate.
- Extending the application component and the application assembly models with matching models of security control implementations.
- Using a Single-Sign-On mechanism that allows propagating the identity and account credentials of an Application Owner among the SSP, CSPs and MSPs.
- Using a technology that enables the integration and instrumentation of the CSP programmatic interfaces for Virtual Machine and Cloud Platform management. Technology options 12 range from policy-based XML integration point (e.g. 38), proprietary connectors or an integration framework such as J-Clouds 40) in order to instrument the set-up of virtual machines and
- An orchestrator to perform staged Cloud deployment using the information captured in the meta-data descriptions of the application assembly elements and the corresponding security controls. The execution of staged deployment processes is assisted by scripts automating installation and in-life configuration in some cases supported by automation tools such as Chef 41 and Puppet 42.

A detailed description of the integration design is beyond the scope of this industry experience paper and subject to awarded patents and patents pending award. The corresponding author can provide further detail to interested parties upon request.

5 User Experience

In this section we present the experience of using Intelligent Protection in two scenarios:

1. Deploying and managing applications via a Cloud Service Store such as AppStack *43* - the user experience described is based on live system trials on BT's Beta environment but application scenario and corporate user details have been abstracted and generalized as appropriate.

2. Cloud Infrastructure Integration via a managed Cloud re-seller service, in effect allowing any client to access and manage the necessary tools to run a Cloud service which they can customize to the needs of their customers.

5.1 User a Cloud Service Store

Let Omega be a user that wishes to deploy an Apache web server application deployed into a Cloud environment with Intelligent Protection enabled. In order to do this Omega first registers with the Service Store which allows deployment applications ranging from operating systems, database servers, ERP application and web servers to web store front-ends, etc. The customer is then able to assemble and deploy simple or multi-tier applications. BT Compute Service Store offers pre-defined workloads for multi-tier applications that can be instantiated within five clicks and also allows Omega to define new assemblies that fit better with their specific business needs.

Having been exposed as a horizontal service via the BT Compute Service Store, in order to be able to use the security capability, Omega will have to subscribe to BT Intelligent Protection (Error! Reference source not found.**)** and either create a new security management account or provide the details of an already existing account. Omega notices that the overall the Service Store application assembly portal adapts their offering with a selection of options about the selected qualities and corresponding types of protection. Configurable options about these qualities will automatically be made available for all compatible application security elements and assembly workloads in all catalogues available to Omega.

Omega is then able to select a pre-defined application assembly from the catalogue that includes the required Apache web server. The resulting application may be a single or multi-tier and be contained in a single server or distributed over a group of networked nodes, and even across Cloud regions.

Intelligent Protection is able to enforce the policies on the targeted Cloud environment that Omega may choose. This is achieved via the service quality and policy enforcement controls and the advanced service management mechanisms. This allows the user to enforce a different set of security policy based on the application assembly and Cloud infrastructure. Upon deployment the user is then able to monitor and manage the status of all their deployments from a common Intelligent Protection dashboard as shown in Figure 4.

Fig. 3. Subscription to BT Intelligent Protection – Omega can select among a mixture of functions, each function coming with its own policy scheme

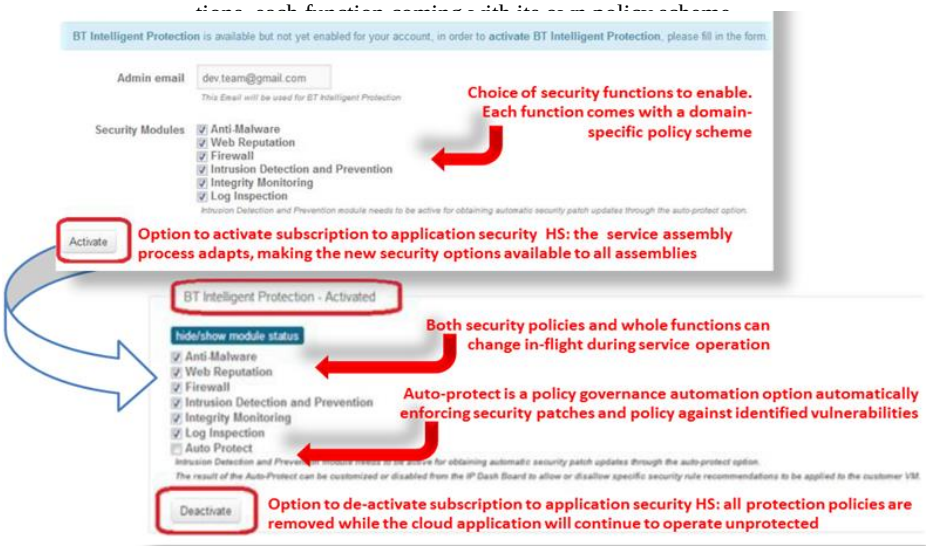


Fig. 4. Example of Intelligent Protection Dashboard

5.2 Cloud Infrastructure Integration

BT Cloud Compute is an IaaS service with a wide range of availability zones including public and private service offerings across different geographical locations. The forthcoming generation of BT Cloud Compute (currently in Beta testing) also extends IaaS and provides on top a PaaS service store with a range of security services for customer applications. Upon this forthcoming extension BT is building a managed Cloud re-seller service, in effect allowing any client to access and manage the neces-

sary tools to run a Cloud service which they can customize to the needs of their customers.

As already discussed, offering Cloud consumers visibility and control of their resources and their security policy are key enablers to cloud service adoption. The philosophy underpinning the Cloud re-seller model for the virtual server and application security in this case includes the following aspects: security of the Cloud host, protection and integrity of re-sellers' information and security compliance required by end customers.

Creating security features in re-seller's portfolio requires those features to be contextualized at the customer level. This requires a tight integration of four Cloud management components: the identity management solution, the customer management service, the virtualization layer, and the service store.

Re-sellers are then able to build catalogues and select appropriate products with appropriate levels of security on intelligent protection as a horizontal service for the vertical markets. On the Intelligent Protection subscription page users are able to select security features from check boxes. The service enforces the selected security features on future and past applications deployed in the Cloud environment. Depending on the compliance requirements, some features can also be overridden by end users.

6 Conclusion and Further Work

In this paper we have shared experiences for integrating a Cloud-based security service for host and application protection with a Cloud Service Store and described how this can give rise to the first instance of a new kind of security capability for PaaS, IaaS and Cloud-hosted Applications. This approach provides users with similar, or even enhanced, security management experience over diverse, dynamic and elastic cloud environments, compared with a traditional static IT infrastructure.

In relation to Intelligent Protection, our current and future work involves validating the usability and capability in vertical market sectors through further trials and experimentation with a range of partners in collaborative projects. We are also working towards integrating more security capabilities with the service store and the forthcoming Cloud Services Management layer of BT Compute including Cloud-based services for data protection ("encryption as a service"), security analytics, identity and federation services, information assurance reporting and content cleansing (e.g. email filtering) among others.

Protecting IT assets on a Cloud environment against cyber-threats and accounting for security incidents are prerequisites to Cloud adoption by business across the globe and a fundamental element of UK and Europe's cyber-security and Cloud strategies 71011. An underlying cause for many successful cyber-attacks on Cloud services is the lack of a suitable security, resilience and protection mechanism for applications that run on 3rd party or hybrid Cloud environments. The work presented here directly addresses these concerns.

Finally we believe that the concepts presented in this paper can provide the basis for more fundamental research on concepts as “Horizontal Security Services” while also extending the scope to a wider class of Cloud-based services beyond security, integrity and assurance. A future paper will explore this further.

7 References

1. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications Volume 34, Issue 1, January 2011, Pages 1–11
2. Huiming Yu, Nakia Powell, Dexter Stembridge, Xiaohong Yuan. Cloud computing and security challenges. ACM-SE '12 Proceedings of the 50th Annual Southeast Regional Conference Pages 298-302
3. Cloud Security Alliance. Top Ten Big Data Security and Privacy Challenges. November 2012.
4. Cloud Security Alliance. Cloud Computing Vulnerability Incidents: A Statistical Overview. May 2013
5. Catteddu, D. and Hogben, G. “Cloud Computing Risk Assessment”. European Network and Information Security Agency (ENISA), 2009
6. Cloud Security Alliance. Cloud Controls Matrix v3.0.1 July 2014..
7. European Commission Communication on “Unleashing the Potential of Cloud Computing in Europe” http://eurlex.europa.eu
8. Skyhigh, Cloud Adoption & Risk Report, http://www.skyhighnetworks.com/
9. Lachal L., “Public Clouds are becoming vertical market-centric” Ovum. http://ovum.com/
10. UK Government CloudStore http://govstore.service.gov.uk/Cloudstore/
11. ECP “Trusted Cloud Europe: Have your Say”, http://europa.eu/
12. El-Moussa F., Dimitrakos, T. " Protecting systems and applications on virtual data centres and in the Cloud: challenges, emerging solutions and lessons learnt" https://Cloudsecurityalliance.org/events/secureCloud-2012/#_downloads
13. Dimitrakos, T. " Cloud Security Challenges and Guidelines", EIT ICT Labs Symposium on Trusted Cloud and Future Enterprises, Oulu, Finland August 2014. http://www.eitictlabs.eu/news-events/events/article/eit-ict-labs-symposium-on-trusted-Cloud-and-future-enterprises/
14. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, Muttukrishnan Rajarajan. A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications Volume 36, Issue 1, January 2013, Pages 42–57
15. Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Júnior. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications Volume 36, Issue 1, January 2013, Pages 25–41
16. Hassen Mohammed Alsafi, Wafaa Mustafa Abdullah and Al-Sakib Khan Pathan. IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment. International Journal of Computing and Information Technology. Volume : No.4 (2012) Issue No. :1(2012). Pages : 1-16
17. A. V. Dastjerdi, K. Abu Bakar, and S. Tabatabaei, "Distributed Intrusion Detection in Clouds Using Mobile Agents," in Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175-180.
18. AppStack by Appcara http://www.appcara.com/products/appstack-r3

19. Jamcracker Services Delivery Network (JSDN) http://www.jamcracker.com/jamcracker-servicesdelivery-network-jsdn
20. Canopy by Atos, EMC, VMWare http://www.canopy-Cloud.com/enterprise-application-store
21. Parallels Automation http://www.parallels.com/uk/products/automation/
22. SixSQ Slipstream http://sixsq.com/products/slipstream.html
23. CloudSoft AMP http://www.Cloudsoftcorp.com/product/
24. Brooklyn project http://brooklyncentral.github.io/
25. Ubuntu Juju https://juju.ubuntu.com/
26. G-Cloud Cloudstore http://govstore.service.gov.uk/Cloudstore/
27. Gartner: Market Trends: Cloud-Based Security
28. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for Cloud computing," J. Internet Serv. Appl., vol. 4, no. 1, pp. 1–13, 2013
29. Trend Micro Deep Security http://www.trendmicro.com/us/enterprise/Cloud-solutions/deep-security/
30. McAfee Cloud Security http://www.mcafee.com/uk/solutions/Cloud-security/Cloud-security.aspx
31. Symantec Cloud Security suite http://www.symantec.com/en/uk/productssolutions/solutions/detail.jsp?parent=Cloud&child=extend_Cloud
32. Trend Micro Secure Cloud http://www.trendmicro.co.uk/products/secureCloud/
33. Vormetric http://www.vormetric.com/
34. SafeNet: ProtectV http://www.safenet-inc.com/data-protection/virtualization-Cloud-security/protectv-Clouddata-protection/
35. Z-Scaler http://www.zscaler.com/
36. CA CloudMinder http://www.ca.com/gb/Cloud-identity.aspx
37. SailPoint IDaaS http://www.sailpoint.com/solutions/customer-solutions/iam-for-todays-Cloudenvironments
38. Nair S.K., Dimitrakos, T.,"On the Security of Data Stored in the Cloud" SecureCloud 2012 https://Cloudsecurityalliance.org/events/secureCloud-2012/
39. CA Layer 7. "The Value of Application Service Governance for Cloud Computing". Cloud Computing White Paper http://www.layer7tech.com/resources/files/white_papers/Value%20of%20SOA%20Governance%20for%20Cloud%20Computing.pdf
40. Apache J-Clouds: Java Multi-Cloud Toolkit https://jClouds.apache.org/
41. Chef IT Automation http://www.getchef.com/chef/
42. Puppet Enterprise http://puppetlabs.com/solutions
43. Appcara. "Cloud Management versus Cloud App Management" http://www.appcara.com/wp-content/uploads/2014/07/Cloud-Management-versus-Cloud-App-Management-v2.0.pdf
44. D. Armstrong, K. Djemame, S. Nair, J. Tordsson, and W. Ziegler, "Towards a Contextualization Solution for Cloud Platform Services," 2011, pp. 328–331.
45. D. Armstrong, D. Espling, J. Tordsson, K. Djemame, and E. Elmroth, "Runtime virtual machine recontextualization for Clouds," in *Euro-Par 2012: Parallel Processing Workshops*, 2013, pp. 567–576.