



The Security Division of EMC

White paper

The Role of Security in Trustworthy Cloud Computing



What are the security implications of cloud computing?

Enthusiasm for cloud computing has as much to do with economics as technology. Growth in the number of applications and the volume of data that must be managed have made data centers a major item of corporate expense, with no end in sight. Public cloud computing looks like a way to get a handle on some of these costs.

The concept of cloud computing is straightforward: you replace capital-intensive IT assets that must be internally managed with rented “pay-as-you-go” IT capacity and services at commoditized prices. These services are built with new technologies such as virtualization and service-oriented architectures and

leverage the Internet to reduce the cost of IT hardware and software resources for computing, networking and storage. At the same time, enterprises are using the same concepts and technologies to build out private clouds to capitalize on centralized, commoditized IT services that meet their security needs.

Today, both public and private cloud deployments must embody an appropriate set of core security principles and thereby assure users and customers of a trustworthy cloud computing environment.

Contents

I. Overview	page 1
II. Public Cloud Computing: Scalability and Multi-tenancy	page 2
III. The Challenges of the Cloud: Security is the Big Question Mark	page 3
Changing relationships	page 3
Standards	page 3
Portability between public clouds	page 4
Confidentiality and privacy	page 4
Viable access controls	page 4
Compliance	page 4
Security service levels	page 5
IV. Principles for Securing the Cloud: Secure Identity, Information, Infrastructure	page 5
Identity security	page 5
Information security	page 6
Infrastructure security	page 7
V. Conclusion	page 8

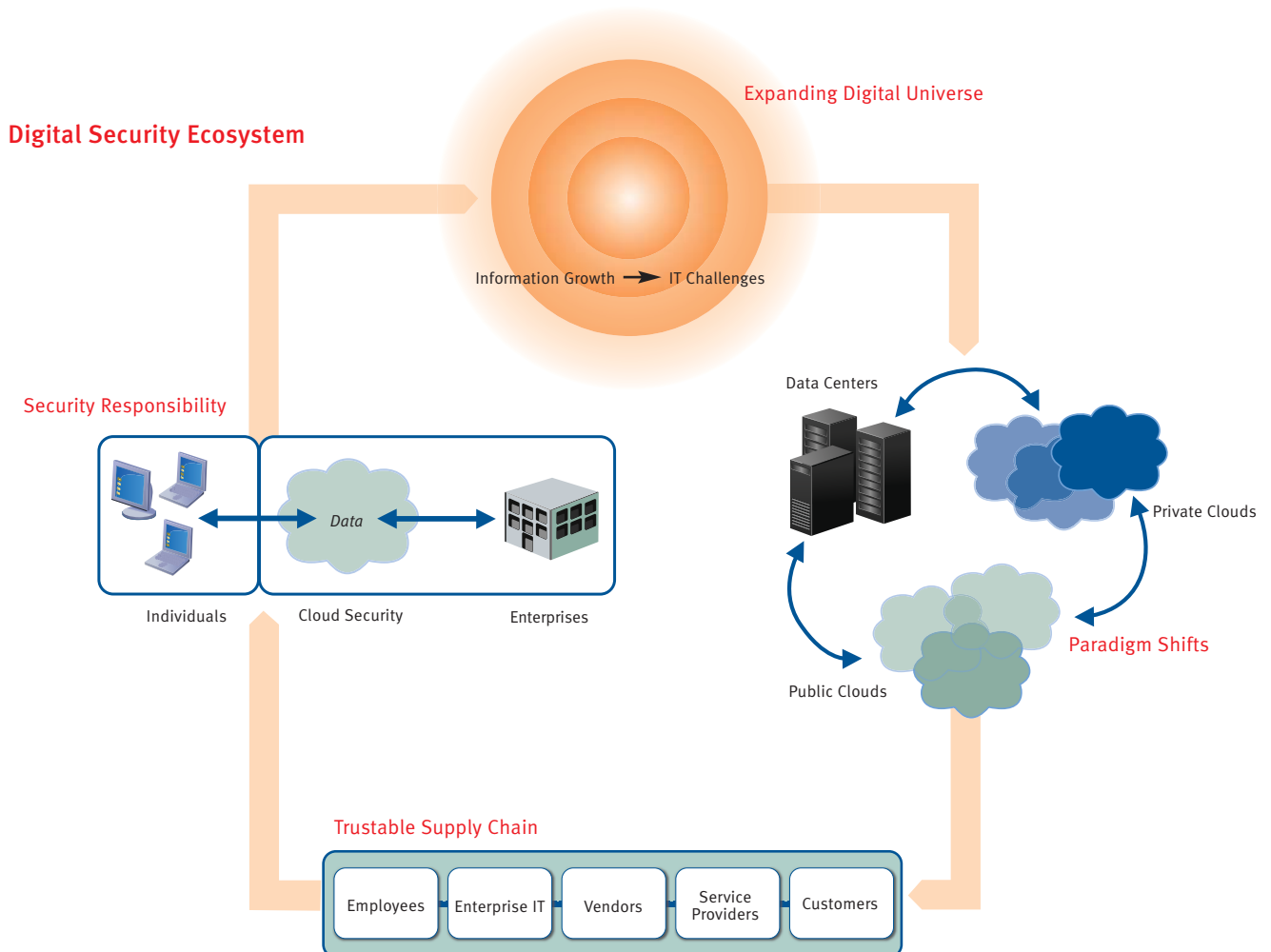
I. Overview

At this early stage in the development of public clouds, the offerings are a mix of commodity consumer and mainstream enterprise applications that deal with relatively non-sensitive data such as email, instant-messaging services and Web-based shared spaces and those that handle more sensitive data like Salesforce.com and EMC's Mozy. But if cloud computing is going to meet enterprise needs for confidentiality of customer data and compliance with legal directives, it will have to provide increased levels of security to support more sensitive enterprise applications.

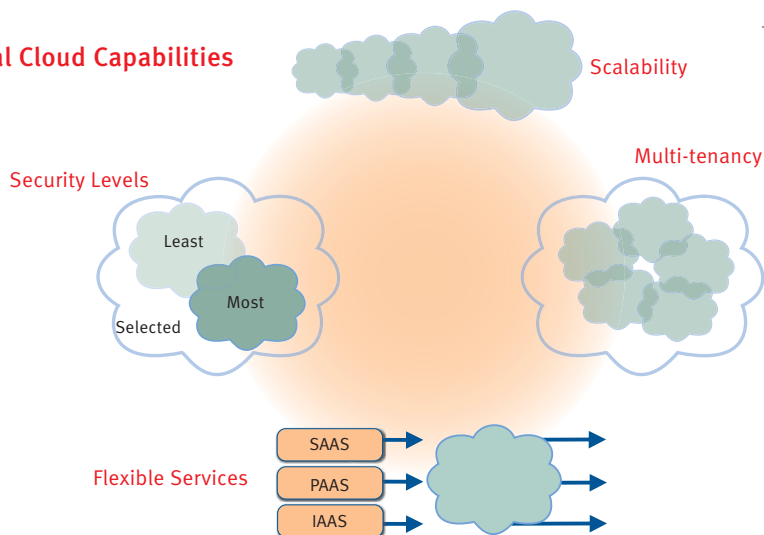
Public cloud computing also introduces new stakeholders into the security equation – third party service providers, infrastructure vendors and contractors – and loosens the control that IT has on each of these three areas.

Public cloud computing introduces new stakeholders into the security equation and loosens IT's control.

If cloud computing is to succeed as an alternative to the corporate data center, IT departments will require relationships with cloud providers that allow them to trust cloud services and verify events in the cloud. It will have to effectively support a high level of security, similar to current control-centered models, and be implemented in a way that allows enterprises to develop confidence in extending portions of their own data centers into a public cloud.



Essential Cloud Capabilities



- Infrastructure as a service (IaaS). Facilities commonly provided locally, by a desktop computer or a data center, are offered as remote resources so that a customer can define and manage computational or storage tasks. Examples include EMC's Atmos policy-based storage services and Amazon's Elastic Compute Cloud ("EC2") for computing services.

But before cloud computing can live up to its promise for the enterprise, it needs further refinement, especially in the area of security. To date, most of the public cloud-oriented applications have been consumer-centered applications built on commoditized data storage and transaction processing. At this initial stage, the applications and data being processed in clouds are predominantly non-sensitive, and the cloud services offer minimal or only generally available security. The cloud offerings themselves are proprietary computing islands, with few standards and only limited possibilities for interoperability.

Trends in information growth will only make the problem more pressing for enterprises. In the IDC study, "The Expanding Digital Universe," the "explosive growth in the volume of sensitive information being created is examined; the rate at which data is created and stored will grow by a factor of six by 2010. The study notes that while individuals will create most digital information, corporations will be responsible for the security, privacy, reliability, and compliance of at least 85 percent of the rapidly expanding digital universe.

It is clear that public cloud computing must become more secure if it is to become more accepted by the enterprise. With this progression, trust and verification will again be the key security enablers. Enterprises will need to assure the confidentiality, integrity and availability of their data as it is transmitted, stored or processed by third parties in the cloud services chain.

II. Public Cloud Computing: Scalability and Multi-tenancy

Public cloud computing describes a computing architecture that extends the service-oriented approach (exemplified in such concepts as "utility computing," "service-oriented architectures" and "software as a service") into a marketplace model. Providers offer services that "run in the cloud" as they are accessible using Internet Protocol and are location independent, meaning that users have no need to know where the underlying IT resources exist.

Cloud services have two hallmarks: They are scalable (the required resources of storage and computing power can be increased or decreased based on customers' needs), and they are multi-tenant (they provide simultaneous, secure hosting of services for various customers utilizing the same cloud infrastructure resources). Today's cloud computing comprises three types of services:

- Software as a service (SaaS). An application is hosted as a service provided to customers. Examples include Salesforce.com's Web-based CRM application and Gmail and Google Docs from Google.
- Platform as a service (PaaS). The combination of software and infrastructure services with application development tools so that Web applications and services can be built and hosted. Examples include Google AppEngine and Salesforce.com's AppExchange.

Before enterprises can make more innovative use of clouds, security technologies, standards, and interoperability must be improved.

III. The Challenges of the Cloud: Security is the Big Question Mark

Taking advantage of cloud computing means major changes for enterprise IT organizations. The biggest will be reduced control even as they are being tasked to bear increased responsibility for the confidentiality and compliance of computing practices in the enterprise. This makes security a major issue as IT departments look at cloud services and providers.

Changing relationships

A key issue for cloud computing is that aspects of traditional infrastructure security move beyond an organization's control and into the cloud. This will lead to fundamental changes in the number and roles of security stakeholders as enterprises turn over control of security infrastructure and processes to outside contractors. Trust relationships between the various cloud stakeholders

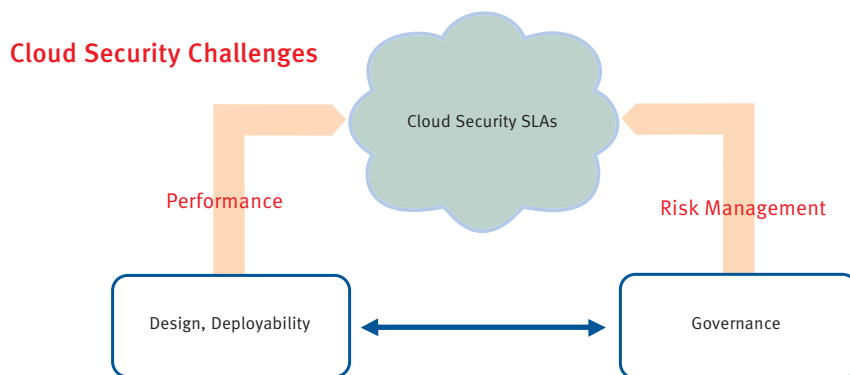
(users, corporations, networks, service providers, etc.) need careful consideration as public cloud computing evolves to manage sensitive enterprise data.

Conventional data centers have based security on fortress-like structures that protect the data within secure physical, hardware, and software infrastructures: their security rests primarily on controlling access by users and maintainers of the data and infrastructure. In cloud computing, a data center still exists – somewhere – but who controls it? Cloud computing diffuses many of the traditional corporate security boundaries and substitutes transient chains of custody for the data, with major implications for security and trust for sensitive enterprise data and applications.

The sharing of control raises many questions of responsibility. How will you know which employees of your cloud provider have access to what information and applications? That access needs to be fine-grained with only a selected and controllable few having broad access.

Standards

Before sensitive and regulated data move into the public cloud, issues of security standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections, and regulatory reporting. How will these requirements be met across individual cloud infrastructures and across multiple clouds chosen by the consumer as best practices? Existing cloud service providers may become the de facto models around which security and federation of authorization controls might emerge. Or answers may come from work currently being conducted by various agencies to questions such as which existing standards could be applied to cloud computing, what gaps exist, and what new standards need to be developed.



Portability between public clouds

While cloud computing conveys a promise of open architecture and easy integration, the early cloud offerings have tended to create security "silos"— users need an Amazon account to use Amazon's EC2 service and a Google account to access AppEngine applications. Enterprises will require information and identity portability between varying clouds so that they can mix and match their services in an open, standards-based environment that permits interoperability.

Portability will become a major issue as more complex services get delivered by multiple cloud infrastructures. Imagine, for instance, that you want to rent a massive amount of CPU power from Amazon for a few days to do a deep analysis of your customer data using a custom-built analytical tool – but the data resides in Salesforce.com. Clouds will have to talk to each other securely.

Confidentiality and privacy

Business units are already tasking IT departments to protect their data in the private and public clouds, with the expectation that sensitive information will either be desensitized or deployed with verifiable access authorization to protect its privacy and confidentiality. IT organizations have historically not developed the capability to effectively identify and classify users and sensitive data. Without this ability, they will face hurdles in extending security functionalities to cloud environments.

How will your cloud provider ensure confidentiality and privacy? Recently, one cellular provider was embarrassed, for example, when its employees viewed Barack Obama's past phone records. How will such incidents be prevented? How will you protect against insider threats, like an employee of the cloud provider walking off with sensitive enterprise information? Cloud providers will have to address this fundamental responsibility.

Viable access controls

Information governance requirements will need to be balanced with the users' desire for efficient yet robust access control. Users and corporations will expect transparency and convenience of access. For many clouds such as those delivering popular services to the general public, a token-based approach may not be tolerated by the users.

Another major pain point is the lack of delegated authorization. While some cloud services provide for delegated strong authentication (e.g., Salesforce.com) that enables access control based on user identity, few, if any, provide delegated authorization to enable access control based on the content of the information itself. This capability is turning out to be increasingly important given the advent of Web 2.0 where fine-grained entitlements for authorization management and control will be most essential.

Compliance

Many business units are being drawn into using cloud services by the attractive economics, bypassing IT departments to host their applications and data in the cloud directly. This creates several problems for the IT organizations with reduced internal and external control. The business units' activities multiply the IT department's compliance challenges even while legal and compliance departments are expecting the IT departments to be able to report on and demonstrate control over sensitive information. Additionally, a cloud provider's SAS-70 compliance must be carefully assessed by each enterprise customer to see if the certification meets the compliance policy established by their own enterprise.

Reporting will be a key requirement for any cloud environment where personally identifiable information (PII) and other sensitive or regulated data live. Who will be accountable for ensuring compliance is met – you or your cloud provider? Will you have access to log data from the cloud environment where your company's information lives so you can correlate it with events in other systems? What if someone steals data from your cloud-based system in an attempt to break into systems in your company's internally managed data center?

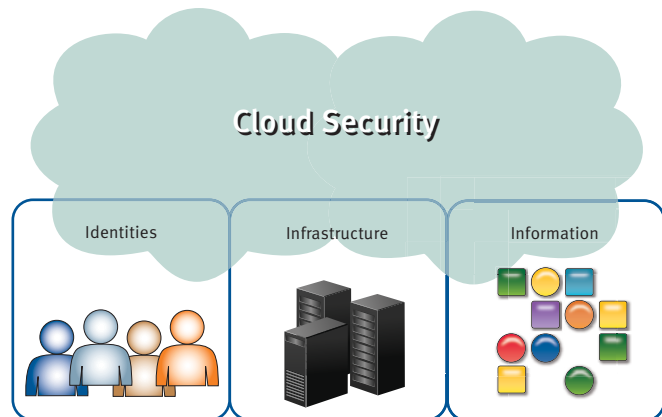
How do those events get correlated? Who is accountable if there's a breach of PII? Will you even know where your information is physically located? These questions could potentially create an issue for compliance with international regulations.

Security service levels

As all types of data will end up in the clouds – from high-value data to bulk and non-sensitive data – there will be an increasing need for varying security service levels that match the sensitivity of different types of data. The real challenge will be mapping security levels to information or business processes so that they can be transferred to the cloud at the lowest possible cost, but the highest necessary level of security.

Varying security service levels will be required to match the sensitivity of different types of data.

Principal Elements for Securing the Cloud



IV. Principles for Securing the Cloud: Secure Identity, Information, Infrastructure

Public cloud computing requires a security model that reconciles scalability and multi-tenancy with the need for trust. As enterprises move their computing environments with their identities, information and infrastructure to the cloud, they must be willing to give up some level of control. To do that, they must be able to trust cloud systems and providers, and verify cloud processes and events. Important building blocks of trust and verification relationships include access control, data security, compliance and event management – all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud.

Identity security

End-to-end identity management, third-party authentication services, and federated identity will become a key element of cloud security. Identity security preserves the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components will be a major requirement for cloud computing, and identity will have to be managed in ways that build trust. It will require:

- Strong authentication: Cloud computing must move beyond weak username-and-password authentication if it is going to support the enterprise. This will mean adopting techniques and technologies that are already standard in enterprise IT such as strong authentication (multi-factor authentication with one-time password technology), federation within and across enterprises, and risk-based authentication that measures behavior history, current context and other factors to assess the risk level of a user request. Additional tiering of authentication will be essential to meet security SLAs, and utilizing a risk-based authentication model that is largely transparent to the users will actually reduce the need for broader federation of access controls.
- More granular authorization: Authorization can be coarse-grained within an enterprise or even a private cloud, but in order to handle sensitive data and compliance requirements, public clouds will need granular authorization capabilities (such as role-based controls and IRM) that can be persistent throughout the cloud infrastructure and the data's lifecycle.

Sensitive data in the cloud will require granular security, maintained consistently throughout the data lifecycle.

Information security

In the traditional data center, controls on physical access, access to hardware and software and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. To compensate, security will have to become information-centric. The data needs its own security that travels with it and protects it. It will require:

- **Data isolation:** In multi-tenancy situations, data must be held securely in order to protect it when multiple customers use shared resources. Virtualization, encryption and access control will be workhorses for enabling varying degrees of separation between corporations, communities of interest and users. In the near future, data isolation will be more important and executable for IAAS, than perhaps for PAAS and SAAS.
- **More granular data security:** As the sensitivity of information increases, the granularity of data classification enforcement must increase. In current data center environments, granularity of role-based access control at the level of user groups or business units is acceptable in most cases because the information remains within the control of the enterprise itself. For information in the cloud, sensitive data will require security at the file, field, or even block level to meet the demands of assurance and compliance.
- **Consistent data security:** There will be an obvious need for policy-based content protection to meet the enterprise's own needs as well as regulatory policy mandates. For some categories of data, information-centric security will necessitate encryption in transit and at rest, as well as management across the cloud and throughout the data lifecycle.

- **Effective data classification:** Cloud computing imposes a resource trade-off between high performance and the requirements of increasingly robust security. Data classification is an essential tool for balancing that equation. Enterprises will need to know what data is important and where it is located as prerequisites to making performance cost/benefit decisions, as well as ensuring focus on the most critical areas for data loss prevention procedures.
- **Information rights management:** IRM is often treated as a component of identity, a way of setting broad-brush controls on which users have access to which data. But more granular data-centric security requires that policies and control mechanisms on the storage and use of information be associated directly with the information itself.
- **Governance and compliance:** A key requirement of corporate information governance and compliance is the creation of management and validation information – monitoring and auditing the security state of the information with logging capabilities. Here, not only is it important to document access and denials to data, but to ensure that IT systems are configured to meet security specifications and have not been altered. Expanding retention policies for data policy compliance will also become an essential cloud capability. In essence, cloud computing infrastructures must be able to verify that data is being managed per the applicable local and international regulations (such as PCI and HIPAA) with appropriate controls, log collection and reporting.

Sensitive data in the cloud will require granular security, maintained consistently throughout the data lifecycle.

The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS.

Infrastructure security

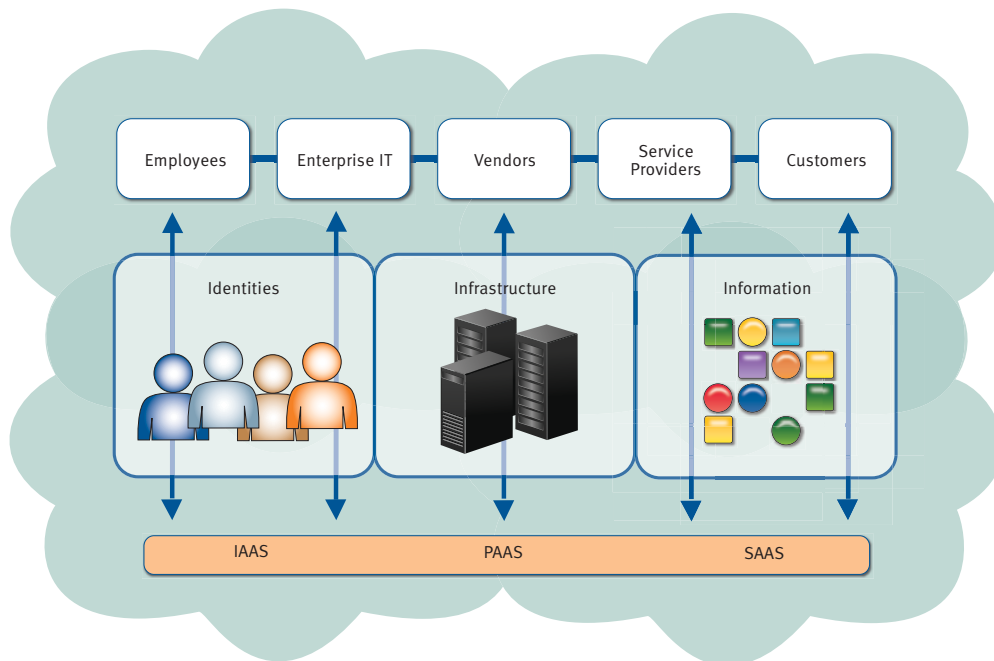
The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS. It will require:

- **Inherent component-level security:** The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components, and, finally, supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust. For these flexibly deployed components, device fingerprinting to ensure secure configuration and state will also be an important security element, just as it is for the data and identities themselves.
- **More granular interface security:** The points in the system where hand-offs occur – user-to-network, server-to-application – require granular security policies and controls that ensure consistency and accountability. Here, either the end-to-end system needs to be proprietary, a de facto standard, or a federation of vendors offering consistently deployed security policies.
- **Resource lifecycle management:** The economics of cloud computing are based on multi-tenancy and the sharing of resources. As a customer's needs and requirements change, a service provider must provision and decommission those resources – bandwidth, servers, storage, and security – accordingly. This lifecycle process must be managed for accountability in order to build trust.

V. Conclusion

Cloud computing promises to change the economics of the data center, but before sensitive and regulated data move into the public cloud, issues of security standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections, and regulatory reporting. All are elements of a secure identity, information and infrastructure model, and are applicable to private and public clouds as well as to IAAS, PAAS and SAAS services.

In the development of public and private clouds, enterprises and service providers will need to use these guiding principles to selectively adopt and extend security tools and secure products to build and offer end-to-end trustworthy cloud computing and services. Fortunately, many of these security solutions are largely available today and are being developed further to undertake increasingly seamless cloud functionalities.



Building a Trustworthy Cloud

EMC, RSA and Secure Cloud Computing

Identity, Information and Infrastructure Security

To manage identity in the cloud, RSA leverages its strong authentication capabilities, multi-factor authentication, one-time passwords, federated identity management and risk-based authentication solutions such as Authentication Manager, Federated Identity Manager, Access Manager and Adaptive Authentication. RSA's Transaction Monitoring system goes beyond assuring the identity of users logging in by authenticating the transactions they perform to boost online security, reduce fraud and mitigate the risks of advanced threats, based strongly on the RSA eFraudNetwork™ service – a cross-institution, collaborative online fraud network dedicated to sharing and disseminating information on fraudulent activity. To manage context aware authorization with fine grained entitlements and authorization administration based on intelligent central policy management, RSA® Entitlements Policy Manager protects resources even beyond web applications.

For information security in the cloud, EMC Information Rights Manager offers content-aware authorization for documents, while RSA® Data Loss Prevention Suite offers content-aware discovery, classification and data loss prevention solutions. Together these products offer private and public clouds the ability to deploy consistent content-aware security policies for data governance, control and compliance. Additionally, RSA® Key Manager enables encryption capabilities in the cloud for data protection and control.

Finally, for infrastructure security, EMC's broad portfolio of products not only offer secure foundations for virtualization, data separation and data protection and availability capabilities, but in addition, EMC's products are also built, deployed and supported securely to give the cloud infrastructures further security assurance. EMC's infrastructure resources management products combined with the RSA enVision® log management and analysis product enables effective management and control of infrastructure components with health check, configuration management, event management and control functionalities – all important for optimizing cloud operations and meeting compliance requirements.

EMC and RSA are increasingly working to develop solutions for cloud security that are being designed from a Security SOA perspective to support the flexible security levels required by emerging cloud models.

Secure SaaS, PaaS, IaaS

EMC and RSA also deliver products and services to the cloud computing marketplace. A few examples include:

RSA's Security-as-a-Service (SaaS) model to federate the security controls in SaaS and PaaS environments with access control and authentication services that have been available since 2002;

RSA® Key Manager can take over management of data security controls (encryption keys) from SaaS/PaaS administrators and maintain control with the data owners or customer corporations;

EMC's Atmos is a Storage-as-a-Service provider for the IaaS model with policies on information storage distribution performance and security.

Author, Contributors

Satchit Dokras, Bret Hartman, Tim Mathers, Brian Fitzgerald, Sam Curry, Magnus Nystrom, Eric Baize, Nirav Mehta

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, enVision, eFraudNetwork and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC, Mozy and Atmos are registered trademarks or trademarks of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2009 RSA Security Inc. All rights reserved.

CLOUD WP 0209