

RSA Security Brief

November, 2009



Identity & Data Protection in the Cloud

Best Practices for Establishing
Environments of Trust

Authors

Eric Baize
Senior Director, Secure Infrastructure Group,
EMC Corporation

Roland Cloutier
Chief Security Officer, EMC Corporation

Bret Hartman, Chief Technology Officer
RSA, the Security Division of EMC

Dr. Stephen Herrod
Chief Technology Officer and Sr. VP of R&D, VMWare, Inc.

Chuck Hollis
VP and CTO of Global Marketing, EMC Corporation

Uri Rivner
Head of New Technologies, Identity Protection and
Verification
RSA, the Security Division of EMC

Ben Verghese
Chief Management Architect & Senior Director, R&D,
VMware, Inc.



The Security Division of EMC

RSA Security Briefs provide security leaders and other executives with essential guidance on today's most pressing information security risks and opportunities. Each Brief is created by a select response team of security and technology experts who mobilize across companies to share specialized knowledge on a critical emerging topic. Offering both big-picture insight and practical technology advice, RSA Security Briefs are vital reading for today's forward-thinking security practitioners.

Contents

Cloud Formation: A Cloud Computing Overview	1
Cloud Control: An Overview of Cloud Security	1
Establishing Cloud Relationships: Deciding Who to Trust	2
1. Set clear policies to define trust and be equipped to enforce them	4
2. Evaluate whether cloud vendors can deliver on their security claims	4
3. Require transparency into cloud operations to ensure multi-tenancy and data isolation	4
4. Preserve segregation of administrator duties	5
5. Manage policies for provisioning virtual machines	6
6. Employ data encryption and tokenization	6
7. Adopt federated identity policies backed by strong authentication practices	7
Fraud Protection: Keeping the Bad Guys Out	7
1. Implement strong authentication services	8
2. Deploy multiple lines of defense to protect against sophisticated malware attacks	9
3. Map the "Dark Cloud" of cybercrime	9
Managing Data Compliance in the Cloud	10
1. Monitor cloud vendors for compliance	10
2. Ensure adherence to jurisdictional-specific regulations in borderless clouds	10
Executive Summary	11
About the Authors	14
Cloud Solutions: Guidance for Practitioners Protecting Identity and Data in Clouds	15
Data Center Monitoring and Multi-tenancy	15
Data Encryption & Tokenization	15
Federated Identity Management	15
Strong, Risk-based Authentication	16
Fraud Prevention and Malware Detection	16
Cloud Event Management and Audit	17
Data Loss Prevention	17
Regulatory Compliance in Borderless Clouds	17

Cloud Formation: A Cloud Computing Overview

Cloud computing delivers convenient, on-demand access to shared pools of data, applications and hardware over the Internet. The cloud computing paradigm — made possible by sophisticated automation, provisioning and virtualization technologies — differs drastically from today's IT model because it decouples data and software from the servers and storage systems running them and allows IT resources to be delivered as a service, either in component parts (where users subscribe to specific applications or simply lease computing power) or as an integrated whole.

There has been considerable hype surrounding cloud computing — and for good reason. It truly has the potential to change enterprise IT. Just as most people find flying on commercial airlines more efficient and practical than owning and operating their own jets, provisioning IT capabilities from the cloud provides many organizations with a more efficient, convenient and flexible alternative to owning and operating their own private networks, servers and software.

Whether they realize it or not, many organizations have already shifted some of their IT and business functions to the cloud. They may be running sales force and customer relationship management applications as cloud services, or they've outsourced payroll and other sensitive enterprise functions to specialists running software as a service in the cloud. It seems that companies with reservations about cloud computing oftentimes are less concerned about the technology or physical differences and more concerned about the procedural and policy differences.

Cloud computing erases many of the traditional, physical boundaries that help define and protect an organization's data assets. Physical servers are replaced by virtual ones. Perimeters are established not by firewalls alone, but by the transit of virtual machines. Risk factors become more complex, as the cloud introduces ever expanding, transient chains of custody for sensitive enterprise data and applications.

As companies migrate their IT infrastructure to the cloud, they effectively relinquish some control over their information infrastructure and processes, even while they are required to bear greater responsibility for data confidentiality and compliance. This shift has wide-ranging implications for a broad set of corporate stakeholders, especially leaders who are responsible for information security.

Cloud Control: An Overview of Cloud Security

As organizations begin to migrate to the cloud en masse, there's still considerable confusion about how best to handle information security in the cloud. In a report commissioned by RSA titled [As Hyper-extended Enterprises Grow, So Do Security Risks](http://www.rsa.com/innovation/docs/IDGRResearchWhitePaper_Final_060409.pdf),* two-thirds of the respondents who are running applications or business processes in the cloud admitted that they haven't developed a security strategy for cloud computing. A majority of respondents weren't sure how prospective cloud computing vendors would safeguard data or how corporate security teams would meet compliance requirements upon moving data into the cloud.

Cloud computing erases many of the traditional, physical boundaries that help define and protect an organization's data assets. Risk factors become more complex, as the cloud introduces ever expanding, transient chains of custody for sensitive enterprise data and applications.

*http://www.rsa.com/innovation/docs/IDGRResearchWhitePaper_Final_060409.pdf

Some information security leaders might find it reassuring to know that information security in the cloud doesn't deviate dramatically from ensuring information security in traditional enterprise IT infrastructures. The same requirements, threats, policies and controls, as well as governance and compliance issues, carry over. Today's information security practices and tools can also be inventively reused. There are, however, a few adaptations to how time-tested security practices and tools are applied given the inherent differences in how cloud resources can be shared, divided, controlled and managed.

First and foremost, the cloud presents those of us in information technology and security a once-in-a-career opportunity to make information security better: faster, cheaper, more efficient and less intrusive. Because cloud platforms are still developing, we have unprecedented opportunities to embed information security processes and technologies deeper into the infrastructure. Information security can finally break out of the legacy paradigm of bolting security code onto operating systems, networks and applications as a reactive measure or afterthought. In the cloud, security protocols can be built into the virtualization layer, creating stronger, simpler and more unified information security systems. As virtual machines move across clouds to perform their functions, they take their policies and protection with them. Cloud security has vast potential to surpass the levels of information security that are possible today.

Secondly, the cloud requires information security leaders to expand their definition of user identity. IT transactions are increasingly automated: today, interactions between software and systems often equal or exceed those between people and machines. The cloud only accelerates this trend. Consequently, it's imperative for IT and security processes to account for the reality that a "user" in the cloud may more likely be a machine than a person (or a machine acting on behalf of a person). This has profound implications on how identities are provisioned, authenticated and managed.

Finally, the cloud forces organizations to reexamine their methods for evaluating IT solutions providers and to revise their models for establishing trust and consequences. Because parts of their IT infrastructure will now be owned and operated by third-parties, security leaders must be able to ensure those vendors are adequately able to secure not just the physical infrastructure, but also the virtual one. Organizations must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs. Organizations must also have transparency into cloud providers' performance against agreed-upon security and business protocols. Specifically, organizations should clearly acknowledge that they can retain control over IT policies and assets, even if they don't own or directly operate those assets. By retaining control over policy-setting, the attendant risks of operating in the cloud aren't necessarily higher, they're just different.

Policy-setting in the cloud usually involves establishing trust relationships between organizations. Trust relationships form the conceptual foundations for cloud security.

Establishing Cloud Relationships: Deciding Who to Trust

Fundamentally, cloud security is not so much a technology issue as it is a trust issue. Much (though not all) of the technologies, services, methodologies and know-how needed to secure the cloud already exist and need to be extended from the enterprise into the cloud. What's needed to make cloud computing a truly ubiquitous services platform is a higher degree of trust, particularly between the owner-providers of cloud resources and the companies that use those resources.

Differences Between Private and Public Clouds

Private clouds describe an IT infrastructure in which virtualized servers, storage, networks and applications are administered for the sole benefit of an organization or enterprise. The organization or enterprise needn't physically own or operate the IT assets that form its private cloud. Some assets can be outsourced or leased from cloud providers — for instance, computing capacity leased from an outside data center. Nevertheless, the organization still effectively “owns” its private cloud by controlling and setting policies governing how virtual IT assets are operated, with cloud vendors guaranteeing specific levels of service and conformance to agreed-upon standards for information access, security and compliance. If all the

IT assets of a privately run cloud are physically owned and operated by the organization itself, the cloud is sometimes referred to as an “internal cloud.”

Public clouds refer to similar virtualized IT infrastructure and services, except policies are not defined and enforced by the enterprise. Although organizations or enterprises may use a public cloud for private business benefit, they don't control how the cloud is operated, accessed or secured. Popular examples of public clouds include Amazon's Elastic Compute Cloud (EC2), Google Apps and Salesforce.com.

For definitions of the security terminology included in this paper, please consult the glossary available on RSA's website: <http://www.rsa.com/glossary/>.

There are many companies providing services through private and public clouds. (See “Differences Between Private and Public Clouds” above.) Each has its own requirements and processes for authenticating and authorizing users. As these services connect and share information with each other, each service provider must be sure that it knows the degree to which it can trust the clouds, services and users — whether human or machine — with which it transacts. The services provider may have the best information security system in the world, but its efforts are useless if it's granting peer-level access to cloud partners with less stringent security standards.

Trust relationships are about establishing hierarchies and knowing who can be counted on to protect and treat shared resources and sensitive information appropriately. It's about trusting not just who you're transacting with, but also how they provide services and security. When expectations between parties are formalized and organized through ties of federation, the result is not just a safer community of users, but one that interacts more conveniently, openly and productively.

To illustrate, consider a scenario in which an enterprise user needs to access a cloud-based CRM application. What typically happens is that the user must follow separate access procedures to connect to his enterprise network and to the CRM service. As the IT industry moves forward with cloud technologies, such redundancies in credentials and procedures will eventually become obsolete. To create a more seamless experience between enterprises and clouds, companies will develop federated trust policies and strong authentication systems to enable a single log-in that grants users appropriate access to all IT-based services, whether they're inside or outside the enterprise. By leveraging strong authentication to link cloud services, companies aren't just creating a convenient user experience; they're also strengthening enterprise security by reducing the number of places where authentication occurs and, thus, the overall threat surface for unauthorized access.

Most of the time-tested practices and technologies for managing trust in traditional enterprise IT environments can be ported to manage trust in enterprise private clouds. For example, organizations can extend traditional information security practices such as data encryption, strong authentication and fraud detection to their private clouds to protect against intrusion, phishing, malware and even information espionage. To improve information portability and protection, enterprises can institute policies for federated identity management.

Following are some best practices for managing trust in private clouds:

1. Set clear policies to define trust and be equipped to enforce them

In a private cloud, trust relationships are defined and controlled by the organization using the cloud. While every party in the trust relationship will naturally protect information covered by government privacy and compliance regulations — employee tax ID numbers, proprietary financial data, etc. — organizations will also need to set policies for how other types of proprietary data are shared in the cloud. For instance, a corporation may classify information such as purchase orders or customer transaction histories as highly sensitive — even as trade secrets — and may establish risk-based policies for how cloud providers and business partners store, handle and access that data outside the enterprise.

For trust relationships to work, there must be clear, agreed-upon policies for what information is privileged, how that data is managed and how cloud providers will report and validate their performance in enforcing the standards set by the organization. These agreed-upon standards must be enforced by binding service level agreements (SLAs) that clearly stipulate the consequences of security breaches and service agreement violations.

2. Evaluate whether cloud vendors can deliver on their security claims

Because information security is only as strong as its weakest link, it's essential for organizations to evaluate the quality of their cloud vendors. Having a high-profile "brand name" vendor and an explicit SLA is not enough: organizations must aggressively verify whether cloud vendors can deliver upon and validate their security claims.

Enterprises must make a firm commitment that they will protect the information assets outside their corporate IT environment to at least the same high standard of security that would apply if those same information assets were preserved in-house. In fact, because these assets are stored outside the organization, it could be argued that the standard for protection should be even higher. Security practitioners must be particularly diligent in assessing the security profiles of those cloud vendors entrusted with highly sensitive data or mission-critical functions. The sidebar on page 5, "Questions to Ask Cloud Providers," presents some important considerations for information security leaders as they assess the security profiles of potential cloud providers.

3. Require transparency into cloud operations to ensure multi-tenancy and data isolation

In the virtualized environment of the cloud, many different companies, or "tenants," may share the same physical computing, storage and network infrastructure. Cloud providers need to ensure isolation of access — that software, data and services can be safely partitioned within the cloud and that tenants sharing physical facilities cannot tap into their neighbors' proprietary information and applications.

The best way to ensure secure data isolation and multi-tenancy — partitioned access to appropriate cloud resources for all tenants — is for enterprise customers to require maximum transparency into their cloud providers' operations. Cloud vendors should furnish log files and reports of user activities. Some cloud vendors are able to provide an even higher degree of visibility through applications that allow enterprise IT administrators to monitor the data traversing their virtual networks and to view events within the cloud in near-real-time. Specific performance metrics should be written into managed service agreements and enforced with financial consequences if those agreed-upon performance conditions are not upheld.

Finally, organizations with private clouds should work with cloud vendors to ensure transferability of security controls. In other words, if and when data or virtual resources are moved to another server or to a backup data center, the security policies established for the original server or primary data center should automatically be implemented in the new locations.

4. Preserve segregation of administrator duties

While data isolation and preventing data leakage are essential, enterprise systems administrators still need appropriate levels of access to manage and configure their company's applications within the shared infrastructure. Furthermore, in addition to systems administrators and network administrators, private clouds introduce a new function into the circle of trust: the cloud administrator. Cloud administrators — the IT professionals working for the cloud provider — need sufficient access to an enterprise's virtual facilities to optimize cloud performance while being prevented from tapping into the proprietary information they're hosting on behalf of their tenants. Enterprises running private clouds on hosted servers should consider requiring that their data center operator disable all local administration of hypervisors, using a central management application instead to better monitor and reduce risks of unauthorized administrator access.

Questions to Ask Cloud Providers

Organizations outsourcing portions of their IT infrastructure must be able to trust the companies providing them with cloud-based services. Trust cannot be granted on the cloud provider's reputation alone; it should be validated through thorough assessments to determine if the cloud provider needs to take additional steps to comply with the organization's information security requirements and policies. Furthermore, performance conditions and standards must be written into SLAs and managed services agreements.

Here are some basic questions that organizations building private clouds should ask prospective cloud infrastructure providers:

- May we see a sample of your logs to gain a better understanding of what types of data can and will be reported?
- How is data protected within your various systems and networks? For instance, what data is encrypted and under what circumstances (in transit, at rest)?
- What practices do you employ to ensure safe multi-tenancy, authentication, authorization and activity monitoring? Have these practices been verified by a third-party auditor? If not, would you be willing to participate in an audit by either our staff or an independent auditor?
- Do you support federated identity management? If you cannot support our assertions and will be providing user identities to us, how are those accounts created and validated? How are user identities provisioned, managed and deprovisioned?
- What specific audit rights, as well as liability controls and protections, do you typically offer in your managed services agreements?
- Are your data centers open for physical inspection? May we visit them if desired to assess physical environmental security?

As an added security measure, enterprises should preserve a separation of administrator duties in the cloud. The temptation may be to consolidate duties, as many functions can be centrally administered from the cloud using virtualization management software. However, as with physical IT environments, in which servers, networks and security functions are split among several administrators or departments, segregating those functions within the cloud can provide added security by diffusing control. Furthermore, organizations can use centralized virtualization management capabilities to limit administrative access, define roles and appropriately assign privileges to individual administrators. By segregating administrator duties and employing a centralized virtualization management console, organizations can safeguard their private clouds from unauthorized administrator access.

5. Manage policies for provisioning virtual machines

Within the cloud, virtual machines are prolific and highly mobile. In fact, they account for most of the activity in the cloud. Virtual machines are typically provisioned on an automated basis to meet application service level agreements, optimize application execution time and maximize overall resource usage. The fundamental role that virtual machines serve in cloud environments has profound implications on information security. To secure their virtual infrastructure, companies using private clouds must be able to oversee how virtual machines are provisioned and managed within their clouds. In particular, managing virtual machine identities is crucial, as they're used for basic administrative functions such as identifying the systems and people with which virtual machines are physically associated and moving software to new host servers.

Organizations establishing a security posture based on virtual machine identities should know how those identities are created, validated and verified and what precautions their cloud vendors have taken to safeguard those identities. Additionally, information security leaders should set their identity access and management policies to grant all users — whether human or machine — the lowest level of access needed for each to perform their authorized functions within the cloud.

6. Employ data encryption and tokenization

Enterprise data used in cloud applications is sometimes stored by the cloud provider — in online backups, for instance. Encrypting data is often the simplest way to protect proprietary information against unauthorized access, particularly by administrators and other parties within the cloud. Organizations should encrypt data residing with or accessible to cloud providers. As in traditional enterprise IT environments, organizations should encrypt data in applications at the point of capture. Additionally, they should ensure cloud vendors support data encryption controls that secure every layer of the IT stack.

An additional precaution to secure data residing in clouds is to segregate sensitive data from the users or identities they're associated with. For instance, companies storing credit card data often keep credit card numbers in separate databases from where card holders' personal data is stored, reducing the likelihood that security breaches will result in fraudulent purchases.

Companies also can protect sensitive cardholder information in the cloud through a form of data masking called tokenization. This method of securing data replaces the original number with a token value that has no explicit relationship with the original value. The original card number is kept in a separate, secure database called a vault.

The fundamental role that virtual machines serve in cloud environments has profound implications on information security. To secure their virtual infrastructure, companies using private clouds must be able to oversee how virtual machines are provisioned and managed within their clouds.

7. Adopt federated identity policies backed by strong authentication practices

In the simplest terms, a federated identity allows a user to access various web sites, enterprise applications and cloud services using a single sign-on. Federated identities are made possible when organizations agree to honor each other's trust relationships, not only in terms of access but also in terms of entitlements. Establishing "ties of federation" — agreements between parties to share a set of policies governing user identities, authentication and authorization — provides users with a more convenient and secure way of accessing, using and moving between services, whether those services reside in the enterprise or in a cloud.

Federated identity policies go hand-in-hand with strong authentication policies. Whereas federation policies bridge the trust gap between members of the federation, strong authentication policies bridge the security gap, creating the secure access infrastructure to bring all members of the community together.

The federation of identity and authentication policies will eventually become standard practice in the cloud — not just because users will demand it as a matter of convenience. For organizations, federation also delivers cost benefits and improved security. Companies can centralize the access and authentication systems maintained by separate business units. They can reduce potential points of threat, such as unsafe password management practices, as users will no longer have to enter credentials and passwords in multiple places.

For federated identity policies to become more widely used, the information technology and security industry will have to knock down barriers to implementing such policies. Thus far, it appears the barriers are not economic or technological, but trust-related.

Federated identity models, like the strong authentication services that enforce them, are only as strong as their weakest link. Each member of the federation must be trusted to comply with the group's security policies. Expanding the circle of trust means expanding the threat surface where problems could arise and increasing the potential for single points of failure in the community of trust.

The best way of ensuring that trust and security are preserved within communities of federation is to require all community members to enforce a uniform, acceptable level of strong authentication. Some IT industry initiatives are attempting to establish security standards that facilitate federated identities and authentication. For instance, the OASIS Security Services Technical Committee has developed the Security Assertion Markup Language (SAML), an XML-based standard for exchanging authentication and authorization data between security domains, to facilitate web browser single sign-on. SAML appears to be evolving into the definitive standard for enterprises deploying web single sign-on solutions.

Fraud Protection: Keeping the Bad Guys Out

As rapidly as the cloud is developing, a cybercrime-driven "dark cloud" is growing even more quickly in parallel. In the past, the dark cloud has been used by cyber criminals to lead consumers to infection points where a Trojan or other piece of malware is downloaded to their machine. For fraudsters, the emergence of private clouds represents an opportunity to kick open the doors to the enterprise. If establishing trust relationships is essential for getting productive participants into the cloud, fraud prevention is essential for keeping "the bad guys" out.

One of the most essential forms of fraud prevention is identity protection: ensuring users actually are who they claim to be. Fraud prevention and identity protection are among the most challenging and fast-changing disciplines within information security. Emerging threats arise at an ever-growing pace.

Cloud providers vary greatly in their ability to protect against fraud and unauthorized access. Public clouds are particularly vulnerable to cybercrime, especially that caused by phishing and malware.

The financial services sector has been on the front lines of fighting online fraud for many years. Financial firms have developed sophisticated security practices and tools that could be adapted for use in clouds by other industries. As cloud security continues to evolve, risk-based authentication, which balances security, usability and cost by applying appropriate safeguards based on the risk associated with each activity, will undoubtedly play a major role in preventing fraud within both private and public clouds.

The financial services sector deploys risk-based authentication as one of many lines of defense that allow security practices to evolve with the threat. For example, financial organizations use behind-the-scenes monitoring tools to automatically flag and report financial transactions and activity patterns that don't conform to an account holder's historic profile. In high-risk scenarios, typical authentication protocols would be deemed insufficient and the financial institution would require additional challenges to verify user identity. This could take several forms: secret questions whose answers should be known to the organization and the intended user; an out-of-band automated phone call requesting users to enter a code appearing on their computer screens by using their telephone keypads; or a one-time-password sent via SMS.

In the coming years, organizations will need to extend their private cloud capabilities in strong authentication and fraud detection to protect against phishing, malware and even intellectual property theft. In building stronger defenses against unauthorized access and online fraud, organizations can borrow from the following fraud prevention practices pioneered by the financial services industry:

1. Implement strong authentication services

Authentication is often the first line of defense in identity protection. It's a set of security practices that verify users are indeed who they claim to be, so those users may be properly paired with appropriate access rights and user privileges. Authentication methods vary from the weak forms often associated with public cloud services (i.e., user name and password) to strong forms, such as security token devices often used by companies to validate employees working off-site.

Some public cloud providers choose to deploy two-factor authentication tokens to their user base. Other public cloud providers find this too difficult to justify for their entire user base, because of provisioning and maintenance costs. Instead, these cloud providers may offer security devices to a subset of their users. Protecting the other users poses a challenge, as static passwords are considered too weak. Therefore, many cloud providers are actively seeking to implement a "better than password" authentication technology.

One of the most promising ways to secure online identities in the public cloud is risk-based, or adaptive, authentication systems, which intelligently vary authentication processes based on real-time calculations of risk. Risk-based identity protection employs behavior profiling and "invisible," or transparent, authentication processes in which users' requests for cloud services are compared with records of what those users have done in the past. Suspicious activities or patterns that deviate from the norm are automatically challenged.

Transparent authentication is often based on device recognition, which looks at various parameters of the user's device, in addition to IP geographic location and network intelligence, in order to determine whether a user is trying to access services from an unknown location or from an unfamiliar device that has never transacted with the cloud before. Combined with behavioral profiling, these transparent authentication procedures trigger red flags when an anomaly is suspected, such as illegal access into the cloud. In these cases, adaptive authentication systems can automatically activate a "stepped up" authentication requirement: asking users to answer security questions — who was your employer in 2007? — or requiring them to sign in with a one-time password sent via text to a mobile phone. Risk-based authentication methods are now being broadly deployed in many public clouds, particularly those run by financial institutions.

Organizations with large numbers of employees working off-site have also implemented advanced risk-based authentication processes. Usually, these organizations further strengthen user authentication procedures by issuing security tokens to employees. Security tokens store inalterable, unique identities in protected memory on a small device (often a key fob). The tokens serve as secondary methods of verifying identities after users enter other credentials, such as passwords or PINs. Such multi-step, token-based authentication processes ensure the highest levels of authentication and identity protection.

Although risk-based authentication techniques and security tokens provide an organization with strong identity verification and protection, the organization itself may only be part of a broader access chain. An organization's deployment of strong authentication techniques may prove useless if its IT infrastructure is connected to a cloud provider who employs less rigorous forms of access security. For enterprises to achieve consistent, guaranteed levels of identity protection, they need to push cloud services providers to deploy identity access and authentication tools that are equal in strength to those used in their enterprise.

2. Deploy multiple lines of defense to protect against sophisticated malware attacks

Fraudsters and the techniques they use become more sophisticated every day. Phishing attacks grow at a steady pace each year while malware infections — including Trojans such as Zeus and Sinowal — have grown ten times faster than the rate of infection observed in 2008. Tens of thousands of identities are stolen each week by fraudsters, who use malware to capture people's user names and passwords by recording their online activities and keystrokes.

Up to this point, the fraud threat has focused mostly on banks and credit card companies. In the coming years, the fraud threat will likely expand to include other types of companies, particularly as more of them move sensitive data and applications to cloud-based infrastructures. Because of the explosion in malware, enterprise access credentials could potentially be captured by Trojans in the same way that credentials are being harvested now in the public clouds operated by financial institutions. For an example of how credentials can be intercepted — even when using strong authentication techniques — please see RSA's recent white paper, "Making Sense of Man-In-The-Browser: Strategies for Mitigating a Menacing Threat."*

The threat posed by increasingly sophisticated malware attacks is a prime example of why layered approaches to identity protection are critical. Companies operating in the cloud should not rely on strong authentication processes alone to prevent unauthorized access. Instead, risk-based authentication tools should be supplemented with additional safeguards such as device or IP tracking, behavioral profiling and "out-of-band" techniques that skirt around the online channel entirely — such as authenticating users over the phone. Enterprises can also participate in external threat protection and intelligence services, such as subscribing to a fraud monitoring network, to minimize the impact of malware attacks.

3. Map the "Dark Cloud" of cybercrime

In the cloud, organizations use third-party resources to promote their business. In the "Dark Cloud," cyber criminals use an organization's resources to promote their business. The Dark Cloud is the infrastructure fraudsters have built using resources they hijacked from individuals and organizations.

Fraudsters and the techniques they use become more sophisticated every day. Phishing attacks grow at a steady pace each year while malware infections — including Trojans such as Zeus and Sinowal — have grown ten times faster than the rate of infection observed in 2008. Tens of thousands of identities are stolen each week.

* <http://www.rsa.com/go/wpt/wpindex.asp?WPID=10459>

The financial sector and other verticals plagued by phishing and malware often employ cybercrime intelligence services to give them visibility into the Dark Cloud's infrastructure. Such services provide them with the ability to detect malware attacking their users, recover credentials stolen from users, shut down infection points and spoofed phishing websites and monitor botnets and command & control motherships. To help stay one step ahead of fraudsters, many organizations use cybercrime intelligence services to gather information about cyber criminals' methods of operation and their ecosystems. Cloud providers are beginning to see the value of such services in monitoring Dark Cloud threats to their users.

Managing Data Compliance in the Cloud

Within cloud environments, the virtualization layer provides an unprecedented degree of visibility into the activity on a system. Hypervisors are exposed to every component and function in the virtual system, from CPU instructions and memory accesses to disk I/O and network packets. This extraordinary degree of visibility means just about every activity involved in providing application services can be monitored and reported for auditing and compliance with relatively little or no extra software instrumentation.

While the highly granular monitoring capabilities of hypervisors can often simplify audit reporting in cloud environments, the lack of physical borders in clouds can complicate jurisdiction-specific regulatory compliance. Here are some best practices for dealing with each of these issues and for handling compliance in private clouds:

1. Monitor cloud vendors for compliance

Audit logging is critical to managing the security of any IT environment and a specific requirement of many government regulations and standards. Organizations deploying private clouds should coordinate with their various cloud providers to ensure the data needed to prove regulatory compliance is fed back into the organization. Specific performance metrics for reporting and audit should be written into managed service agreements. Additionally, cloud vendors' logs can be imported into the organization's security information and event management (SIEM) solution. This allows virtual events from the private cloud to be monitored and analyzed in the organization's central security operations console, alongside the organization's in-house IT infrastructure. Logs and reports from a SIEM solution are irrefutable tools for demonstrating compliance to internal and external auditors.

2. Ensure adherence to jurisdictional-specific regulations in borderless clouds

Countries and jurisdictions impose variable regulations governing the privacy of personally identifiable information, as well as how such data can be stored, transmitted and shared. While large, multinational corporations are accustomed to differences in international requirements and have developed complex procedures to cope with them, many smaller companies using cloud services are now being affected by international regulatory compliance mandates in the borderless environs of the cloud. In the cloud, where computing and storage resources are virtualized and can be hosted in several distant locations at once, it's easier for regulated information to "leak" someplace it doesn't belong. Regulatory compliance makes it necessary, in some cases, to manufacture artificial boundaries within borderless clouds.

Organizations needing to ensure compliance with the ever-changing global patchwork of government mandates will benefit from deploying intelligent cloud storage platforms capable of smart provisioning and data loss protection. To illustrate how such platforms work, consider the extreme example of the German Federal Data Protection Act, or Bundesdatenschutzgesetz, which essentially

prohibits the storage or transfer of German citizens' personal data outside the jurisdiction of Germany. To comply with the German Federal Data Protection Act and other jurisdictional-specific mandates, some organizations are deploying intelligent cloud storage platforms that can identify the characteristics of the data they hold and act appropriately upon it. In the case of the German Federal Data Protection Act, these "data aware" storage clouds are able to automatically segregate the applicable personal data and store it in German data centers in compliance with the legislation.

Executive Summary

The number of organizations using the cloud is expected to grow exponentially over the next decade, as more and more organizations realize they can exploit the cloud's high scalability to grow their IT capabilities quickly and conveniently while simultaneously conserving resources and lowering costs. Companies entering the cloud should take steps to ensure they can trust the companies providing them with services, as well as the entities they're transacting with inside the cloud. Enterprises must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs. Enterprises must also have transparency into cloud providers' performance against agreed-upon security protocols. Furthermore, users will expect a high level of identity mobility from cloud to cloud, while keeping their identities secure. Users will also expect cloud services providers to protect them from fraud. All of these issues relate to establishing trust relationships, which form the conceptual foundations for cloud security.

Many of the time-tested practices and technologies for managing trust relationships in traditional enterprise IT environments can be extended to work effectively in both private and public clouds. For example, organizations can adapt traditional information security practices such as data encryption, strong authentication and fraud detection to their private clouds to protect against unauthorized access, phishing, malware and even intellectual property theft. To improve information portability and protection, enterprises can institute policies for federated identity management.

Within this paper, we identified some core best practices for managing trust in private clouds:

1. Set clear policies to define cloud trust and be equipped to enforce them: For trust relationships to be effective, there must be clear, agreed-upon policies for what information is privileged, how that data is managed and how cloud providers will report and validate their performance in enforcing the standards set by the enterprise.
2. Evaluate whether cloud vendors can deliver on their security claims: Organizations cannot afford to rely on a cloud vendor's reputation alone; they must aggressively verify whether cloud vendors can deliver upon and validate their performance and security claims.
3. Require transparency into cloud operations to ensure multi-tenancy and data isolation: The most effective means of ensuring secure data isolation and multi-tenancy is for enterprise customers to require maximum visibility into their cloud providers' operations. This can be achieved by inspecting logs and other reports of events and activities.

Companies entering the cloud should take steps to ensure they can trust the companies providing them with services, as well as the entities they're transacting with inside the cloud. Enterprises must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs.

4. Preserve segregation of administrator duties: It may be tempting for organizations to consolidate administrator duties in the cloud because many functions can be conveniently and centrally administered using virtualization management software. However, as with physical IT environments, in which servers, networks and security functions are split among several administrators or departments, segregating those functions within the cloud can provide added security by diffusing control.
5. Manage policies for provisioning virtual machines: Organizations establishing a security posture based on virtual machine identities should know how those identities are formed and what precautions their cloud vendors have taken to safeguard those identities.
6. Employ data encryption and tokenization: Organizations should encrypt data residing with or accessible to cloud providers. Additionally, organizations should ensure cloud vendors support data encryption controls that secure every layer of the IT stack.
7. Adopt federated identity policies backed by strong authentication practices: Federated identity policies, like the authentication services that accompany them, are only as strong as their weakest link. Each member of the federation must be trusted to comply with the group's security policies. Employing a uniform, acceptable level of strong authentication among all members of the federation will be crucial for creating a climate of trust that will allow federated identity models to become more widespread.

In the coming years, organizations will need to extend their private cloud capabilities in strong authentication and fraud detection to protect against phishing, malware and even information espionage. In building stronger defenses against unauthorized access and online fraud, organizations can borrow from these practices commonly used to prevent online financial fraud:

1. Implement strong authentication services: Deploying risk-based identity access and management systems, which intelligently vary authentication processes based on real-time calculations of risk, is one of the most effective ways to secure user identities in the cloud.
2. Deploy multiple lines of defense to protect against sophisticated malware attacks: The growing use of strong authentication techniques has spurred fraudsters to develop new, more sophisticated methods for intercepting user identities to commit crimes. Companies can protect their private clouds from fraudsters' malware attacks by deploying multilayered approaches to prevent intrusion and to verify user identities.
3. Map the "Dark Cloud" of cybercrime: Cybercrime intelligence services can provide valuable, timely insight into cyber criminals' methods of operation and their ecosystems. Such insight can be used to help organizations detect malware attacking their users, recover credentials stolen from users, shut down infection points and spoofed phishing websites and monitor botnets and command & control motherships.

For trust relationships to be effective, there must be clear, agreed-upon policies for what information is privileged, how that data is managed and how cloud providers will report and validate their performance in enforcing the standards set by the enterprise.

Within cloud environments, the virtualization layer provides an unprecedented degree of visibility for auditing. Following are some best practices for organizations to employ when handling identity compliance in private clouds:

1. Monitor cloud vendors for compliance: Companies deploying private clouds should coordinate with their various cloud providers to ensure the data needed to prove regulatory compliance is fed back into the enterprise.
2. Ensure adherence to jurisdictional-specific regulations in borderless clouds: Complying with government regulations to preserve data privacy can pose a challenge in clouds, where data can be automatically shared and stored in several locations at once. “Data-aware” clouds are among the many sophisticated tools that are emerging for enterprises to use in complying with regulations within the cloud environment.

The coming years will mark a dramatic shift in the way new information security products are brought to market. Because the cloud is developing rapidly and needs are changing even faster, we anticipate security products and services will be developed in a far more collaborative way than they have been in the past. Leading-edge security practitioners with unmet real-world needs will help security and cloud vendors define requirements for future generations of products and services. This should speed up solutions development and result in offerings that are more tailored — even customizable — to practitioners’ needs.

About the Authors

Eric Baize

Senior Director, Secure Infrastructure Group, EMC Corporation

Eric has EMC-wide responsibility for product security assurance, and leads RSA's product strategy for securing virtual and physical IT infrastructures. Eric was a founding member of the leadership team that defined EMC's vision of information-centric security, which drove the acquisition of RSA Security and Network Intelligence in 2006. He is a Certified Information Security Manager, holder of a U.S. patent and an author of international security standards.

Roland Cloutier

Chief Security Officer, EMC Corporation

Roland leads EMC's Global Security & Business Protection Programs and has functional and operational responsibility for EMC's information & cyber security, business risk, crisis management and corporate protection operations worldwide. He is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security and the FBI's Infraguard Program. He also serves as a member of Security for Business Innovation Council, the Center for Information Policy Leadership, and as an advisor to the Board for Vigilant Corporation.

Bret Hartman

Chief Technology Officer, RSA, the Security Division of EMC

Bret is responsible for defining the corporate security technology strategy for EMC, as implemented by the RSA division. He has over twenty-five years of experience building information security solutions for major enterprises. His expertise includes Service Oriented Architecture (SOA) and Web Services security, policy development and management, and security modeling and analysis.

Dr. Stephen Herrod

Chief Technology Officer and Sr. VP of R&D, VMware, Inc.

Stephen is responsible for VMware's new technologies and collaborations with customers, partners and standards groups. Stephen joined VMware in 2001 and has led the VMware ESX group through numerous successful releases. Prior to joining VMware, he was Senior Director of Software at Transmeta Corporation co-leading development of their "Code Morphing" technology.

Chuck Hollis

VP and CTO of Global Marketing, EMC Corporation

Chuck is a key member of EMC's management team, working on strategic aspects of marketing, business development and technology. He is also a well-known industry blogger (<http://chucksblog.emc.com>) and leads EMC's social media proficiency initiative.

Uri Rivner

Head of New Technologies, Identity Protection and Verification, RSA, the Security Division of EMC

Uri is responsible for moving new technologies and innovations from concept to reality at RSA. He played a key role in developing the division's risk-based authentication and anti-fraud technologies, as well as the RSA eFraudNetwork. He has 15 years of experience in business development, international marketing and project management and has worked closely with several of the world's largest financial institutions on developing solutions against online attacks. Uri is a regular speaker on global trends in online fraud

Ben Verghese

Chief Management Architect & Senior Director, R&D, VMware, Inc.

Ben is responsible for architectural coordination and consistency for VMware's management-related products and platforms. Ben joined VMware in 2000 as part of the VMware ESX Server 1.0 team and has subsequently led the VMware vCenter product from its inception. Prior to VMware, Ben conducted computer architecture and operating systems research at DEC Western Research Labs. He has also worked at Apollo Computers and Hewlett-Packard.

Cloud Solutions: Guidance for Practitioners Protecting Identity and Data in Clouds

The emergence of cloud computing will create new opportunities for stronger and simpler-to-use information security solutions. This will come about as information technology and security companies collaborate to take full advantage of the monitoring and control capabilities inherent in the virtualization layer.

To implement best practices for data and identity protection within clouds, organizations may need to consider new technology solutions. The products and services described below align with the best practices described in this RSA Security Brief. The solutions overview is not intended to provide a comprehensive list of applicable solutions from RSA, from EMC or from VMware. Rather, it's intended as a starting point for security technology practitioners to learn about some of the options available to them.

Data Center Monitoring and Multi-tenancy

VMware offers a comprehensive range of security solutions and services for virtualized platforms that provide fine-grained access controls for greater transparency into cloud provider operations.

- VMware ESX® and ESXi are the most widely deployed hypervisors in the world. Both allow enterprises to use their own security certificates when securing remote sessions. The user name, password and network packets sent to ESX Server over a network connection when using the VMware Remote Console or the VMware Management Interface are encrypted in ESX Server by default when medium- or high-security settings are activated for the server.
- VMware vCenter® Server gives IT administrators unprecedented visibility and centralized control of every level of the VMware vSphere virtual infrastructure. It provides granular privilege management that limits who can deploy virtual machines to specific clouds and storage devices. Combined with well-defined operational processes and work flows, these capabilities can provide maximum mobility for virtual machines while managing risk.
- VMware vCenter Lifecycle Manager enables IT administrators to track ownership of virtual machines and to keep records of when virtual machines are created, deployed and decommissioned. It gives IT administrators more control over virtual machine deployments and optimizes resource utilization for greater ROI.
- VMware vShield Zones enables enterprises to run applications efficiently within a pool of shared computing resources, while preserving network segmentation of users and data. It allows administrators to bridge, firewall or isolate virtual machines between multiple zones, as defined by organizational and trust boundaries. It also allows for convenient, centralized management by providing highly granular views of the entire virtual machine and virtual network deployment, easing configuration of zone-based policies and reducing the risk of errors.

Data Encryption & Tokenization

Encryption solutions typically have many different applications, clients and devices performing cryptographic functions. Managing the permissions — the ability to encrypt, decrypt and generate keys — for all these components is complex, time consuming and costly. RSA offers an enterprise encryption key management system that can easily be extended into private networks.

- RSA® Key Manager Suite is an enterprise encryption key management system designed to manage encryption keys at the application, database and storage layers. RSA Key Manager lowers the total cost of ownership associated with encryption by giving administrators fine-grained control over the vaulting and management of keys from a single, central console.
- RSA Professional Services offers a new Tokenization Service that is engineered to extend the RSA Key Manager Suite by enabling the use of token values to mask and protect sensitive data. The RSA SafeProxy™ architecture employs a unique combination of tokenization, advanced encryption and public-key technologies to protect sensitive data with a layered approach to security.

Federated Identity Management

Federated identity systems strike a balance between ensuring secure transactions and making users' experiences in accessing cloud services easier and more convenient. A federated identity makes it possible for users to reuse a set of credentials they already have to access information and services on another web site or in another cloud. Ultimately, federated identity models offer organizations a more convenient and secure way of accessing distributed resources without losing control over sensitive identity information.

- RSA® Federated Identity Manager is cloud-ready, flexible identity federation solution that uses the latest web

services standards to enable enterprises to securely exchange user identities between internal business units and with customers and partners. RSA Federated Identity Managers provides out-of-the-box functionality with an intuitive user interface and a powerful management console, enabling simplified administration of federation relationships. Designed to be easily integrated into any identity management infrastructure and to be fully compatible with other systems, RSA Federated Identity Manager is based on industry standards such as XML, SOAP, SAML 2.0 and WS-Federation 1.0 and is evolving in step with emerging standards, as well.

- RSA® Access Manager gives legitimate users single sign-on access to applications within intranets, extranets, private clouds and exchange infrastructures. It allows organizations to manage large numbers of users while consistently enforcing a centralized security policy, ensuring compliance and protecting organizational resources from unauthorized access.

Strong, Risk-based Authentication

RSA helps organizations confidently secure identities and information access with its industry-leading authentication solutions. RSA protects more than 250 million user identities, safeguards billions of business transactions each year and manages the confidentiality of data in tens of thousands of applications worldwide.

- RSA® Identity Verification provides knowledge-based authentication for the initial registration process, asking users to verify their identities by answering questions based on information obtained from public records and commercially available sources. The answer choices presented by RSA Identity Verification are unique to each individual and greatly reduces the likelihood that someone other than the genuine user can provide the correct responses. RSA Identity Verification also provides improved accuracy in authenticating users by measuring the level of risk associated with an identity. The system can be configured to address high-risk identities or transactions by adjusting the difficulty of the questions during the authentication process.
- The RSA SecurID® solution is the gold-standard in two-factor authentication with a 25-year history of outstanding performance and innovation. Its hallmark is a security token — either a physical device (key fob or USB) or a software token stored in mobile phone — that generates a new authentication code every 60 seconds. The RSA SecurID solution is regarded as a far more secure alternative to authentication systems based on

reusable passwords. Plus, the RSA SecurID solution is easier to use than challenge-and-response systems that require multiple steps to generate a valid access code.

- RSA® Adaptive Authentication is a risk-based, multifactor authentication platform providing strong protection for Web portals, SSL VPN applications and cloud access management solutions. It measures over one hundred risk indicators to identify high-risk and suspicious activities. Most risk assessments are conducted behind the scenes, drawing from device identification profiles, behavioral patterning profiles, user profiles and RSA eFraudNetwork™ feeds. This transparent, multifactor authentication process enables organizations to increase security without compromising user convenience. Available either as a software-as-a-service or as an on-premise deployment, RSA Adaptive Authentication protects more than 250 million online users worldwide and is deployed by more than 8,000 organizations in the healthcare, financial services, government, insurance, automotive, real estate, manufacturing and pharmaceutical industries.

Fraud Prevention and Malware Detection

RSA provides cutting-edge tools and services to help companies protect themselves and their customers against fraud. RSA's fraud detection and prevention solutions build on the company's deep knowledge of fraud trends and intelligence, forensics and modeling to provide end-to-end protection to online users and the activities they perform. The RSA eFraudNetwork™ and RSA FraudAction™ services are both broadly used to guard against financial fraud, but they also protect against enterprise cyber threats and the risk of unauthorized access, such as industrial espionage and accidental exposure of customer information and transactions.

- The RSA eFraudNetwork™ service is the industry's first and largest online fraud network dedicated to identifying and sharing information on fraudulent activity. Members include over 50 of the world's leading financial institutions, as well as credit and debit card issuers, thousands of regional banks and credit unions and most major ISPs. The eFraudNetwork service is engineered to proactively identify and track fraudster profiles, patterns and behavior across more than 65 countries. When an active fraud pattern is identified, detailed information about the fraud is disseminated to all network members, providing financial institutions and their customers proactive protection against new, potentially debilitating incidents.

- RSA FraudActionSM service is a market-tested, managed service chosen by more than 300 organizations to defend their customers from online phishing, pharming and Trojans attacks. Offered as an outsourced, turn-key service, the RSA FraudAction service helps organizations to minimize resource investment while deploying a solution quickly. It counters online attack vectors through 24x7 monitoring and detection, instant alerts and reporting, attack forensics and advanced countermeasures. The service also works with leading ISPs around the world to block and shut down fraudulent sites.

At the core of the FraudAction service is RSA's state-of-the-art Anti-Fraud Command Center (AFCC), whose experienced teams of fraud analysts provide services in nearly 200 languages to better detect and counter fraud on a global scale. Since 2003, the FraudAction service and the AFCC have helped stop \$1.5 billion in financial fraud and 225,000 phishing attacks.

Cloud Event Management and Audit

- The RSA enVision[®] log management platform provides collection, alerting and analysis of log data that enables organizations to simplify compliance and quickly respond to high-risk security events. The RSA enVision *3-in-1* platform offers an effective security and information event management (SIEM) and log management solution, capable of collecting and analyzing large amounts of data in real-time, from any event source and in computing environments of any size. The RSA enVision platform is easily scalable, eliminating the need for filtering and to deploy agents. Over 1,700 customers, including major global enterprises and government agencies, have selected the RSA enVision solution to simplify compliance, enhance security and optimize IT and network operations.

Data Loss Prevention

Today's enterprise workforce highly depends on collaboration with colleagues, suppliers and customers who share vast amounts of digital information via email, instant messages, or other cloud- and network-based applications. A significant percentage of this data can be sensitive in nature and governed by compliance regulations. This introduces business risks if such data is shared inappropriately with outside parties. Data loss prevention solutions prevent unauthorized transmissions, whether by accident or with malicious intent, by monitoring, tracking and, if necessary, blocking data flows.

- The RSA[®] Data Loss Prevention (DLP) Suite provides a policy-based approach to securing data in data centers, networks and end points, enabling customers to classify their sensitive data, locate and track data across the enterprise, enforce controls, and report and audit activities to ensure policy compliance. The RSA DLP Suite reduces total cost of ownership with high scalability, automated data protection services and the most extensive data policy and classification library available in the industry. It features three components:

RSA DLP Datacenter

DLP Datacenter helps companies locate and track sensitive data no matter where it resides in the data center — on file systems, databases, email systems and large SAN/NAS environments.

RSA DLP Network

DLP Network monitors and controls sensitive data leaving your network.

RSA DLP Endpoint

DLP Endpoint helps you discover, monitor and control sensitive information on endpoints such as laptops and desktops.

The RSA DLP suite integrates with the RSA enVision log management and analysis product to simplify security operations by streamlining incident handling and workflows.

Regulatory Compliance in Borderless Clouds

EMC improves regulatory compliance through cloud-optimized services that perform smart provisioning and automated data placement. These cloud-based services help enterprises efficiently deliver the right information at the right time to the right location globally — automatically.

- EMC Atmos is a cloud-optimized service for storing and distributing information. Atmos combines massive scalability and multi-tenancy with multiple access mechanisms, giving enterprises tremendous flexibility to use web service APIs for cloud-based applications or legacy protocols for file-based systems. When combined with the RSA Data Loss Prevention Suite, EMC Atmos becomes an intelligent, “data-aware” storage cloud, capable of policy-based information management to automatically distribute information to different geographies.



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

The Security Division of EMC

RSA, RSA Security, eFraudNetwork, FraudAction, SecurID and enVision are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. VMware, vCenter and ESX are registered trademarks or trademarks of VMware, Inc. in the U.S. and/or other countries. EMC 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.

CLWD BRF 1009