EMC'S VISION FOR TRUST IN THE CLOUD

Proof, not Promises: Creating the Trusted Cloud

EXECUTIVE SUMMARY

Clouds and virtualization offer powerful new ways to manage and use digital information, but they also create new complexities for organizations in meeting the fundamental challenge of getting the right information to the right people over an infrastructure that they can trust. Why? Because clouds and virtualization irrevocably change the nature of control and visibility. Infrastructure becomes virtual, not physical. People access infrastructure from devices that are outside of IT's direct control. Information moves with incredible speed across networks and the cloud, making it hard to know where sensitive information resides. And with an IT infrastructure that is virtual and shared via the cloud, organizations must learn new ways to achieve visibility into risks, threats, and compliance performance. The good news is forward-thinking businesses can clear these hurdles today.

The formula for building trust in the cloud is to achieve control over and visibility into the cloud's infrastructure, identities, and information. The technologies needed to establish this level of cloud control and visibility already exist. Organizations are applying these technologies in creative ways to build trusted clouds that can meet the most rigorous security and compliance requirements while delivering the flexibility, fluidity, and massive scale that hold such business promise for organizations worldwide.

EMC²

THE CHALLENGE

Over the decades, IT architecture and platform strategies have evolved from mainframe to client-server to the Web. Still, one of the fundamental goals of IT organizations endures: that is, getting the right information to the right people over a trusted infrastructure so information can be leveraged for business advantage.

Realizing this goal has become exponentially harder and more difficult to verify as:

- Digital information rises in value and becomes pervasive in every business process
- Bandwidth grows and access points proliferate
- Business risks multiply, particularly as employees increasingly use consumer devices to access enterprise IT services
- Infrastructure evolves to the new world of virtualization technology and cloud computing

As a result, a dangerous trust void has opened up, standing squarely between organizations and their ability to reap the cloud's well-documented business benefits in efficiency, agility, and cost savings.

Management teams, auditors, and regulators need proof that today's organizations are adhering to security and compliance requirements, while still ensuring that digital information can flow more rapidly and freely than ever.

However, proving security and compliance in virtualized and, ultimately, cloud environments requires a fundamental rethinking of long-standing security beliefs and practices. This is because of two pivotal shifts, both of which center on control and visibility.

1. Virtualization forever changes how organizations achieve control and visibility over core elements of their IT environment.
   - Infrastructure becomes logical not physical, rendering static, perimeter-based approaches to security and policy enforcement fruitless. Logical, dynamic boundaries pose new challenges (and opportunities) for cloud control and visibility.
   - Identities (the people, devices, and systems accessing IT-based services) become harder to confirm, simply because there are more of them. Interactions between machine identities outnumber interactions between human ones, and the cloud accelerates exposure to threats from mobile devices and social media tools, which IT organizations typically don't control and can't fully secure. Furthermore, strong authentication becomes essential as organizations increasingly add external cloud services to the IT mix.
   - Information can replicate and relocate at instantaneous speed in the cloud, making it hard to safeguard sensitive workloads and prove that information is managed according to policy.
2. Organizations increasingly surrender control and visibility to external providers in the cloud service-delivery chain. This applies whether it's IaaS for private and hybrid cloud hosting, PaaS for application development, or SaaS for applications such as Salesforce.com. In contrast to having complete ownership, management, and inspectability over all IT service components in traditional data centers, organizations must now rely on outside providers to implement controls and ensure compliance.

A major pharmaceutical company typically conducted production-scale tests with internal IT resources, a process that required hundreds of servers, took several months to set up, and resulted in operating costs of about $150,000 per second. The pharmaceutical company decided to pilot IaaS for its next production-scale test. The company rented computing infrastructure in the cloud and spent a few days setting up the test and the necessary data-security precautions. The test cost about $50 to run and was completed in one afternoon.

The reality is organizations don't yet know how to compensate for these fundamental shifts in control and visibility, nor do they understand how to take advantage of the opportunities these shifts represent.

This should not be. *The vision, expertise, experience, and technology to architect a foundation for trusted clouds are available now*.

SOLVING THE TRUST EQUATION: CONTROL + VISIBILITY^2 = TRUST

There is no denying trust in the cloud hinges on control and visibility.

Establishing trust first requires control and second a level of internal visibility that can be stepped up or expanded for external service providers. However, if control plus visibility is the formula for trust, how do we go about solving for it?

Solving for trust in internal (private) clouds is less challenging than in public and hybrid clouds because organizations control all IT assets, as well as the geographic location of their data. Control and visibility in internal clouds is about adapting existing processes to the virtual environment while capitalizing on the new advantages of virtualization.

When it comes to public and hybrid clouds, most organizations have begun cautiously moving forward, migrating low-risk (tier 2) functions and bestowing trust based on contractual assurances, strong vendor relationships, and brand reputations.

However, while performance promises and contractual penalties may provide an adequate standard of trust for some applications, a much higher standard of trust is needed for mission-critical (tier-1) functions.

Mission-critical functions require control and visibility into the cloud's performance. They also require additional precautions to ensure that information in the cloud is protected against loss or system unavailability, as well as from external threats and privacy breaches. Only this heightened level of control and visibility can deliver the critical proof (evidence) that leads to trust:

- Proof that cloud infrastructure meets security specifications and that information is managed in accordance with policies
- Proof that authorized users are who they say they are
- Proof of performance and compliance to satisfy internal management as well as auditors and regulators

Essential to proof is the ability to inspect and monitor actual conditions first-hand and not just rely on outside attestations, especially for applications handling regulated information or sensitive workloads. Organizations need transparency into service providers' environments to ensure compliance with policies and SLAs. They need an integrated view of their IT environments, both internal and external, to correlate risks, spot threats, and coordinate the implementation of countermeasures.

Today, organizations struggle to have control and visibility in their physical IT environments. This struggle need not be exacerbated in the cloud. The good news is virtualization technology creates the right conditions for organizations to improve control and visibility beyond what's available in today's physical environments.

A global payment processor wanted to virtualize its IT infrastructure, but was concerned about how to govern security and prove compliance in virtual environments, especially for regulated applications. The VCE Coalition and RSA addressed the client's security and compliance concerns, offering an integrated view of the payment processor's IT environment—both virtualized and conventional—from within a central management console.

VIRTUALIZATION: THE CORNERSTONE OF VISIBILITY AND CONTROL

Security and compliance reshape what's possible in the cloud just as much as the cloud reshapes what's possible in security and compliance.

While trusted clouds are attainable using today's technologies, innovations are coming to market that enable clouds to actually become safer and more trustworthy than conventional, non-virtualized IT environments. Given the low state of trust in the cloud today for mission-critical applications, this assertion may seem surprising. What makes this future possible? Virtualization.

VIRTUALIZATION IS A CATALYST FOR TRUST

Virtualization fuels the cloud's ability to surpass the level of control and visibility that physical IT delivers. By consolidating multiple systems on a single platform, organizations gain a centralized control point for managing and monitoring every virtual infrastructure component.

Virtualization's unparalleled visibility and consolidated control over the entire virtual environment transforms IT into a vital resource for improving security and compliance in three striking ways.

1. **Logical and information-centric**

   In clouds, the strongest security results when organizations protect information, not infrastructure. That's because in virtualized environments, static, physical perimeters give way to dynamic, logical boundaries. Logical boundaries form the new perimeters for trust, and virtual machines adapt security to their particular workloads, carrying their policies and privileges with them as they travel across the cloud.

2. **Built-in and automated**

   In clouds, where information, VMs, and entire virtualized networks can relocate in the blink of an eye, security measures must be just as dynamic as the virtual assets they protect. Achieving this means building security into virtualized components and, by extension, distributing security throughout the cloud. In addition, automation will be absolutely essential to enabling security and compliance to work at the speed and scale of the cloud. Policies, regulations, and best practices will increasingly be codified into security-management systems and implemented automatically, reducing the need for intervention by IT staff.

3. **Risk-based and adaptive**

   Static security approaches based on rules and signatures can't address advanced external threats or insider threats. Instead, organizations are developing capabilities to assess risks instantly and to initiate countermeasures. In the near future, trusted clouds will employ predictive analytics based on their understanding of normal states, user behaviors, and transaction patterns to spot high-risk events and enable organizations to proactively adapt defenses.

These three principles fundamentally change how security is applied and how compliance is proven in virtualized and cloud environments. Solutions based on these principles are transforming the cloud from an IT environment fit only for low-risk functions to an IT environment fit for an organization's most important business processes.

Security for PCI data can become stronger and more dynamic in virtualized environments. Automated discovery of sensitive data, combined with the ability to bind policies and controls to information, means PCI zones are dynamically created wherever PCI information is found. Security policies and controls move with PCI data, providing mobile, fluid, information-centric protection.

Cloud services employing risk-based and adaptive security measures are rapidly emerging and will soon become commonplace. The financial-services industry is at the forefront of this transformation. Already, more than 2,600 financial institutions use RSA's SaaS model for risk-based authentication, protecting more than 225 million users worldwide.

THE EMC AND VMWARE DIFFERENCE: PROOF NOT PROMISES

Stronger security (control) proven through direct monitoring (visibility) is the highest standard for trust in the cloud. This proof-driven standard of trust is the difference that EMC and VMware are delivering today.

We believe in the transformative power of virtualization—so much so that we're focusing our cloud-security strategy, solutions portfolio, and development initiatives on making security and compliance in the cloud 1) logical and information-centric, 2) built-in and automated, and 3) risk-based and adaptive.

Our adherence to these three principles enables us to provide organizations with cloud solutions that are adaptable to any type of workload—even mission-critical ones. This means organizations can deploy trusted clouds that meet the security and compliance requirements of any business process currently running in their conventional data centers. It also means organizations can gain the ability to directly inspect and monitor conditions in virtual environments, enabling them to base their trust on first-hand observations, not just outside attestations. Finally, it means organizations can leverage shared virtualization platforms to consolidate control over their clouds.

EMC isn't just evangelizing the cloud; we're living it. To date, EMC has achieved 75 percent virtualization on our journey to the private cloud. Our private cloud currently holds more than seven petabytes of information, including EMC data and content backed up from more than 20 external cloud services.

For years, EMC, its security division RSA, and VMware have worked to embed security, management, and compliance controls into the virtualization platform. We're also leveraging virtualization to improve security, management, and compliance in the cloud. Our cloud solutions are engineered to take full advantage of the powerful introspection and control capabilities inherent in VMware's industry-leading virtualization platform, which runs 84 percent of virtualized applications today.

For additional information about how EMC is delivering proof not promises for trusted cloud computing, please see our appendix titled, "Delivering Control and Visibility for Trusted Clouds."

CONCLUSION

Countless surveys cite organizations' concerns about security and compliance as reasons for not adopting clouds, despite cloud computing's enormous efficiency, agility, and cost benefits. It's time for all of us in IT to look beyond our fear, re-evaluate our assumptions about cloud security, and move forward with clouds for our critical business functions. To accelerate this journey, *EMC is mobilizing to provide the very highest standard of trust for the cloud—one derived from proof, not promises.*

ABOUT THE AUTHORS

ARTHUR W. COVIELLO, JR.

Executive Vice President, EMC Corporation
Executive Chairman, RSA

Art Coviello is responsible for RSA's strategy and day-to-day operations as it delivers EMC's global vision of information-centric security.

Coviello was Chief Executive Officer of RSA Security Inc., prior to its acquisition by EMC in 2006. He joined the company in 1995 and has been a driving force in its rapid growth, increasing revenues from $25 million in 1995 to revenues of more than $700 million in 2010. Coviello's expertise and influence have made him a recognized leader in the industry, where he plays a key role in several national cyber-security initiatives. Coviello speaks at numerous conferences and forums around the world.

He has more than 35 years of strategic, operating, and financial management experience in high-technology companies. In addition, he currently serves on the Board of Directors at EnerNOC, a leader in Demand Response Systems for energy conservation.

Coviello graduated magna cum laude from the University of Massachusetts.

HOWARD D. ELIAS

President and Chief Operating Officer,
EMC Information Infrastructure and Cloud Services
Executive Office of the Chairman, EMC Corporation

Howard Elias has overall responsibility for setting the strategy, driving execution, and creating best practices for EMC services that enable our customers' journey to cloud computing. He oversees EMC's consulting services, technology professional services, and award-winning global customer-support organization. In addition, Elias leads EMC's strategic Cloud Service Provider partner program, helping our customers and partners accelerate and benefit from their adoption of cloud services.

Previously, Elias was President, EMC Global Services and EMC Ionix™, and an EMC Executive Vice President. Prior to his role managing EMC Services, Elias was Executive Vice President, Global Marketing and Corporate Development, overseeing all of EMC's marketing, sales-enablement, communications, and technology-alliances activities. In that role, he was also responsible for Corporate Development and New Ventures, which focused on M&A, new business development, and the integration of acquisitions, as well as investments and the incubation of new businesses.

A veteran IT executive, Elias joined EMC in October 2003 from Hewlett-Packard Company, where he held a number of leadership positions, including Senior Vice President of Business Management and Operations for the Enterprise Systems Group. Prior to HP's acquisition of Compaq in 2002, Elias spent a year as Senior Vice President and General Manager of Compaq's Business Critical Server Group and three years as Vice President and General Manager of the company's Storage Products Division, during which Compaq became a leader in mid-tier storage systems. He has also held various senior business and product-management positions at Digital, AST Research, and Tandy Corporation.

Elias is a director of Gannett, one of the USA's leading media and marketing solutions companies and serves as a Director of the National Action Council for Minorities in Engineering (NACME). Elias attended Wayne State University and Lawrence Technological University, where he studied electrical engineering and computer science.

PAT GELSINGER

President and Chief Operating Officer, EMC Information Infrastructure Products
Executive Office of the Chairman, EMC Corporation

Pat Gelsinger is responsible for EMC's Information Infrastructure products portfolio. Gelsinger oversees EMC's entire range of information storage products, including Symmetrix VMAX, VNX, Atmos, Iomega, and the recently acquired Isilon product lines. Gelsinger is also responsible for Information Protection products, including the market leading Data Domain and Avamar lines, and the Information Security products of RSA – critical to delivering trust in the cloud. In addition, Gelsinger oversees Information Management and Information Intelligence products, which includes the recently acquired Greenplum product line.

Before joining EMC, Gelsinger was Senior Vice President and Co-General Manager of Intel's Digital Enterprise Group, the company's largest business group accounting for more than half of Intel's annual revenue. His final microprocessor, the well regarded Nehalem family, is credited for Intel's rebound in processor leadership. Prior to this, Gelsinger was Intel's first chief technology officer (CTO) where he managed Intel's longer-term research efforts. This role included leading Intel Labs, which encompasses many Intel research activities, including leading Corporate Technology Group and Intel Research and many industry standard efforts such as USB and PCI Express.

Gelsinger also led Intel's Desktop Products Group, where he was responsible for its desktop processors, chipsets, and motherboards for consumer and commercial OEM customers, as well as many of Intel's technology initiatives and the Intel Developer Forum. He also led the development of the Intel ProShare video conferencing and Internet communications product line. He was general manager of the division responsible for the Pentium Pro, IntelDX2, and Intel486 microprocessor families. He was also architect of the original 80486 and a design engineer on the 80386 and 80286 processor-design teams.

Gelsinger holds six patents in the areas of VLSI design, computer architecture, and communications; is a well-known speaker on technology trends; and has received a variety of industry awards. He received a bachelor's degree from Santa Clara University and a master's degree from Stanford University. His degrees are in electrical engineering. He is a Fellow of the IEEE and was awarded an Honorary Doctorate of Letters from William Jessup University.

RICHARD MCANIFF

Chief Development Officer and Member of the Office of the President, VMware, Inc.

Richard McAniff leads research and development across VMware's Server and Desktop Business Units. He brings more than 28 years of software-development leadership experience to VMware.

Most recently, McAniff spent 21 years at Microsoft. As corporate vice president for Microsoft Office, he was responsible for several major software tools, including Excel and Access. He also oversaw the Business Intelligence effort within Office and development of Web components for the SharePoint Portal Server. In addition, McAniff helped guide the development of Office 2000, Office XP, Office 2003, and Office 2007. Before serving as corporate vice president, he served as general manager of the Visual Basic development system.

Prior to joining Microsoft in 1987, he was a member of the technical staff at Sandia National Laboratories in Albuquerque, New Mexico, where he worked on numerous projects, including probability analyses for alternative fuels.

McAniff holds a master's degree in systems and industrial engineering from the University of Arizona, a master's degree in resource economics from the University of Massachusetts, and a bachelor of science degree in economics from the University of Massachusetts.

APPENDIX

PROVING EMC'S VISION FOR TRUST IN THE CLOUD

DELIVERING CONTROL AND VISIBILITY FOR TRUSTED CLOUDS

EMC's vision for trusted cloud computing, described in "Proof, not Promises: Creating the Trusted Cloud," asserts that trust in the cloud hinges on having control and visibility over both internal (private) clouds and cloud services delivered through external providers.

For years, EMC, its security division RSA, and VMware have leveraged our experience and expertise in information management, security, and virtualization to deliver extraordinary control and visibility in the cloud. Our solutions are closely integrated within VMware's virtualization platform to take full advantage of the virtual layer's unique control and visibility capabilities.

Today, we each offer products and services addressing the biggest challenges surrounding trust in the cloud:

- Information: How can organizations discover and control sensitive information to ensure compliance with policies and regulations? Can organizations ensure the availability and recoverability of mission-critical data in cloud environments?
- Infrastructure: How can organizations ensure their cloud infrastructure conforms to security specifications and has not been tampered with? How can organizations sharing cloud resources achieve secure multitenancy? How do they accelerate deployment of trusted clouds in a standardized manner?
- Identity: How can organizations be confident users are who they say they are to prevent fraud and unauthorized access to sensitive information? How can they ensure that only authorized devices and virtual machines have access to appropriate information and resources?

Gaining control over information in the cloud and preserving full visibility into where and how it's handled for security and compliance reporting is arguably the most significant challenge facing organizations in the cloud.

CONTROL AND VISIBILITY OVER INFORMATION

Information is becoming the currency of business and is among the most valuable and sought-after assets in clouds.

Protecting digital information is a requirement of doing business. It is tantamount to protecting business advantage. Gaining control over information in the cloud and preserving full visibility into where and how it's handled for security and compliance reporting is arguably the most significant challenge facing organizations.

Control and visibility over information in the cloud is challenging primarily because information can move instantly. Often, information moves for perfectly legitimate reasons such as load balancing, data backup, and disaster recovery. While information mobility is great for resource utilization and service availability, it can be a nightmare for information compliance.

Like all computing models, clouds have historically been "information blind," meaning they can't distinguish credit card data from the corporate cafeteria menu. Sensitive information must be handled with great care—it must be encrypted, mapped to hardware clusters with specific security profiles and/or geographic attributes, and closely monitored for compliance and auditing. In addition, multinational corporations now regard the geographic location (or "geolocation") of their data as a hot compliance issue, as countries have enacted laws forbidding certain kinds of information about their citizens from leaving their jurisdictional boundaries.

DISCOVERING AND CONTROLLING SENSITIVE INFORMATION

The intelligence to identify high-risk, high-value information and govern how it's treated is a challenge that EMC has worked to address since the earliest days of the cloud.

The intelligence to identify high-risk, high-value information and govern how it's treated is a challenge that EMC has worked to address since the earliest days of the cloud. Several of the solutions described below integrate with the RSA® Data Loss Prevention (DLP) Suite, which is designed to discover where sensitive or regulated information resides or is moving and alerts organizations of high-risk events or activities that may violate governance policies. DLP is also engineered to automate first-line remediation functions, such as blocking the transmission of sensitive data or quarantining, deleting, archiving, or applying rights management to files that contain private data.

VMware is also helping to create information awareness in clouds with its VMware® vShield™ suite of security products, which provides control and visibility at the hypervisor level to enable security and compliance for dynamic virtual environments. The VMware vShield security suite includes virtual firewalls, logical zoning, and edge network security. Supplemental capabilities are being integrated to enhance information security for customers.

For example, RSA and VMware are integrating policy modules from RSA DLP into the VMware vShield solution to discover sensitive or regulated data and create information-centric zones of secure IT resources. Designed to comply with the most exacting security and compliance standards, VMware vShield with DLP will be a ready-made solution engineered to accelerate organizations' deployment of virtualized environments and clouds with the embedded intelligence to manage and monitor the most heavily regulated data types, including personally identifiable information, payment card information, and patient health information. By using the solution's secure zones to automate the control and monitoring of sensitive, valuable information, organizations can move mission-critical business processes that formerly consumed a lot of IT resources to a far more efficient and scalable cloud delivery model.

RSA DLP's data-intelligence functions are also available with EMC's cloud solutions to help ensure information is managed in compliance with policies and regulations. For example, EMC demonstrated that RSA DLP capabilities can be integrated into the EMC Atmos® cloud storage service to make it content-aware. The EMC Atmos distributed cloud storage platform can combine its metadata-tagging system with RSA DLP to automate the distribution and placement of information in compliance with business policies. Atmos solutions are engineered to combine massive scalability—petabytes of storage across hundreds of nodes—with intelligent, automated controls for data management. Cloud services such as the Atmos platform give organizations the flexibility of on-demand storage, while preserving content-aware controls, to help ensure geolocation in compliance with jurisdictional privacy laws.

ENSURING AVAILABILITY AND RECOVERABILITY OF MISSION-CRITICAL INFORMATION

Trusting tier-1 applications to the cloud means ensuring the availability and recoverability of critical information. EMC's Data Domain® systems are designed to reduce the footprint for virtual-machine backups by as much as 40 to 60 times. Backups are easier to manage and store, and the unique deduplicated data is small enough to replicate over existing networks for highly efficient disaster recovery, without the risks and costs of tape-based backups. When using Data Domain storage with well-understood best practices for backup and VMware system snapshots, a deployment can simplify management of consistent images. Once stored, the images are ready to restore locally or, with network-efficient replication, at a remote disaster-recovery site. This enables cost-efficient protection of even massive volumes of information in virtual environments.

Verifying secure conditions in the foundations of the cloud is important for one simple reason: if organizations can't trust the safety of their computing infrastructure, the security of all the information, applications, and services running on top of that infrastructure falls into doubt.

CONTROL AND VISIBILITY OVER INFRASTRUCTURE

Proving that the physical and virtual infrastructure of the cloud can be trusted can be prohibitively difficult, particularly when it comes to cloud services from external service providers.

Verifying secure conditions in the foundations of the cloud is important for one simple reason: If organizations can't trust the safety of their computing infrastructure, the security of all the information, applications, and services running on top of that infrastructure falls into doubt.

INSPECTING THE CLOUD'S FOUNDATIONS

EMC is collaborating with Intel to make the cloud's foundational infrastructure as open to inspection, analysis, and reporting for compliance as the cloud's application-services layer. By combining the VMware vSphere™ platform and the RSA Solution for Cloud Security and Compliance with Intel Trusted Execution Technology (TXT), EMC will enable cloud service providers and organizations to validate launch-time security for every physical and virtual component in the entire computing stack. This security data can be streamed into the RSA Archer™ eGRC console to furnish proof to tenants, auditors, and regulators that the cloud infrastructure stack is secure. Clouds implementing an integrated solution stack built on Intel's hardware root of trust will enable organizations and IaaS tenants to self-inspect, validate, and prove the integrity of their cloud infrastructure, from processor through the virtualization layer. For organizations running sensitive workloads in clouds, the visibility provided through this integrated solution promises to greatly simplify and streamline compliance reporting and audits.

Solutions based on a hardware root of trust can verify a secure infrastructure, but when that infrastructure is shared, even between different groups within the same organization, how can organizations ensure virtual partitions stay intact?

LAYING THE INFRASTRUCTURE FOR SECURE MULTITENANCY

To achieve secure partitions and multitenancy, virtual environments and clouds based on the industry-leading VMware vSphere platform can leverage built-in security features within the VMware vShield product family. The hypervisor-level firewall in the VMware vShield platform is engineered to enforce proper segmentation and trust zones for applications. In private clouds, this means organizations can set up virtual firewalls so that applications with different security requirements—for example, production and testing, finance, and sales—can be hosted in the same virtual data

center. In a service-provider environment, VMware vShield solutions enable different tenants to share IT resources safely by creating logical security boundaries that provide complete port-group isolation.

To ensure secure storage in public clouds, the EMC Symmetrix® VMAX™ platform is the industry's first cloud storage solution capable of secure multitenancy. The platform embeds RSA Data Protection Manager to safeguard cloud-based information through hardware-based encryption and key management. The VMAX platform's hardened data security features ensure sensitive information can be encrypted and rendered unusable to outside parties, all without slowing down the performance of the system. EMC Symmetrix VMAX systems scale to two petabytes and are designed for mission-critical virtual data centers.

ACCELERATING DEPLOYMENT OF TRUSTED CLOUDS

Ensuring service levels for availability, scalability, and recoverability requires trusted platforms. That's what EMC, VMware, Cisco, and Intel have delivered through the Virtual Computing Environment coalition. The VCE coalition's Vblock™ platform is engineered to provide a standardized, complete virtual infrastructure, from storage and networks to management, security, and compliance—all integrated and tested to ensure performance and scalability. Vblock systems greatly simplify and accelerate the deployment of enterprise-class clouds, giving organizations and service providers the ability to meet high service levels for performance, availability, and scalability.

CONTROL AND VISIBILITY OVER IDENTITY

While protecting against unauthorized or fraudulent users is a challenge in any IT environment—virtualized or not—clouds heighten the risk of intrusion simply because they increase potential points of exposure and because the number of identities, most of which are machines, becomes more plentiful and ephemeral in clouds. Furthermore, clouds heighten the organization's exposure to mobile devices and social-media platforms, which IT organizations typically don't own, control, or secure.

The best way to deal with mounting risks of unauthorized access to private clouds is to be more discerning about who's trying to get in and to detect high-risk activities once they're inside.

VERIFYING USERS IN HIGH-RISK TRANSACTIONS

Essential to this is risk-based authentication, which detects abnormal conditions, such as a user signing in from an unknown device at an IP address in the Ukraine when earlier in the day that same user logged in from a corporate office in Dallas, Texas. RSA Adaptive Authentication is designed to conduct instantaneous, behind-the-scenes risk assessments of users attempting to log into enterprise services. When it detects suspicious conditions, the system automatically takes secondary steps to verify the user's identity by posing additional authentication challenges using information that only the genuine user would know (e.g., "Enter the ZIP code for your home address"). RSA Adaptive Authentication is engineered to evaluate more than 100 risk indicators, correlating factors such as the type of access device being used, the user's past behavioral patterns, and external threat intelligence from RSA eFraudNetwork™ feeds. A unique risk score is assigned to each activity, and users are only interrupted when high-risk conditions are identified and/or organizational policies could be violated.

DETECTING FRAUDULENT USERS INSIDE CLOUDS

It's inevitable that some enterprise access credentials will be compromised with the thousands of malware variants out there stealing passwords. RSA® Transaction Monitoring can help identify and mitigate damage from fraudulent users after they've gained access to an organization's cloud. RSA's fraud-detection platform leverages the same risk assessment engine used by more than 8,000 financial institutions to protect their 250 million online users worldwide. It layers on top of any authentication system to recognize deviant and potentially malicious activity in real time. When it spots high-risk events, RSA Transaction Monitoring is engineered to interrupt user activities by presenting additional authentication challenges, including out-of-band verification techniques, such as requiring a suspicious user to enter randomly generated passwords sent to the genuine user's mobile phone.

THE VALUE OF UNIFIED CONTROL AND VISIBILITY

Designed for static, physical computing systems, conventional security-management systems are too slow and rigid to handle inherently dynamic, virtualized environments and clouds. Traditional security management relies disproportionately on manual processes and human intervention to manage dependencies and configure policies—an unreliable, unscalable process that won't work in clouds, where entire virtual networks can move at the blink of an eye.

As the rate of change accelerates and users' expectations grow, IT teams need to streamline management processes so they can more rapidly and efficiently control, monitor, and report performance across their IT environments, physical and virtual, internally operated and externally hosted. Addressing these challenges will require IT management tools that leverage automation.

AUTOMATING SECURITY AND COMPLIANCE MANAGEMENT

Automation can deliver the efficiency, control, and scale needed for cloud environments while minimizing costs and ensuring security and compliance.

Automation can deliver the efficiency, control, and scale needed for cloud environments while minimizing costs and ensuring security and compliance.

Automation can deliver the efficiency, control, and scale needed for cloud environments while minimizing costs and ensuring security and compliance. VMware virtualization and cloud-management solutions replace inefficient, manual processes for change control and configuration with policy-based controls and built-in automation. Designed into each layer of the virtualized technology stack, VMware virtualization and cloud management solutions offer policy-driven processes and "set and forget" administration for change management and configuration. This enables organizations to dynamically map application dependencies across their data centers, monitor application performance, and help ensure compliance.

The RSA Archer eGRC Platform is designed to provide a highly flexible, well-integrated framework for managing, monitoring, and reporting on governance, risk, and compliance conditions across the IT environment. The platform integrates with an organization's other IT systems to automate data exchange without requiring IT teams to touch a single line of code. It merges hundreds of disparate data streams from different IT systems to create holistic models of key business processes, which can be analyzed and managed from within a single console. These integrated models give organizations point-and-click controls for configuring policies, automating processes, governing workflows, and setting user privileges simultaneously across multiple environments. More importantly, they also enable organizations to report on governance, risk, and compliance at a business level, not at an individual application level. This business-level visibility, combined with the Archer eGRC Platform's ability to set controls for multiple IT environments simultaneously, establishes a unified operating system for critical business processes and greatly simplifies governance, risk, and compliance.

BUILDING THE EXPERTISE TO BUILD THE CLOUD

As cloud technology rapidly matures, public and private cloud offerings have ballooned in popularity, with hybrid clouds beginning to pick up traction as well. The next question organizations must answer is how to tie together business requirements for trust with their cloud policies, controls, and governance models. This process begins with examining applications or workloads to define their optimal placement in relation to cloud models or an organization's legacy computing environment. It then makes a comprehensive evaluation and transformation of the governance of information to ensure the proper stewardship, ownership, and classification of assets.

OPTIMIZING CLOUD STRATEGIES

EMC Consulting has developed an adaptable methodology to provide customized workload analysis through three filters: economic, trust, and functional. EMC Consulting helps customers optimize their cloud infrastructure, including significantly lowering risk by adhering to a set of secure and compliant trust requirements.

Balancing the need for transparency and compliance with private, public, and hybrid cloud options based on economics, feasibility, and trust, EMC Consulting has created the EMC Cloud Advisory Service with Cloud Optimizer. This innovative service is designed to establish benchmarks to measure information assets in accordance with industry and organization-centric trust, delivering potential savings of up to 25 percent of IT budgets. EMC Consulting works with customers to set strategy, develop the business case, define the architecture, and build governance models to achieve cloud operational excellence.

EMC Consulting's Cloud Optimization approach starts by identifying workloads that are candidates for movement to the cloud based on usage, the asset's origination and destination points, and the sensitivity of the information. This is followed by an economic-impact analysis to judge how an asset's value will change once the workload shifts to the cloud. However, before trust filter analysis can be applied, organizations must understand the characteristics and requirements of a trustworthy computing environment. These six non-mutually exclusive requirements as defined by EMC Consulting include:

CONTROL

- **Availability**: Ensure access to resources and recovery following interruption or failure
- **Integrity**: Guarantee only authorized persons can use specific information and applications
- **Confidentiality/Privacy**: Protect how information and personal data is obtained and used

VISIBILITY

- **Compliance**: Meet specific legal requirements and industry standards and rules
- **Governance**: Enforce policies, procedures, and controls and establish usage rights
- **Risk Management**: Manage threats to business interruption or derived exposures

WHAT'S SAFE TO DEPLOY IN CLOUDS?

Concerns surrounding trust in the cloud can be addressed by making judicious decisions about which workloads and IT-based services to deploy on what types of clouds. EMC recently published a paper titled, "Building a Trusted Path to the Cloud: Deployment Strategies for Private & Hybrid Clouds," which helps organizations step through this decision-making process.

After an organization understands the different trust profiles of the potential destinations for workloads (public, private, and hybrid clouds, and in-house legacy environments) and how their own infrastructure satisfies the six trust requirements, a trust filter analysis will help determine what cloud options are best suited for their specific industry and architecture needs. A functional evaluation is applied to specify which workloads can be moved to which cloud model without loss of functionality. Once economic, trust, and functional filters are successfully applied, the preferred cloud-deployment destination for each workload will emerge, providing a purposeful and built-in secure framework for trust enablement within clouds.

CONTROL AND VISIBILITY FOR THE CLOUD, DELIVERED BY THE CLOUD

As organizations move IT-based services to the public or hybrid cloud, they traditionally lose both control and visibility over the information, infrastructure, and identities in those clouds. The loss of control and visibility is compounded when organizations deploy cloud services from multiple providers.

The Cloud Trust Authority will address this problem. It will provide a unified platform for managing security controls and gaining visibility to prove compliance across multiple cloud providers. Incorporating technologies from RSA and VMware, the Cloud Trust Authority will deliver a core set of functions required across a wide variety of clouds, including identity management, data security, and security and compliance reporting. Customers will be able to manage all these services via the Cloud Trust Authority console, making it simple and easy to configure and deploy the capabilities needed to enable trusted, compliant use of cloud service providers.

Among the highlights of the Cloud Trust Authority's inaugural set of capabilities will be its Identity Service. The Identity Service federates access privileges and identity management across multiple clouds to enable secure and federated single sign-on and directory synchronization with options for strong authentication.

Beyond its Identity Service, the Cloud Trust Authority will also enable organizations to compare the trust profiles of various cloud providers against the standards and best practices developed by the Cloud Security Alliance, among other security frameworks. By developing a linked community of private and public clouds with similar trust profiles, RSA will make it easier for enterprises to rapidly add capabilities and on-board new cloud providers, dramatically lowering the barriers to trusted cloud computing.

By developing a linked community of private and public clouds with similar trust profiles, RSA will make it easier for enterprises to rapidly add capabilities and on-board new cloud providers, dramatically lowering the barriers to trusted cloud computing.

EMC's technology partnerships with IT industry leaders have resulted in a variety of innovative solutions that deliver superb control and visibility into virtualized and cloud environments.

SUMMARY

Before organizations can take advantage of the cloud's agility, efficiency, and cost benefits for a wide range of IT services, they need to first ensure the cloud can be trusted. EMC believes trust in the cloud can be achieved by establishing control and visibility in two vital ways:

- Providing organizations sufficient control over cloud security and compliance to adapt to any type of workload, even mission-critical ones
- Giving IT teams the ability to directly inspect and monitor conditions in both internal and hybrid clouds, thus enabling organizations to base their trust on first-hand observations, not just outside attestations

EMC's technology partnerships with IT industry leaders have resulted in a variety of innovative solutions that deliver superb control and visibility into virtualized and cloud environments. To help organizations accelerate their deployment of trusted clouds, EMC Consulting provides strategic guidance and technology expertise for pervasive virtualization, application migration to virtual infrastructure, and risk/readiness assessments for moving applications and business processes to the cloud.

CONTACT US

For more information, please visit www.EMC.com.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com