



A GUIDE TO STAYING SECURE AMIDST GROWING THREATS AND THE EXPANDING DIGITAL UNIVERSE

Security management needs to evolve to protect business, government, and individuals from growing cyber threats. This EMC[®] Perspective outlines challenges facing security executives and teams and uses an “air traffic control system” analogy to show how advanced security management systems can deliver better security by providing a single point of visibility and coordination for physical, virtual, and cloud assets. Solutions are presented where business processes, policy, controls, and data work in concert to achieve the vision of an air traffic control system for information security.

THE THREAT LANDSCAPE AND DIGITAL UNIVERSE ARE GROWING RAPIDLY.

Average monetary value of losses due to cyber crime was \$394,700.

– 2010 Cybersecurity Watch Survey

According to Eric Schmidt, CEO of Google, “Every two days now, we create as much information as we did from the dawn of civilization up until 2003.”

The Digital Universe will expand 44-fold to 35 trillion gigabytes by the year 2020—and grew to 800 billion gigabytes, 62 percent over 2008.

– IDC Digital Universe Study, 2010¹

Today more than ever, IT and security teams are challenged by the growing sophistication and volume of cyber attacks on businesses, governments, individuals, and infrastructures. IT professionals see a steady increase in the types and number of malicious website infections and botnet activity. Exposure grows daily with more elaborate phishing, pharming, and Trojan attacks perpetrated by both external and internal online fraudsters. Risk of IP theft increases as businesses share information with individuals and partners across the globe—often through devices that are personally owned, yet connected to corporate devices.

At the same time, compliance requirements, based on international controls and standards, are becoming more stringent. CIO Magazine² estimates that IT professionals spend as much as 20 percent of their time devoted to compliance. Yet people continue to take pictures, send email, blog, and post videos. Companies keep adding to their data warehouses. And governments are requiring that more information be retained. With the digital universe continuing its exponential growth—by a factor of almost five over the next four years—IT and security teams will remain highly pressured.

IT’s transformation to new, cloud-based operating models further complicates the challenge. Internal and external cloud and virtualized environments are growing exponentially. The number of virtualized assets now exceeds the number of physical servers. IDC estimates that by 2014, much of our digital information will be travelling through the cloud. To realize the business benefits of this next wave in IT, virtualization of business applications and networks must be done without compromising security.

SECURITY AND IT ARE NOT EQUIPPED TO HANDLE THIS CHANGE

In many organizations, security management practices are limited to periodic assessments of procedures, ad-hoc vulnerability scans, and occasional log reviews, so IT’s view into the security posture is often outdated. Security management is evolving slowly from basic perimeter and endpoint security, and is still often reactive in nature. While adoption of proactive security event and information management and data loss prevention is on the rise, the information from these systems is isolated. As a result, there is little automation, analytics, or context to prioritize risks that really matter to the business. Although organizations are moving quickly to adopt new business models that depend on cloud, mobile, and virtualization technologies, their security teams are hard pressed to keep abreast of how this is affecting their security risk posture.

In addition, many security teams lack a single view of information, infrastructure, and identities across both physical and virtual environments. This makes it difficult for both the business and IT to understand how they relate and the security risks they pose. Many organizations have been impacted by stolen corporate credentials and identities and by devices that have been infected by a wide range of malicious attacks. As a result, security measures often don’t adequately address both internal and external threats. IT teams are slow to respond to incidents and to adapt to changing threats including risk introduced by untrained and security-unaware employees and partners. Yet pressure mounts steadily on business, IT, and security professionals alike to ensure that threats are efficiently and effectively prioritized by their potential impact on the business—and remediated swiftly. Better tools are needed for behavioral analysis, which requires data mining and evaluation of a huge volume of data types such as logs, vulnerabilities, configuration state, identities, and data classification. No current system architecture can facilitate such analysis.

Security professionals can no longer just focus on “checking the box.” Rather, they need to look at the entire spectrum of threats and bring value to the overall business by leveraging prioritized risk management techniques already being performed by their finance and operational colleagues.

THE COSTS OF SECURITY AND COMPLIANCE ARE GROWING—ALONG WITH THE COSTS OF A BREACH

Management, customers, and partners all understand that the security industry needs to get better at security management. The risks of not evolving existing systems are high; brand and reputation can be severely impacted by publicity around security breaches. Understandably, organizations do not want to make security an obstacle to expanding the business or developing new intellectual property. Organizations considering whether or not to make the investment in developing advanced intensive threat/risk management processes must recognize the tremendous cost of remediating security breaches and the damage to brand and reputation those breaches can cause.

THE SOLUTION: ADVANCED SECURITY MANAGEMENT

ADVANCED SECURITY MANAGEMENT IS ESSENTIAL TO LOWERING RISK AND COSTS

The right security management strategy, conceptual architectures, systems, and programs can lower risk and cost. An advanced security management system provides a single point of visibility and coordination for physical, virtual, and cloud assets. This enables security teams to prioritize threats relevant to the business and proactively remediate and track incidents with minimum impact.



Information security professionals can take a lesson in security management from the air traffic control industry. Every day, over 400,000 airplanes are in flight around the world, safely sharing airports, runways, and airspace due to the monitoring and orchestration of air traffic control operations around the globe. Consider the number of inputs that an air traffic controller receives to manage the flights of numerous aircraft travelling at different air-speeds, altitudes, and headings. If those inputs were not correlated, and if the air traffic controller had no system for distinguishing the importance of one from another, the results would be disastrous. To oversee large volumes of air travel, controllers leverage a system that has been refined over the past 50 years for managing flight traffic. This system is so sophisticated that on 9/11 operators were able to safely land 5,000 planes in just a few hours thanks to a complex mix of manpower, technology, procedure, and judgment.

The security executives and their teams, within and between organizations, need to evolve to integrate context, analytics, and enforcement at point of use. Viewed as a system, security management needs to integrate people, process, and individual security controls with the same kind of correlated, contextual, and comprehensive view used by the aviation industry to guarantee the safety of our airways. Information security management needs to function as a system capable of effectively and efficiently managing information infrastructures, providing visibility, manageability, and control across all three domains—physical, virtual, and cloud. Security professionals need systems that enable them to close the gaps of protection and apply controls in a more holistic, systemic manner, centralizing management—not just for some controls—but for all.

The goal of advanced security management is to simplify and enhance alignment between the security team responsible for defining security policy and the operations team charged with implementing that policy. The integration of technologies, systems, and feeds enables a holistic approach to risk management and compliance, providing a single view to the most important security and compliance elements across the entire IT environment. In effect, IT organizations need to build their version of air traffic control for the traditional information infrastructure.

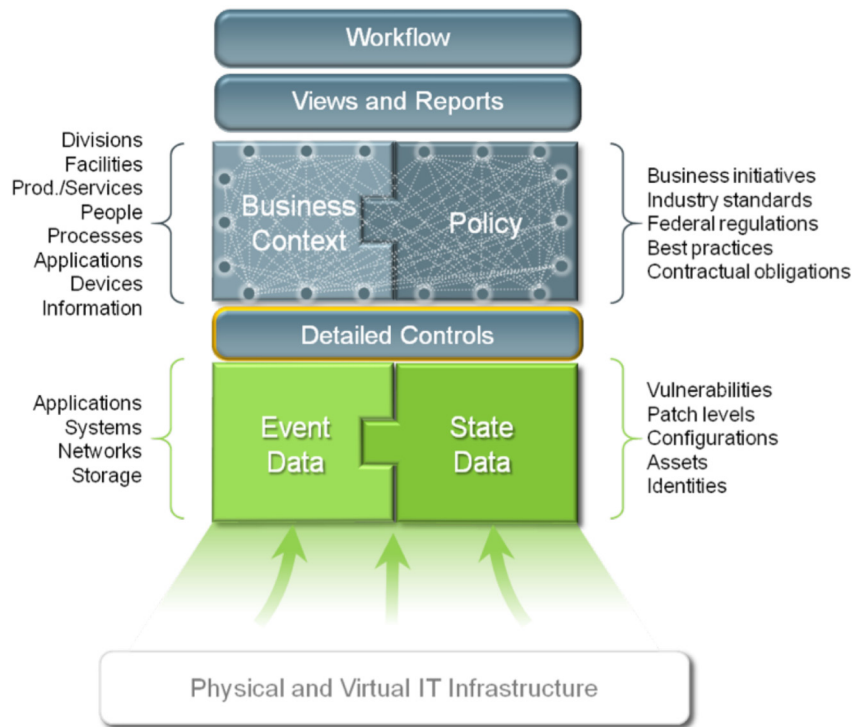


WHAT DOES ADVANCED SECURITY MANAGEMENT LOOK LIKE?

First and foremost, advanced security management needs to be an end-to-end, closed-loop process that is highly automated. From detection through incident management to forensic analysis, a comprehensive, near-realtime view of threats to sensitive or critical identities, information, and infrastructure provides a complete view across the organization of threats to identities, infrastructure, and information that are relevant to the business, as well as remediation recommendations that are easily prioritized and tracked.

Advanced security management systems are continuously updated on emerging threats and attack vectors from different industries and geographies, leveraging easy-to-use tools for dashboarding, compliance reporting, and forensic analysis. These systems have integration with embedded detection tools and controls such as encryption, authentication, and event monitoring. Correlation and analytics help prioritize incidents and ensure that they are dealt with swiftly and with minimum impact to the business. This means that IT resources spend more time proactively protecting the business, and authorized employees follow policy more often, reducing exposure to insider risk. The benefits of an advanced security management system are many:

- Accelerated and more effective response to stolen credentials, identities, and data, reducing potential incidents and business impact
- Security operations focused on the right priorities
- Centrally managed security policies across both physical and virtual endpoints
- Tighter controls for local and remote access to virtual desktops
- More secure collaboration with third parties/non-employees
- Controlled access to and use of sensitive data by end users
- Streamlined security incident reporting, escalation, and remediation
- Lower costs due to streamlined processes and fewer exposures
- Security seen as an enabler of the business to meet its goals



CONCEPTUAL MODEL FOR A LAYERED APPROACH TO ADVANCED SECURITY MANAGEMENT

Let's consider a layered conceptual model that can achieve the vision of a successful air traffic control system for information security. Organizations can use this approach as they journey to the cloud, leveraging virtualization to deliver better security by providing a single point of visibility and coordination for physical, virtual, and cloud assets. The key layers of this model include the following.

- **Workflow**—automates step-by-step processes for key security management functions such as policy management, risk, and compliance assessments and incident response.
- **Views and Reports**—brings visibility to what were once isolated technologies, inputs, and feeds into a single platform or framework, as in an air traffic control system.
- **Business Context and Policy**—this is where policies that govern the organization and information infrastructure are defined based on compliance requirements, best practices, and the nature of risk. Policy is enforced with workflow and reports, and by connecting to detailed controls and procedures that are, in turn, tied directly to IT assets. This layer stores enterprise infrastructure information such as business processes, supporting applications, and infrastructure elements, rated by criticality.
- **Controls**—manual and automated controls are provisioned and monitored in this layer. These controls are mapped through to policies, and satisfy multiple regulatory and business requirements. This is the point of security detection enforcement across the infrastructure. In an ideal environment, many controls are embedded directly into IT infrastructure such as operating systems and networks, providing ubiquitous coverage without deploying and managing hundreds of point tools.
- **Event and State Data**—in this layer, events and states are collected and correlated from applications, systems, network, and storage, from both the physical and virtual infrastructure. IT context is achieved when state data (for example, DLP data at rest scans, vulnerability scans, patch state, configuration state, and fraud and threat data) and event data (for example, SIEM, Netflow, and forensics) are collected into a single warehouse for analysis.

ADVANCED SECURITY MANAGEMENT SOLUTIONS FOR PHYSICAL, VIRTUAL, AND CLOUD ENVIRONMENTS

A number of solutions based on this conceptual model exist today, providing the vision of air traffic control to advanced security management.

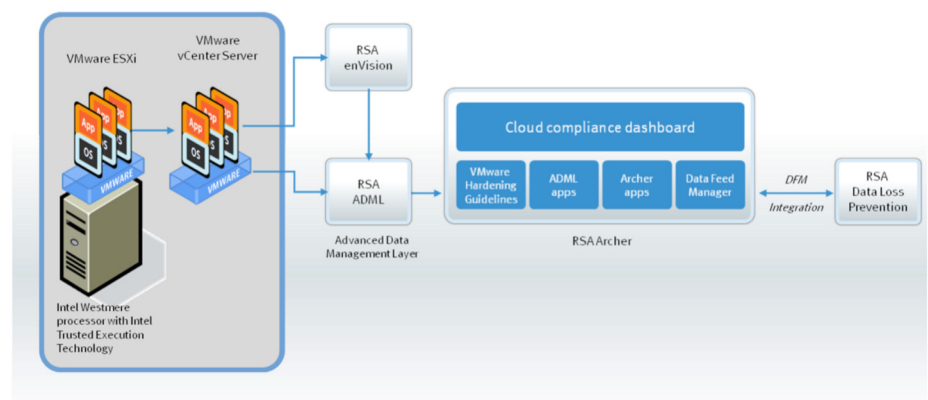
For example, the RSA® Solution for Cloud Security and Compliance enables VMware® security policy implementation and management, security and compliance measurement, issue remediation, and reporting—all from a single console. Based on the RSA Archer® eGRC platform, the solution helps organizations rationalize compliance requirements, controls, standards, and best practices into centralized security policies administered consistently across virtual and physical infrastructures. In addition, IT and security operations teams can cooperate to manage compliance to security policies, streamlining processes and reducing administrative costs. With the RSA Solution for Cloud Security and Compliance, organizations can control security and compliance across physical and virtual infrastructures today—building the foundation for cloud computing.

Another example is a proof of concept created by RSA, VMware, and Intel that leverage Intel's Trusted Execution Technology and the RSA Archer Enterprise Governance, Risk, and Compliance platform to create a chain of trust from the processor through the hypervisor and to the operating system. This capability is engineered to make it possible to actually verify that virtual applications are running on infrastructure that has not been compromised by malware.

The resulting integrated proof of concept feeds highly precise data on physical hardware and virtualization layer conditions into specialized data analysis tools, which examine the data for events and conditions affecting security and compliance. The information is then evaluated in the context of larger business requirements by RSA Archer, which presents a unified, policy-based assessment of the organization's security and compliance posture through a central dashboard. Comprising a hardware root of trust, trusted virtualization environment, security information and event management tools, and GRC management software, this solution provides truly unprecedented visibility into actual conditions within the bottom-most layers of the cloud.

The third example is a new technology demo that leverages the Intel TXT processor, VMware vCenter™, and the RSA Archer eGRC platform to control and manage geographic location of virtual machines. This technology demo is engineered to enable policy-based restrictions preventing sensitive data and processes in the cloud from travelling to unauthorized locations.

Advanced Security Management Measuring and monitoring Cloud infrastructure security



CONCLUSION

With the threat landscape growing—and no abatement of the growth of digital information in sight—advanced security management is clearly the way forward for organizations that must proactively remediate, prioritize, and track incidents with minimum impact to the business. With the right strategy, conceptual architectures, systems, and programs, advanced security management can lower costs and significantly reduce exposures through automation. Organizations benefit from a comprehensive view of threats that are relevant to the business, as well as reporting and analytics that help demonstrate compliance. Using the air traffic control system analogy, advanced security management systems deliver better security by providing a single point of visibility and coordination for physical, virtual, and cloud assets. A layered model where business processes, policy, controls, and data work in concert achieves the vision of air traffic control system for information security.

As previously discussed, enabling technologies exist today, and security professionals must embrace them. Advanced security management is essential to lowering risk and costs throughout the growing digital world—in business, government, infrastructure, and even in the home.

ABOUT EMC CONSULTING

As part of EMC Corporation, the world's leading developer and provider of information infrastructure technology and solutions, EMC Consulting provides strategic guidance and technology expertise to help organizations exploit information to its maximum potential. With worldwide expertise across organizations' businesses, applications, and infrastructures, as well as deep industry understanding, EMC Consulting guides and delivers revolutionary thinking to help clients realize their ambitions in an information economy. EMC Consulting drives execution for its clients, including more than half of the Global Fortune 500 companies, to transform information into actionable strategies and tangible business results. More information about EMC Consulting can be found at www.EMC.com/consulting.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk, and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. Combining business-critical controls in identity assurance, encryption and key management, SIEM, Data Loss Prevention, and Fraud Protection with industry-leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com.

CONTACT US

To learn more about how EMC Consulting and RSA can help solve your business and IT challenges, contact your local representative—or visit us at www.EMC.com/consulting and www.RSA.com.

¹ <http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm>

² CIO MAGAZINE 2010 STATE OF THE CIO SURVEY <http://www.cio.com/documents/pdfs/StateoftheCIOJanuary2010.pdf>

EMC², EMC, RSA, RSA Archer, RSA enVision, the RSA logo, the EMC logo, and where information lives are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware, ESX, and vCenter are registered trademarks or trademarks of VMware, Inc., in the U.S. and other jurisdictions. All other trademarks used herein are the property of their respective owners. © Copyright 2010 EMC Corporation. All rights reserved. Published in the USA. 12/10 EMC Perspective H8540