

# RSA Security Brief

February 2011



## Mobilizing Intelligent Security Operations for Advanced Persistent Threats

### Authors

Sam Curry  
Chief Technology Officer, Global Marketing, RSA

Bret Hartman  
Chief Technology Officer, RSA, EMC Fellow

David P. Hunter  
Chief Technology Officer, World Wide Public Sector, VMware, Inc.

David Martin  
Chief Security Officer, EMC Global Security Organization,  
EMC Corporation

Dennis R. Moreau, Ph.D.  
Senior Technology Strategist, RSA

Alina Oprea, Ph.D.  
Principal Research Scientist, RSA Laboratories, RSA

Uri Rivner  
Head of New Technologies, Consumer Identity Protection, RSA

Dana Elizabeth Wolf  
Senior Manager, New Business Development, RSA

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

---

Executive Overview	1
APTs: Wars of Subversion	2
APTs in the Enterprise: An Inevitable Escalation	4
Countering APTs with Intelligent Security Principles	6
Advanced Security Operations: the First Step toward Intelligent SOCs	8
Disciplined execution	8
Information-centric security	8
Integrated compliance monitoring and threat detection	8
Awareness of cybercriminal activities	9
The Intelligent SOC, a New Model for Security Operations	9
Summary and conclusions	13
Appendix: About the Authors	14
Solutions for Advanced SOCs and APTs	16
Solutions from RSA	16
Solutions from VMware, Inc.	16

## Executive Overview

---

Advanced Persistent Threats (APTs) are one of the most menacing and fast-growing information security threats facing organizations today, particularly as companies move into the cloud. People often associate APTs with political targets, but attackers are increasingly using APTs to strike enterprise targets for financial gain. Over the past couple of years, APTs have become incredibly sophisticated and diverse in their methods and technologies, particularly in their ability to use an organization's own unwitting employees to penetrate IT systems and pull off attacks. While traditional attacks start with mapping networks and collecting intelligence on technical vulnerabilities, an APT often starts with mapping the human organization and collecting intelligence on employees, who are nowadays a weaker link than network components. This suggests that investing more in network defenses might be counterproductive, and a new defense doctrine is required.

APT techniques have proven so successful and rewarding to attackers that today's organizations must operate under the assumption that such attacks are inevitable. While it may be impractical, even impossible, to prevent APTs, organizations nevertheless can deflect such attacks by making themselves difficult, unprofitable targets, or by discovering APTs early to prevent large-scale damage. This involves developing intelligent, comprehensive approaches to help organizations become faster and more efficient at detecting APTs, neutralizing them and identifying perpetrators. Evolving these defensive capabilities to work at the speed and scale of the cloud will require security operations centers (SOCs) to develop new models for mapping risks, attack vectors and threats.

1. Assess risks at the business-level to discover the "crown jewels" of the enterprise – the information and infrastructure assets that matter most, as well as which people and systems have access to them.
2. Model IT resources and potential attack vectors to neutralize attacks and proactively identify the security technologies and processes needed for implementation.
3. Leverage threat planning models and security events to test, evolve and improve security operations, particularly ways to minimize windows of exposure to future risks and damages.

Emerging technologies will also help manage the risk of APTs:

1. **Dynamic Virtualization** will be used to gain visibility, control and integrity, dramatically complicating the infiltration of sensitive resources.
2. **Adaptive Analytics** will enable real-time risk management decisions and allow defenses to evolve with the threat.
3. **Cybercrime Intelligence** will be used to prioritize asset allocation, identify emerging threats and spot unmapped vulnerabilities.

In this security brief, leading security experts from RSA and VMware provide a front-line perspective on APTs, and how these threats require us all to adapt our security strategies and practices to effectively mitigate damage from such attacks.

---

### What's a SOC?

Security operations centers (SOCs) go by many names, including critical event response teams (CERTs) and critical incident response centers (CIRCs), but they all fundamentally have the same responsibility: to take care of an organization's day-to-day information security requirements, most notably monitoring IT infrastructure and services for security threats and managing the technologies and procedures to protect against electronic intrusion and misuse. SOCs typically employ specialized security processes, personnel and technologies to conduct risk analyses, detect unauthorized access and prevent and manage security-related incidents. The technologies and techniques SOCs use to perform their functions are evolving rapidly in response to the threat environment.

---

## APTs: Wars of Subversion

---

Advanced Persistent Threats (APTs) are garnering heightened attention among CIOs and security executives as APTs are increasingly used to attack private sector companies in addition to military and political targets. While the threats underlying APTs are not new – after all, corporate espionage and sabotage have occurred for centuries – APTs represent a fundamental and dramatic escalation in tactics exploiting trusted social connections, sophisticated malware and determined and patient attackers.

The defining hallmark of APTs is that their characteristics are deliberately randomized to make detection using traditional threat indicators extraordinarily difficult. Abnormal trusted user activity, out of context data retrieval or an unusual sequence of otherwise low-risk security events may be the only telling signs. Here are a few reasons why APTs are so hard to detect:

- APTs often piggyback on employee resources and privileges, rather than try to take direct control of actual network components and applications.
- Unique, novel attack signatures and behavior patterns make attacks hard to correlate on signatures and footprint.
- Activities are distributed across long periods of time, making them hard to correlate based on time stamps.
- Perpetrators appear to come from a wide variety of sources – distributed botnets are often used to host attacks – making it difficult to identify attackers.
- Data traffic generated by the attack is often obfuscated through encryption, compression, or by hiding transmissions within the behavior of compromised executables (covert/side channels). These techniques make it hard to determine where the stolen information came from or where it's moving.

Although no two APTs are the same and the methods and technologies used in attacks vary widely, APTs generally exhibit these qualities:

1. **Purpose-driven and tailor-made for individual targets** – The criminal operators behind APTs select their targets with great care, and they custom-design their infiltration and attack methods to have the greatest effect against the targeted organization's known systems, defenses and personnel. Attackers scope out employees within the target organization who have high-level access to the systems and processes needed for the attack. Attackers conduct reconnaissance to understand the target organization's systems, applications and networks to exploit unpatched, undetected or unknown (zero-day) vulnerabilities. APTs have clear objectives, typically ranging from stealing intellectual property and other sensitive data to altering the performance of critical infrastructure to manipulate or cripple an organization's operations.
2. **Low and slow** – To help evade detection, APT attackers keep low profiles within an infiltrated organization's IT environment and can sometimes lie dormant for months waiting patiently for optimal conditions to strike. Sustained monitoring and interaction over time are hallmarks of APTs. Where most electronic thefts organizations have experienced in the past are akin to pickpockets, APTs are more like con artists who carefully study and cultivate their marks over time.
3. **Organized and well-funded** – The groups behind APTs have the financial backing to wage resource-intensive attacks over a long period of time. The sophistication of most APTs suggest there are formally constituted, multidisciplinary teams behind them, with team members possessing specialized expertise and access to complex IT infrastructure and capabilities. These groups have highly evolved criminal supply chains and R&D capabilities, as well as the ability to procure cloud computing resources, undiscovered malware exploits, entire botnets and whole populations of already compromised enterprise assets.

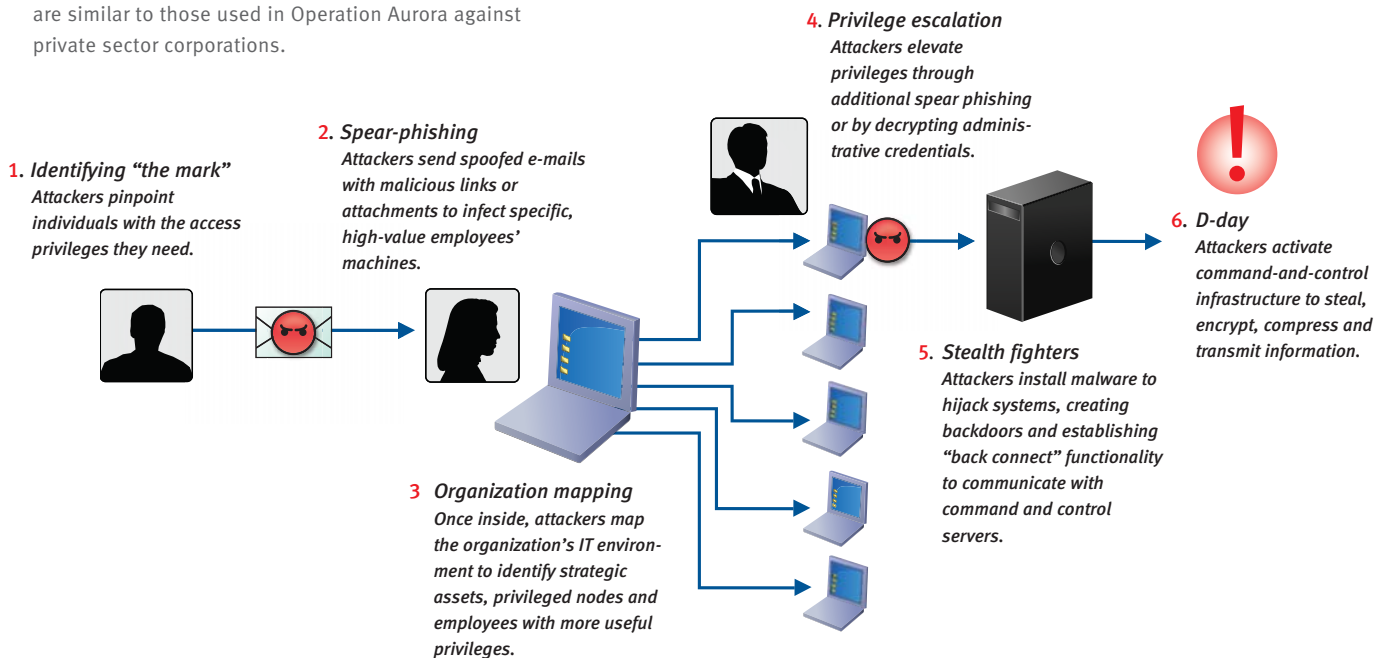
**4. Diverse, concurrent attack methods** – APTs frequently use multiple attack vectors simultaneously, both automated and human. Because attackers are well-funded and have strong motivation to succeed in their attacks, they employ a range of creative methods and technologies to infiltrate and infect nodes in their targets’ IT environments. They frequently employ zero-day vulnerabilities to compromise systems or identify holes in network armor through port scanning or other methods. Simultaneously, attackers will often use an organization’s own employees as unwitting participants in APT attacks. APTs frequently use social media tools such as spoofed LinkedIn® invitations to create false pretenses for trust to compromise employees’ access credentials and systems.

The human element of APTs is particularly important to understand, as this is what makes these attacks so insidious and effective. When it comes to APTs, it is people, not networks, on the battlefield’s front lines. APTs usually target and exploit authorized users of an IT environment to gain access to protected systems and valuable information. Feigning trusted connections is a common tactic used in APTs. Criminal operators may contact an organization’s employees through social media sites – “We went to school together at Michigan” – and trick employees into clicking links or opening attachments that download malicious code onto their computers. Such malware often enables attackers to hijack employees’ access credentials so they can gain illicit access to the organization’s IT environment. Nowadays, APT operatives view an organization’s employees as its weakest line of defense and easiest point of entry, often much easier than trying to defeat the network.

The human factor is also a distinguishing feature on the attacking side. Most data thefts today are executed by automated botnets infiltrating systems indiscriminately, but APTs are driven by highly directed human intelligence: patient operatives with malicious motives and the specialized planning and IT expertise to pull off their crimes. It’s the perpetrators’ intelligence, creativity and commitment that make APTs so extraordinarily adaptive, unpredictable, hard to identify and effective.

**HOW APTs WORK**

APT’s are unique and attack processes are custom-tailored to the target. The techniques depicted here are similar to those used in Operation Aurora against private sector corporations.



## ATTACKS vs ADVANCED PERSISTENT ATTACKS

APTs are sometimes confused with more simplistic, run-of-the mill ATs or “advanced threats.” This chart summarizes some of the key differences.

	ADVANCED THREATS (ATs)	ADVANCED PERSISTENT THREATS (APTs)
TARGET SELECTION	Opportunistic and random – ATs propagate malware as broadly as possible to improve their chances of landing in a profitable place, such as computers used to log into credit card and bank accounts.	Targeted and specific – APTs are tailored to a specific organization and its known assets, network architecture and vulnerabilities.
MOTIVATION	Financial gain, usually through theft of bank and credit card information, is the primary motive, but the speed and ease with which attacks can be carried out are also important considerations. When countermeasures foil an attack, instead of modifying the attack to pursue the target further, perpetrators stop or move to an easier target.	Objectives for enterprise APT attacks may be financial (i.e., blackmail), but they tend to be far more insidious: to conduct corporate espionage, to steal intellectual property sought by competitors or to gain control over a company’s critical infrastructure to cripple operations.
ATTACK VECTORS	ATs typically use Trojans such as Zeus, SpyEye, Sinowal and Qakbot, alongside zero-day vulnerabilities, unpatched systems and yet-to-be released patches for known software flaws.	Operators combine multiple attack methodologies and tools to reach and compromise their target. These typically include electronic intrusion technologies such as the ones used in ATs, but APTs can also use specially crafted code, as well as conventional intelligence-gathering techniques such as phone taps and physical theft. If one intrusion technique fails to work, attackers will try others.
REMEDICATION	Addressing the threat’s method of execution – usually a single method such as a specific Trojan – can usually disrupt the threat. Virtualization technologies, combined with prompt patch management, stronger authentication and integrated cybercrime intelligence can neutralize many ATs.	Even if infected nodes are detected and remediated, attackers usually have contingency plans and redundant nodes in place that enable them to continue operations.

## APTs in the Enterprise: An Inevitable Escalation

Only 18 months ago, APTs were a problem confined to three-letter government agencies and critical industries. Now, APTs are attacking enterprise assets as well. Operation Aurora proved last year that APTs have compromised private sector organizations, including some of the world’s most technically sophisticated and well-armed companies. *APTs will be the primary attack vector against corporations, particularly as they move IT services to the cloud.*



APTs are inevitable for most large organizations. It's just a matter of time: a question of when, not if. Here's why the conditions are particularly ripe for enterprise exploitation through APTs:

1. **Rising complexity of IT environments** – The complexity of today's IT environments offer attackers more potential points for exploitation and more places to hide. Most large organizations today support heterogeneous IT environments made up of legacy servers, mainframes, virtualized data centers, private clouds and even some public cloud services. These diverse systems create many challenges for IT and security teams, including expanding the threat surface for electronic attacks and increasing the complexity of monitoring and correlating security events across the environment as a whole. In the [2010 Verizon Data Breach Investigations](#) report, 87 percent of organizations experiencing information theft had evidence of the breach in their log files but failed to identify it.

IT complexity is further compounded by the mounting [pressure from corporate IT users to have more flexibility](#) in their applications and devices. Consumer applications such as social networks, chat and other Web 2.0 applications, as well as employee-owned smart phones and tablets, have become new pathways for introducing malware and vulnerabilities into the enterprise.

2. **Ready supply of stolen enterprise access credentials** – *RSA research found that 88 percent of Fortune 500 companies have employees infected with Zeus*, and [RSA Cyber Crime Intelligence](#) reports routinely identify enterprise access credentials in criminal information harvesting points. While these signs don't necessarily point to current APT activity in the private sector, they demonstrate attackers already have the malware tools and access points to compromise enterprise IT environments.



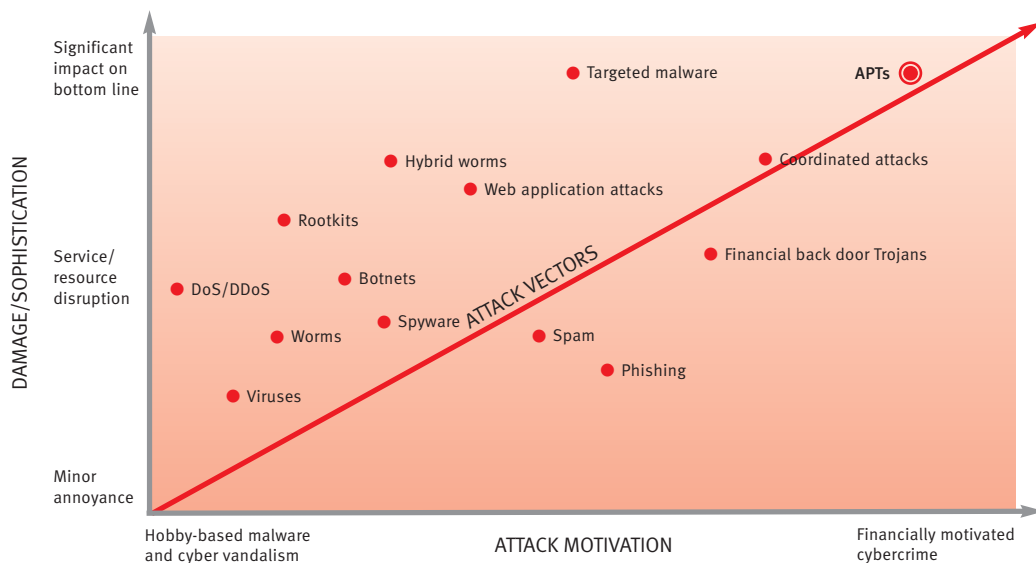
3. **Private sector organizations becoming more lucrative targets** – Striving for higher utilization and greater efficiency, organizations are standardizing on fewer IT platforms. This increases the value and concentration of high-value targets and makes these targets potentially more rewarding and attractive to attack. Focusing criminal R&D resources on identifying exploits in widely used technology platforms can create attack techniques that work against a large number of organizations, increasing criminals' return on investment.

Further increasing the attractiveness of APTs against enterprise targets is the decreased profitability of attacks against financial institutions. Until recently, the interception of financial institution user names and passwords through malware paid off handsomely in criminal markets. Those attack vectors, however, have become too accessible and are getting downright crowded. Today, lazy thieves (or those just pressed for time) can rent full-functioning malware exploit kits for about \$1 per hour. DIY thieves can buy prepackaged software to build Zeus botnets for \$1,000. The rise in the number of suppliers is lowering payouts, forcing ambitious cybercriminals (and the organized crime groups that often fund them) to turn to more lucrative private markets for corporate data. As thieves become increasingly efficient at monetizing corporate data for espionage and blackmail, APTs will likely become a preferred means of stealing enterprise information. Specifically, we expect APTs to consolidate vectors, shorten their time to payoff and become more directed and effective in stealing corporate intellectual property.

4. **Decreasing costs of launching APTs** – APTs have become less expensive to manufacture and host, with many criminal enterprises taking advantage of the cost, performance and scalability benefits of cloud computing. Combined with the aforementioned trend of technology platform consolidation, which has enabled criminal operators to focus their R&D activities more efficiently, the cost of carrying out APTs has declined dramatically, while increasing the potential return on investment for attacks.

Because of their stealth, ambition and complexity, APTs are changing the enterprise threat landscape. RSA and VMware believe organizations cannot prevent APTs, only minimize their damage. APTs will be pervasive threats in computing environments – just as viruses and disease are in the real world – but APTs can be neutralized and, most importantly, risk can be managed to acceptable levels affordably.

Organizations must learn to factor emerging threats such as APTs into their risk assessments and security planning. This will require fundamental and strategic changes in the way organizations prioritize their security activities and identify threats. It will also compel IT and security teams to take a comprehensive, risk-based view of security practices, using business requirements to drive security policies and embed automated controls. Lastly, it challenges security teams to focus on security management, monitoring and response processes that are more granular, dynamic and scalable.



### HOW APTs FIT INTO THE THREAT ENVIRONMENT

While the underlying tactics aren't new, APTs represent a dramatic escalation in potential risk and damage, as well as in the sophistication and capabilities of attackers.

### Countering APTs with Intelligent Security Principles

APT force organizations to evolve beyond traditional security techniques and act more strategically and adaptively. This presents a major challenge for IT and security teams, which have been conditioned to think in silos, such as desktop, server and network, and often design highly manual processes focused on protecting a particular segment with only limited coordination within the broader IT environment. To detect and deflect stealth attacks such as APTs, today's static, compartmentalized, procedural approach to security operations needs to change.

Organizations should adopt five core principles to help their IT and security operations develop the capabilities to counter APTs and other fast-evolving threats.

- 1. Find and focus on the value** – Instead of exhausting organizational resources on never-ending routines of remediation, organizations need to step back and evaluate if they're applying the proper protections to the assets they value most. This is where governance, risk and compliance (GRC) assessments come in. Security management teams can set priorities based on the GRC policies that the enterprise has created. For example, an organization may be continually upgrading perimeter security, but is that where the problem is? Or is the problem actually unauthorized access to sensitive information using stolen credentials, meaning the highest walls in the world won't help?

Security teams need to conduct risk assessments that focus on the "crown jewels" of the enterprise. This may sound simplistic, but it demands extensive situation awareness. It also demands a clear, comprehensive and actionable understanding of how critical information and services are distributed, along with their security posture and operational context. What patterns are considered normal for a particular IT environment and what can IT teams learn from these patterns? Where does the organization's most valuable information live? Who and which systems have access to this information? By knowing these things, organizations can do a better job of protecting their most valuable assets. Organizations can also create planning models that map their IT resources with the information that is most important to safeguard. Such models can help organizations devise highly efficient and effective defensive tactics that neutralize attackers' ability to do damage, even if they manage to penetrate the IT environment.

- 2. Act selectively** – The noise level in today's IT environments is too high: there are too many devices, machines and users to manage; too many events to analyze; and too many patches to distribute and threats to remediate. Security operations teams cannot do it all. They may want to, but the end result is usually they're spread so thin that they're hard pressed to protect what's truly important. Security teams may have to let go of the goal to provide moderate security to everything and focus instead on the goal of securing strategic assets extremely well. Security teams also need to develop a selective tolerance for malware, balancing the risks they pose with the opportunity cost of remediation. Striving for a malware-free environment is a distraction; striving for an environment that's safe for employees and sensitive information is entirely worthwhile.

- 3. Correlate risks comprehensively** – Organizations need a unified view of their IT environment, whether internal or external, non-virtualized or cloud. Only by having an integrated view of their various environments can organizations begin to monitor, analyze and correlate events to detect subtle cues belying APT activity and to determine what damage has been attempted or was done. For instance, by comparing routine data fetch requests with automated software updates (such as antivirus definitions), organizations can detect small changes in the footprint or pattern of outside communications that may indicate APTs are using the channel to contact their remote command-and-control infrastructure.

To aid in event correlation, security monitoring and management software can integrate event logs, patch management status updates and other security information from various IT environments into a central console to give organizations a complete picture of the situation. These centralized analysis and reporting tools eliminate much of the work of finding security needles in the IT haystack. They allow organizations instead to compile a new stack composed only of security needles – a place where threats can be evaluated in the aggregate for small signs of potentially large problems. Achieving this highly granular yet big-picture view of IT environments requires interdisciplinary collaboration between IT and security operations to align efforts across groups and technology platforms.

- 4. Automate extensively** – Organizations must leverage automation and virtualization to streamline systems configuration, management and monitoring to move beyond the constant battle of managing exceptions and anomalies. Only by automating the handling of dependencies and managing updates through master images will organizations achieve the predictability and standardization to simplify security operations.

**5. Behave adaptively** – Security practices built on rigid rules and signatures deal only with known threats and aren't effective against APTs. To deal with the unknown, security operations need to rapidly respond and adapt when events or conditions deviate from established norms. They need embedded, automated intelligence to adapt user verification techniques, switch host machines and even rewire entire virtual networks to disrupt high-risk activities. Finally, security operations must learn from and then adapt their automated, orchestrated and policy-driven actions to continuously improve countermeasures, as well as their efficiency and effectiveness in responding to threats.

These five principles all point to a big change ahead: tomorrow's enterprise security operations centers (SOCs) must become more intelligent:

- More intelligent in **perceiving which strategic assets to protect** and where threats are emerging, both outside and inside the organization
- More intelligent in **analyzing and learning from normal states** to identify deviations, potential problems and threats at their earliest stages
- More intelligent in **determining adaptive responses** to dynamically evolving threats and automating the infrastructure and procedural changes needed to mitigate risks

SOCs meeting the above conditions – Intelligent SOC – will require a steady transition to new security technologies, techniques and procedures, some of which are still under development. Nevertheless, by using these five principles as guide posts, organizations can reorient their security operations to put themselves on the path toward the Intelligent SOC.

## Advanced Security Operations: the First Step toward Intelligent SOC

---

It's a long road from where most organizations are today to the futuristic capabilities required for the Intelligent SOC. Many organizations have begun the journey by evolving their security practices and technologies to an operational model RSA presented last year: the [Advanced Security Operations](#) function. Advanced SOC share several fundamental qualities with the Intelligent SOC of the future.

### Disciplined execution

Security operations teams need to cover the basics quickly, consistently and well. Despite never-ending advancements in malware and IT environments becoming increasingly complex to manage, the best security operations teams have scaled their procedures and processes to handle patch management and other routine processes efficiently. They've also become very fast and agile in adopting best practices such as layering passive intrusion detection/prevention systems, anti-virus, deep packet inspection systems, etc. to create stronger defenses. These fundamental security requirements remain important, but they're not a viable primary defensive strategy for the business.

### Information-centric security

Advanced SOC invest considerable time and energy into identifying which information repositories and assets are most important to protect, and they prioritize their investments and activities accordingly. They've also amassed information on normal activity levels and conditions within their IT environment to use as baseline data in threat assessments. Because the best security teams know what's typical for their environment and they've mapped the people, machines and processes with access to sensitive data, they know where to focus when breaches occur and can respond and remediate much more effectively.

### Integrated compliance monitoring and threat detection

SOCs have fused information from different parts of their IT environment to get a big-picture view of operations and traffic. Many organizations have done this by funneling the analytics of a data loss

prevention system and the log management and correlation activities of a security information and event management (SIEM) solution through a centralized reporting console. Having a single, integrated system to monitor and report on multiple IT environments enables organizations to identify high-risk events more quickly, enabling them to speed up remediation and minimize damage.

### Awareness of cybercriminal activities

Analyzing threats is a core expertise of many security operations teams, but analyzing cybercriminal activity isn't. That's why in the past five years, every major financial organization has established an e-crime team to study the motivation, methods and resources used by attackers, not just their technical capabilities and penetration tools. Now that sophisticated attacks are expanding beyond financial institutions to the corporate sector, the same cybercrime know-how can greatly benefit enterprise security management. Cybercrime intelligence can help organizations stay ahead of attackers rather than simply reacting after they strike.

SOCs increasingly subscribe to external intelligence sources that track communities of cyber criminals (a.k.a. "the Dark Cloud") and report on their behaviors and activities, including on the posting of sensitive corporate data on public sites or Trojan drop zones. Additionally, SOC are forming into communities themselves, pooling information about threats they've encountered and how to combat them so they can benefit from each other's experiences. These types of threat intelligence services help organizations learn from and react to newly discovered threats.

Solutions for Advanced SOC are available today and are being implemented by many organizations. Advanced SOC, however, are just the first step in evolving security operations to fully counter the threat of APTs.

## The Intelligent SOC, a New Model for Security Operations

---

As organizations deploy more cloud services, their threat surface and the log events they'll need to analyze greatly increase. To manage security at the speed and scale of the cloud and to deal with unpredictable, adaptive threats such as APTs, organizations need to build upon the capabilities of advanced SOC and evolve security operations so they conform to the five principles of Intelligent SOC presented earlier.

RSA has developed a demonstration of cutting-edge capabilities for Intelligent SOC that effectively mitigates the impact of known APTs in lab studies and trials. The demonstration, which combines experimental technologies and theoretical approaches with commercial products and best practices, counteracts adaptive threats such as APTs at the scale and speed of the cloud.

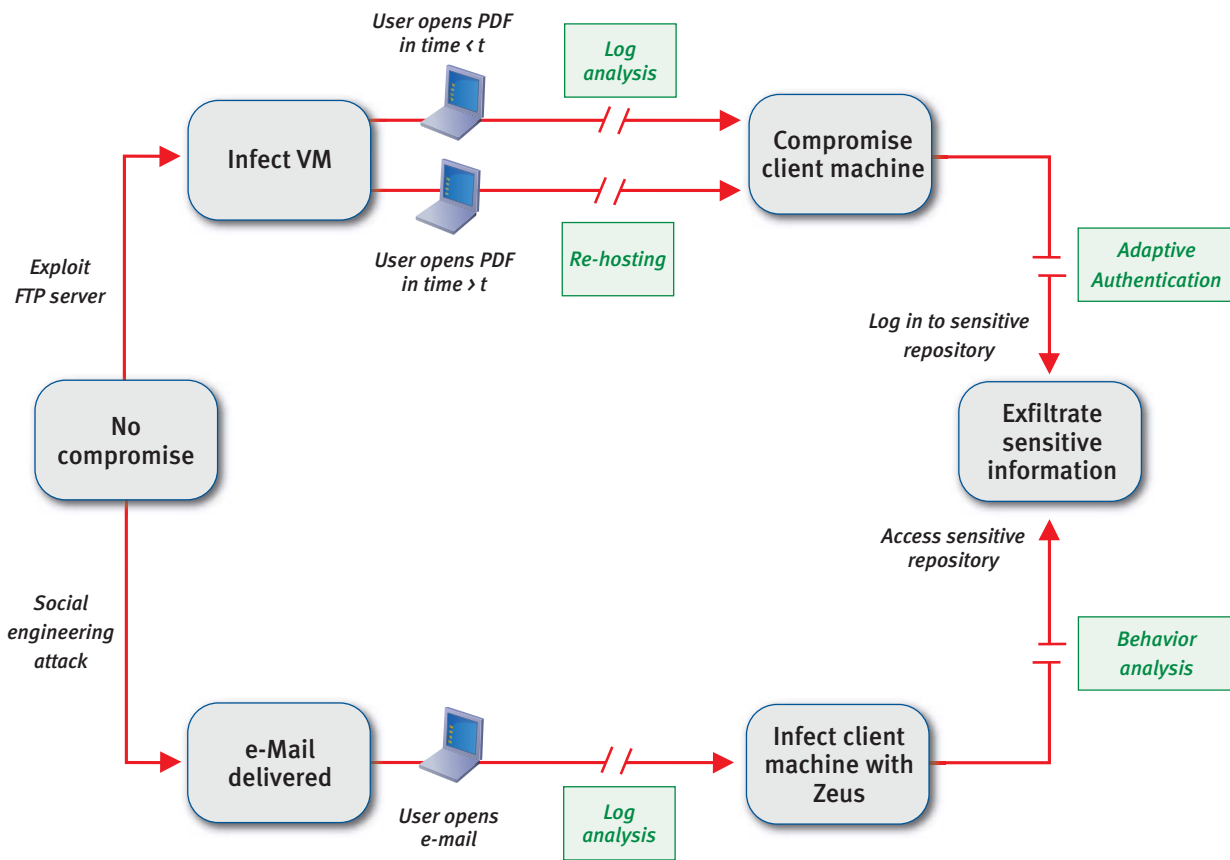
Following are the core elements of the Intelligent SOC model, as well as prescriptive guidance on how to begin incorporating some of these elements into security operations today.

### 1. Risk planning

The Intelligent SOC takes an information-centric approach to security risk planning and invests in understanding which organizational assets are highly valuable and essential to protect. For a technology company, this could be the source code and designs of its products. Critical assets, however, aren't necessarily tied to intellectual property or commercial value. For example, critical assets at a utility company could be the software controlling reactor cooling systems at nuclear power plants. The need for business-driven risk planning has been discussed at length in previous sections of this security brief (see information-centric security and items 1 and 2 in intelligent security principles), but it's sufficiently important to highlight again as the first and foremost requirement for building a focused, effective security operations program. In short, the depth of an organization's up-front knowledge determines how fast and how well it can react in the event of a problem.

## 2. Attack modeling

Determine which systems, people and processes have access to valuable, protected information, and model the normal traffic patterns and potential attack vectors for this information. After modeling the threat surface, determine potential attack vectors and examine defensive steps that the organization could take to isolate compromised access points efficiently and quickly. Such steps could include implementing adaptive authentication or reprovisioning virtual servers and desktops based on a trusted master image. RSA Laboratories® has developed theoretical models to help organizations devise optimal defenses for known APT techniques. Employing game theory principles, lab researchers can identify the most efficient means of severing an attack path and optimizing defense costs. These threat models can also be used to help identify which parts of an IT environment need to be strengthened, either through additional security precautions or complementary tools.



### MODEL FOR COUNTERING “TYPICAL” APTs EXPLOITING MULTIPLE ATTACK VECTORS

RSA Laboratories and MIT professor [Ron Rivest](#) have developed graph-based models to predict APT attack vectors and plan efficient countermeasures that have minimal impact on the enterprise. These models can help in security systems design and in organizational threat planning. This particular model depicts avenues of attack (red arrows) and remediation (line cuts/green boxed text) for APTs exploiting compromises in an FTP server alongside a social engineering attack using malware.

### 3. Virtualized environments

With appropriate planning, visibility and analytic support, security in all-virtualized IT environments can be far stronger than in conventional IT environments because of the encapsulation controls, introspection capabilities and potential agility inherent in the virtualization platform. Virtualization will be a core capability of the Intelligent SOC and will deliver a variety of security benefits. Here are a few examples, with additional ones presented in subsequent sections on automation and forensic analyses:

- Desktop virtualization, which organizations are deploying widely, offers many security operations benefits, most notably improving both the speed and consistency of deploying software updates while reducing both operating and support costs.
- Organizations may “sandbox” e-mails, attachments and URLs suspected of harboring malware. For example, an e-mail containing a suspicious PDF could be launched in an isolated hypervisor and VM cut off from the rest of the system. The VM would open the PDF within this self-contained environment and, if the PDF tried to write files to the system, the VM would be deprovisioned and the original e-mail destroyed. Conversely, if no malicious activity was detected after launching the PDF, the system would authorize the delivery of the e-mail through normal channels.
- Virtualization can partition workloads or even whole zones of IT resources at the data, computing and network levels, creating new opportunities to isolate high-value IT-based assets from those requiring less security. An example might be to align traffic boundaries defined by VLANs, virtual firewalls, and IPv6 link local address resolution in a way that a flaw, compromise or misconfiguration of one isolation mechanism is “backstopped” by co-aligned mechanisms. In this way, SOCs can provide “isolation in depth” for their most sensitive information and virtual nodes.

### 4. Self-learning, predictive analytics

Intelligent SOCs will take integrated compliance monitoring and risk management to a whole new level. The system will continually monitor the environment to learn typical states, which can then be applied to identify problematic patterns early. Configuration data will be combined with SIEM logs, contextual information and risk profiles to connect seemingly unrelated events to detect high-risk activities instantaneously. Statistics-based predictive modeling will help to correlate various alerts. Integrated feedback loops will use SOC operators’ confirmed alerts to help the system improve its threat detection capabilities. Developing this intelligent, heuristic system will require innovations in real-time behavior analysis, but some of the elements (i.e., SIEM, DLP and security management dashboards) are already available as integrated solutions to speed deployment.

### 5. Automated, risk-based decision systems

The crowning achievement of Intelligent SOCs may be their ability to assess risks almost instantly and vary responses accordingly. Today’s risk-based authentication services give organizations a glimpse into how self-adapting systems could work at a much broader level in the future. Risk-based authentication services detect unusual log-in conditions, such as a user attempting to tunnel in from an IP address in Russia within hours of logging in from a PC at corporate headquarters in Ohio. When authentication systems detect suspicious conditions, they automatically take secondary steps to verify the user’s identity by posing additional challenge questions that only the genuine user would know (e.g., “What make and model car did you drive in 2005?”) or by prompting the user for a one-time password delivered via text message. In a similar way, Intelligent SOCs will employ predictive analytics to spot high-risk events and then initiate investigation, planning, mitigation and, finally, remediation activities more proactively. Moreover, intelligent automation will simplify the job of IT professionals in SOCs by handling mundane remediation tasks without human intervention and by orchestrating system changes without breaking dependencies.

One of the most exciting things to emerge from systems automation in the cloud is the prospect of dynamic topography. To implement an APT, attackers must first be able to map and model the network. In other words, attackers need to know what IT resources are monitored, where the information they're seeking resides and which applications can access it. This type of environmental reconnaissance enables attackers to find multiple routes to the information they need, as well as identify zero-day vulnerabilities that can then be used to propagate malware to other parts of the organization's IT systems.

In virtualized environments, organizations can remap their entire network infrastructure to disrupt attackers' reconnaissance efforts – not just by employing dynamic IP addresses, but also by changing the MAC addresses of the virtual mix. This is akin to physically rearranging a city at frequent intervals – and the entire process can be automated so that links between systems stay intact and dependencies are handled without human intervention. Changing the topography of the network forces attackers to increase their reconnaissance activity, which not only raises the risk of detection, but it also greatly increases the time and cost of activating and propagating an exploit.

#### 6. Continual improvement through forensic analyses and community learning

Forensic analyses of APTs can be resource-intensive in terms of manpower, computing power and analysis expertise, but they must be done to mitigate the impact of subsequent attacks. Virtualized systems equipped with SIEM tools can take snapshots of the IT environment at the time of a security event, which can be very useful in analyzing how attacks occurred if detection is delayed.

In analyzing APTs in virtualized systems, consider not blocking the APT's attack vectors and reprovisioning infected systems right away. Instead, execute the infected VMs within a sandbox environment that duplicates the actual environment but is completely isolated from it. The security operation teams can examine the sandbox environment and learn from the APT's activities. What nodes is it talking to? What data is it trying to access? What ports is the APT using to communicate outside? Where do the outsiders appear to be located? Knowing this information makes it far more likely that organizations can eradicate the APT throughout their environments, and not just in the node in which the APT was first identified.

Finally, because APTs pose such a high risk, organizations will likely want to share information about attack patterns – on a sanitized basis, of course – with clearinghouses for threat information. Information would be collected centrally and shared among partnering organizations to analyze and help defend against similar security threats. For example, the financial services industry has already established very active, collaborative networks for sharing threat information about data breaches and fraudulent activities. In a similar way, Intelligent SOCs of the future will exchange threat information within their respective industries to predict the path of APTs and to determine effective countermeasures.

The Intelligent SOC is simply a concept today, but *RSA expects the Intelligent SOC to become the operative norm for security in most Fortune 500 companies by 2015*. The rapid migration to Intelligent SOCs will be driven in small part by their ability to neutralize APTs. For the most part, however, Intelligent SOCs will be driven by the cloud.



As organizations deploy a broader variety of cloud services, IT environments will grow in complexity. Traditional SOC models with their reactive, manual processes cannot scale efficiently, much less manage change at cloud speed. The dynamic, automated and adaptive qualities of the Intelligent SOC, however, will enable this innovative model to deliver enterprise security at the speed and scale of the cloud.

## Summary and Conclusions

---

Today's security operations are highly vulnerable to targeted, adaptable security threats such as those posed by APTs. For most large organizations, the question is not if they'll be attacked by APTs but when – and how they'll deal with it.

APTs require security operations teams to shift their focus from identifying security threats in several different IT environments (i.e., looking for needles in haystacks) to analyzing security events in a big-picture way (i.e., looking at stacks of needles). Only by finding correlations in seemingly unrelated security events can organizations hope to detect APTs in a timely way.

Today, organizations can take three steps to help them deal with APTs:

1. Engage in thorough and rigorous governance, risk and compliance (GRC) assessments to produce predictable, scalable environments and prioritize which information and strategic assets are most important for the organization to protect. Such assessments are absolutely essential in designing and implementing defensive strategies and in reacting quickly in the event of a security breach.
2. Model IT resources and vectors of attacks to determine optimal strategies for protecting the organization's GRC priorities. Such models are also instrumental in helping organizations identify which parts of their IT environment need reinforcement through additional security procedures and/or technology investments.
3. Focus on developing capabilities that enable the analysis of security information in real time and the automatic adaptation of IT-based defenses. Automation will be essential in minimizing reaction times to attacks: the faster organizations can adapt and stay ahead of the attack, the less time the APT has to cause damage.

Technology solutions are available today to help organizations integrate, monitor and analyze security events from across various IT environments – conventional and cloud – from within a central console. Virtualization platforms can help defend against APTs by enabling faster, more consistent patching of known vulnerabilities. In the future, virtualization will also vastly improve organizations' abilities to neutralize APTs by encapsulating threats in disposable VMs and by automating the reprovisioning of entire virtual networks, which will make IT environments harder for attackers to navigate.

RSA and VMware expect most of these emerging capabilities and GRC-driven planning programs to become core components of the Intelligent SOC, a concept for how most Fortune 500 companies will conduct security operations by 2015. The rapid migration to Intelligent SOCs will be driven in part by their ability to neutralize APTs. For the most part, however, RSA and VMware expect organizations to embrace the concept of the Intelligent SOC, because it will enable them to deliver strong security at the speed and scale of the cloud.

## About the Authors

---

### **Sam Curry, CTO, Marketing, RSA**

Sam Curry is the Chief Technology Officer for the go-to-market arm of RSA. Mr. Curry has more than 18 years of experience in security product management, marketing, product development, quality assurance, support, sales and marketing. Mr. Curry has also been a cryptographer, researcher and writer. Prior to his current role, he was Vice President of Product Management for two years, where he led and set the strategic direction for all aspects of product management for RSA's solutions.

### **Bret Hartman, Chief Technology Officer, RSA, EMC Fellow**

Bret Hartman is responsible for defining the corporate security technology strategy for EMC, as implemented by the RSA division. Prior to RSA, Mr. Hartman was Chief Technology Officer, Information Security, at EMC Corporation.

Mr. Hartman has more than 25 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. Mr. Hartman has spoken at dozens of security and privacy industry events and is a recognized authority on distributed systems security.

Prior to EMC, Mr. Hartman was Director of Technical Services for SOA Appliances at IBM Corporation and was also Vice President of Technology Solutions at DataPower Technology, which was acquired by IBM. Mr. Hartman's previous roles include Chief Technology Officer at Quadris Security (Hitachi Computer Products); Vice President, e-Security Services and Chief Security Architect at Concept Five Technology; President and Co-Founder of BlackWatch Technology Inc; and Director of Information Security at Odyssey Research Associates. Mr. Hartman began his distinguished career as a U.S. Air Force officer assigned to the U.S. National Security Agency.

At the U.S. National Security Agency, Mr. Hartman helped to create the "DoD Trusted Computer System Evaluation Criteria" (Orange Book). He was a co-author of Object Management Group's CORBA Security specification, and co-edited the Security Scenarios document produced by the WS-I Basic Security Profile Working Group. Mr. Hartman also co-authored Mastering Web Services Security (Wiley 2003), Enterprise Security with EJB and CORBA (Wiley 2001), and U.S. patent 6,807,636: "Methods and Apparatus for Facilitating Security in a Network."

### **David P. Hunter, Chief Technology Officer, World Wide Public Sector, VMware, Inc.**

David Hunter serves as the senior technical liaison between VMware and the public sector community, evangelizing the value of virtualization and cloud computing to improving the business of government and education. Mr. Hunter also leads VMware's Platform Security Engineering Initiative overseeing various internal initiatives focused on ensuring secure development practices across the company. He has over 25 years of industry and government experience having held senior engineering leadership and management positions at Digital Equipment Corporation, Compaq Computer Corporation and the United States Navy. Mr. Hunter is the co-inventor on several U.S. patents and has served three years as a member of the Secretary of the Navy's Reserve Force Policy Board. He holds a B.S. in Electrical & Computer Engineering from Northeastern University and is a graduate of both the United States Naval War College and Joint Forces Staff Officer College. He is a former technical editor of Home Business Magazine and a current member of the Industrial Advisory Board for the College of Electrical & Computer Engineering at Northeastern University, as well as a member of National University's Cyber Security and Information Assurance Advisory Council.

### **David Martin, Chief Security Officer, EMC Corp.**

Dave Martin manages EMC's efforts to protect \$30 billion in assets and \$17 billion in revenue. As EMC's most senior security executive, he is responsible for establishing EMC's brand of trust with its customers and for providing business protection operations worldwide through the management of EMC's industry-leading, converged Global Security Organization. Mr. Martin is a Certified Information Systems Security Professional and brings a range of experience to EMC in information security and management that he developed through more than a decade of professional business protection experience from various roles in internal audit, security

services development and consulting. Prior to joining EMC, Mr. Martin built and led security consulting organizations, focusing on critical infrastructure, technology, banking and healthcare verticals, where he developed and delivered enterprise security programs, incident response, investigations, policy and assessment practices. He holds a BEng in manufacturing systems engineering and provides frequent testimony to the U.S. Congress and government agencies as an expert witness on corporate enterprise protection issues.

**Dennis R. Moreau, Ph.D., Senior Technology Strategist, RSA**

Dennis Moreau specializes in the application of leading-edge technologies to the solution of complex problems in information systems management and security domains. His primary focus is in developing solutions to improve IT efficiency and effectiveness for service, systems, security, compliance and configuration management/optimization. He works actively with the National Institute of Standards and Technology (NIST), the U.S. Department of Defense (DoD) and the Mitre Corporation on the development of security information standards. Dr. Moreau has more than 35 years of experience in designing systems and security management solutions. Prior to joining RSA, he was a founder and the CTO for Configuresoft and CTO for Baylor College of Medicine. He holds a doctorate in computer science and has held faculty positions in computational medicine and computer science, conducting research programs under the sponsorship of the National Aeronautics and Space Administration, Jet Propulsion Laboratories, the National Institutes of Health, the National Library of Medicine, Bell Laboratories and IBM. He speaks regularly at IT management and security conferences worldwide.

**Alina Oprea, Ph.D., Principal Research Scientist, RSA Laboratories**

Alina Oprea is a principal research scientist at RSA Laboratories, where she works on developing cutting-edge security research technologies that influence the company's strategy, as well as the larger research community. Her research interests span multiple areas in computer security, but recently she has focused on cloud and storage security. Dr. Oprea holds a Ph.D. in computer science from Carnegie Mellon University and joined RSA Laboratories in 2007.

**Uri Rivner, Head of New Technologies, Consumer Identity Protection, RSA**

Uri Rivner is responsible for moving new cybercrime fighting technologies and innovations from concept to reality. He was a key player in the development of risk-based authentication, the RSA eFraudNetwork and other anti-cybercrime technologies now used by thousands of organizations worldwide. Mr. Rivner joined RSA in December 2005 through the acquisition of the anti-fraud company Cyota, where he gained a deep perspective on international fraud. Uri has been fighting cybercrime for ten years and works closely with major corporations on developing long-term strategies against cybercrime. He is a regular speaker on global trends in cybercrime and writes a blog on Finextra.com and RSA's [Speaking of Security](#).

**Dana Elizabeth Wolf, Senior Manager, New Business Development, RSA**

Dana Wolf is responsible for creating and developing new security technologies and business opportunities for RSA from the Office of the CTO. She also manages CTO operations and RSA's advanced development engineering team. Ms. Wolf joined RSA in 2004 as a principal software architect and served two years as an Entrepreneur in Residence at RSA for her graduate school work on payment card security.

## Solutions for Advanced SOCs

---

### Solutions from RSA

- The RSA® Archer™ eGRC Platform is designed to serve as the foundation of an advanced security operations function by providing a repository of threat and incident data and a centralized, automated incident handling process. The Platform is engineered to pull risk and security-related information from third-party systems, such as the RSA enVision® platform, the RSA® Data Loss Prevention Suite and RSA FraudAction™ service, to create meaningful, real-time intelligence across the enterprise. The ability to integrate intelligence on security alerts and threats, to gather and present metrics about the effectiveness of security controls and security management processes, and to analyze contextual information about the security and business environment helps enable organizations to more successfully assess business impact.
- The RSA enVision® platform is engineered to provide an integrated security information and event management (SIEM) and log management solution that collects, correlates and retains complete log records from every system that generates logs. RSA enVision technology is designed to produce real-time alerts of high-risk events and offers visibility into the behavioral aspects of users to assist in remediation.
- The RSA® Data Loss Prevention (DLP) Suite is built to alert organizations of sensitive data activity that is suspicious or violates organizational policy. DLP also executes first-line remediation functions, such as blocking the transmission of sensitive data, or quarantining, deleting, moving or applying rights management to documents that contain private data.
- RSA FraudAction™ service is engineered to provide a proven service geared toward stopping and preventing phishing, pharming and Trojan attacks that occur in the online channel. This service is designed to offer a comprehensive view of the current and emerging threat environment by identifying employees, machines or other internal resources that may be under attack or compromised. RSA FraudAction service helps enable organizations to minimize resource investment while deploying a solution quickly, including 24x7 monitoring and detection, real-time alerts and reporting, forensics and countermeasures, and site blocking and shutdown.
- Services from EMC Consulting leverage the security expertise and industry leadership of RSA to accelerate and optimize security strategies and risk postures, while transforming security to a business enabler. These capabilities range from strategies and architectures appropriate to the client's Security Operations and Incident Response objectives, through the roadmap, business and operational procedures and workflows, deployment, and lifecycle optimization of an advanced security operations function.

### Solutions from VMware, Inc.

- VMware vShield™ App protects applications in the virtual datacenter from network-based threats. It gives organizations deep visibility into network communications between virtual machines and enables granular policy enforcement with security groups. The solution also eliminates the hardware and policy sprawl associated with traditional measures, resulting in a cost-effective solution that helps customers to go beyond the limitations of physical security. The key benefits of the solution are it increases visibility and control over network communications between virtual machines. Next, it eliminates the need for dedicated hardware and VLANs to separate security groups from one another. Finally, it optimizes hardware resource utilization while maintaining strong security.
- VMware vShield™ Edge provides comprehensive perimeter network security for virtual datacenters. vShield Edge integrates seamlessly with VMware vSphere™ and includes essential network gateway services like firewall, VPN and load balancing that organizations can use to quickly and securely scale their cloud infrastructure. The key benefits of the solution are it reduces cost and complexity by eliminating multiple special-purpose appliances and rapidly provisioning network gateway services. In addition, it increase scalability, performance and simplifies IT compliance with detailed logging.
- VMware vShield™ Endpoint strengthens security for virtual machines and their hosts while improving performance by orders of magnitude for endpoint protection. vShield Endpoint enables offloading of antivirus and anti-malware processing to dedicated, security-hardened virtual machines delivered by VMware partners. The solution is designed to leverage existing investments and allows customers to manage antivirus and antimalware policies for virtualized environments

with the same management interfaces. The key benefits of the product are it streamlines and accelerates antivirus and antimalware deployment. Next, it improves virtual machine performance and eliminates antivirus and anti-malware bottlenecks. Finally, it reduces risk by eliminating agents susceptible to attacks.

- VMware cloud infrastructure and management solutions are the foundation for a new, evolutionary IT model based on virtualization that unifies private and public cloud resources with consistent security, compliance, management and quality of service. Built on VMware vSphere, these solutions leverage existing investments to help evolve an enterprise IT infrastructure into one that can anticipate and respond to changing IT and business needs. By leveraging a common management and security model across private clouds and vCloud™ public cloud services, these solutions make enterprise hybrid cloud computing a reliable, secure reality and create a cost effective platform to deploy cloud-ready applications and services.
- VMware cloud application platform solutions enable developers to rapidly build and run modern cloud applications while deploying on-premise or off for maximum flexibility. Using these solutions, organizations deliver applications that intelligently leverage underlying infrastructure for the highest application performance, quality of service and resource utilization.
- VMware end-user computing solutions create a modern, user-centric approach to personal computing that delivers secure access to applications and data from any device, where and when a user needs it. These solutions leverage virtualization to modernize the desktop so that it can be managed independently in the cloud. Users get secure access to their applications, data and services, from any computing device, including PCs, Macs, thin clients and mobile devices. IT gets flexibility, cost efficiency and control. VMware empowers the workforce and enables freedom of choice for end users, while making it easier for IT to maintain control and securely manage users and data.

EMC, RSA, enVision, Archer, FraudAction and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.  
©2011 EMC Corporation. All rights reserved.

APT BRF 0211

