virtualization

Ensuring compliance on the journey to the secure private cloud

Transitioning a physical IT environment to a virtual one is a journey—a long one for many companies, because such a journey is generally done in stages and can have different destinations. For example, some companies simply want the cost savings of virtualizing their data centers without really changing the way IT services are delivered to the organization, whereas others are on their way to the ultimate destination: the private cloud. As with life, however, the journey itself is what is most important. And making it a secure and compliant one is essential.

"Many enterprises have moved ahead with virtualization quickly in order to take advantage of the flexibility and cost savings it provides, letting security considerations lag behind as the complexity, maturity, and risk and compliance profile of the virtual environment grows," says Robert Griffin, director of security architecture at RSA, The Security Division of EMC. "But an effective security strategy enables more rapid progress along the journey, serving as a map that organizations can use to guide their efforts."

The typical journey to the private cloud occurs in three stages, and as mentioned above, some companies will be comfortable stopping or at least spending time at any of these stages:

1. **IT PRODUCTION STAGE**—In search of lower costs, IT production systems are identified as primary targets of virtualization. Security issues include visibility into the virtualization infrastructure, privileged user monitoring, access management, and network security.
2. **BUSINESS PRODUCTION STAGE**—To improve quality of service, organizations virtualize their business-critical applications. Security issues include compliance, information-centric security, risk-driven policies, and alignment between IT and security operations.
3. **PRIVATE CLOUD**—To improve agility and responsiveness, organizations approach near-total virtualization as most IT services are delivered via a secure private or hybrid cloud. Security issues include secure multitenancy arrangements and establishing a chain of trust.

According to Griffin, most organizations today are somewhere between the first and second stages. But regardless of where they start and where they finish, organizations need to take a holistic view of their risk and compliance profile and plan their efforts in light of their desired end state and a sober assessment of their current vulnerabilities.

GETTING A HANDLE ON THE HYPEREXTENDED ENTERPRISE

In "Managing Risk on the Journey to Virtualization and the Cloud," a report issued by Enterprise Management Associates (EMA) in August 2010, the authors note that "the journey of IT from the physical to the virtual, and from there to internal as well as external approaches to cloud computing and IT-as-a-service is, in many ways, no different from other new advances in technology. Many organizations find success in building maturity at each stage of the journey, leveraging the tools and applying the lessons learned at each phase in order to build further maturity going forward."

The key is that each stage should be a secure and compliant one; even

"If you wait until the end of the journey to audit yourself, you probably won't like what you find. Like a gymnast, you want to be sure your footing is firm before you make your next move."

ROBERT GRIFFIN, DIRECTOR OF SECURITY ARCHITECTURE, RSA, THE SECURITY DIVISION OF EMC

Photograph by Webb Chappell

if the organization is planning to transition to a later stage, you don't ever want to operate in a vulnerable state. "If you wait until the end of the journey to audit yourself, you probably won't like what you find," Griffin says. "Like a gymnast, you want to be sure your footing is firm before you make your next move.

"Typically, we suggest that enterprises begin by taking stock of their people, processes, and technologies," he continues. "But in today's hyperextended enterprise that is more challenging to do, and with the rapid growth of the regulatory environment, organizations have to look farther afield than they have in the past."

When Griffin speaks of a hyperextended enterprise, he means the disappearing—or at least radically redefined—boundaries of today's business entities. Rather than being a self-contained organization, the hyperextended enterprise comprises an intricate, far-reaching web of business relationships. Through technologies such as cloud computing, virtualization, social networking, mobile devices, and VoIP services, critical information is exchanged with more constituencies in more ways and more places than ever before. This makes fertile soil for unpredictable and new sources of risk.

Even the category of "user" today encompasses not just employees in various offices and geographies, but business partners, contractors, consultants, outsourcers, and suppliers—all of whom must be counted upon to operate in a way that does not introduce unnecessary risk to the enterprise. Which essentially means that anyone with access to an organization's information—whether a third-party cloud provider or a remote product development team—has to comply with every regulation that affects onsite, full-time employees.

But with ever-increasing regulatory requirements, more serious penalties for noncompliance, and more assertive (and global) regulators, assurances that a partner or provider is doing the right thing is simply not enough. Organizations need proof. In fact, compliance today requires not only the act of adhering to regulations but also to the ability to demonstrate and sustain adherence. For this reason, it's absolutely essential for organizations to be able to verify for themselves that third-party and cloud infrastructures are secure. And that requires a broad-based approach. (See sidebar, "All Comers, All Corners.")

INSTILLING TRUST, ENSURING COMPLIANCE

Unfortunately, managing compliance becomes increasingly difficult as much of the world moves toward principle-based regulation, which focuses on outcomes rather than checklists of requirements. Organizations are not told *how* to comply but rather *what* they have to achieve—which includes the ability to clearly document their compliance program and provide evidence of its effectiveness.

According to "A New Era of Compliance," the fall 2010 report of RSA's Security for Business Innovation Council (SBIC), a group composed of security executives from Global 1000 enterprises in a variety of industries, this trend is forcing enterprises to evolve their compliance programs from tactical point solutions to the level of strategic business initiatives. (See News and Notes, Page 4) Vishal Salvi, chief information security officer and senior vice president of HDFC Bank Limited, is quoted in the report as saying, "Security practitioners must link the compliance program to the strategy of the organization. Doing compliance for compliance sake is just using up your resources. Ensure that whatever you're doing for compliance actually derives value for your organization and is not just something

ENABLING THE CYCLE OF SECURITY COMPLIANCE

The cycle of security compliance comprises policy management and implementation, security and compliance measurement, issue remediation, and reporting, all within a single management system that encompasses both the physical and the virtual infrastructures. It is an incremental, four-stage process, where organizations look at policies, identify discrepancies and redundancies, and ensure they have the controls in place to present and respond to security incidents throughout the enterprise.

Such controls include many of the security capabilities and processes familiar from the older, physical world, such as identity management, data loss prevention, data encryption, and event collection across the environment. These existing controls, extended across the physical and virtual environments, should be complemented by controls unique to the virtual environment, such as virtual firewalls and invocation of security capabilities directly from interfaces in the virtual infrastructure itself.

It is by necessity a labor-intensive process unforgiving of human error, which is why an automated system is recommended.

STAGE 1: DISCOVERY. Inventory existing policies and controls, define new policies and controls based on—and mapping to—relevant regulations and standards.

STAGE 2: ASSESSMENT. Test whether policies and controls in fact address compliance requirements, and whether they are distributed, known, and being adhered to throughout the enterprise.

STAGE 3: REMEDIATION. When noncompliant controls are found, they must be fixed. Where there are gaps, they must be filled.

STAGE 4: MANAGEMENT. The system ideally collects, analyzes, and feeds information about security incidents that affect compliance in real-time, allowing appropriate action to be taken quickly.

The process enables organizations—and particularly their beleaguered IT departments—to rationalize a multitude of compliance requirements, control frameworks, standards, and best practices into a set of centralized security policies that can be administered consistently across both the physical and virtual infrastructure. Automation helps, but it's not plug and play; it requires strategic vision and oversight and a commitment to a process that will take time to fully implement but that will pay off with robust compliance and risk management capabilities.

ALL COMERS, ALL CORNERS

Regulations are often described as "sweeping." Compliance efforts must be sweeping as well, encompassing internal policies and external laws, physical and virtual environments, and employee and third-party users. Piecemeal, reactive efforts consume resources, create redundancies, and cause unnecessary risk. That's why a systematic, proactive approach—though a large effort—is ultimately a wiser course of action.

For the most part, regulations do not distinguish between a physical and a virtual IT infrastructure, although some, such as the Payment Card Industry Data Security Standard (PCI DSS), are being revised to include guidelines specifically for virtualized systems. This is not a bad thing, as most physical controls can easily be ported over to the virtual environment. But it does send a signal that regardless of what kind of IT infrastructure an organization has—and most if not all organizations will likely be running some manner of hybrid environment for the foreseeable future—that infrastructure is subject to scrutiny and must be secured.

Griffin recommends that organizations look beyond their borders to other sources of information about actual or potential threats. For example, the RSA® eFraudNetwork™ monitors and tracks fraudster profiles, patterns, and behavior across 150 countries. When an active fraud pattern is identified or suspected, the fraud data, transaction profile and device fingerprints are moved to a shared data repository. The information within the eFraudNetwork is continually updated and frequent contributions on fraud intelligence are provided by analysts at RSA's Anti-Fraud Command Center.

Additionally, organizations may want to try having confidential conversations with value chain partners and third-party cloud providers about what they're seeing and experiencing. "Third parties may be reticent to expose their own vulnerabilities, especially to customers and partners, but if it's a reciprocal arrangement, everyone could benefit," says Griffin. "After all, every organization is going through the same thing and it would be better if there were more open communications around these issues."

which pleases a regulator."

In other words, just as any virtualization effort should be a strategic undertaking, so should security, which means that corporate governance has to have a holistic, real-time view of how sensitive information is being protected, used, moved, and accessed throughout the enterprise. This is the realm of governance, risk, and compliance (GRC), which increasingly is a critical aspect of the journey to the secure private cloud.

Not surprisingly, according to Griffin, the top three customer trust-related concerns he hears about are compliance, governance, and risk management. The challenge is to ensure that safety is designed and built into the cloud in advance, and the way to do that is to ensure that each stage of the journey is taken with security and compliance in mind. With the right implementation, private clouds can be even more secure than most physical IT environments.

As the EMA report notes, "A unified platform for managing risk and compliance efforts can improve efficiencies by extending proven principles to these new environments, and centralizing visibility into risk management and control that assures greater consistency in a comprehensive, systematic approach."

According to Griffin, such a platform must encompass a "cycle of security compliance" (see sidebar, "Enabling the Cycle of Security Compliance") that enables organizations to secure the complex virtual environment across the entire hyperextended enterprise. Essentially, the cycle of compliance is a four-stage process, involving the discovery, testing, and strengthening of existing controls—as well as closing gaps by building in new controls that address the complete regulatory requirements the organization faces—and then managing and reporting on security incidents that compromise compliance. The cycle helps to build trust, reduce risk, and enforce adherence.

MANAGING COMPLIANCE BY PRIORITIZING RISK

Such a system also helps to address a significant finding in the EMA report, which states: "One of the key points to remember in this journey is that not only a phased but a *systematic* approach often yields the best results. In EMA research into the realities of enterprise governance, risk management and compliance, the highest performers are those who are thorough in achieving *all* milestones of defining objectives, actually implementing them, monitoring the environment for expected performance as well as for deviations and events warranting follow-up, and responding to events and changes in the risk landscape."

An organization can only respond to and remediate so many situations at once, so the process has to provide the visibility needed to be able to prioritize risks and actions based on accurate and timely data. A compromised server within IT that has no mission-critical applications or information on it is something that requires attention. But if there is a more serious situation going on at the same time in Finance that may result in Sarbanes-Oxley noncompliance, that obviously must be the highest priority. Unless organizations have a way to surface that information throughout the enterprise, they will inevitably respond to the latest incident but not necessarily the most significant incident, wasting time and resources while at the same time leaving the enterprise vulnerable to bigger problems down the line.

According to Griffin, "The journey to the secure private cloud encompasses an unusually broad range of issues and technologies. Organizations have to understand that the scope of this effort has to go beyond the traditional boundaries of the enterprise and reach into the realms of third-party cloud service providers and other individuals and institutions with access to their information."

Ultimately, though other parties may have access to your digital assets, you own them and are liable for anything that goes wrong. The best way to protect them—whether on a physical server or in a private cloud—is to start from the bottom and the inside—with good policies and controls based on relevant regulations—and work up and out through the physical and virtual infrastructures and all internal and external endpoints. ▦