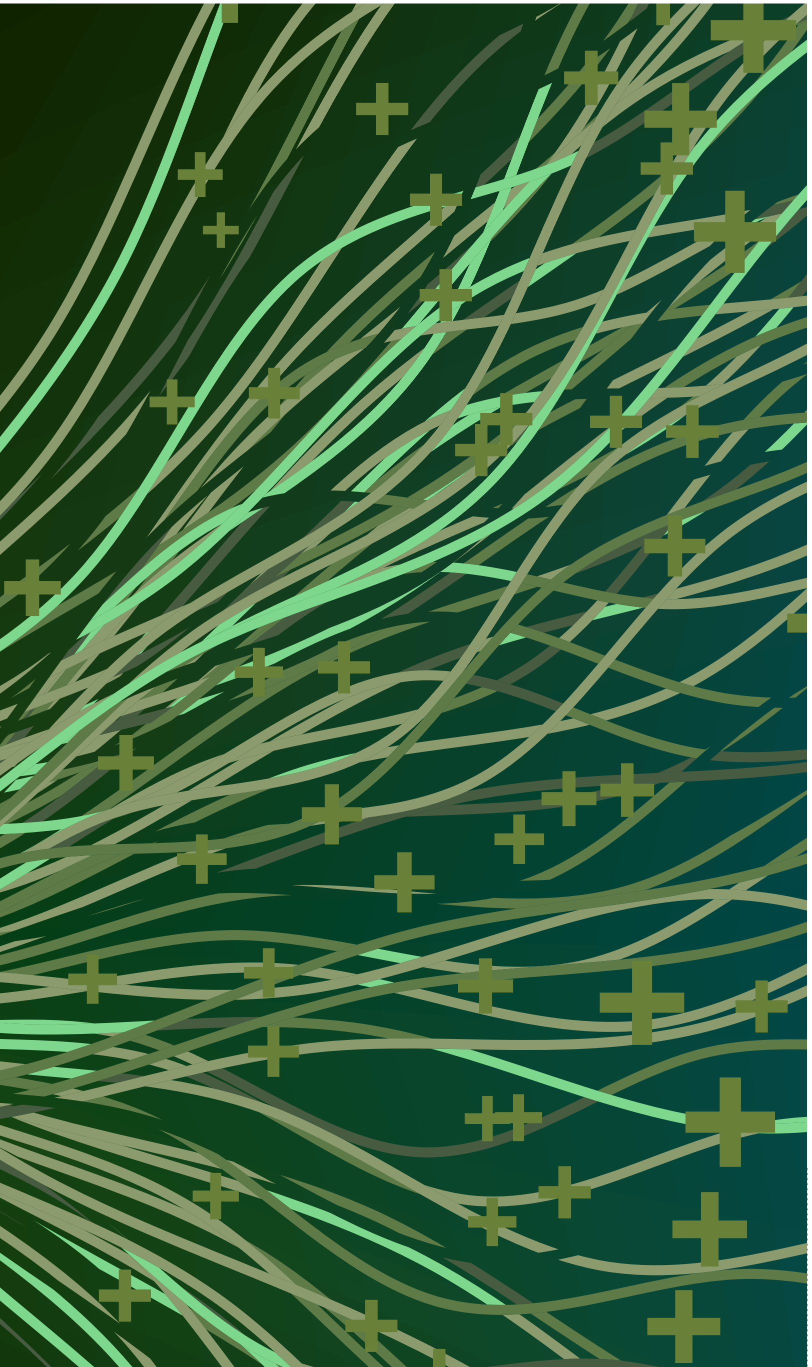
SearchSecurity



E-Guide

CONVERTING TO THE CLOUD AND TACKLING THE CHALLENGES WITHIN

TechTarget

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

IN THIS EXPERT E-Guide, discover how to convert your company to the cloud. Security experts will take you through the positives and negatives of investing in the cloud and bring to light the compliance challenges that may arise when doing so.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

CONVERTING TO CLOUD: RANUM Q&A WITH LEE HEATH

Marcus J. Ranum, Contributor

Is Marcus Ranum changing his views on cloud computing? The Information Security magazine columnist chats with Lee Heath, a 20-year veteran of vulnerability management and compliance at companies such as Yahoo! and JPMorgan Chase & Co. Heath is currently working on data loss prevention, classification and cloud storage as an information security business partner for Alliance Data Systems Inc. and its line of businesses.

Marcus Ranum: We were talking in Dallas a couple of weeks ago and you said some things that pretty much made me do a complete 180 on the whole cloud computing thing. You were, basically, embracing it and using it as a way to steer other business problems, specifically, data custodianship and classification. Tell us about it.

Lee Heath: My colleagues -- Brian Mork and Houston Hopkins -- and I are somewhat new to our positions, and we were tasked with a few specific jobs. We were to look for ways to improve upon several standard security practices, such as data loss prevention, file usage monitoring, data ownership and data

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

classification, as well as trying to stay ahead of the curve with shadow IT.

Each quarter, we try and come up with a shadow IT topic and discuss how we can prevent it, or if we can use it. Of course, one the first topics that came up was the "Dropbox effect" and figuring out that upper management was already using it, not to mention the usual marketing and sales folks. After some thought -- and talking to several providers about our wants and needs -- we saw an opportunity to embrace cloud storage, make it work to our advantage and clean up the state of data management in the process.

The idea seemed simple at first -- everything moved to the cloud has an owner. By using the promise of access to your data from "anywhere" as a carrot, we're able to get users to migrate their data from traditional network file storage up to the cloud. As they move it, their data is flagged with a default classification. This allows for data retention policies that are easier to stick to and monitoring of who is accessing what, from where and with what tool. Overall, it seems like a win-win for everyone, but there is no perfect solution.

Ranum: It sounds like you're asking for the cloud service providers to stretch their business models a bit and do some technology and policy development. The good news is that once you've "broken them in" for us, everyone gets those capabilities, right? How did you manage

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

to get a sufficient level of responsiveness?

Heath: The nice thing about the cloud is that it is agile. We talked to several providers, and none of them really had what we wanted. Luckily, some [providers] can see the advantages of listening to our security concerns and utilizing our suggestions as a way to improve their products. Some [providers] did not feel like dealing with the requirements. But a good sales rep can go a long way; someone [willing] to make a sale, and sit with both us and the engineers, really made a difference.

I think for a cloud storage provider, or any online service provider, to be successful in the corporate world, they need to have more accountability and control over more aspects of their product and the product has to be usable.

Some providers had all the controls in the world, but the product was not usable or they did not support, for example, a device with iOS (which is popular among the C-level). Most [services] are really user friendly, but they have limited security controls or accounting capabilities associated with their tools. In the end -- which has taken about six months and is not really the end -- we have the bulk of what we wanted. It has been an ongoing, iterative process with the vendor we decided to go with. It would be interesting to go back and see if any other [vendors] took what we had to say and improved their offerings.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Ranum: Did you keep any metrics about the effectiveness of the data classification? How many of the units just moved everything up and marked it with the "default" markup? Still, this sounds like a huge win -- because, no matter how you slice it, you now have an audit trail of all the files a unit moved to the cloud; and I suppose you could do more detailed analysis from the audit trail. What metrics did you keep during the migration, and what have you done with them?

Heath: Actually, you caught us at the end of the testing and design phase, and we are about to start on-boarding the general masses. Thus far, we have only had a few key test groups that are sending in feedback for tweaks and features. Brian and Houston have been playing with the API, which allows us to pull the detailed logs of all actions, plus all metadata associated with every file on the system. The API is mainly for creating your own apps, but we are using it to get to the details held within [the storage system].

One of the big things we are looking at tracking is, as you mentioned, whether people are using the tags and classification at upload time, going back, or just leaving the default. We are already tracking where people are accessing the files they have uploaded from and who they are sharing items with. Some of this data will be fed into SIEM solutions for alerting, because we don't want

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

to muddle the signal-to-noise ratio in email alerts. Some [data] will be tracked for trending, and for alerts of anomalies, such as bulk downloads.

One upcoming feature from the provider is a rules engine, so some of the data we will be pulling and parsing on-site will end up being in the product itself at a later date. Until the rules engine is complete, the features will be managed by us via scripts and the API. For instance, data retention policy adherence is an example of how we use the API. We can pull the metadata from each object; therefore, we can see how long [it's been] since a file has been updated and how it is classified and tagged. Based on that data, we can automatically move the file to a trash folder to be deleted at a later date, notify the owner that it will be deleted or whatever we see fit. Overall, it is very flexible.

Ranum: I have to admit I'm surprised that the cloud providers were willing to make modifications for you. I suppose that what you're seeing is maturation of the market with newer and hungrier providers trying to distinguish themselves. The provider you went with is one of the top-tier providers, though, right? Were you early adopters? How did you get into their technology lifecycle so effectively?

Heath: I will admit we were not the only ones asking for these features. The sales guy has several big name companies that are asking for similar features.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Luckily, we had worked with him before on other projects, and through other companies, so we have a good rapport with him and he understands that the sale is dependent on doing the right thing.

Security is the big concern with cloud services for most companies, to the point that they are unwilling to use them. For some reason, many cloud companies are, as you mentioned, not willing to meet the requirements of their customers. Whether they think they know better or think it is the corporate user community being overly paranoid, it doesn't matter. Just because the general public accepts security shortcoming does not mean that companies that have knowledgeable staff will. I hope we see more of a change and get the cloud providers to be more flexible and to meet our needs as an industry, and not just stick with what they feel is "good enough."

We ask most of the smaller to midrange companies we work with if they have a technical advisory board we can be part of; for some, it works quite well. I don't expect a company like IBM or HP to really listen when we have feature requests, but there are a lot of companies that do, and they benefit from it as much as we do. One of the key things is not just asking for a feature, but having justification and reasoning behind it. You may not end up with exactly what you asked for, but often what you get will fill the need.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Ranum: Have you attempted any redundancy analysis? I wonder if you could do something like pull back checksums and see how many exact copies you have of certain files in your entire enterprise? Or, perhaps filename analysis to see how many variant versions you have of files? I can see a lot of potential for "big data" style analysis, treating your file storage -- once you've got it all in one place -- as the subject of study. You could do some cluster analysis to see how many people shared files outside of their group. If you could tie some departmental data into the analysis -- via Microsoft Active Directory [AD] or human resources -- you could actually start to do queries against stuff like, "Tell me about people in sales who have files that came from HR." Are you doing anything like that now?

Heath: Brian and Houston have started pointing out some of the bits of information we could use for data mining and some trending. While we have technically unlimited space, using the SHA-1 hashes that are part of the metadata provided by the cloud service, we can easily pull that information and look for duplication. The duplication detection would be more of a concern for which one is "official" and making sure that is the one people are utilizing. The file and folder objects have a lot of attributes we can pull and manipulate. There is

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

also access and revision history, so we can see that while Bob may own the file, Alice is the maintainer.

Along with the revision history, the cloud provider keeps the previous versions, so we can see if and when a large amount of data is added or deleted from specific documents. If a file has been consistent for a period of time and suddenly changes, then we can notify the owner and/or updater to make sure that a mistake wasn't made.

We can also take that one step further to monitor the SHA-1 of specific documents to do basic file integrity monitoring of policies or procedural documents that should not change often, for instance. Beyond that we are already monitoring file sharing. We cannot only see who has shared files, but we can see if the share has been accepted and whether or not the objects have been accessed. We can also see if specific documents or whole folders have been shared internally or externally. Some groups will have more control over who they can share with than others, based on culture and business need, but we still need to monitor for abuse.

We are tying the solution into AD for authentication using SAML [security assertion markup language], but we don't see a way we can comfortably use AD groups for access controls. The cloud system allows for adding details about

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

the user such as title, address and phone number, but not organizational info. With the enterprise console, we can add groups of users and assign access to a group, but again it is not tied to AD -- at this time -- and the groups are just for ease of use. The actual file attributes list all users with access and the type of access, not the group.

Ranum: I guess one of the biggest "data management nirvana" aspects of what you're doing is that you more or less move away from unauthenticated access to important data. What you guys have done is figured out a way to take advantage of the nature of the cloud in a way that offsets the security disadvantages of it. That's fantastic! I may become a cloud computing advocate after this. What's the most important thing you've learned from this effort?

Heath: In my last position, I was right there with you and would have not considered using the cloud for any storage. While I now feel there are some good use cases, and ways we can make it fit a need, there are still cases where I would not use it. I don't want to keep, for instance, credit card data in bulk in the cloud. I don't feel the risk warrants it, but, as you mentioned, it might be better than having it on a wide open share, even if the network is protected.

I think the main thing we took away from this as a company is, to some

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

extent, to embrace shadow IT and leverage it to your advantage. At the same time, don't back down from what you know you need. If a vendor is not willing to work with you, explain why you don't want to use them. Many [providers] are aware of security concerns and have good ideas on their roadmaps, but until more companies push the issue, security won't be high priority over usability bells and whistles... It is a trade-off of usability versus security with users' wants thrown in to make it even more complicated, and we all know that is the ultimate balancing act for infosec.

MARCUS J. Ranum, chief security officer of Tenable Security Inc., is a world-renowned expert on security system design and implementation. He is the inventor of the first commercial bastion host firewall.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

CLOUD COMPLIANCE: TACKLING COMPLIANCE IN THE CLOUD

Davi Ottenheimer

Most organizations already have started to use virtualization technology or cloud computing. Yet some still may be reluctant to move their mission-critical—tier-1 – applications to these relatively new environments. While the flexibility and cost benefits of virtualization are widely accepted, questions linger on how to adapt to new and different risks. Security and compliance top the list of organizations' reasons to delay adoption.

Concerns about security in a virtual environment almost always begin with a study of the relationship between guest and host. That is just the tip of the iceberg. In the end a far more comprehensive view of risk management is necessary, which includes virtual machines (VMs), hypervisors, networking, storage and management. From configuration of software-based networking devices to software-based data centers, the process and procedures for managing resources are an important part of an assessment of cloud risk and compliance. An assessor not only will review configuration of the VM and hypervisor

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

technology, but also look at how logical concepts such as port groups, resource pools and clusters are being managed in relation to data flows and business logic.

Let's take a look at some of the ways virtualization and cloud computing impact compliance and how organizations can tackle cloud compliance issues.

START WITH A STANDARD BASELINE

A good strategy to manage cloud compliance is to establish a clear and transparent relationship with a cloud service provider. This can be facilitated by standards such as the SSAE 16 SOC 2 or ISO 27001. A framework that both parties can agree on makes it easier to get through the sections to focus on finding resolution in areas of concern. A provider that refuses to provide on-site physical assessments, for example, may not be acceptable to an assessor or a cloud customer. They might be concerned that despite what cloud providers say about identical controls in their many physical locations, which can be verified on paper, the human element of managing controls can still cause controls to drift out of place and warrant on-site audits.

Perhaps the easiest way to work through cloud compliance challenges with cloud providers is to approach them first at a technical level and in terms of how

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

compliance has been handled in the past. An operating system has typically been brought into compliance by hardening it to a set of published guidelines. Systems within government must adhere to a set of documented security standards, such as the U.S. Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), or publications from the National Institute of Standards and Technology (NIST). Systems within a commercial environment may need to be measured against completely different guidelines from the Center for Internet Security (CIS) or by an industry group such as the Payment Card Industry (PCI) Security Standards Council (SSC). Like the ISO and SSAE 16 standards, although with a regulatory authority overseeing their adoption, they can help clarify what exactly has to be done by a provider to achieve compliance.

TAKE CONTROL OF CONTINUOUS CHANGE

Let's say that a Windows 7 system on hardware could be configured to meet the CIS Benchmark version 1.2.0 released on March 30. Move that same Windows 7 system from hardware to a VM on a hypervisor managed by a provider and an assessment of compliance for that system can be seriously different. Move it into a cloud environment and it changes again. The operating system itself

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

remains almost identical, but an updated benchmark is required to account for the relationship with the hypervisor and then the systems used to manage hypervisor resources. Consequently, hardening takes on new and different meanings based on virtualization and how it is managed. Why? The flexibility and efficiencies of cloud mean new and different configuration options, which have different risks compared to hardware-based infrastructure.

For example, a hardware-based operating system will have configuration files that define storage. Migration to a virtual machine means the configuration files that describe the hardware move outside the system and onto the hypervisor. The boundaries for a VM are defined by those configuration files. In other words, a Red Hat Enterprise Linux system would normally use a configuration file in the OS (e.g. /etc/fstab) to determine which hardware file systems to mount when it boots. The OS file has to be very particular to equipment it was installed with (e.g. bus type, file system type, partition number). Virtualization, however, will make the same file in the OS generic to reflect the typical—or at least reduced—set of options available from the hypervisor. It then moves the hardware details to a file read by the hypervisor but invisible to the VM's OS.

In terms of compliance, this means there has to be a shift in how to assess technical controls when looking at a virtual environment. A hypervisor should

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

put a VM in a sandbox, isolated from other VMs. The sandbox is defined in part by how the hypervisor controls access to its hardware. A VM therefore should have no expectation that it can achieve direct hardware access by changing its configuration file; it should only see what it is provided. At a cloud provider level, this means a provider always should be validating configuration information that is uploaded with a VM before allowing that VM to run. A simple failure to validate a VM setting, such as allowing a VM to directly mount hypervisor storage, could potentially compromise other VM data on that hypervisor. Optical drives have little or no need to be connected to a VM in a data center environment, so they usually can be disabled. Likewise, attacks on serial and parallel ports do not work if those ports are disabled.

The key to this example is that a customer will need to know whether a provider validates VMs as well as disables features unused or unnecessary. It is the same concept as traditional compliance requirements—validate input and reduce the attack surface—but applied to the new processes and control points of cloud.

While the requirements in regulations do not yet spell out this level of technical detail for provisioning and de-provisioning systems, they do have language that is relevant and useful to assessors. The PCI Data Security Standard

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

(DSS) version 2.0 states in Requirement 2.2 that a regulated entity must "develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards."

Cloud providers and vendors already are stepping forward to address the language of this regulatory requirement for standards. New security and compliance products, as well as detailed hardening guidelines, address the need for industry-accepted control requirements or recommendations. VMware's vCenter Configuration Manager (VCM) is the type of tool that customers can request from their cloud providers to get a centralized and continual collection of configuration changes to infrastructure. A unified report will show systems that are out-of-sync with vendor hardening guides, or in violation of policy or regulations such as SOX, PCI DSS, HIPAA and FISMA. An emerging standard called the NIST Security Content Automation Protocol (SCAP), also supported by VCM, can even provide a detailed guide on current security configuration of operating systems and applications.

ESTABLISH TRUSTED ZONES

Software-based networks also can be a sticking point for compliance.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Segmentation between VMs, explained above in terms of the hypervisor, also is relevant to the configuration and maintenance of virtual switches. The migration of a VM from one hypervisor to another is often done in the clear for reasons of performance and availability. In other words, the VMs are sent by providers without encryption, so anyone with access to the network would potentially intercept and view or modify data. The memory contents of a VM could be viewed or altered. Confidentiality and integrity both are at risk when this is the configuration.

To reduce the risk of these attacks, the management-related traffic of the hypervisor should be set to isolated and dedicated networks that are non-routable (i.e. no layer-3 route to other networks). The port group should be on a dedicated VLAN. The virtual switch can be shared but the port group VLAN should never have any other VM connected. This also allows for monitoring for that VLAN ID on other port groups. Another option is to further separate the port group with a management-dedicated virtual switch and to monitor the switch for non-management traffic.

Taking this one step further, a management network should be set up at a cloud provider to restrict access only to known endpoints. Although requirements such as PCI DSS do not explicitly state this, the PCI Security Standards

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Council (SSC) in 2011 made it clear with the publication of its virtualization guidelines that reducing the management interface attack surface is a best practice. An attacker is likely to target the network to gain privileged access to a cloud provider's management interface.

That is why the management layer should be protected by giving it a dedicated VLAN for the management port group on a shared virtual switch. Other VM traffic may be allowable on a switch if the port group for the management VLAN is restricted only to management traffic. An additional level of security, such as stateful packet inspection and intrusion detection monitoring, will help further segment the traffic and tends to be required under some regulations such as PCI DSS. An even better step to segment management communication is to move the management VLAN to a dedicated virtual switch that does not allow for any non-management port groups. The network segment also should not be routed except to other isolated and protected management networks.

Another important step in overcoming cloud compliance challenges is related to the human element; The cloud provider's administrators and users must be trained on policy and procedures. SSL certificates not only have to be carefully managed and secured, but the administrators themselves also have to be vigilant about verifying SSL certificates before entering their passwords.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

Impersonation of a VMware vCenter Server or vCloud Director with an incorrect SSL certificate would force the client software to display a security warning. An administrator might override the warning if he or she isn't properly trained to report it and/or investigate the error as a security incident.

COMPLIANCE AS A COST-SAVER

One of the more interesting effects of cloud environments is that, when engineered properly, they actually can reduce compliance costs while improving security coverage. Anti-malware controls are an excellent example of how automation and consolidation reduce overhead. There is no doubt that antivirus is required under practically every regulation; from SOX to PCI DSS, there is a need to prevent unauthorized code. Requirement 5 of PCI DSS v2 states simply, "Use and regularly update antivirus software or programs." Finding viruses with an ever-increasing blacklist is a resource-intensive process. Software to catch viruses tends to disappear into the underutilized capacity common on dedicated hardware. A virtual environment, by comparison, makes far more efficient use of shared hardware; however, VMs can end up performing scans in competition with each other out of a limited pool of resources.

Hypervisor companies and their antivirus vendor partners are working to

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

address this problem. For example, VMware's vShield Endpoint offloads work from VMs to a shared and dedicated security VM on the same host. Centralized control and elimination of redundant load means a dedicated agent per VM is no longer necessary for virtual environments to achieve compliance requirements. The increased efficiency, while performing the same or better level of protection and compliance, might seem familiar to those wanting to move to cloud.

Consider how taking this newly centralized model of compliance in the cloud can affect the storage footprint for each VM versus a traditional anti-malware agent. The traditional agent, plus several signature files for rollback capability, often is several GB in size. For the sake of argument, run a quick calculation for 1,000 VMs on 10 hosts with an anti-malware footprint of roughly 5 GB per host and SAN storage for the VM at $5K per TB:

(1,000 VM) x (5 GB per VM) = 5 TB
5 TB x ($5K per TB on SAN) = $25,000 in host-based antivirus storage space

Next, for comparison, run a calculation for a host running anti-malware on behalf of the VMs. The host-based anti-malware is likely to be larger than a VM anti-malware agent, so 7 GB instead of 5 GB gives the following result:

(10 Hosts) x (7 GB per host) = 70 GB

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

.07 TB x ($5K per TB on SAN) = $350

The cost savings for cloud compliance using a host-based anti-malware model shows storage is reduced more than $24K (or $24 per VM) and saves 4 TB. Network resource benefits also are possible. The hypervisor-based solution downloads malware signatures once for all the guests on a host; 10 systems have to communicate updates and events instead of 1,000. Factoring in keep-alive packets, scan start/stop status and signatures for 1,000 systems is roughly 2 MB of overhead that could be eliminated from the network. A carefully planned and controlled cloud provider environment may therefore find significant financial benefits when properly addressing the challenges of cloud compliance.

Today, organizations are eager to take advantage of the cost efficiencies of cloud computing, but they need to ensure the move won't jeopardize their compliance efforts. Emerging standards and improved solutions from vendors are helping to guide customers and their providers to comply with many governmental and industry regulations. In some cases, it is proving to easier to be compliant in the cloud than ever before.

DAVI OTTENHEIMER is president of security consultancy flyingpenguin and author of the new book Securing the Virtual Environment: How to Defend the Enterprise Against Attack. He is a QSA and PA-QSA for K3DES with more than 17 years of experience in security operations and assessments, including a decade

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

of leading incident response and digital forensics. Davi formerly was global communication security manager at Barclays Global Investors and a “Dedicated Paranoid” at Yahoo responsible for digital home, broadband and mobile security. Send comments on this article to feedback@infosecuritymag.com.

Home

Converting to cloud: Ranum Q&A with Lee Heath

Cloud Compliance: Tackling Compliance in the Cloud

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.