UNITAS GLOBAL

WHITEPAPERS

HOW TO SLEEP SOUNDLY WHILE UTILIZING THE CLOUD

UNITAS GLOBAL

CONTENTS

UNITAS GLOBAL

3

GIVE IT TO ME STRAIGHT

"55% said service providers who specialize in private cloud offerings would be the best choice..."

The cloud can be a dangerous place for data, but so can a swimming pool for a toddler who doesn't know how to swim. Yet, slipping well tested water-wings on the little tike's arms along with a rubber nostril pincher for his nose, and that once skittish land-lover will become an amphibian in no time. The same holds true for jumping into the EPC - Enterprise Private Cloud. That is, with the proper readiness, coupled with professionals who know how to secure and monitor your applications, the IT leap will safely and effectively reduce costly overhead, saving both time and money.

YOU'RE NOT ALONE

PwC recently released a series of articles entitled, "The Future of IT Outsourcing and Cloud Computing," showing that several surveyed companies saw IaaS as the future of IT outsourcing. Of the surveyed CIOs and senior executives, "55% said service providers who specialize in private cloud offerings would be the best choice in three years." But even though these business leaders see the EPC as the future, they are still hesitant to move forward. Another survey conducted by Intel found a resounding 69% of global enterprise leaders were either 1) very or 2) moderately concerned with cloud security.

So how can CIOs alleviate anxiety and move forward? Simple. Businesses need to embrace the proven security and monitoring solutions within the Enterprise Private Cloud. Empowered with this knowledge, companies can capitalize on the cost saving EPC experience.

4 SECURING THE INFRASTRUCTURE

By its mere nature, the infrastructure is a multi-layered system, with each layer requiring its own plan of defense. The first step towards securing the infrastructure, is to have a basic understanding of each layer and its correlating security solution.

PHYSICAL DATACENTER

The first layer of defense is relatively simple in concept- Secure the actual physical datacenter. The datacenter location is crucial; avoid floodzones, earthquake fault lines, and heavy traffic areas. Next, protect the facility's grounds with barrier walls, vegetation, and guarded/ gated entrances. Limit access to the actual facility with guards, biometric hand readers, keycards, mantraps, exit-only fire doors, and separate bathrooms for visitors. Also, eliminate single points of failure by utilizing concurrently maintainable utilities to ensure reliable power and water supplies.

Continuous CCTV monitoring of the facility multiplies the effectiveness of your guards and increases employee accountability. Properly securing the physical datacenter keeps your background-checked employees safe and is the first step towards information assurance.

NETWORK

The network serves as the virtual highway in and out of your EPC. Basic defense tools in this layer consist of network firewalls (i.e. F5s BIG-IP Local Traffic Manager), Intrusion Detection Systems (i.e. Cisco's Catalyst 6500 Series), and Intrusion Prevention Systems (i.e. Cisco's IPS 4500 Series). These virtual plug-and-play solutions offer comprehensive protection on the network level, but can never replace real time monitoring. Network monitoring on a 24/7 basis adds a human level of defense, prevention, and protection.

Sufficiently staffed Network Operations Centers (NOCs) can effectively provide this necessary real-time, and in-depth monitoring. Lastly, Network Access Control devices (i.e. Forescout's CounterACT), placed in front of your virtual machines, provide comprehensive visibility and control of your network.

5 SECURING THE INFRASTRUCTURE

Understanding the functionality behind this layered defense approach pushes companies to the forefront of EPC security.

VIRTUAL MACHINE MANAGEMENT

Hypervisors, like VMware's ESXi, make up the majority of this next layer. By managing and instructing the virtual machines, hypervisors not only play an extremely important role within your EPC, but also serve as a vulnerable point of attack. Hardening the machine that hosts your hypervisor can protect against intruders from gaining access and control to this critical component. To see an example of hardening guides, check out VMware's Vsphere hardening guides. In addition to hardening the machine, severely limiting and meticulously managing internal access to this critical layer mitigates insider threats.

OPERATING SYSTEMS & GUEST HOSTS

This layer consists of the different guest hosts running different operating systems under the management of the hypervisor. For this reason, host-level security is required: Anti-virus, anti-malware, and file integrity monitors (i.e. Tripwire). In addition to installing security software, it is imperative to configure the operating systems according to the guides created by the National Security Agency.

APPLICATIONS & DATA

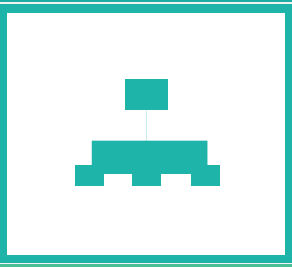
Easily the most penetrated and attacked level within your infrastructure, applications are first made secure during development, not during deployment. A more in-depth security solution for the application level is available in the next section of this white paper. However, in regards to your servers, always remember to clean them after application installations. For example, after an application's installation there are usually a large amount of sample files, scripts, code, and directories - delete them - hackers can and will hide malware in them.

UNITAS GLOBAL

6

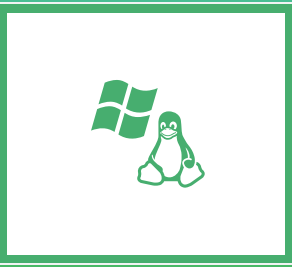
SECURING THE INFRASTRUCTURE (VISUAL)

PHYSICAL DATACENTER
- Strategic Facility Location
- Guarded & Monitored Facility Access
- Concurrently Maintainable

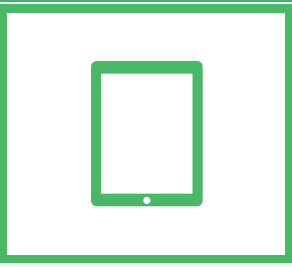


NETWORK
- Network Firewalls, IDS & IPS
- 24/7 Network Monitoring
- Network Access Control Device

VIRTUAL MACHINE MANAGEMENT
- Follow Hypervisor Hardening Guides
- Limit Internal Access



OPERATING SYSTEMS & GUEST HOSTS
- Anti-Virus & Anti-Malware
- File Integrity Monitors
- NSA Configuration Guides



APPLICATIONS & DATA
- Vulnerability Scanner
- File Integrity Monitor
- Web Application Firewall
- Data-Missing

7 SECURING APPLICATIONS & DATA

The Gartner Group found that 75% of attacks are at the application level.

Since this is the most penetrated level, it must also be the best protected and it's easy to see that, again, a layered solution is the best approach. A three step approach towards layrered application security is outlined below.

STEP 1

Run a web application vulnerability scanner (i.e. Qualys' QualysGUARD). Developers scan applications that pinpoint vulnerabilities, mitigate the found vulnerabilities, then rescan to confirm the vulnerabilities were mitigated. Placing your applications in the cloud without first securing them is like sending that toddler into the pool without his water wings.

STEP 2

Apply a file integrity monitor (FIM) to the application (i.e. Tripwire). This will verify the current file state with that of the good, baseline file state (i.e. original) and notify if the file's integrity has been compromised (i.e. the occurrence of unauthorized changes). The FIM can also be configured to automatically return to the last known good state, thereby preserving integrity.

STEP 3

Front-end the applications with a Web Application Firewall (i.e. ModSecurity- an open source WAF). While traditional firewalls are still necessary for the overall network, the more precise WAF conducts deep packet inspections specifically looking for scripts that launch XSS (cross-site scripting), SQL injections and other OWASP (Open Web Application Security Project) identified vulnerabilities. WAF's can also guard against unknown attacks by thoroughly screening inquiries, detecting anomalies, even if the attack is that of an unknown variety.

8 DATA PROTECTION

Armor your data. Data-masking techniques, such as encryption, protects your sensitive data and makes it indecipherable to unauthorized environments.

The previously mentioned security measures prevent unauthorized access to the data housed within your infrastructure and applications, but knights still wear armor, even behind castle walls. Armor your data. Data-masking techniques, such as encryption, protects your sensitive data and makes it indecipherable to unauthorized environments.

Encryption is a popular data masking approach in which algorithms shuffle and scramble the data into calculated nonsense. However, only when the keys to these encryptions are properly secured and managed, does this data masking technique actually become effective. Combining data-masking techniques, thus creating a hybrid armored approach, significantly increases the strength of your data protection solution.

NETWORK MONITORING: NOC

Preparing and protecting your data is always the necessary first step, but it would be naïve to think that placing armored apps into a properly secured infrastructure is enough. The array of problems that can occur (i.e. overloaded/crashed servers) when using any type of storage system, not just the cloud, proves the need for continuous monitoring. This unwavering commitment to detail is the final step towards proper EPC deployment and implementation. A Network Operations Center (NOC) provides a constant, 24/7 monitoring approach guaranteeing the viability of your network, your EPC, and inevitably, your business.

UNITAS GLOBAL

9

BUT I STILL HAVE CONCERNS

What kind of visibility can private clouds offer in regards to abstracted resources?

How do I make my cloud compliant? How do you control data visibility on an internal level? These are common questions asked by cloud-skeptic CIOs and rightfully so. There are still challenges, threats, and risks outside of hackers and network malfunctions. The simple answer is customization. These problems are all remedied when EPCs are built on an individual customer basis. An "out-of-the-box" or "pay-per-use" cloud approach may seem financially enticing, but it will always cost more time and money at the enterprise level, mainly due to the fact that these solutions lack customization capabilities.

An EPC designed and built to your company's necessary requirements and specifications proves the private cloud's synonymy with business agility: Agile IT means agile business. The EPC provides a simple path towards agility, however true agility is realized only when efficient deployment and effective implementation occurs.

Take the issue of compliance as an example. For some industries, EPC may seem like an unattainable solution, due to its perceived non-compliance, but this perception is nothing more than an ill-informed thought. Experienced private cloud providers have the ability to create entirely compliant environments. For instance, with recent government incentives to convert medical records into Electronic Medical Records (EMRs), healthcare companies can now benefit from the enterprise private cloud more than ever, but jeopardizing HIPAA compliance has deterred many CIOs from adopting a cloud solution.

Nonetheless, when given the chance, a seasoned EPC provider can explain to even the most skeptic CIO, step by step, the HIPAA Security Rule Standards as well as each Standard's correlating implementation specifications (Both the required and the addressable). Then the proper EPC solutions to successfully implement these specifications can be outlined (A handful of which were already outlined in this white paper). It is through a customized plan of action that a cloud provider can deploy and implement a HIPAA compliant private cloud.

REALISTIC SOLUTIONS

Companies are given the option of taking on the financially-draining and time-consuming task of launching a private cloud infrastructure or they can outsource this large complex project to a group of experts that can coordinate all aspects, from design to deployment and monitoring, all as one simple service. When choosing that expert, companies must be vigilant in selecting a private cloud provider that puts securing your data first, and when that is done, then you can truly sleep soundly while your data lives in the cloud.

WWW.UNITASGLOBAL.COM

453 S Spring Street 2nd Floor Los Angeles, CA 90013 +1 855.586.4827 inquiries@unitasglobal.com