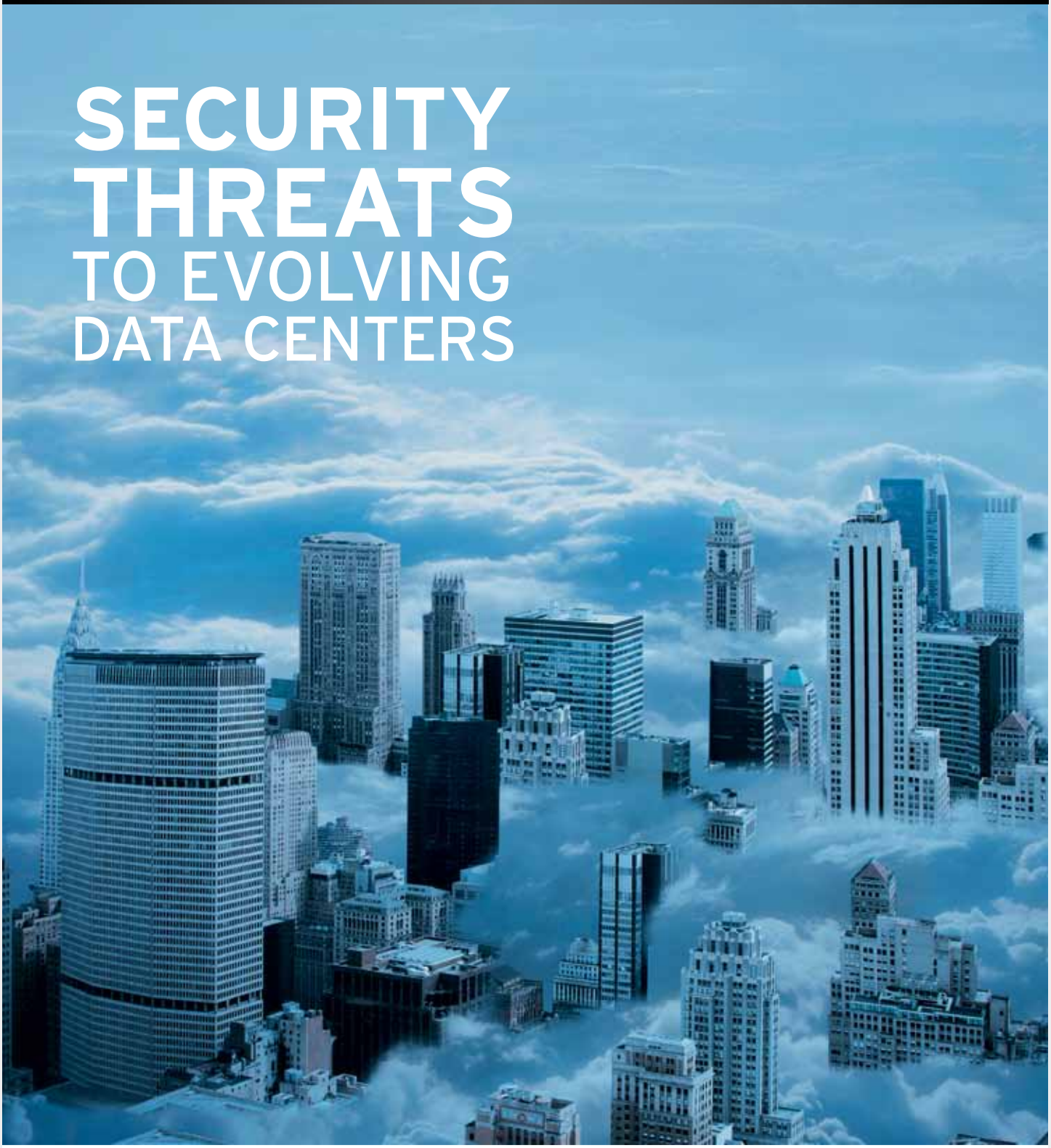
VIRTUALIZATION AND CLOUD COMPUTING

SECURITY THREATS TO EVOLVING DATA CENTERS



Data Center Security

TREND MICRO™

Securing Your Journey to the Cloud

Executive Summary

Many businesses are evolving their data centers to include virtualization and cloud computing to improve resource utilization, accelerate development and deployment of computer resources, and reduce costs. However, these new platforms open additional avenues for threats against data, systems, and reputation. For the most part, these threats are presented through the same types of attacks – data-stealing malware, web threats, spam, phishing, Trojans, worms, viruses, spyware, bots, and more. However, virtualization and cloud computing raise new infrastructure issues that security providers must consider when creating a security foundation to protect against these threats.

This report discusses the security threats that enterprises face when deploying and using virtualization and cloud computing infrastructures. The report contains real-world examples of attacks and attack tools that cyber criminals use to exploit vulnerabilities in virtualization and cloud computing environments, as well as recommendations for security best practices.

Introduction

In a recent global survey conducted by Trend Micro, IT decision makers indicated which virtualization and cloud technologies they have deployed or are currently piloting. Worldwide, over one-half of companies surveyed have implemented some form of server virtualization and virtual desktop infrastructure (VDI). Also of those surveyed, 45 percent are using a public cloud, and 46 percent are using a private cloud (see Table 1).

Table 1: Virtualization and Cloud Computing Implementation (responses from IT decision makers)

% that have currently deployed or are piloting	Total	US	Japan	India	Germany	UK	Canada
Server Virtualization	59%	70%	58%	51%	61%	68%	47%
VDI	52%	62%	42%	48%	55%	63%	45%
Public Cloud	45%	54%	37%	38%	48%	52%	42%
Private Cloud	46%	56%	34%	42%	54%	51%	38%

Security must support virtualization and cloud computing deployments and enable organizations to realize the full benefits these platforms can provide. In a rush to implement these new IT infrastructures, many enterprises simply deploy their current physical server security on their virtual machines (VMs). However, traditional physical server security does not adequately address the new security risks unique to virtualization and cloud computing. At the same time, such security negatively impacts performance on these platforms.

Virtualization Security Threats

Introduction

Some security risks unique to a virtualization infrastructure include communication blind spots, inter-VM attacks, and mixed trust level VMs. Instant-on gaps and resource contention are also important considerations. This section addresses each of these threats and issues.

Communication Blind Spots

In virtualized environments, traditional network security appliances are blind to the communication between VMs on the same host unless all communications are routed outside the host machine to this separate appliance. But this security configuration introduces significant time lags. One way to eliminate blind spots while reducing time lags is to place a dedicated scanning security VM on the host that coordinates communication between VMs. This solution works well in a virtualized environment. However, a dedicated security VM is not ideal for a cloud environment. The dedicated security VM integrates with the hypervisor to communicate with other guest VMs. In some cloud environments, such as in a multi-tenant public cloud, users do not have access to the hypervisor. In the cloud, protection is best provided as self-defending VMs. Protection is self contained on each VM and does not require communication outside of the VM to remain secure.

Inter-VM Attacks and Hypervisor Compromises

Virtualized servers use the same operating systems, enterprise applications, and web applications as physical servers. Hence, the ability of an attacker to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized environments as well. And once an attacker compromises one element of a virtual environment, oather elements may also be compromised if virtualization-aware security is not implemented.

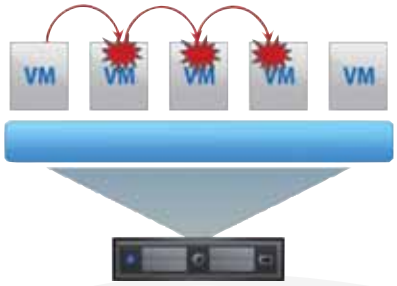


Figure 1: Inter-VM Attack

In one scenario, an attacker can compromise one guest VM, which can then pass the infection to other guest VMs on the same host. Co-location of multiple VMs increases the attack surface and risk of VM-to-VM compromise. A firewall and an intrusion detection and prevention system need to be able to detect malicious activity at the VM level, regardless of the location of the VM within the virtualized environment.

Another attack mode involves the hypervisor, which is the software that enables multiple VMs to run within a single computer. While central to all virtualization methods, hypervisors bring both new capabilities and computing risks. A hypervisor can control all aspects of all VMs that run on the hardware, so it is a natural security target. Therefore, securing a hypervisor is vital, yet more complex than it seems.

Virtualization Security Threats

Inter-VM Attacks and Hypervisor Compromises (contined)

In an attack known as "hyperjacking," malware that has penetrated one VM may attack the hypervisor. When a guest VM attempts this attack, it is often called a "guest VM escape" because the guest VM breaks out of, or escapes, its isolated environment and attacks the host hypervisor. Once compromised, a hypervisor can then attack other guest VMs on that host.

VMs make requests to the hypervisor through several different methods, usually involving a specific application programming interface (API) call. An API is the interface created to manage VMs from the host machine. These APIs are prime targets for malicious code, so virtualization vendors attempt to ensure that APIs are secure and that VMs make only authentic (i.e. authenticated and authorized) requests. Because this is a critical path function, speed is a significant requirement in all hypervisors to ensure that overall performance is not impeded.

When attackers targeted a zero-day vulnerability in a virtualization application called HyperVM made by LXLabs, as many as 100,000 web sites were destroyed [1]. In addition, certain virtualization vendors like Amazon Web Services have made their APIs public. These will undoubtedly become interesting targets for cybercriminals. Vendors that have not made their APIs public like vSphere, while not usually externally exposed, can also become potential targets for attacks within their perimeters. There is a risk that, owing to the rapid change in the API space and the current race to market, virtualization management systems will not be secure in the future.

Mixed Trust Level VMs

VMs with mission-critical data may reside on the same host as VMs with less critical data – resulting in mixed trust level VMs. Enterprises can attempt to segregate these different levels of secure information on separate host machines, but in some cases, this can defeat the purpose of a virtualized environment – to make the most efficient use of resources. Enterprises need to ensure that mission-critical information is protected while still realizing the benefits of virtualization. With self-defending VM security, VMs can remain safe even in mixed trust level environments, with protection such as intrusion detection and prevention, a firewall, integrity monitoring, log inspection, and antivirus capabilities.

Instant-On Gaps

Virtualized environments are not necessarily inherently less secure than their physical counterparts. However, in some cases, the practical uses of virtualization can introduce vulnerabilities, unless administrators are aware of these vulnerabilities and take steps to eliminate them. Instant-on gaps are an example of such a vulnerability.

Beyond server consolidation, enterprises take advantage of the dynamic nature of VMs by quickly provisioning, cloning, migrating, and decommissioning VMs as needed, for test environments, scheduled maintenance, and disaster recovery, and to support task workers who need computational resources on-demand. As a result, when VMs are activated and inactivated in rapid cycles, rapidly and consistently provisioning security to those VMs and keeping them up-to-date can be challenging.

Virtualization Security Threats

Instant-On Gaps (continued)

After a period of time, dormant VMs can eventually deviate so far from the baseline security state that simply powering them on introduces significant security vulnerabilities. And even if VMs are dormant, attackers may still be able to access them. Also, new VMs may be cloned from VM templates with out-of-date security. Even when VMs are built from a template with virus protection and other security applications, the VMs need the security agent to have the latest security configurations and pattern file updates.

When dormant, reactivated, or cloned VMs have out-of-date security, attackers may be able to leverage an exploit for a longer period of time – the attack may have more longevity. Generally, if a guest VM is not online during the deployment or updating of antivirus software, it will lie dormant in an unprotected state and be instantly vulnerable when it does come online. One solution is a dedicated security VM on each host that automatically updates VMs with the latest security when activated or cloned, and safely allows enterprises to realize the benefits of virtualization.

Resource Contention

When resource-intensive operations such as regular antivirus scans and pattern file updates designed for physical environments are applied to VMs, these operations can quickly result in an extreme load on the system. When antivirus scans or scheduled updates simultaneously kick into action on all VMs on a single physical system, the result is an "antivirus storm." This storm is like a run on the bank, where the bank is the underlying virtualized resource pool of memory, storage, and CPU. This performance impact hampers server applications and VDI environments.

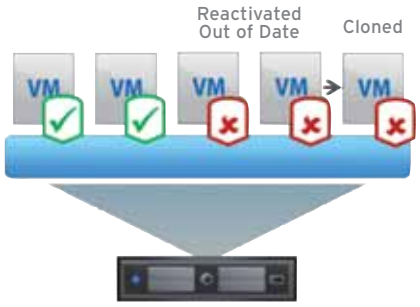


Figure 2: Instant-on Gaps

The legacy security architecture also results in linear growth of memory allocation as the number of VMs on a single host grows. In physical environments, antivirus software must be installed on each operating system. Applying this architecture to virtual systems means that each VM requires additional significant memory footprint – an unwanted drain on server consolidation efforts.

Products that are not virtualization-aware suggest the use of randomization or grouping to avoid resource contention. However, randomization does not help to avoid times of high system usage and requires that a long period of time be reserved for the full scan cycle. Grouping does not allow for the mobile nature of virtualization, requiring reconfiguration when VMs are migrated or cloned.

Virtualization-aware technology is required to minimize resource usage and increase VM densities. A dedicated scanning VM can coordinate staggered scans across VMs to preserve host resources. And agent-less antivirus removes the antivirus software from the guest VMs and centralizes these functions on the dedicated security VM, enabling a massive reduction in memory footprint for security on virtual hosts.

Cloud Computing Control and Security

Introduction

Cloud computing is an extension of virtualization, adding automation to a virtual environment. Advancements in virtualization technologies enable enterprises to obtain more computing power from the underutilized capacity of physical servers. The traditional datacenter footprint is shrinking to enable cost savings and "greener" IT through server consolidation. Service providers have discovered that they can use virtualization to enable multi-tenant uses of what used to be single-tenant or single-purpose physical servers. And private clouds are also generally founded on a virtual infrastructure for better resource usage and ease of provisioning. The structure of these different cloud models – private, public, and hybrid – allow different levels of control and influence over security.

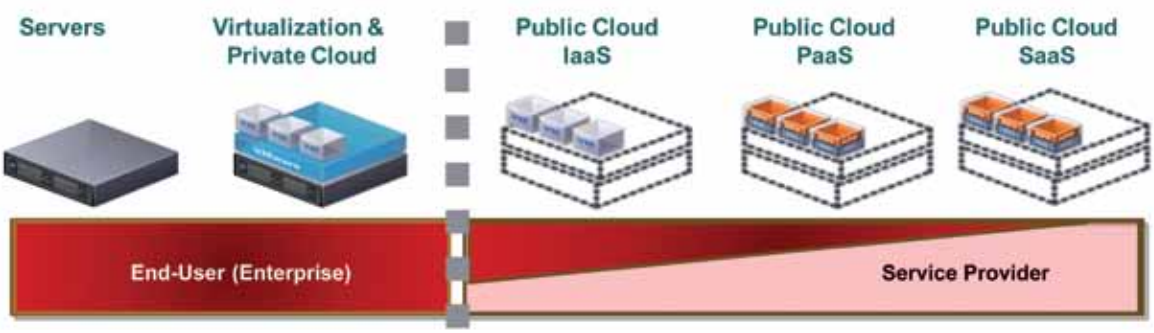


Figure 3: Enterprise Versus Service Provider Security Control

Private Cloud Service Models

The private cloud extends virtualization by adding automation to provide a self-service portal that allows enterprise departments to obtain on-demand access to computing services. With a virtualized infrastructure, different departments can share storage on the same host. This can eliminate departmental separation that complicates internal governance and compliance standards. While enterprises can also choose to open the private cloud to an extended team of partners, contractors, suppliers, and others, this broadens the level of exposure. On-demand provisioning can also lead to VM sprawl and the need for IT management solutions.

Private cloud computing can be handled completely in-house or can use dedicated hardware from a third party. For the latter, the third party houses the underlying hardware. However, if the third party is also responsible for virtualization and network infrastructure, this becomes a virtualized private cloud, and the provider has more control. This can lead to issues of transparency into the third party's processes and procedures (e.g., their hiring practices, employee access procedures, compliance procedures, and more). Because a private cloud is based on dedicated hardware and can provide hypervisor control, it allows for more customization and security than a public cloud.

Cloud Computing Control and Security

Public Cloud Service Models

The public cloud is a multi-tenant environment offered by a service provider, with less control than a private cloud and even greater exposure to security risks. Three models are typically used, in order of decreasing enterprise control: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

- Infrastructure as a Service (IaaS) - In IaaS, generally the service provider offers a VM platform and underlying infrastructure with CPU, memory, storage, and networking. Enterprises then deploy their VMs into this environment. The enterprise retains control of operating systems (OS), storage data, and applications. In the IaaS model, the enterprise does not control the underlying hardware or hypervisor, but retains significant control over security on the VM level.

- Platform as a Service (PaaS) - In PaaS, the enterprise retains control of applications and limited control over application hosting environment configurations. Otherwise, the enterprise relies on the service provider to provide security.

- Software as a Service (SaaS) - In SaaS, the enterprise retains control of only limited user- specific application configuration settings. In SaaS models, the enterprise relies on the service provider to provide security.

For these latter two models, the onus is on the enterprise to inquire as to the level and type of security provided, and the level of transparency of this information varies by service provider. If an organization goes down the SaaS path, there is very little security to actually address. In fact, the chief information security officer's only responsibility is to protect the username, password, and browser sessions of their staff with the appropriate endpoint security controls. The SaaS provider handles all other security, so it is reassuring to know that most big-name providers apply significant security resources to their services. For the most part, reputable cloud providers are likely to apply significant resources, attain security accreditation to a good standard (i.e., Statement on Auditing Standards, SAS70), and apply a dedicated and highly trained security team that can protect their customers' applications and underlying infrastructure better than many IT managers could themselves.

This paper focuses more on the IaaS model when discussing the public cloud, because it provides the greatest opportunity for the enterprise to control or influence cloud computing security. In IaaS, the enterprise is deploying VMs and hence can deploy security for these VMs. Many public cloud IaaS environments provide only minimal security. Those providers that have enhanced their services with improved security measures have done so in a piecemeal fashion, so that there is no uniform landscape in the IaaS industry. Some providers may offer little more than a bare, open VM for the customer, while others may provide options such as a virtual private network that enables customers to securely connect their cloud and on-premise resources.

Cloud Computing Control and Security

Public Cloud Service Models (continued)

Even large, well-established IaaS providers are not immune to security breaches. GoGrid, which calls itself "the world's largest pure-play IaaS provider specializing in cloud infrastructure solutions," [2] sent its customers a letter on March 30, 2011 describing their data breach. "Our Security Team discovered that an unauthorized third party may have viewed your account information, including payment card data." [3]

This means that IT managers must proceed with caution. They need to carry out due diligence on any prospective IaaS vendor to ensure they know where security is provided and where there are gaps that they need to fill themselves. Also, organizations must be prepared to implement strong encryption on all of their data as an emergency failsafe in case their security controls fail to prevent a data breach.

Hybrid Cloud Service Models

Hybrid clouds, which are a combination of public and private clouds, enable mission-critical data to be maintained securely in the private cloud, while less critical data can be placed in the public cloud. The public cloud portion can also be used to provide additional computing resources as needed that do not involve mission-critical data. Hence, the hybrid cloud can present similar issues to those of public cloud and private cloud computing, with the added flexibility of being able to choose which type to use for various different resource, control, and security needs. Encryption can be a great equalizer here because if data is effectively encrypted, it may be storable securely in either a public or private cloud. This allows enterprises to select a cloud deployment based on resources and cost savings rather than based on security concerns.

Cloud Computing Threats

Introduction

Because cloud computing is founded on a virtual environment, the threats described above that apply to virtualization also apply in the cloud computing space. But in addition, extending virtualization to cloud computing causes the enterprise network perimeter to become more elastic. As cloud computing expands to cover data stored in private and public clouds and on numerous roaming mobile devices, new threat avenues are introduced and new approaches to securing data wherever it is located must be implemented.

Cloud security threats:

- Cloning and rapid resource pooling
- Motility of data and data remnants
- Elastic perimeter
- Unencrypted data
- Shared multi-tenant environments of the public cloud
- Control and availability
- How attackers use the cloud

Cloning and Rapid Resource Pooling

Whether in a private or public cloud, the on-demand nature of IT resources can create a glut of VMs, causing VM sprawl. Through the cloud self-service portals, VMs can quickly be provisioned. VMs can be reverted to previous instances, paused, and restarted, all relatively easily. They can also be readily cloned and seamlessly moved between physical servers. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it can be difficult to maintain an auditable record of the security state of a VM at any given point in time.

A risk was recently revealed when it was found that a pre-built machine image uploaded by a member of the Amazon Web Services (AWS) community that was made available for use by others on the service was found to still have the publisher's secure shell (SSH) key on it. This meant that the publisher in question could technically log in to any instance running that image. Although pre-built images can be a handy way of saving time and speeding the start-up process, this incident raised important questions about the potential security risks inherent in the use of shared pre-built images.

Cloud Computing Threats

Motility of Data and Data Remnants

In a cloud infrastructure, data is often moved to make the best use of resources. This means that enterprises may not always know where their data is located. This may be true in any cloud model, but is particularly true in the public cloud. To offer the best cost savings, businesses want service providers to optimize resource usage. But service providers generally do not provide any visibility into how resources are shifted to achieve this.

Also, if data is moved, residual data may be left behind that unauthorized users can access. Any remaining data in the old location should be shredded, but depending on the security practice, data remnants may remain. This can be a concern with confidential data in private clouds and any sensitive data in public clouds.

Elastic Perimeter

A cloud infrastructure creates an elastic perimeter. More departments and users throughout the organization can provision computer resources, and a cloud portal can also be extended to external sources such as partners. With this increased access also comes an increased risk of data leakage.

In addition, businesses are faced with managing and securing a diverse set of mobile devices, often acquired by the employee, not the business. With this trend towards consumerization, the cloud is often used for consistent access to applications and data on roaming endpoints. Businesses can also use the cloud to implement security on its employees' mobile devices. Security must provide a balance of flexible access and data protection.

Unencrypted Data

Unencrypted data is obviously a vulnerability for sensitive data. Data encryption helps address external threats, threats from malicious insiders, and the need for regulatory compliance. With data encryption, issues such as data remnants and an elastic perimeter become less relevant because even if data is accessed by an unauthorized user, it cannot be deciphered. However, many traditional encryption solutions can leave customers vulnerable in the cloud. If a solution does not provide policy-based key management with identity-based and integrity-based server validation, unauthorized servers may acquire the encryption keys and gain access to the encrypted data.

For example, in May 2011 popular file sharing service Dropbox was accused in a complaint to the Federal Trade Commission of using "a single encryption key for all user data the company stores." The concern is that if a hacker were able to break into Dropbox's servers and obtain the key, it could gain access to all of Dropbox's user data [4].

Cloud Computing Threats

Shared, Multi-Tenant Environments of the Public Cloud

The cloud security risks above can apply to both a private and public cloud. However, the multi-tenant architecture and provider control of the public cloud raises additional security concerns about who can see a business' cloud data, or who may be attaching to their storage volumes. And with these concerns comes a desire for visibility. Are businesses able to run reports that audit who has accessed their data?

Service provider staff should not view customer data stored within their service. However, in July 2010, Google fired an employee for accessing the customer data of its communication services users. In a statement, Google said, "...a limited number of people will always need to access these systems if we are to operate them properly – which is why we take any breach so seriously [5]."

One customer in a multi-tenant environment should not be able to access the data of another tenant. In an IaaS environment, service providers should configure hypervisors to create VM isolation between users. But as mentioned in the virtualization section, inter-VM attacks are possible, and even hypervisors are not immune to penetration by attackers. An example of this sort of vulnerability arose in early 2010, when Microsoft issued a security update to correct a vulnerability in Windows Server 2008 Hyper-V. The vulnerability allowed a user on one guest VM hosted by the Hyper-V server to run machine instructions that could allow denial of service [6]. In another example, in December 2010, a Microsoft misconfiguration error meant customers of the firm's hosted Microsoft Business Productivity Online Services Standard Suite (BPOS) could access and download data belonging to other users of the service [7].

Encryption is a critical safeguard in a multi-tenant environment, ensuring that service provider employees and other customers of the service cannot view a business's data. In addition, self-defending VMs can protect against inter-VM attacks and other vulnerabilities in an IaaS public cloud.

Cloud Computing Threats

Control and Availability

Using an on-premise data center or private cloud may give enterprises a greater feeling of control over their data, both in terms of security and availability. However, the enterprise may actually gain improved availability through a service provider that is dedicated to offering on-demand computing services through a public cloud. Such service providers can build out their cloud infrastructure to provide high availability and performance, supported by their cloud computing experts. Often this infrastructure and staff exceeds what an enterprise can provide in house. However, all data centers – whether in-house or through a service provider – can suffer outages. So, what happens when a major cloud provider suffers a major availability or security problem?

Amazon Web Services' (AWS) Elastic Block Store (EBS), which store Amazon Elastic Compute Cloud (EC2) instances, experienced an outage that lasted four days in April 2011. Amazon stated that 0.07 percent of the volumes in their US-East Region were not fully recoverable. The length of the outage, the fact that some data was lost, and the complexity of the outage, as subsequently explained in detail by AWS, caused much discussion in the industry about the incident. AWS has stated that it is treating this incident as an opportunity to improve its infrastructure, and other prominent Silicon Valley companies such as Netflix have published blogs on lessons learned from the outage [8].

How Attackers Use the Cloud

The previous sections discuss how attackers target business cloud deployments. However, attackers also use cloud computing to support their attacks. Computing resources of the public cloud can launch attacks. In a recent example, Bloomberg News reported that hackers used AWS's EC2 cloud computing unit to launch an attack against Sony's PlayStation Network and Qriocity entertainment networks. The attack reportedly compromised the personal accounts of more than 100 million Sony customers [9].

Also, in the multi-tenant environment of the public cloud, attackers can launch inter-VM attacks, installing their own VM and then infecting the guest VMs of other tenants on the same host machine. This type of attack can result in stolen computer resources for use in botnets or confidential data access.

Attackers also create their own clouds to disseminate resources. Botnets themselves are a form of cloud computing, pooling resources for criminal activities. And a growing number of tools are provided through clouds to help attackers, including Robopak's "Exploits as a Service" [10].

More Information

Virtualization and cloud computing eliminate traditional boundaries and perimeters in networks. And these new data center technologies must support consumerization with a widening array of devices to access data, including smartphones, tablet computers, netbooks, notebooks, and traditional laptops. Cloud security must accommodate these shifting usage patterns while supporting the infrastructure benefits of flexibility and cost savings.

Read about the security best practices that address the virtualization and cloud computing threats discussed in this report

To learn more about how to secure your journey to the cloud, visit www.cloudjourney.com

Follow these links for more information on specific security solutions for virtual and cloud environments:

- Security for Physical, Virtual, and Cloud Servers: Deep Security
- Data Protection Using Encryption with Policy-based Key Management: SecureCloud
- Virtual Desktop Security: VDI Solution Page

TREND MICRO™ | Securing Your Journey to the Cloud

About Trend Micro

Trend Micro Incorporated (TYO: 4704;TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud security infrastructure, our products and services stop threats where they emerge – from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

Please visit www.trendmicro.com

References

1. Goodin, Dan. "Web Host Hack Wipes Out Data for 100,000 Sites." The Register. June 8, 2009. http://www.theregister.co.uk/2009/06/08/webhost_attack/. 2. GoGrid. n.d. http://www.gogrid.com/about/. 3. Balding, Craig. "GoGrid Security Breach." CloudSecurity.org. March 30, 2011. http://cloudsecurity.org/blog/2011/03/30/gogrid-security-breach.html. 4. Schwartz, Mathew J. "Dropbox Accused of Misleading Customers on Security." Information Week. May 16, 2011. http://www.informationweek.com/news/storage/security/229500683. 5. Chen, Adrian. "GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)." Gawker. September 14, 2010. http://gawker.com/5637234/. 6. "Microsoft Security Bulletin MS10-010 – Important, Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894)." Microsoft TechNet. February 9, 2010. http://www.microsoft.com/technet/security/Bulletin/MS10-010.mspx. 7. Asprey, Dave. "Data Breach at Microsoft Highlights Security Problem in SaaS." Trend Cloud Security Blog. December 27, 2010. http://cloudsecurity.trendmicro.com/data-breach-at-microsoft-highlights-security-problem-in-saas/. 8. Chandrasekhar, Bharath. "Did Amazon's Aggressive Algorithms Prevent Customer Data Loss?" Trend Cloud Security Blog. http://cloudsecurity.trendmicro.com/did-amazons-aggressive-algorithms-prevent-customer-data-loss/. 9. Alpeyev, Pavel, Joseph Galante, and Mariko Yasu, "Amazon.com Server Said to Have Been Used in Sony Attack," Bloomberg News. May 14, 2011. http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html. 10. Asprey, Dave. "New Type of Cloud Emerges: Exploits as a Service (EaaS)," Trend Cloud Security Blog. April 7, 2011. http://cloudsecurity.trendmicro.com/new-type-of-cloud-emerges-exploits-as-a-service-eaas/.