Executive Summary

Many organizations have embraced cloud computing to host their data and applications. Still, cloud computing is far from perfect. On the contrary, serious security risks can be posed by moving data and applications from conventional enterprise data centers into cloud environments, especially public clouds.

Even in private clouds, organizations face increased risks posed by having multiple data sets and applications sharing the same physical server. This is particularly noteworthy when the data is sensitive, such as the personally identifiable information (PII) of customers or employees.

But in most cases, reasonable security measures can be taken to ensure that data and applications are safeguarded. This white paper addresses the ways that the enterprise can manage risk in cloud architectures.

It assesses the current state of cloud computing security and reviews the fundamental principles that an organization should follow when it comes to managing cloud risk. It also examines the types of controls most commonly needed for data and application security in the cloud.
The Situation

Cost savings are among the primary reasons that IT shops are turning to cloud computing. Organizations pay only for the services that they actually consume — such as storage, processing and network bandwidth — instead of acquiring and maintaining an oversized infrastructure that’s intended to handle peak needs, but far too large for typical daily needs.

This service model is particularly helpful when an organization has temporary needs, such as seasonal demand for a particular application and little or no demand for that application during the rest of the year. Such an application can be deployed within the cloud when needed at the appropriate level of resource consumption. For the rest of the year, hosting charges for the mostly idle application should be very low.

This setup can provide great cost savings compared with building an infrastructure to handle the seasonal demand and having it sit idle at other times. By sharing resources, cloud customers can financially benefit from each other.

Unfortunately, by sharing resources, cloud customers also put themselves and each other at greater risk of compromise. An attacker could exploit weaknesses in one cloud application to gain access to other applications on the same physical server.

Ideally, applications within a cloud are all logically isolated from each other. An attacker would have no way to “hop” from one application to another without first compromising the underlying infrastructure — the hypervisor — which is designed to be ultra-secure.

However, nothing is invulnerable, and hypervisor vulnerabilities can be exploited, endangering all the applications and data on that hypervisor’s server. Moreover, because many (possibly all) of the servers in a cloud environment use the same type of hypervisor, a vulnerability in one hypervisor likely means the entire cloud is at risk.

Visibility within the cloud also raises some security concerns. Once an organization’s application is moved from a traditional computing environment into cloud architecture, IT shops may not be able to monitor the application’s security to the same extent it did previously.

In many cloud deployments, organizations assume that the cloud provider is responsible for security. But often this security involves only the physical infrastructure and the cloud computing software (hypervisors and management software, for example). It does not include the security of the guest operating systems, applications, data or other organization-controlled resources running within the cloud.

Ultimately, the enterprise is largely responsible for the security of its own applications and data, regardless of where they are hosted. Cloud providers may be held partially responsible in some cases for security incidents where they were clearly negligent (such as failing to secure hypervisors). But it’s up to the enterprise to ensure that proper security monitoring, maintenance and incident response actions are occurring for their own cloud workloads.

Self-Hosted Private Clouds

Many organizations have chosen, primarily for security reasons, to use self-hosted private clouds instead of third party–hosted public clouds or private clouds. Self-hosted clouds typically are more expensive than third party–hosted clouds, but they offer superior control over security, because no part of the security responsibility or infrastructure is turned over to a third party. The IT shop has complete control over its cloud workloads, and thus it has full visibility into its cloud security.

The decision of whether to use a self-hosted private cloud, a third party–hosted private cloud or a public cloud is a complex one. Many factors must be considered in addition to security, such as cost, agility and flexibility.

The enterprise also must consider regulatory factors. For example, many organizations are subject to the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes–Oxley Act (SOX) or Payment Card Industry Data Security Standards (PCI DSS), as well as other initiatives that dictate, either indirectly or directly, which cloud architectures are acceptable for hosting particular types of data (for example, health information, financial information or medical records).

Considering the Cloud

When evaluating the risks inherent in cloud computing for a particular data set or application, it’s important to start with how the enterprise interacts with the cloud. The answers to just a few straightforward questions could dictate the use of a particular cloud architecture, not to mention highlighting important security issues that must be addressed before cloud migration:

**1. Does the application contain sensitive data?** Sensitive data generally refers to data that must have its confidentiality kept intact. Common examples include financial information, medical records and proprietary intellectual property.

Organizations also must consider the regulations to which they are subject. For example, an organization that maintains...
medical records is almost certainly subject to Health Insurance Portability and Accountability Act (HIPAA) regulations, which will affect its data security and privacy practices. Simply put, sensitive data needs greater protection than nonsensitive data. Thus, the more sensitive the data is, generally, the riskier it is to have in a cloud architecture (especially a public cloud).

2. Who uses the application? Is the application to be used by customers, business partners or employees? Where will these users be located (for example, anywhere on the Internet, within the enterprise only or on a few designated partner servers)? An application that’s going to be widely used is often a good candidate for migration to the cloud. An application that is used only by internal employees may be a better candidate for a private cloud deployment. Regardless of cloud architecture, any applications used only in particular locations (in the enterprise or on partner sites, for example) can benefit from firewalling and other controls that restrict access – preventing access by attackers and malware from other locations.

3. Does the organization need to transfer data between the cloud environment and the internal environment? Data transfer can significantly complicate cloud deployments, particularly if the organization conducts frequent, high-volume data transfers. For reliability, cost and other reasons, it may make more sense to keep such data and applications at the organization’s own facilities (perhaps in a self-hosted private cloud) instead of an externally hosted location. If a public cloud is used, IT administrators should factor in the overhead involved with securing the traffic – generally by encrypting the communication or passing the traffic through an encrypted tunnel.

4. Does the application demand high availability? In other words, does it truly need to be available all the time, with no scheduled outage windows? This may favor a public cloud architecture. If part of a public cloud has a systemic failure (due to such circumstances as a natural disaster, power outage or Internet outage), then another part of the same cloud at a different location could continue to make the application available. An organization might even want to use multiple clouds with different Internet service providers or electricity companies for additional redundancy.

Managing Risk

Over the past several years, approaches to addressing data and application security have changed significantly. Instead of focusing on securing the system, organizations now tend to focus on securing the data. Yes, the system still needs to be secured, but risk management methodologies are being employed to ensure that each type of data receives the security it needs.

Compare that with past security approaches that focused on system security only, and at best protected data through the use of access control lists (ACLs). Today, a wide variety of storage encryption technologies are in use, not to mention data loss prevention (DLP) technologies and other security controls that are specifically geared toward protecting sensitive data.
Application security has also changed over time. Many entities are just starting to recognize the threat that poorly secured custom-written applications pose to their data. Putting in extensive security controls for protecting the data isn’t necessarily going to matter if the application accessing that data is so riddled with vulnerabilities that anyone can readily steal all the data behind it. The focus of application security is really protecting the data behind the application. Application security can be thought of as a logical extension of data security.

Cloud Security and Data Security

It’s not surprising that cloud security is all about data security. The concept of “system” has become very fluid, with cloud workloads seamlessly transporting data and applications from one physical host to another, which may be running an entirely different operating system or no host operating system at all.

The security of the virtualization layer — the hypervisors — and the security of the guest operating systems running on top of the hypervisors are important. However, access to data is of paramount concern. This is why isolation is such an important concept to the cloud.

It’s important to ensure that each data set is kept logically separate from other data sets, and that corresponding applications are kept logically separate as well. That way a weakness in one instance of data and application security cannot be leveraged to compromise other data and applications.

In a cloud architecture, security policies must follow the data. When a workload is migrated from one server to another, the workload’s security policies must stay with it, along with the security controls. It does no good to protect data by using firewalls, DLP technologies or other means, only to have these controls unavailable or incorrectly configured when the data’s associated workload is migrated. And it does little good to implement security policies that don’t take the nature of the data to be protected into account.

Each cloud scenario provides a unique security situation. Its risks must be managed effectively. Organizations should avoid underprotection, where the data is not protected sufficiently. Likewise, they should avoid overprotection, in which money is squandered on security controls that are ineffective or potentially harmful to the organization (such as inadvertently blocking benign production activity). An effective risk management program minimizes both underprotection and overprotection.

Security Responsibilities

Third-party cloud providers (for both public and private clouds) are typically responsible for protecting only the physical infrastructure and the virtualization layer (the hypervisors). An IT shop that deploys organizational data and applications to the cloud should be responsible for securing them, as well as the guest operating systems underlying them, regardless of the cloud architecture and hosting model in use.

When thought of in this way, cloud security responsibilities are not much different than they are for a traditional enterprise data center. The operating system, applications and data must all be protected from attack; in particular, the confidentiality of sensitive data must be preserved. Plus, an organization

---

**Risk Management Primer**

Although IT staffers often think of risk management in terms of planning security controls, risk management is truly an ongoing process. The widely used, basic risk management process outlined by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800–39, *Managing Information Security Risk: Organization, Mission, and Information System View*, has four components:

- **Framing Risk:** This involves creating a risk management strategy that outlines how the other risk management components (assessing risk, responding to risk and monitoring risk) will be performed. Think of this as the planning phase of the risk management process.

- **Assessing Risk:** As the name implies, this component involves performing a risk assessment to identify threats, vulnerabilities, the likelihood that these vulnerabilities would be exploited and the potential impact of such exploitation.

- **Responding to Risk:** IT decision-makers must determine how each risk should be handled — such as accepting a risk or mitigating a risk — and then implement the appropriate responses. Examples of such responses include patching a vulnerability or purchasing an insurance policy.

- **Monitoring Risk:** In the monitoring component, a organization makes sure that the risk responses are maintained and looks for necessary adjustments to the risk response. For example, an IT shop might note the existence of a new vulnerability or a new threat that it considers substantial enough to merit an updated risk assessment. The risk assessment update, in turn, may trigger new responses to risk.
must rely on the cloud provider’s use of the proper security controls to prevent the cloud environment itself (physical infrastructure and virtualization layer, including hypervisors) from becoming a vector for attack, further complicating cloud security.

A cloud provider’s failure to live up to its security responsibilities could lead to a compromise for the enterprise, even if it follows sound risk management principles, implements all the recommended security practices and doesn’t directly contribute to the cause of the compromise. Once the damage has been done, customers, business partners and other affected parties generally don’t care if fault lies with the cloud provider or the organization. All they know is that they entrusted their important data to the organization, which ultimately failed to keep that trust intact. This is why many organizations are concerned about cloud security.

Data and Application Security Controls

Data and application security controls are necessary for assessing, responding to and monitoring risk in every environment, including cloud computing. These security controls can identify current vulnerabilities and threats, mitigate risks and identify changes to risk (such as a new vulnerability or an increased likelihood of a particular threat). Organizations using a cloud architecture — regardless of whether the cloud is public or private, and whether it is hosted by a third party or by the organization itself — should implement the data and application security controls discussed in this section as part of their defense-in-depth plans. Although traditional perimeter-based architectures may be obsolete, the old concept of defense in depth — having several layers of security controls working in parallel — is still an important principle for protecting data and applications.

General Threat Detection and Mitigation

Data and applications in cloud architectures face a variety of threats, such as malware and other attacks from adversaries. Known threats, such as malware that has been analyzed by anti-virus vendors, are relatively easy to detect and stop through threat detection and mitigation technologies. Unknown threats, such as customized forms of malware or attacks manually generated by a skilled attacker, are generally much harder to detect and stop. However, threat detection and mitigation technologies can still prevent many of them from succeeding. This section covers the most widely implemented threat detection and mitigation technologies.

Anti-virus Software

Perhaps the best known technology for detecting and mitigating threats is anti-virus software. Anti-virus software is primarily signature-based, which means that it looks for known characteristics of malware. It is very effective at stopping known malware but not good at stopping customized malware.

Anti-Malware Software

Anti-virus software falls under the larger umbrella of anti-malware software. Different anti-malware utilities are appropriate for various operating systems and applications. For example, rootkit detectors are well suited for Unix architectures. The advantage of using anti-virus software is that it can monitor many aspects of a cloud server for malware — everything from the file system and memory to incoming emails and file transfers.

Intrusion Detection and Prevention Systems

Another major category of threat detection and mitigation technologies are IDPSs. These tools analyze network or host activity for malicious behaviors and block any activity that is deemed harmful or overly suspicious.

An intrusion prevention system (IPS) typically uses a combination of signature-based techniques, to identify known attacks, and anomaly-based techniques, to identify previously unknown attacks. Some IPS technologies also use reputation-based techniques, such as IP address and website reputation scoring.

Anti-malware and IPS technologies may overlap in the threats they detect, but generally not by much. IPS technologies often focus on network and application protocols, unlike anti-malware software, which tends to focus on content.

File Integrity Monitoring

This software detects attempts to change sensitive files, such as operating system executables and password files. File integrity monitoring can work in two ways: preventative or reactive. Some file integrity monitoring utilities actually inject themselves into the file access process, so they have the ability to intercept and stop file change requests that should not be permitted, thus preventing compromises. Other file integrity monitoring utilities strictly work after the fact, scanning files periodically and detecting files that have changed since the previous scan.

Preventive technologies are preferable from an incident prevention standpoint. But both types of technologies can indicate that a threat may have already infiltrated the server and is attempting to gain a stronger foothold. Unfortunately, these technologies can also detect benign system changes, such as the result of patching. Still, file integrity monitoring software is very effective at identifying unauthorized system changes, and it is required by various compliance standards, such as the Payment Card Industry Data Security Standards (PCIDSS).
Data Loss Prevention
Another form of threat detection and mitigation technology is data loss prevention. DLP can monitor activities within a host, such as copy-and-paste between applications and outgoing network communications, to look for signs of sensitive information being copied or transmitted without authorization. DLP is effective at detecting both malicious actions, such as malware that copies sensitive files to a remote host, and inadvertent actions, such as an employee accidentally emailing a sensitive file to an external address. DLP can be used within a cloud environment to help ensure that sensitive data stays within the intended application and is not inadvertently or intentionally placed elsewhere in the cloud environment or outside the cloud altogether.

General Vulnerability Detection and Mitigation
While threat detection and mitigation technologies look for evidence of attacks, vulnerability detection and mitigation technologies look for and remediate known vulnerabilities in the operating system and applications. Every IT system has vulnerabilities, so both threat and vulnerability detection and mitigation technologies are needed to reduce the number of successful compromises. This section briefly reviews three common forms of vulnerability detection and mitigation technologies: patch management, configuration management and web application vulnerability scanning.

Patch Management
This software identifies missing patches in the operating system and major applications and ensures that the necessary patches are downloaded and installed at the appropriate time. Patch management software is often tied into a system that is used to validate, test and deploy patches throughout the enterprise, including cloud locations.

Alternatively, many operating systems and applications can be configured to update themselves. However, this can cause problems related to deploying untested patches and failing to ensure that patches take effect (for example, when a reboot of the operating system is needed to complete patch installation). Fortunately, these problems are less significant in the cloud, because workloads can be moved while a cloud instance is being patched, restarted or reconfigured.

Configuration Management
This type of software ensures that the operating system and major applications (such as security tools, web browsers, email clients and office productivity tools) are configured using secure settings. Configuration management software typically works by having a security baseline of approved settings.

The software compares the baseline settings with the actual settings on a host (such as a cloud workload) and reports any discrepancies, such as security settings that have intentionally or accidentally been disabled. Some configuration management software can also implement baselines on hosts, thus eliminating vulnerabilities caused by security configuration weaknesses. Security baselines are often recommended for cloud environments because they tend to be standardized.

Web Application Vulnerability Scanners
This surveillance software can survey an organization's web applications to identify weaknesses in their design and coding. If the applications can be accessed by the public, attackers can use the same scanners to find the same vulnerabilities, so organizations should run scans frequently — even continuously — to identify security problems in web application code.

Security Still a Significant Cloud Barrier

<table>
<thead>
<tr>
<th>Concerns with security of proprietary data or applications?</th>
<th>46% SAY YES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concerns with performance of cloud services?</td>
<td>32% SAY YES</td>
</tr>
<tr>
<td>Concerns with technical aspects of integrating cloud applications or infrastructure with legacy systems?</td>
<td>25% SAY YES</td>
</tr>
</tbody>
</table>

Source: CDW 2013 State of the Cloud Report, Survey of 1,242 IT Decision Makers

Communication Protection
The security controls for cloud data and applications discussed so far have focused on either eliminating vulnerabilities or stopping threats. Other security technologies — for example, communication protection tools — perform a blend of these two functions. Network communications must be thoroughly protected against a variety of threats by both eliminating known vulnerabilities in those communications and blocking known attacks.

Firewalls
The most common security control for communication protection is the firewall. Firewalling technologies have been in use on networks and individual hosts for many years to restrict both inbound and outbound communication.

Guest operating systems in the cloud should use host-based firewall technologies to allow only necessary communication, both inbound and outbound. This will minimize the “attack surface” that attackers may attempt to exploit. Also, firewalls should be configured to record blocked activity (through
logging) and to alert administrators when failures occur or suspicious activity is seen (for example, unusually high volumes of traffic, potentially indicating the start of a denial-of-service attack).

**Virtual Private Network**
The other primary security control for communication protection is cryptography. One example is a virtual private network (VPN), which creates a secure tunnel through which sensitive communication can pass. A VPN prevents attackers from eavesdropping on communication, particularly those carried over public networks (such as the Internet).

The most popular protocol for VPNs is IP Security, better known as IPSec. Another form of cryptography is Secure Sockets Layer (SSL), which has been largely replaced by Transport Layer Security (TLS). SSL and TLS are most commonly used to encrypt web traffic and thus to protect it from eavesdropping. However, these protocols are also used with email and other application protocols, and can be used with VPNs as well.

**Storage Protection**
An area of cloud data and application security that is often overlooked is storage protection. When data is accessed frequently, organizations may not think to encrypt it when stored. However, significant threats must be considered. One is physical security — the loss or theft of a physical cloud server.

If sensitive data resides on the server, it should be encrypted using full-disk encryption or an encryption product of similar scope so that the data cannot be recovered without proper authorization. Another threat is compromise within the guest operating system — if sensitive data is encrypted within the guest operating system (on top of the full-disk encryption), then a breach of the guest operating system won't necessarily compromise that sensitive data.

This discussion raises an interesting point: How can cryptographic keys be managed in a cloud environment? It may seem that an organization would need to turn over its secret keys to the cloud provider, but this isn't necessarily the case.

Most of the time, IT managers can maintain control over cryptographic keys. This is often necessary to achieve compliance with various regulations, because an organization that has shared its keys with others has lost accountability for the data being safeguarded by those keys. Advanced cryptographic techniques for key generation allow cloud providers to have only the necessary keys while leaving the “master” keys with the organization.

**Auditing**
Auditing — a final category of cloud data and application security controls — involves logging information about the security events occurring within a cloud instance and then analyzing that information to detect anomalous activities. Auditing is necessary for compliance reporting, which typically requires regular updates about security activities. This also allows an organization to keep track of who has been performing which actions. Auditing should cover not only user activities, but also administrator actions.

To gain the proper level of insight into cloud-based activities, IT administrators should perform auditing within the guest operating system, and often within individual applications as well, especially if those applications access sensitive data.

The audit logs should record all activity regarding access to sensitive data, including who accessed it, at what time, from what location and what action they performed (such as viewing data, modifying data or deleting data). This provides accountability and ensures a thorough audit trail, should it be needed for investigative purposes.

**Security Checklist for Data and Applications**

- **General threat detection and mitigation**
  - Anti-virus software and other forms of anti-malware software to monitor content and stop known malware
  - Intrusion Prevention System (IPS) to monitor network and application protocols and stop both known and unknown attacks
  - File integrity monitoring software to find evidence of compromise
  - Data loss prevention (DLP) to detect sensitive information being copied or transmitted without authorization

- **General vulnerability detection and mitigation**
  - Patch management software to ensure that missing patches are downloaded and installed properly
  - Configuration management software to verify and enforce compliance with a security baseline
  - Web application vulnerability scanners to continuously identify new vulnerabilities in web applications

- **Communication protection**
  - Firewalls to allow only necessary inbound and outbound communication
  - Cryptography to encrypt sensitive communication and thus prevent eavesdropping

- **Storage protection**
  - Full-disk encryption (or similar encryption technologies) to protect sensitive data at rest
  - Cryptographic key management to maintain accountability for safeguarded data

- **Auditing**
  - Logging within the guest operating system and individual applications
  - Analysis of logs to identify anomalous activities and provide accountability
CDW: A Cloud Security Partner That Gets IT

Keeping pace with cloud computing security isn’t a luxury, it’s a necessity. CDW offers a dedicated team of security experts, as well as dozens of solution architects committed to designing custom cloud architectures, cloud strategies, services and solutions.

We also have advanced technology engineers to assist with implementation and long-term management solutions. And CDW’s cloud portfolio includes more than 200 products spanning 36 categories.

Let us help you with the entire cloud computing lifecycle, from selecting which cloud models are best for your organization to simplifying the challenging process of migrating applications and data from your existing infrastructure to the cloud.

Our approach includes:
- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Telephone support, as well as product lifecycle support

Your CDW account manager and solution architects are ready to assist with every phase of choosing and leveraging the right solutions for your cloud security needs.

To learn more about CDW’s cloud computing solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/cloud

Citrix XenApp is a Windows application delivery system that manages applications in the data center and delivers them as an on-demand service to users anywhere. XenApp reduces the cost of application management, increases IT responsiveness when delivering an application to distributed users and improves application and data security.

As you migrate your critical data and applications to cloud-based and virtual environments, your security strategy must evolve too. Trend Micro cloud and data center security solutions protect your physical, virtual, cloud-based, and hybrid data center deployments without impacting the cost, efficiency, and agility benefits promised by advanced cloud and virtualization technologies.

McAfee Cloud Security helps organizations safely and confidently leverage secure cloud computing services and solutions. Rather than adopting the unique — and sometimes unknown — security practices and policies of each cloud vendor, McAfee Cloud Security allows businesses to extend and apply their own access and security policies into the cloud by securing all the data traffic moving between the enterprise and the cloud, as well as data being stored in the cloud.

Websense Cloud Web Security Gateway analyzes web content and detects threats with inline, real-time composite defenses. Global data centers are ISO 27001 certified and provide high availability, easy provisioning and lower costs for users in any location. An optional cloud-assist appliance can be deployed to improve local control over traffic flow to the cloud, ideal for deployment in countries with national firewalls.

CDW.com/citrix  
CDW.com/trendmicro  
CDW.com/mcafee  
CDW.com/websense

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW-G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT® is a trademark of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. Together we strive for perfection. ISO 9001:2000 certified 145533 – 140325 – ©2014 CDW LLC