CDW PEOPLE WHO GET IT

PLAYBOOK: OVERCOMING CLOUD SECURITY CONCERNS

While risks can hinder secure, successful cloud deployments, organizations can take concrete steps to protect data and applications.

Executive Summary

Numerous successful cloud deployments demonstrate that security concerns involving cloud computing can be overcome. While novices rank security first among their concerns about the cloud, organizations that are experts on cloud technologies rank security a distant fifth.

While security is an important consideration regarding cloud deployment, it's no longer a valid excuse for staying out of the cloud. Today, organizations must understand current cloud security weaknesses and threats, and be well informed about security controls to mitigate cloud risks.

According to the Cloud Security Alliance (CSA), there are nine major categories of threats that face cloud technologies. Organizations must weigh these threats as part of a rigorous risk assessment, to determine which security controls are necessary.

Without following this assessment process, IT leaders likely will waste money on unnecessary security controls. They also may miss some necessary controls, leading to an increased likelihood of data compromises.

Table of Contents

The Situation

Cloud computing continues to grow in popularity due to the efficiency, scalability and flexibility it can deliver to entities of all sizes and missions. The cloud has matured from an emerging technology into a proven delivery platform used widely throughout mainstream enterprises. The use of cloud technologies has many benefits, including enhanced agility, availability and collaboration.

Unfortunately, organizations looking to adopt cloud technologies face several potential barriers, including security, compliance, privacy and legal issues. Many organizations consider security to be the primary hurdle they face in their cloud use. To reap the benefits, IT shops must secure their sensitive data and applications before migrating them to the cloud.

Organizations must recognize the threats against their resources. They must also understand that cloud computing often presents an additional level of risk because critical services are being outsourced to a third party – the cloud service provider.

The cloud customer and the cloud service provider share responsibility for addressing security issues. The division of this responsibility is dependent on several factors, including the type of cloud services being used – for instance, Software as a Service (SaaS) or Infrastructure as a Service (IaaS) – the cloud deployment model (private, public or hybrid), and the terms of the contract between the cloud customer and the service provider.

Generally speaking, the cloud service provider is responsible for securing the shared applications and the organization workloads (including sensitive data), while the customer is responsible for access control and authentication, such as password management.

Organizations that migrate to the cloud still must pay attention to application and data security. In fact, a major cause of cloud security failure comes from customers assuming that the cloud provider has implemented security measures that it has not.

Security, Virtualization and the Cloud

Virtualization technologies are at the heart of cloud computing. Virtualization in the cloud most commonly refers to running an operating system in a simulated hardware and software environment.

This virtualized environment is isolated from all other virtual environments and is run on top of a strictly hardened hypervisor, which provides an additional layer of security. This isolation and hardening is necessary because, when using virtualization in a cloud environment, data and applications from multiple customers are likely to reside on the same physical server.

An exploit of one application or operating system instance should not lead to the compromise of other instances on the same server, and certainly not other servers. Keep in mind, virtualized guests are only as secure as their host system.

In a worst-case scenario, an attacker could potentially compromise a hypervisor, leading to immediate compromise of all the data and applications sitting on top of that hypervisor. However, hypervisor-based attacks have remained largely theoretical.

Cloud breaches are most likely to be caused by stolen user credentials (for example, passwords), human error or other causes. Accordingly, security experts recommend the use of data loss prevention (DLP) technologies to prevent intentional and inadvertent breaches of sensitive data in cloud environments.

Cloud Security Concerns

Several major security concerns are related to cloud computing technologies:

- **External data storage** – Sensitive data stored in the cloud, such as financial information, credit card numbers, medical records and educational records, may no longer be under the direct control of the organization. This poses significant concerns, not only in terms of ensuring the security of the data but also in complying with laws and regulations that govern the handling of such data. Some entities choose to store their most sensitive data locally, in private clouds or traditional data centers, because of the increased risk posed by hosting it in public clouds.
- **Dependence on the Internet** – Migrating applications and data that are primarily accessed by an organization's internal users to the cloud may actually hamper availability and reliability because these resources become dependent on the stability of Internet access. For applications and data that are accessed by Internet-based users, migration to the cloud may improve availability because of the redundancy that cloud service providers typically offer.
- **Lack of control** – The lack of control over cloud-based data and applications may force some organizations to avoid cloud deployment of some resources. Many cloud workloads are seamlessly transferred from one cloud location to another, which can create problems for some cloud customers. If these locations are in different legal jurisdictions, different security and privacy laws may apply. Organizations that migrate data to a public cloud provider also should consider the insider threat posed by the cloud provider's own employees. These employees may be able to gain unauthorized access to sensitive data without the organization being aware of it.

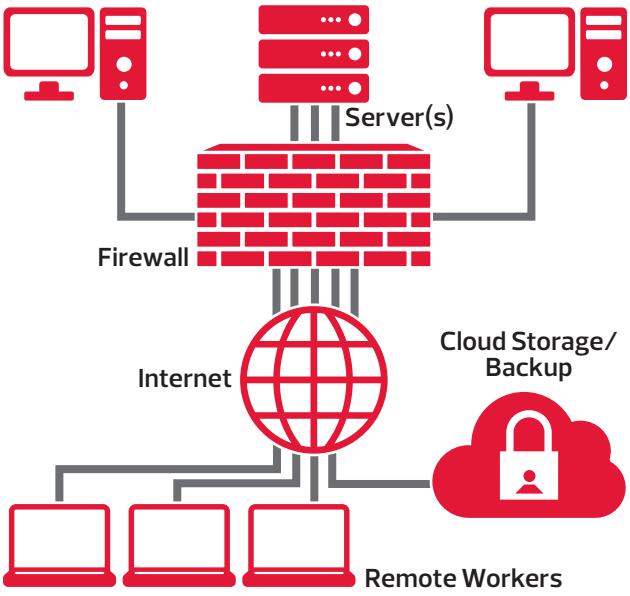
- **Multitenancy policy** – One of the principles of cloud computing is that data and applications from multiple customers may reside on a single server. Such multitenancy introduces additional risk, as an exploit within one virtual instance could allow a cyberattacker to take advantage of a hypervisor's weakness and exploit other virtual instances on the same server.
- **Integration with internal security** – It is increasingly common for resources placed in a cloud to "reach back" to internal security controls within the organization's traditional data center. Authentication services are a prime example. This allows the customer's users to be authenticated using a single method whether they are located on the Internet or on the organization's internal network. This reach-back capability exposes the internal security services to external usage, often putting them at additional risk of compromise.

Implementing Security Controls

Effective management of security in the cloud requires the use of a comprehensive set of complementary security controls. These controls may differ significantly from those normally deployed to a standard data center, because of the particular threats to which cloud environments are susceptible and the characteristics of cloud architectures.

Security controls serve several purposes. However, ultimately they are intended to reduce risk, either by lowering the likelihood of a successful attack or shrinking the potential impact of one.

Basic security with data storage and backup in the cloud



IT leaders should recognize that security controls cannot eliminate all risk. Even in the most highly secured environments, incidents may happen – due to human error, unknown vulnerabilities, malicious insiders and other causes. And, of course, many organizations are constrained by limited resources.

Security takes time and money, so organizations should spend appropriately based on their security needs. For example, high-risk applications and data sets should probably be more tightly controlled than low-risk applications and data sets.

The enterprise should select security controls for its cloud implementations through a robust risk assessment process. Such a process takes into account the unique characteristics of a particular implementation and prioritizes the security controls that are recommended to protect that implementation.

Organizations performing a risk assessment for security may wish to consider integrating it with other enterprise risk assessment purposes. Take note, security risk is by no means the only type of risk that an organization faces.

ISACA Security Control Types

Cloud security controls can be categorized in many ways. The IT security organization ISACA, a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance, defines four types of controls: deterrent, preventive, detective and corrective.

- **Deterrent Controls** – They simply discourage a casual attacker. They are not strong enough to prevent serious attacks. An example of a physical security measure would be a standard 6-foot chain-link fence around the perimeter of an organization's facility. Such a fence could easily be climbed by a determined attacker.
- **Preventive controls** – These stop an attack from being performed successfully. An example would be a 10-foot electrified fence with barbed wire on top. Although no preventive control is 100 percent effective, such a control is likely to cause attackers to seek other vulnerabilities that are easier to exploit.
- **Detective Controls** – They determine if an attack is underway or has been successful. To extend the fence example, a video camera might detect an unauthorized person walking on the grounds of a facility, inside the fence.
- **Corrective Controls** – They are used to reduce the impact of a successful attack. For instance, a guard with a guard dog patrolling the grounds of a facility. When notified that an intruder has been detected, the guard can act swiftly to intercept the intruder and prevent further compromise of the physical security of the facility.

Top Nine Threats of Cloud Computing

The conventional wisdom for securing computing technologies is to follow generally recommended best practices. Unfortunately, this does not necessarily take into account the current threats that computing technologies – cloud computing in particular – face today. It is increasingly important to assess the risk posed by current threats and ensure that an organization is employing the appropriate security controls to address that risk.

To help IT shops better understand threats against cloud technologies, the CSA conducted research to categorize these threats in order of severity. The alliance compiled the top nine threats, along with their implications to enterprise security and possible solutions to address each threat.

1. Data Breaches

Major data breaches have been reported at every type of organization: businesses, educational institutions, government agencies and others. Each data breach involves one or more unauthorized parties gaining access to portions of the organization's sensitive data.

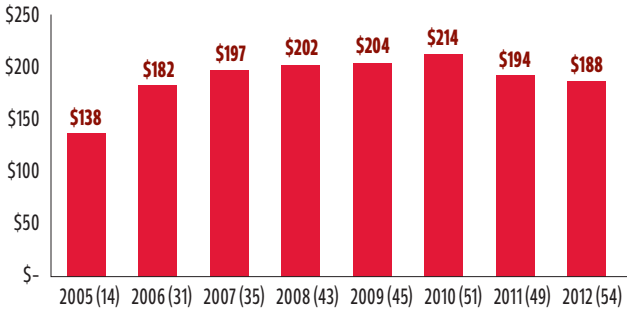
A data breach can be as small as a few customer files improperly accessed by a disgruntled insider. It can also be as large as a lost notebook computer containing millions of sensitive unprotected data records.

Of course, most data breaches fall in between these two extremes. But the cost of handling and recovering from a data breach is often much higher than organizations expect.

A recent study by Symantec and the Ponemon Institute reported that the average breach involves tens of thousands of records, with an average cost per record of nearly $200. By these figures, a breach of 25,000 records would cost an organization $5 million.

The average per capita cost of data breach over eight years:

Bracketed number defines the benchmark sample size.



Per capita cost is defined as the total cost of a data breach divided by the size of the data breach in terms of the number of lost or stolen records. Source: Ponemon Institute, May 2013

This underscores why breaches are such a concern: A single unmitigated security vulnerability or an innocent mistake by an employee could cost an enterprise millions, not to mention the damage to its reputation.

Most data breaches involving cloud technologies are not specific to the characteristics of those technologies. Usually, they involve human error, such as copying a sensitive database to an unsecured secondary storage location; or existing software vulnerability, such as exploitable bugs in the design and coding of a web application used to access sensitive data.

However, some security experts have expressed concerns about an increased likelihood of data breaches in shared cloud environments due to potential weaknesses in the mechanisms that isolate the cloud workloads from each other. Also, in cloud environments with applications shared among organizations, vulnerability in a single application could allow cyberattackers to access data belonging to other users of that application.

The primary control for preventing data breaches is establishing strong access control and authentication. By strictly limiting who can access sensitive data, an organization can significantly reduce the risk of that data being compromised.

One of the most common controls for accomplishing this goal is encryption. Effective use of this measure requires organizations to encrypt both stored data and data in transit. An organization that stores sensitive data in cloud environments should encrypt all such data. Further, it should keep all encryption keys in a different environment. If private encryption keys are kept in the same environment as the data they protect, then a single compromise could reveal both the keys and the encrypted data, allowing that data to be compromised.

Another major control for preventing data breaches is the use of data loss prevention (DLP) technologies. These are typically deployed within an organization's cloud workloads and networks to halt the unwanted usage and proliferation of sensitive data.

2. Data Loss

Data loss generally occurs when data that has not been properly duplicated and secured to protect its availability is lost, deleted or otherwise made unavailable. Unfortunately, data loss has become more prevalent in cloud environments because many IT managers operate under the false assumption that the cloud inherently provides superior protection for availability.

While clouds are fault tolerant and resilient, they do not sufficiently safeguard the availability of data. Possible threats against data availability include malicious attacks, human error (such as an employee accidentally deleting data sets or the loss of private encryption keys) and natural disasters.

The impact of data loss can be grave. The loss of critical data such as a customer database, patient medical records, financial transaction logs, proprietary designs or intellectual property would be devastating to any enterprise. All too often, these resources cannot be reconstructed easily, if at all.

Depending on the nature of the lost data, the organization may be forced to reconstruct it at great expense or to suffer the effects of losing such irreplaceable data. This could include the loss of customers, loss of reputation and customer lawsuits to recover damages incurred because of the lost data. A major data loss could even threaten an organization's continued operation.

IT shops must be aware of the risks of data loss, particularly in cloud environments, and act proactively to mitigate these risks. Cloud providers often state that they will take care of backups for their customers, but mistakes can happen and backups may not occur. Ultimately, a cloud customer must ensure that its data is being properly safeguarded through backups.

One effective technique would be to back up cloud data to a separate cloud from a different provider. Use of this technique greatly reduces the risk that the loss of one cloud would affect the status of another cloud.

Organizations can also choose to perform in-house backups of cloud data. Regardless of where the cloud data backup occurs, the entity likely would have to pay the cloud provider for the bandwidth needed to transfer data to the backup site.

Data Loss versus Data Breach

Data loss is sometimes confused with data breach. Unlike a data breach, which always involves an unauthorized party gaining access to sensitive data — an exploitation of confidentiality — data loss simply means that an organization's data has been deleted or overwritten, a failure of availability.

It is possible for a single incident to involve both data loss and a data breach, such as the only copy of sensitive data (which happens to be unprotected) being lost or stolen. To further complicate this distinction, some entities, such as the European Union, consider data loss to be a type of data breach for compliance purposes (such as the mandatory reporting to customers of a data breach).

In addition to backups, organizations should also be careful to safeguard their information through strong access control measures, such as requiring multifactor authentication for administrators and putting strict controls in place to prevent mass deletion of database records. These measures can help prevent accidental deletion of important data, as well as safeguard against an attacker gaining knowledge of passwords through malware, social engineering or other common techniques.

3. Account or Service Traffic Hijacking

This threat involves the practice of gaining unauthorized access to a user account or service, such as stealing a user's password and logging into a system as that user, or exploiting vulnerability in a service to gain access to that service. Hijacking is most often performed to gain access to sensitive data to which a user or service has access, or to perform actions under the user's or service's privileges.

Hijacking is a common attack technique in all environments. However, it can be particularly damaging in a cloud environment if administrator accounts are safeguarded only by a password. Gaining access to a cloud administrator's user account can allow an attacker to gain remote unauthorized access to all sensitive data controlled by that cloud administrator and read, modify or delete that data.

The result can be data breaches, data loss and even data modification, where the integrity of the data itself is compromised. This is typically unbeknownst to users and administrators.

Similarly, services with significant vulnerabilities may be publicly accessible because of their deployment in the cloud, putting them at extremely high risk of being exploited and granting attackers unauthorized access to the services. Organizations offer a wide variety of services through cloud technologies, greatly increasing the potential impact of these services being monitored, manipulated and shut down by attackers.

The methods for mitigating the risks from hijacking attacks are relatively straightforward. The major control for user accounts is enforcing strong authentication, especially multifactor authentication for all administrators, and even for users when feasible.

When this level of authentication is not feasible, organizations should employ strong, unique passwords that are changed on a regular basis. IT security professionals also should implement anti-phishing measures and other controls to prevent the theft of user passwords, although multifactor authentication reduces the need for these controls.

In terms of mitigating the risks from attacks against services, the primary security controls involve removing vulnerabilities from the services themselves. Keeping service software current through patching is important, and it is critical for enterprises to operate only currently supported versions of software. Developers that end support for their software no longer issue patches to correct serious vulnerabilities.

4. Insecure Interfaces

Software interfaces, such as application programming interfaces (APIs), provide access to cloud-based services by allowing commands to be issued against the service. Generally, some parts of an API allow for service usage, while other parts allow for service management. An insecure API can lead to compromises of both service usage and management, causing data breaches, data loss and other serious problems.

In enterprise environments, the security of APIs is sometimes a lower priority, because they are internal-facing, so that only authorized personnel can access them. However, in cloud environments, APIs are typically publicly accessible, at least to some extent, so they are more susceptible to attack. Also, exploitation of a management API can give a cyberattacker unauthorized access to a wealth of cloud resources with a single attack, making management APIs a particularly attractive target.

To mitigate the risks of API exploitation, it is important that access to these interfaces be strictly controlled. For example, access to management APIs should be available only from authorized administrator hosts or networks.

An organization also can reduce risk by requiring the use of strong authentication methods for API access. API communications should be strongly encrypted to prevent eavesdroppers from decrypting communications and either harvesting sensitive information or disrupting communications.

5. Denial of service

Denial of Service (DoS) attacks have been a threat against applications and services for many years. These attacks work by consuming resources, thus preventing legitimate users from accessing those resources.

Some observers erroneously believe that a DoS attack consumes all available network bandwidth. In fact, these attacks may consume many other types of resources, such as storage, memory and processing.

The good news about DoS attacks in the cloud is that cloud providers are often already prepared to thwart them. A DoS attack against a single cloud-based application can negatively affect other customers of that cloud provider, so it is in the best interest of the provider to be able to act swiftly to block common types of DoS attacks. The bad news about DoS attacks in the cloud is that, because costs for cloud services are typically based on resource consumption, a single DoS attack can cause an organization to incur high costs.

An obvious mitigation for DoS attacks is to work closely with the cloud provider in planning and executing DoS mitigation strategies. For example, intrusion prevention systems (IPSs) can be deployed at the cloud-provider level to detect and automatically respond to significant changes in usage patterns.

However, IT administrators must be aware that these systems may inadvertently block benign activity if it results in major changes in usage, such as a one-day special event that quadruples traffic to an application. It is often more effective to use an IPS in monitoring mode, so that it can generate alerts when it detects a possible DoS attack without automatically blocking that traffic. Administrators could then review the alerts and respond accordingly.

Other mitigations are directly available to cloud customers. For example, many applications can establish boundaries for resource usage, such as limiting storage space per user or limiting the number of concurrent connections from any single user account. These limits can reduce the potential effect of a DoS attack and ensure that a single user does not cause the organization to incur excessive charges related to resource usage.

6. Malicious Insiders

Malicious insiders are authorized personnel — users and administrators — who intentionally violate organizational policy for personal reasons, such as financial gain or revenge. Because they already have access to sensitive data, malicious insiders may readily cause data breaches, data losses and other negative effects. For example, an insider may copy a sensitive database onto a flash drive, then use the information stored on it to commit identity theft.

Malicious insiders represent a serious problem in cloud environments because the situation involves two sets of insiders — those from the organization itself and those from the cloud provider. Depending on the type of cloud services being used, the cloud provider's employees may have significant access to sensitive data controlled by the organization, which increases the risk from insider threats.

A combination of security controls may be needed to reduce the risk posed by malicious insiders. First, access to all sensitive data in the cloud should be strictly limited to only those personnel who absolutely need to have access, and all operations involving this data should be logged and audited.

Another critical element of security against insider threats is accountability. Organizations must know who is performing each operation involving the data, which can be accomplished by prohibiting shared accounts and requiring multifactor authentication for all administrators (preferably for users as well, if this level of security is feasible).

In an environment where accountability is strictly enforced, incidents involving malicious insiders are less likely to occur. And when they do, the guilty parties often can be identified.

Encryption and DLP technologies can also help reduce the risk posed by malicious insiders. Cloud customers should encrypt all sensitive data stored in clouds and make sure to safeguard the corresponding encryption keys internally. Placing the encrypted data and the keys together in the cloud creates a serious security risk, because an insider can more easily access both the data and key, thereby gaining access to the protected data.

DLP technologies can be effective at identifying attempts to transfer sensitive data over networks or locally, via copy and paste, use of removable storage devices or printing. DLP technologies can be configured to automatically stop such attempts, which would prevent insider attacks from succeeding and stop many inadvertent data breaches from occurring.

7. Abuse of Cloud Services

Abuse of cloud services involves parties taking advantage of cloud services to perform malicious acts, such as cracking passwords or launching attacks against other systems. Abuse of cloud services is a threat primarily affecting cloud service providers, not cloud customers.

8. Insufficient Due Diligence

Organizations that are considering the adoption of cloud technologies must fully understand the risks inherent in this step. An enterprise that does not effectively secure its cloud deployment to address the numerous cloud threats faces a significantly increased risk of compromise.

Organizations also must have a better understanding of cloud-centric risks and must perform full-fledged risk assessments before and after performing cloud migrations. There are significant differences in the threats faced by standard data center deployments and cloud deployments, and IT managers must address these differences when migrating data and services to cloud architectures. Otherwise, the confidentiality, integrity and availability of the organization's data and services may all be put in jeopardy.

9. Shared Technology Vulnerabilities

Vulnerabilities within the cloud infrastructure itself, such as hypervisor weaknesses or an application or service shared by cloud users from different organizations, also represent a threat. The risk of these vulnerabilities is that an attacker can exploit a weakness in one piece of software to gain unauthorized access to data and services for multiple cloud customers.

Cloud customers can do little to mitigate these threats, other than to choose the appropriate cloud model (public, private or hybrid) when migrating data and services to the cloud. For example, an organization might choose to keep its most sensitive data in a private cloud, which essentially gives it full control over the security of its cloud infrastructure.

Data that does not need to have its confidentiality preserved, such as publicly accessible data, is a better candidate for public cloud deployment. Organizations can also ensure that their contracts with cloud providers include requirements for how quickly the cloud provider will apply hypervisor patches and other updates to the cloud infrastructure to deal with severe vulnerabilities that could be exploited.

Overcoming Security Concerns

Organizations that are mature adopters of cloud technologies have been able to overcome many of the security concerns surrounding their use. A recent study by RightScale indicates that security concerns are decreasing among both organizations that are new to cloud computing and those that are heavy cloud users.

This suggests that IT leaders and other decision-makers understand that security issues can be overcome and that, in the long run, other issues tend to become more pressing. To be sure, cloud security is an important issue, but IT managers should understand that solutions are available to mitigate the risks.

Organizations should not automatically assume that a cloud deployment will be any more or less secure than a standard internal data center. In some cases, a cloud may offer better security than the standard alternative. An essential element of the decision-making process is understanding the nature of the data and services to be migrated to the cloud.

The sensitivity of this data and services should drive the determination of which cloud model is most appropriate. For example, highly sensitive data, to be used only by internal users, should probably be placed in a private cloud, not a public environment. Organizations often find it imprudent to deploy all their data and services in a single cloud model. Rather, employing a mix of models can better address both security concerns and operational requirements.

CDW: A Cloud Partner That Gets Security

Keeping pace with cloud security isn't just a luxury — it's a necessity. As a leading provider of technology solutions for business, government, education and healthcare, CDW offers a dedicated team of security experts who can help you boost productivity, regulate IT costs, enhance flexibility and drive innovation.

We can get you to the cloud, integrating your new solutions seamlessly with existing solutions. We can even manage your new cloud solution day to day, all while putting plans in place to enhance security and mitigate identified risks.

Your CDW account manager and our cloud client executives use the power of the cloud to boost productivity, regulate IT costs, enhance flexibility and drive innovation. As for selection, we offer a cloud portfolio that includes more than 200 high-profile 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 moving applications and data from your existing infrastructure to the cloud.

The CDW 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 and product lifecycle support

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

Check Point SOFTWARE TECHNOLOGIES LTD.

The Check Point® Intrusion Prevention System (IPS) Software Blade combines outstanding IPS protection with breakthrough performance at a lower cost than traditional, stand-alone IPS solutions. The IPS Software Blade delivers complete and proactive intrusion prevention – all with the deployment and management advantages of a unified and extensible next-generation firewall solution.

CDW.com/checkpoint

KASPERSKY lab

Kaspersky® Lab has the right formula for securing your virtual systems. Virtual machines aren't exempt from the dangers of cybercrime, malware and targeted attacks. Kaspersky provides agentless protection for virtual machines through a single, centralized anti-malware solution that can protect all virtual machines on a physical server.

CDW.com/kaspersky

SOPHOS

Sophos Cloud is based on the same technology that protects over 100 million devices worldwide. Security policies follow the user across devices, platforms and locations. One integrated, lightweight protection agent stops malware using multiple layers of protection, including web-exploit detection, sandboxing, HIPS, buffer-overflow protection and more. And it keeps your protection current using automatic updates and real-time lookups of suspicious files over any Internet connection.

CDW.com/sophos

McAfee® An Intel Company

As a cloud-based service, McAfee® SaaS Email Protection and Continuity delivers access to robust email security with no hardware or software to buy, no backups to run and no maintenance to perform — saving money and freeing up resources to focus on more strategic tasks.

CDW.com/mcafee

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT™