WHITE PAPER

CDW PEOPLE WHO GET IT

SOFTWARE AS A SERVICE

SaaS offers numerous options for gaining efficiencies and reducing costs.

Executive Summary

The principle behind software as a service (SaaS) is easy to grasp: It's client-server computing with a very thin software client. The user accesses applications that run remotely, often in a data center belonging to a service provider. There is usually no need to install or manage any software locally, as most of the functionality is accessible via web browser.

SaaS is often associated with the umbrella term *cloud computing*, a popular buzzword that encompasses a wide range of technology trends, including virtualization, multitenancy, outsourcing, automation, usage-based pricing, on-demand resource allocation and elasticity. One salient feature of the cloud is that it delivers its functionality — whether infrastructure, platform or software — as services rather than packaged and installed components.

TWEET THIS!

Table of Contents

Consistent with the basic notion of cloud computing, SaaS is a model whereby the customer organization licenses applications from a service provider and provisions them to its users as needed. The applications run on the service provider's infrastructure and are accessed through a public-network connection. They may be made available through the Internet as browser-based applications, or they may be downloaded and synchronized with user devices.

SaaS applications are centrally managed and updated. Typically, they are highly standardized, although they may vary in configurability, efficiency and scalability. The most common pricing model is a subscription plan based on the number of users, but there may be additional fees for transactions, bandwidth, storage and processing time.

There are many similarities between SaaS and the services offered by application service providers (ASPs) popular a few years ago. But there are also stark differences, namely in terms of technology, operations and billing, multitenancy, pay-as-you-go pricing, and the ability to provision on demand.

Why Consider SaaS?

Innovation is the core value proposition for software as a service. It is cost-effective, adaptive and secure. Above all, SaaS is easy to deploy, manage and use.

The multitenancy inherent in SaaS maximizes sharing and reuse of hardware, software and networking resources, and therefore results in higher efficiency and lower costs. The pay-as-you-go model, coupled with on-demand provisioning, enhances an organization's flexibility. And a high level of specialization by the service provider can translate into tighter security and better overall performance, thereby relieving the IT department from many of its onerous and nonstrategic housekeeping tasks.

Digging a little deeper, here are some of the key drivers for most organizations considering SaaS.

Financial benefits: The total cost of ownership (TCO) is often lower for SaaS than it is for an on-premise equivalent. In other words, when you add up hardware, software and facilities costs, it is difficult for all but the largest organizations to match the economies of scale and efficiency that a SaaS provider can achieve.

SaaS allows organizations to minimize expenditures for computer hardware and software licenses. In some situations, there may be less of a need to calculate maximum capacity or procure reserve hardware/software to accommodate usage peaks. And the organization may be able to reduce its focus on data redundancy for business continuity and disaster recovery capabilities.

Furthermore, in the SaaS model, implementation, administration and support costs are lower. Planning, piloting and deployment efforts are minimal. And software development, application maintenance and upgrades are handled by the service provider.

Flexibility: Cost isn't the only area where SaaS offers flexibility. It is much faster and easier to roll out, extend and update services that are delivered from the cloud. SaaS applications are designed to be easy to use, thereby minimizing training.

As a result, workers often accept and adopt SaaS applications more readily. If an organization wants to try before it buys, most SaaS vendors offer free trials that the organization can seamlessly convert to a production environment once it's satisfied with the solution.

With remote, zero-touch installation and configuration, IT staff doesn't have to undergo extensive training. Nor is there a need to prepare hardware, install operating systems and applications, fine-tune the configuration settings, and test the solution.

Once running, SaaS applications operate in a distributed environment where they have virtually unlimited resource pools. As an organization's application requirements change (in terms of users, data or tasks), the system can seamlessly allocate additional CPUs, storage and bandwidth to accommodate the enterprise without any degradation in performance.

Furthermore, SaaS provides better flexibility than many on-premise solutions because it is accessible from almost any Internet-connected device. Employees, customers and partners can access the service from their offices, homes or hotel rooms using anything from a PC to a tablet or smartphone.

Higher security, lower risk: In many ways, SaaS can improve data security. Many SaaS applications run in a browser and thereby expose little attack surface to hackers. Software and sensitive data are hosted in the provider's secure facilities.

Look Beyond the Price Tag

In cases where the price tag of a SaaS deployment is not immediately compelling, the process can still be attractive from a cash flow and budgeting perspective.

With SaaS, upfront capital investments in hardware, software and facilities turn into periodic service payments, an option that may be very appealing to finance managers. Pay-as-you-go pricing ties customer costs to usage, which lowers fixed costs.

And SaaS offers flexible licensing options, either at a flat rate per month or based on such measures as transactions, data volume or user count. The customer chooses the model that best fits the organization's goals, whether pursuing predictable costs or aligning expenses with fluctuations in revenue.

Tier 4 data centers, with their sophisticated surveillance, biometric access controls, structural barriers and tight physical perimeters, ensure a safe computing environment. And standards and certifications such as ISO/IEC 27001:2005 and SAS 70 validate sound operating procedures.

It would be costly for most organizations to provide the same level of data security, integrity and fault tolerance because they lack the SaaS vendor's economies of scale. The provider also takes care of important availability concerns such as backup, recovery and network management. And as part of their system monitoring, the SaaS provider commits to fixing any infrastructure problems and notifies customers when there are problems with the hosted applications.

Finally, the risks surrounding an unplanned exit are much lower, should an organization choose to go a different direction with its software needs. As there are no capital expenditures or other fixed costs, it is easy to reduce usage, switch providers or completely shut down the service without significant financial penalties or contractual disputes.

Better applications: In general, SaaS providers deliver newly developed applications. They are designed to be intuitive, as developers build on the added functionality of recent improvements. And they usually come with in-depth online help and online support services. Providers typically employ web analytics to observe user behavior, which they aggregate into a knowledge base that then drives specific enhancements in functionality and usability.

Because there is only a single instance of the software, it is always current. All improvements to SaaS applications are delivered continuously, at no cost, to the end user. SaaS vendors tend to fix bugs quickly and deliver innovative features in order to reduce their support costs and attract new users.

More focused IT: Outsourcing many of the mundane activities related to application deployment and maintenance frees up the IT department for more challenging activities that directly support the value of the enterprise. SaaS requires fewer resources for local support.

The tasks of upgrades, backup and troubleshooting become the responsibility of the vendor. Instead, the IT team can focus on technologies that deliver fresh value, improve performance or create differentiation in a certain marketplace.

Software Categories Ripe for Deployment

SaaS products are incredibly diverse and can leverage any number of web-based tools to meet application requirements. The best way to become familiar with SaaS technologies is to look at the types of software they represent, the range of business sectors they span, and the functionality they can deliver and scale on demand.

Collaboration: There are a growing number of web services that are delivered almost exclusively over the Internet. In fact, some of the most traditional applications, such as desktop productivity and conferencing programs, can benefit from a SaaS model.

E-mail is a popular first choice for organizations looking to outsource software. It's a mission-critical application, but seen largely as a commodity. So, if a provider can offer e-mail service with greater efficiency and reliability than an internal IT staff, organizations will consider it. Vendors, such as Microsoft with its Office 365 offering, have capitalized by offering services for e-mail, discussion and calendaring.

Conferencing applications, such as Cisco WebEx, Citrix GoToMeeting and Microsoft Live Meeting, also lend themselves well to SaaS. Holding a meeting on the Internet simplifies access control. It also makes it easier for users to join in from different devices and locations.

Security as a service: Network security is especially suitable for SaaS delivery because there is no need to share sensitive internal information with the provider. SaaS security providers offer a kind of shield between an organization's network and the Internet that can stop threats before they enter, thereby reducing resource demands for processing, storage and networking.

Security as a service typically acts as a gateway that filters and forwards network traffic. It might process e-mail, web requests or even instant messages.

As the service monitors this type of data passing through it, the provider's system can detect a variety of threats, from viruses and spyware to resource-consuming spam and phishing attacks. In some cases, security services may filter outbound content to prevent an organization from leaking sensitive internal information, or inbound content to protect users from external harassment or distractions.

Security as a service can also protect end-user devices (smartphones, tablets). Though such protection might require a local agent installed on devices, it's possible to host the management server and console with a provider to minimize infrastructure requirements and ensure that the system is protected even when it isn't connected to the network.

Availability as a service: SaaS-based data backup, archiving and recovery services, as offered by EMC's Mozy, Symantec and others, offer an intrinsic benefit over onsite alternatives in that the physical storage component is generally far removed from the organization and its users. As such, it is resilient and offers protection against natural disasters and other localized outages. Disaster recovery and continuity of operations are vastly improved.

IT as a Service

There is a booming market for IT applications that run in the cloud and are delivered as a service. SaaS-based offerings that facilitate service management are a logical choice for organizations that have no in-house platform.

Data integration is another compelling area of SaaS-based IT applications. Vendors and products such as IBM's WebSphere Cast Iron Cloud Integration and Pervasive Software provide integration services to connect on-premise or cloud-based applications at the data level.

Through web-based portals, IT clients can map data between different applications. Some services offer rich templates and prepackaged integration processes, as well as graphics workflow and business logistics development capabilities.

An additional benefit of backup and archiving services is that end users can access the data from a variety of locations and devices. There is usually no need for them to connect to the local area network to retrieve their information.

Operations applications: Organizations can obtain hosted versions of most of the applications they need for day-to-day operations, including accounting, payroll, HR, office productivity and customer relationship management. CRM is one of the best-known varieties of SaaS. By using SaaS for CRM, an organization can tap into and quickly scale functions such as account management, opportunity tracking and marketing campaign administration.

Human resources services, or human capital management, include support for recruiting, developing, retaining and motivating workers. Due to the confidential nature of the data involved, some organizations may be wary of accessing functionality outside the firewall. But a growing number (especially smaller ones) are willing to take on the risk of HR SaaS to capitalize on the cost-efficiency benefits.

Finally, there are several SaaS providers that offer on-demand financial applications for everything from inventory management, financial reporting and customer invoicing, to payroll, taxes, expense-tracking and bank statement reconciliation.

Vertical applications: A community cloud, running vertical-specific SaaS, caters to a group of organizations with a common set of requirements or objectives. The most prominent examples are government clouds that are open to federal and municipal agencies.

Similarly, major industries may have an incentive to work together to leverage common resources. Organizations operating in the same industry are generally subject to the same standards and regulations, and they often share customers and suppliers who may impose additional standards and interfaces.

Healthcare services, for instance, offer real-time patient surveillance systems and online pharmacy staff scheduling solutions. But there are also Internet-based transportation management systems that connect commercial shippers with couriers, ground express truckers and dedicated air charters. And in the retail and consumer products sector, there are technology and logistics service providers.

SaaS Adoption Challenges

Although there are compelling benefits to software as a service, past studies have shown that not all CIOs see its value. Some of their concerns can be attributed to bad experiences, or hype, or just a lack of familiarity with modern SaaS.

However, in fairness, there are also legitimate concerns and challenges that SaaS — like any new technology — brings with it. What follows are some of the deployment challenges an organization must tackle when considering SaaS.

Financial structures: When it comes to SaaS, zero capital expenditures and lower fixed costs may seem attractive, but there will probably be implementation and migration costs associated with moving to a SaaS platform. (Sunk costs in existing infrastructure may also serve as an emotional deterrent toward migration.) Another issue to contend with is the existence of contracts with service providers, which may preclude (or heavily penalize) early exits.

Confidentiality: A common obstacle to SaaS adoption is the fact that the service provider hosts sensitive data — potentially in a multitenant environment. The enterprise must trust that the host won't intentionally, or inadvertently, compromise its information. As part of the SaaS agreement, both parties should document who at the service provider can access sensitive data and under what circumstances, and all access to the data should be logged.

Integration and transition: There are numerous technical challenges an organization needs to address if it's considering a SaaS/cloud model. Integrating the networks in a reliable, scalable and secure fashion is no small task. There may be uncontrollable sources of latency or data transfer bottlenecks. And it can be hard to manage the encryption keys needed to protect all channels of communication.

It's also a challenge to integrate applications, which may need to connect across organizational boundaries. Again, security is a consideration, but there are also issues of interoperability and standardized interfaces.

It can be difficult to maintain data integrity when critical portions of previously synchronous activities need to be handled asynchronously. These challenges can be exacerbated

by the fact that a multitenant architecture usually means code is not customizable, so there is no way for an enterprise to create an ad hoc connection on its own.

Vendor lock-in: A lack of standardization among cloud-based SaaS solutions can lead to a situation where an organization can't move its data and services to another service provider without significant effort. This presents two potential drawbacks.

On the one hand, a provider has the customer organization at a disadvantage. The provider can push disagreeable terms on the customer because it has no viable exit strategy. On the other hand, if the provider goes out of business, the customer may have trouble finding an alternative. It can take considerable time, cost and effort to find a SaaS replacement and migrate all the organization's data.

Compliance: Organizations of all types must comply with rules and regulations. Healthcare groups must comply with the Health Insurance Portability and Accountability Act (HIPAA). Retailers, banks and others adhere to the Payment Card Industry Data Security Standard (PCI DSS).

And many government agencies follow internal and governmentwide regulations concerning everything from data security to records management. It's important to ensure that any SaaS solution deployed either adheres to the same regulations or offers ways to bring them into compliance.

Organizational change: Shifting functionality to the cloud essentially means outsourcing a service — and outsourcing usually has personnel implications. It doesn't necessarily mean that staff members who were performing the service internally are no longer needed.

However, it does mean that there may be a need to reassess their responsibilities and ensure that they continue to add value to the organization. This evaluation is an added burden of SaaS and in some cases may slow the adoption of a new technology.

Governance: If governance isn't taken into account, the organization may have limited recourse in the event a SaaS solution performs unreliably or doesn't scale to required capacity. A conflict of interest between provider and customer often begins with divergent objectives for isolation.

SaaS becomes cost-effective and lucrative to the provider when resources are shared extensively among customers, utilization is maximized and services are standardized. Yet certain organizations may want maximum compartmentalization of the provider's resources to help reduce risk; low utilization to ease bottlenecks; and a high degree of customization.

How SaaS Fits into a Software Portfolio

When examining applications that an enterprise may want to acquire via SaaS, it is important to understand the difference between applications that are already running locally and might fit the SaaS model, and new SaaS-only applications that run in the cloud.

Looking at their existing software portfolios, organizations have several options. They can transition certain applications to public services, or they can replace them with entirely new, cloud-based SaaS solutions that provide similar functionality or help solve the same operations problem.

Alternatively, perhaps as an in-between solution, an enterprise might want to modernize existing applications according to service-oriented principles. This provides a high degree of flexibility for transitioning to a SaaS model in the future.

In some situations, it might make sense simply to retire an existing application because it's no longer necessary or doesn't add sufficient business value to justify investment in licensing and support, regardless of the delivery model. Or, the organization may decide to the leave an application running as-is.

The opportunity to pursue SaaS is greatest when new applications are needed where no legacy functionality exists. In these situations, SaaS must still fit a business case. From a technical perspective, the primary decision will be whether to host the SaaS application internally, in a partner or public cloud, or in a hybrid constellation that involves multiple providers.

Business Criteria

The most obvious place to begin an application assessment is with the financial impact that moving to a cloud service will have on the enterprise. Applications vary in their ability to leverage cloud benefits. If the workloads are constant, there will be little performance advantage to resource pooling. On the other hand, if demand is volatile and processing is highly dynamic, then there is a high potential for flattened utilization.

Even if virtualizing an application into a service is attractive, there is still the question of whether the operational benefits can be achieved internally rather than in a public cloud. This will depend on several factors.

If load demands are counter-cyclical to the resource demands of other internal applications, a private cloud may be sufficient. In other words, if the application tends to peak when other software is running idle, then there is a good opportunity to share internal resources.

Site Unseen

SaaS providers don't usually allow customers into their data centers or offer detailed insight into their operations. This represents a huge risk for some organizations. To establish trust, SaaS vendors may submit to audits or obtain recognized certifications, such as SAS 70 Type II, ISO/IEC 27001:2005, NIST Special Publication 800-53, FIPS 199-200, WebTrust, SysTrust and SCP. These help ensure that the operation is secure and reliable.

It's also a good idea for potential SaaS customers to assess analyst reports and consider what current customers have to say about the service. A strong industry position with a loyal base of users is usually a good sign that the vendor delivers as advertised.

Obviously, one significant financial consideration is the cost of managing the application. The administrative costs may decrease as a result of outsourcing, but the benefit could become diluted if the challenge of integrating the application with internal systems offsets some of the reduced responsibilities.

Support costs may also be affected if a cloud-based SaaS provider takes over the back-end support of a hosted application. Users will probably still call the same internal help desk when they have problems with the SaaS program. Depending on the organization's IT skills, the help desk will have to decide whether to troubleshoot or refer incidents for resolution.

Technical Criteria

The architectural design and technical implementation of a services-based application can affect the organization's ability to move it easily into a public, highly distributed environment. Some of the technical criteria to consider includes the following.

Service-oriented architecture: If the application already implements a high degree of service abstraction, reusability and composition, it is much easier to migrate to a service-oriented environment and leverage the benefits that existing services can provide.

Customization: Public services are notable for their dependence on standardization to achieve operational efficiency. Clearly, some degree of customization will be needed in order to accommodate the diverse requirements of different organizations. However, if code and configuration are maintained separately, maintenance burdens will be reduced and the agility of developers will be maximized as they add and change functionality.

Application independence: A high degree of interconnectivity between applications makes it difficult to transfer one or more of them to different service providers. On the other hand, isolating the interactions and ensuring that all requests use standardized interfaces make the applications much more versatile. Consider all the interfaces (web APIs) that may be needed or leveraged and verify whether, and how, they will work when the application is moved or transformed to SaaS.

Loose coupling: Loose coupling and tight cohesion are important architectural principles that carry many benefits. In addition to the number of connections and interfaces among applications, it is necessary to look at the context and implications of each.

What will be the effect if applications experience high and unpredictable latency? How will they perform if network bandwidth suffers a bottleneck? If network conditions affect response times or transaction reliability, then geographically distributing the application may not be wise.

Horizontal scalability: The trend in the industry is toward scaling out (adding more systems/CPUs/cores) rather than scaling up (expanding on existing systems). Computational requirements continue to increase as CPU clock speeds have held steady. As a result, organizations need to look at how they can break up their applications into parallel workloads so that multiple cores, processors or systems can work together to increase performance.

Redundancy: A main tenet of SaaS and cloud computing is better reliability through high levels of replication. The software code can take responsibility for redundancy in one of three ways: It can rely on the provider's platform and infrastructure services to guarantee replication, it can call upon replication services, or it can explicitly duplicate data by storing it in multiple repositories.

Tolerance: A cloud-based environment is uncontrolled and chaotic compared with a single system or private network. As mentioned earlier, network connections can be unstable. Furthermore, underlying data sets may not be fully synchronized, and component services may be unreliable or return incomplete, inaccurate or obsolete results.

Some applications are more tolerant of imprecision than others. An inventory management system will quickly lose its value if there is no two-phase commit, a feature of transaction processing that guarantees system integrity. On the other hand, analytics and search applications can accommodate reasonable amounts of invalid content and still deliver valuable results.

In a Public Cloud

Obtaining software services from the public cloud is relatively easy. The provider does all of the heavy lifting. The biggest design decision the customer organization needs to make is which provider to select. This means getting a good view of the market and finding the best match between internal

requirements and the array of services offered. If an enterprise is in the market for a public cloud to run its SaaS, it should consider several things.

Functionality: This is the most obvious place to begin an assessment. Unless there is an approximate match between what a SaaS provider offers and what the organization requires, there is little point in evaluating further. There may be some customization options, but due to the multitenant model, they're usually very rudimentary.

Integration with existing applications and infrastructure is another functional consideration. How will the customer connect with other systems or migrate data and users? Some providers have flexible connectivity options and migration tools. In other cases, customers will need to develop these themselves or find a third party who can supply them.

Performance: An important extension of functionality is reliability. Key performance indicators include the availability of the service, response times and the accuracy or the information it delivers. Ideally, all SaaS resources would be error-free, available 100 percent of the time and lightning fast. In practice, however, no SaaS provider can achieve perfection. The question of how much margin to allow for is largely a business decision.

For example, it is common to describe service availability in terms of "nines." Five nines (when the software service is up 99.999 percent of the time) is a very ambitious objective, one that typically can only be achieved under tightly enforced conditions. SaaS providers may technically be able to offer such service levels, but an organization has to ask itself and the provider, "At what price?"

The cost of each additional nine can increase exponentially, even though the difference between four nines and seven nines is less than one hour of downtime per year (which is insignificant for most services). Still, it is important to match the business costs of downtime (for example, the revenue impact of order-processing applications or implied liability for consumer-facing services) with the cost of improving uptime.

Contracts: Regardless of advertised performance metrics, what really counts is what is spelled out in black and white in a SaaS contract. Many services use click-through contracts to mandate standard terms and conditions to keep their costs low. However, large organizations often have a mechanism for requesting small modifications in exchange for a significant purchasing commitment.

The portion of the contract that stipulates performance thresholds is the service-level agreement (SLA). It defines the scope of the services, maximum downtime and other performance metrics. Most important, it should also specify the penalties for noncompliance and the jurisdiction for any disputes.

Less obvious areas to examine in SaaS contracts are the exit clauses, including how an organization can opt out of the deal if the service doesn't meet stated requirements, and any assurances that the provider will preserve the confidentiality, integrity and availability of the customer's data.

Trial periods: In many cases, SaaS vendors will offer a trial of their services at no cost. Even when that's not an option, it is advisable to run a pilot program before launching a production service. Testing ensures end-user acceptance, proper configuration, integration with existing infrastructure and services, and reliable management and support from the provider.

In a Private Cloud

Even though the public cloud promises numerous advantages for running software as a service, it can present a major cultural and technical change for small and large organizations that may prove to be too big a hurdle. Many SaaS customers prefer to see (and directly control) their IT assets, especially if they've invested significantly in their current infrastructures.

A private cloud is an attempt to replicate the benefits of cloud computing by pooling and optimizing internal resources in a similar, shared infrastructure, thereby reducing some of the risks associated with public services. The term *private cloud* is disputed in certain circles.

Many argue that anything less than a full cloud model is not cloud computing at all, but rather an extension of the current enterprise data center. Nonetheless, the term has become widespread, and the services it can support can prove useful to organizations.

A private cloud is typically hosted on-premise, scales only to hundreds or thousands of nodes (as limited by the computing resources the organization devotes to its private cloud), and is accessible only over private network links. Because all applications and servers are shared within the organization, the notion of multitenancy is minimized.

Still, as in a public cloud model, a private cloud and the software services it hosts benefit from centralized management, ease of deployment, a degree of application elasticity and other features, such as the ability to "charge" departments for software services they might otherwise take for granted, including e-mail.

Implementing a private cloud is also a good way to start on a journey toward the public cloud. Organizations can break down that journey into steps that deliver increasing efficiency along the way.

Resource efficiencies: Usually the first objective of a private-cloud implementation, standardizing components sets the scene for data center consolidation and optimization. Each level of resource abstraction, from server virtualization to

full multitenancy, increases the opportunity to share physical capacity and reduces overall infrastructure needs.

Operational efficiencies: Human labor is one of the highest cost factors related to information technology, and as such is the next target for deriving efficiencies. Ideally, all systems are self-healing and self-managing.

This implies a high degree of automation and end-user self-service. In addition to reducing administrative costs, operational efficiencies enabled by cloud and SaaS computing models support rapid deployment of new services and functionality.

Sourcing efficiencies: This is the final step in creating a cloud to host an enterprise's SaaS. Once the infrastructure reaches this level, the enterprise is likely ready for a possible move to the public cloud. Sourcing efficiencies represent the flexibility to provision services and allocate resources, from multiple internal and external providers, without modifying the enterprise architecture.

This agility can only be attained if all systems adhere to rigorous principles of service orientation and service management. The systems also must include a defined governance framework, fine-grained metering for cost control, and a granular, role-based authorization scheme that can guarantee confidentiality and integrity of data.

On the plus side, once an organization reaches this level of efficiency, applications will offer a nearly infinite elasticity of resources, and cost can be reduced to the minimum that the market has to offer. Once organizations achieve full sourcing independence, they can be flexible in terms of where they procure their services.

They can continue to obtain them from their own IT resources, or they can switch to an external provider that may be more efficient and reliable. It's simply a question of moving at the rate at which the organization's culture can absorb and embrace.

Microsoft®

Microsoft® Office 365 is a subscription service that combines the familiar Microsoft Office Web Apps with a set of web-enabled tools that are easy to learn and use, that work with your existing hardware, and that come backed by the robust security, reliability and control you need to run your organization. Everyone can work together easily with anywhere access to e-mail, web conferencing, documents and calendars.

CDW.com/microsoft

Symantec™

Symantec™ Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver a powerful defense against malware for notebooks, desktops and servers. It delivers the most advanced technology available to protect against today's sophisticated threats and threats not seen before. It includes proactive technologies that automatically analyze application behaviors and network communications to detect and actively block threats. It also provides device and application control features to manage actions and secure data. Symantec Endpoint Protection seamlessly integrates these essential security capabilities in a single agent that is administered via a single management console to reduce the costs, complexity and administrative overhead associated with managing multiple endpoint security products.

CDW.com/symantec

TWEET THIS!

CDW® PEOPLE WHO GET IT™