Entrust®

IS THE CLOUD READY TO MANAGE SECURITY?

Far from just being a storage space, the cloud is a resource that's changing the very nature of business. It can be leveraged to broaden the sphere of enterprise operations, as well as bolster the efficacy of business transactions and improve company-client relations. The mobility built into the cloud means that organizations of all sizes can enjoy a business world without limits.

But is cloud technology mature enough to manage security? This white paper explores the question and points to real-world use cases where the cloud is applied to reduce costs, improve security and protect users.

White Paper:

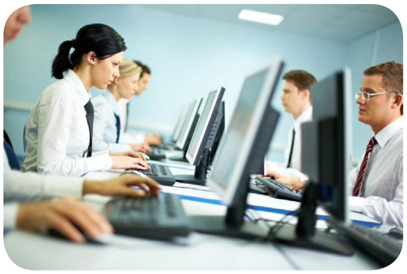
IS THE CLOUD READY TO MANAGE SECURITY

CONTENTS

IS THE CLOUD READY TO MANAGE SECURITY?

Far from just being a storage space, the cloud is a resource that's changing the very nature of business. It can be leveraged to broaden the sphere of enterprise operations, as well as bolster the efficacy of business transactions and improve company-client relations. The mobility built into the cloud means that organizations of all sizes can enjoy a business world without limits.

But with the cloud's growing popularity comes security concerns, which mainly arise from a perceived relinquishing of control on the part of companies. After all, if an enterprise places its data with a third party, how can it guarantee the safety of that information? But an examination of cloud computing puts these fears to rest, illustrating how a virtualization of your enterprise platform actually boosts protection and makes for better business all around.



"Unlike an in-house IT structure — which can be bogged down by technological complexity — the cloud is easily navigable, and its applications are built to be used by everyday employees instead of just IT staffers."

A GENERAL SHIFT TO THE CLOUD AMONG BUSINESSES

The cloud has experienced massive growth in the past few years. According to an Eclipse infographic, the global cloud market was worth roughly $46 billion in 2008. By the end of 2014, that number is expected to have grown to more than $150 billion.

Much of this growth is due to widespread cloud migrations among enterprises. A report released by QuoteColo stated that more than two-thirds of IT staffers currently harness cloud apps and services, while half of companies in the U.S. are planning to boost their cloud budgets in 2014.

To enumerate all the reasons businesses migrate to the cloud would take up far more space than this report permits. But there are several key benefits that serve as a driving force behind almost every enterprise migration. One is the ease with which a cloud platform can be managed. Unlike an in-house IT structure — which can be bogged down by technological complexity — the cloud is easily navigable, and its applications are built to be used by everyday employees instead of just IT staffers. To detractors who argue this accessibility complicates internal identity management, the option to use Single Sign On (SSO) solutions and federated security schemes helps organizations scale authenticated identities across multiple, usually connected, applications.

Another central cloud advantage is the return on investment. According to the QuoteColo report, 84 percent of respondent CIOs said they were able to reduce application costs after shifting to the cloud. Among other things, these savings result from not having to shell out money for hardware, being able to consolidate company IT departments, and having a scalable infrastructure that grows alongside your enterprise, Imagine IT reported.

"84 percent of respondent CIOs said they were able to reduce application costs after shifting to the cloud."

IS THE CLOUD REALLY A PLACE OF RISK?

Despite the myriad benefits of a company cloud migration, the prospect still leaves some businesses uneasy. The notion of moving private data outside the corporate wall can seem, on the surface, to present security hazards, particularly in an age of rampant cyberthreats. The ever-expanding presence of malware in the virtual realm is undeniable. In 2013, an average of 315,000 new malicious files emerged every day, Arellia reported.

But far from elevating a company's chance of attack, the cloud is typically just as secure as on-premise deployments. It is, however, as enterprise computing expert Dave Lithicum points out, important to "educate those in enterprise IT around the real issues and the real risks. Indeed, I've been finding that clouds are more secure than traditional systems, generally speaking."

The reason for this is simple: cybercriminals don't discriminate when it comes to on-premise versus cloud environments. Both platforms are targets.

Because of the widespread nature of cyberthreats, the single most important step in any company's cloud deployment strategy should be securing its virtual infrastructure. Without a secure cloud environment, a business is basically asking to be attacked.

CLOUD COMPUTING: A PROACTIVE DECISION TO BOLSTER SECURITY

A company migration to the cloud not only ensures better enterprise security, but it also makes the security structure far easier to navigate. Because of this, management is spared the onerous task of acclimating to and controlling an on-premise system. With security placed in the hands of a capable cloud provider, management can turn to the more important work of building a better business.

"Healthcare cloud computing could lead to a projected $11 billion in IT savings over the next three years."

CONSOLIDATION OF PLATFORMS

The modern workplace harnesses many different technological platforms to execute business objectives. With the mounting presence of BYOD policies in offices across the globe, employees' personal computing devices are part and parcel of everyday business. But if these devices are to access the company network, they must be secured with the same rigor as in-house equipment.

For a business that's not in the cloud, the prospect of this kind of maintenance presents a managerial headache. Fortunately, cloud-based identity access management (IAM) is designed to ensure that enterprise computing is secured across the board, regardless of its originating platform.

REDUCTION OF COSTS

In the cloud, strong security can come with a relatively cheap price tag, a drawing point that has proven hugely beneficial for the healthcare sector. As an Innotas informational graphic pointed out, hospitals — which oversee sensitive private patient data and, therefore, have stringent security needs — are increasingly turning to the cloud to provide the defensive infrastructure that in-house IT no longer can. And it does it at a much lower cost: According to HealthcareIT News, healthcare cloud computing could lead to a projected $11 billion in IT savings over the next three years.

SOLUTION TO SUBPAR SECURITY MEASURES

The repercussions of a breach are amplified immeasurably when it is discovered that the infringement happened because of failings in proper encryption and identity protection. Unfortunately, many small enterprises lack the IT staff and public-key infrastructure skilled labor to keep a breacher out, and therefore suffer a tarnished reputation and public scrutiny in addition to other consequences from a malicious encroachment.

The cloud presents a cost-effective means of solving that problem. With a robust cloud platform, a company does not have to worry about the potentially insurmountable fallout of a breach.

Some would argue that malicious infringements on cloud platforms occur with as much frequency as other attacks, but a look at the numbers reveals that the vast majority of such incursions take place in the public cloud. A 2013 security report by the Cloud Security Alliance, for instance, found that 56 percent of non-transparent cloud attacks occurred among the top three public service providers.

In a paper prepared for the 2013 Symposium on Information Assurance, Gehana Booth, Andrew Soknacki and Anil Somayaji pointed out that an important distinction must be made between the public cloud—which is built for general use and harnesses an open, and therefore inherently vulnerable, structure—and the private cloud, which is a dedicated platform meant for use by a single entity with direct connection (as opposed to Internet connection) and likely operated with the enterprise in mind.

The tendency to conflate these two separate clouds lead to the misconception that the private cloud is somehow unsecure.

DIFFERENT WAYS THE CLOUD CAN BE DEPLOYED

In order to best understand the cloud, it is worth comparing it to the alternative: on-premise enterprise deployment. According to BetaNews' Derrick Wlodarz, many businesses are attracted to on-premise solutions because of a false notion that this option will somehow be cheaper than cloud computing. But in the long run, virtualizing a company's infrastructure is always going to be the more economical option, since an on-premise solution comes with many costs that the cloud simply doesn't have, such as expenditures for new hardware, software and in-house labor fees.

However, when discussing the cloud, it can be tempting to think of it as a single entity — one vast sphere of activity in which all virtualized data exists. But this is actually not the case. The cloud simply provides a different channel for deployment. The variety of options available for cloud migrators can make for a much more individually tailored enterprise cloud experience.

"The variety of options available for cloud migrators can make for a much more individually tailored enterprise cloud experience."

SaaS:

Software-as-a-Service allows customers to access a range of applications that are supplied by their cloud service provider, according to TechTarget. What makes this delivery model so appealing is that it provides an easy portal through which customers can use commercially available software to strengthen business operations, thereby dodging separate costs for in-house software options. Because SaaS provides its users with across-the-board compatible software, the platform enables easy collaboration within the office, and even between businesses. A popular example of SaaS is Microsoft Office 365, which offers a full package of office application deployments.

IaaS:

Infrastructure-as-a-Service is like a big virtual closet for businesses, providing a space into which companies can store information and not have to worry about it cluttering up their office space. As savvisdirect points out, IaaS assumes the role that a company's hardware solutions typically would. If, for instance, a business switches to an IaaS platform, then they can finally do away with that data center in the basement that's been guzzling up HVAC costs and driving electric bills through the roof. One of the great benefits of IaaS is that it's highly scalable, offering the ability to easily grow with your enterprise, no matter how large it gets. Rackspace is a good example of a typical IaaS offering.

"Within the enterprise cloud it becomes easy to oversee certificate management."

PaaS:

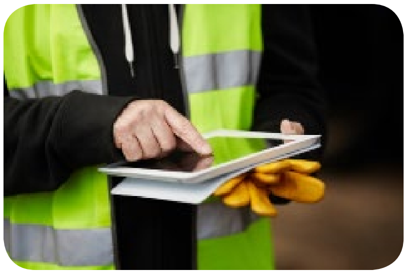
It's helpful to think of Platform-as-a-Service as something of an offspring of SaaS, according to TechTarget. What PaaS does is allow users to rent things like storage, network capacity and hardware. This option is great for transient business operations — say, for example, a pop-up tech store that's testing the waters in a new city. Google App Engine, a platform used by many popular app developers, is one of many PaaS options out there.

Authentication & Federation Services:

Traditionally, federated services were leveraged to securely connect on-premise identity controls to cloud-based applications. Today, however, they're widely used to safely facilitate cloud-to-cloud and mobile-to-cloud access to cloud identities and applications. Federation and other similar identity authentication services have moved beyond enterprise SAML to newer uses like Open ID, Open ID Connect, WS-Federation and OAuth 2.0.

TYPES OF SECURITY SOLUTIONS YOU CAN MANAGE IN THE CLOUD

Enterprises are not limited when it comes to managing security in the cloud. Here are a few of the different solutions:



"Fortunately, the private cloud provides exactly the identity protection measures that law enforcement officials need."

SSL:

Within the enterprise cloud it becomes easy to oversee certificate management, which is a process that otherwise could prove highly cumbersome for businesses. With centralized digital certificate management (Entrust IdentityGuard Cloud Services SSL, for example), companies no longer have to worry about the burdensome work of watching over a multitude of different certificates, and can instead consolidate management for greater efficiency.

Credentialing:

By leveraging the enterprise cloud, businesses can ensure the cohesion and management of different credentialing methods like USB tokens, smartcards and mobile smart credentials.

PKI:

Public key infrastructure plays an invaluable role in business transactions. With hosted cloud-based PKI, organizations can drive down operating costs that would be associated with in-house PKI while still reaping all the benefits.

IaaS:

Infrastructure as a Service is the notion of a cloud provider that takes care of security and other cloud management components for you. This option takes the onus off companies and allows them to direct their attention toward boosting business, knowing their cloud computing is taken care of.

LEVERAGING THE CLOUD: BEST USE CASES

The following examples illustrate the different ways the cloud can and has been harnessed to promote better business without compromising security.

SMALL MEDICAL CENTER ENSURES BIG SECURITY IN CLOUD

"A PKI regulates a company's various keys and certificates to create a single platform of infrastructural management."

As he prepared to open Eppel Family Medical Center in 2012, office manager Ken Adams knew that having a solid enterprise security plan was a top priority, according to InformationWeek. After all, patient records are some of the most privileged documents out there. By situating the center in a private cloud, Adams was able to ensure a high level of data security without having to tend to it all the time.

"The cloud system was definitely a draw right from the get-go," he said. "Even more than the cost and ease of use, we didn't want it here in the office. We wanted somebody else to protect it from the bad guys."

LAW ENFORCEMENT OFFICIALS HARNESSING CLOUD TO MANAGE CREDENTIALS

According to a report released by the International Association of Chiefs of Police, cloud computing has the potential to significantly improve how police systems operate. But because of the inherent sensitivity of police documents, the report stated that any cloud-bound police department would require a virtual platform with the tools to manage credentials in order to keep third-party attackers at bay.

Fortunately, the private cloud provides exactly the identity protection measures that law enforcement officials need, according to a separate report released by Paul Wormeli of the IJIS Institute. Wormeli's report stated that not only is the private cloud safe for law enforcement, but it's actually far safer than on-premise deployment, where instances of misconfiguration — which is in essence like leaving keys in an unlocked car — are 12 times higher.

PKI SOLUTIONS PROVIDING BENEFITS ACROSS THE BOARD

Public key infrastructure is a great solution for businesses whose cloud platform is likely to be accessed from insecure public networks. According to SANS Institute, a PKI regulates a company's various keys and certificates to create a single platform of infrastructural management.

A report by Heena Kharche and Deepak Singh Chouhan posits that PKI represents a crucial step toward establishing trust in the cloud. That is because it paves the way for more fluid computer-to-computer communications that might otherwise be exposed to unwanted third-party observation.

According to a PKI Forum report, there are myriad examples of PKI-enabled applications across many different industrial sectors, including stock purchases, online banking, insurance claim filings and national passports.

"The cloud is the ultimate tool for business security management—a ttresource that is as dependable as it is safe."

SECURING BYOD FOR MAXIMUM EDUCATIONAL BENEFITS

Mobility is now core to the business world we live in. And as a result, bring-your-own-device (BYOD) policies are cropping up in many different industries as a way to increase workflow, provide employee flexibility and enable work to be done remotely. But big companies aren't the only ones benefiting from BYOD — schools, as well, are realizing the advantages.

The possibilities for BYOD in the classroom have been successfully put to the test in many different scenarios. One of them occurred at Forsyth County Schools in Georgia, which decided to enact a BYOD policy across its 36 schools, according to K12 Blueprint. The project centered around developing the district's presence in the cloud, so that students and staff would be able to log on from BYOD devices and access a host of applications that were designed to enhance the educational experience.

But the district realized that in order to launch a successful BYOD program, it needed to ensure the security of all devices in the system. And so it implemented a Service Set Identifier system that made sure any device accessing the network had been properly authenticated and was allowed to be there.

Once the district had firmed up the program's security, it set about getting everyone acclimated. This included district-wide professional development focused on deploying BYOD solutions and tutorials for students to learn how to navigate the system.

The system has been largely successful. And to the detractors who feared an in-school BYOD policy would encourage student distraction, the project report notes that "disciplinary issues regarding technology have gone down" since its implementation.

CHOOSE A PROVIDER TO MEET YOUR BUSINESS NEEDS

By providing well-equipped and individualized virtualization options, cloud providers emerge as an indispensable resource for all types of companies. And by choosing to align itself with a trusted security provider, a business relieves itself of a significant burden, while at the same time knowing that its data is in good hands.

The most important thing for an organization choosing a cloud platform is to be discerning and evaluate prospective providers for the security options they offer. As this report has shown, a well-equipped cloud is more than prepared to meet the security management needs of any enterprise.

In searching for a provider, companies must look beyond price and consider the track records of possible providers. The key is to find a security vendor that has strong segmentation between tenants and leverages proven authentication and certificate solutions for greater security. With these factors in place, the cloud is the ultimate tool for business security management — a resource that is as dependable as it is safe.

About Entrust, Part of Datacard Group

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees. Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards. For more information about Entrust solutions, call 888-690-2424, email entrust@entrust.com or visit entrust.com.

+1-888-690-2424
www.entrust.com

f	in	You Tube
EntrustSecurity	Entrust	Entrust	Entrust

SOURCES

eclipse.net.uk/landing/explosive-growth-of-cloud-computing
visual.ly/cloud-computing-facts-and-predictions-2014
magineiti.com/the-cloud/costs-cloud/
cloudtweaks.com/2014/05/cloud-infographic-corporate-security-stats/
searchcloudcomputing.techtarget.com/opinion/Clouds-are-more-secure-than-traditional-IT-systems-and-heres-why
innotas.com/resources-infographics/Hospitals-Must-Look-to-Cloud
healthcareitnews.com/news/cloud-could-usher-11b-savings
cert.uy/wps/wcm/connect/975494804fdf89eaabbdab1805790cc9/Cloud_Computing_Vulnerability_Incidents.pdf?MOD=AJPERES, 9
albany.edu/iasymposium/proceedings/2013/16-BoothSoknackiSomayaji.pdf
betanews.com/2013/11/04/comparing-cloud-vs-on-premise-six-hidden-costs-people-always-forget-about/
www.entrust.com/products/cloud/ssl/
informationweek.com/healthcare/leadership/physicians-find-security-in-the-cloud/d/d-id/1234839