

Protecting Your Investment:
**THE CURRENT STATE OF
CLOUD SECURITY**

An examination on the evolving state of security
as it relates to your cloud-based
applications and data

Table of Contents

Chapter 1: The current state of cloud security	7-10
Chapter 2: What are we protecting?	11-17
Chapter 3: Cloud security misconceptions	18-22
Chapter 4: Why take your business to the cloud	23-25
Chapter 5: Comparing public & private cloud security	26-30
Chapter 6: Develop a risk assessment	31-34
Conclusion	35



This ebook in a nutshell

This ebook in a nutshell

This eBook offers a glimpse into the ever evolving world of cloud security.

As the technology grows, more concerns and more advantages grow with it. This eBook will examine several studies to give you a current overview of the risks and rewards your organization should be aware of when implementing safeguards around your data.

Review the reports:

The research is out there. We'll do our best to compile some prominent studies that examine every angle of cloud security.

Identify your organization's needs:

Every business is different, so make no mistake that you're doing what is best for your business with each move you make.

Asks questions and seek answers:

As always, the first step when implementing a business-critical solution is to ask a lot of questions. Make sure your desired strategy passes your risk assessment.



**Let's look at
what we know**

Let's look at what we know



- Cloud computing adoption remains on the rise.
- By 2016, Gartner predicts the bulk of new IT spending will be cloud-based rather than on-premises.
- Organizations are moving to the cloud to embrace a more agile, scalable solution that reduces costs and decreases infrastructure and hiring needs.
- A Gartner cloud survey identified that organizations value “robust disaster recovery” and “security certifications and insurance” above lowest price in the cloud.
- The issue of cloud security still manages to be a market driver for some organizations while an inhibitor for others.
- Education plays a big factor in staying up-to-date with the latest threats and utilizing your own or your provider’s best practices to squash hiccups before they become catastrophes.
- Improper protection or a lack of expertise in data security will ultimately make your on-prem deployment a liability.



CHAPTER 1

The Current State of Cloud Security

As the cloud continues to grow in popularity,
so do the attacks...

//

Attacks are happening more frequently and are becoming more advanced.

//

“The Cloud Security Report”
- Alert Logic, Spring 2014

The Current State of Cloud Security

THERE'S BEEN A SHIFT IN SECURITY CONCERNS

Most IT Departments are shifting their security concerns. They've gone from fearing the cloud to embracing it. But now they need to work harder to secure it.

Wherever your data may be, it is subject to attack.

As brute force attacks and vulnerability scans, including malware/botnet attacks continue to threaten on-premises environments and the cloud, IT teams need to rethink their strategy.



From Alert Logic's Research on the Evolving State of Cloud Security

The Current State of Cloud Security



Alert Logic recognizes that “the fears of the cloud being inherently insecure could largely be put to rest”. Why’s that?

Because it’s foolish to call one thing (cloud) insecure and the other (on-prem) not. They are both subject to attack.

Why? Attacks will happen wherever your data resides and regardless of what types of workloads or infrastructure you deploy because, as a wise old Butler once told Bruce Wayne, “Some men just want to watch the world burn...”

BOTTOM LINE: WHETHER YOUR DATA LIVES ON-PREM OR IN THE CLOUD, THE LEVEL OF PROTECTION SURROUNDING IT SHOULD BE YOUR FIRST CONCERN.



CHAPTER 2

So, What Are We Protecting?

If it's paramount to find a proven security solution for your infrastructure, just what exactly should it be focused on protecting?

So, what are we protecting?



Organizations moving to the cloud must understand and pay close attention to their security and compliance requirements and appropriately source a solution.



“The Cloud Security Report”
- Alert Logic, Spring 2014

So, what are we protecting?

The cloud is proving to be too compelling to resist, but security concerns still float to the surface of every cloud conversation.

More and more organizations are understanding that they need to employ an enterprise-grade security solution to protect their cloud-based applications.

YOUR CLOUD SECURITY SHOULD PROTECT:

- Mission critical applications
- Confidential data
- The underlying infrastructure that supports those applications, including:
 - Your network
 - Your compute resources
 - Your database
 - Your identity management

BOTTOM LINE: IDENTIFY YOUR ORGANIZATION'S SECURITY AND COMPLIANCE REQUIREMENTS AND FIND A SOLUTION TO MATCH.

So, what are we protecting?

But protecting your data goes deeper than just permission controls and network administration, it can even extend to how accessible your actual datacenter is.

PROPERLY SECURING YOUR ASSETS

From the parking lot to the panic button, enterprise datacenters have exhausting controls in place that are invisible to the naked eye.

Mitigating the risk and following protocols ensures that proper security measures are executed every time. And when your data is at stake, there are three areas that deserve your full attention:

- Physical Security
- Network Security
- Application Security

BOTTOM LINE: TYPICALLY, AN ON-PREMISES DATACENTER CANNOT AFFORD THE SAFEGUARDS AND OPULENT PROTECTION THAT CLOUD HOSTING PROVIDERS' ENTERPRISE DATACENTERS CAN.

So, what are we protecting?

THREE TYPES OF SECURITY NEEDED TO PROTECT YOUR INFRASTRUCTURE:

PHYSICAL SECURITY

This typically includes:

- Gated parking (to limit access)
- Security cameras
- Lack of signage (so it isn't a target)
- Staffed or unstaffed entryways (as you see fit)
- Door sensors
- Cloaked parking garages
- Check-in for access (usually a badge or, if more advanced, biometrics)
- Fly-trap area at entrance (this stops deliveries or visitors from gaining complete access to the DC)

BOTTOM LINE: MOST BREACHES OCCUR WHEN SOMEONE IS STANDING IN FRONT OF THE SYSTEM.

So, what are we protecting?

THREE TYPES OF SECURITY NEEDED
TO PROTECT YOUR INFRASTRUCTURE:

NETWORK SECURITY

This typically includes:

- Edge of network (where public access begins)
- Routing protocol (protects from the outside in)
- Server security
- Rigid blueprints for everything you stand up
- Maintain patch levels
- Firewall layers (as robust or narrow as you like)
- Keep up with bugs
 - Network Logging (most enterprises log every transaction)
 - Retain as much data as you need
 - Flag any keyword or anomalies if possible
 - If an event or breach occurs, you'll know quickly if logging is tied into alerting

So, what are we protecting?

THREE TYPES OF SECURITY NEEDED
TO PROTECT YOUR INFRASTRUCTURE:

APPLICATION SECURITY

This typically includes:

- Port access (only keep needed ports open)
- Audit open ports and close any not being used
- IDS/IPS behind firewalls (only see the traffic that's getting through)
- HTTPS (obtain a SSL certificate)
- SQL access (make sure it isn't directly accessible from the web)
- Segmentation (this will reduce risk)
- Sync User Accounts (helps user experience)
- Implement and audit virus/malware scanner




CHAPTER 3

Cloud Security Misconceptions

You've likely heard both sides of the argument:
"the cloud IS secure – the cloud ISN'T secure"
So which one is right?



Elements such as data confidentiality, privacy, service contract commitments and regulatory compliance are items that need to be reconsidered in the cloud. 

["Customized Security and Risk Attachments in the Cloud Contracts Protect Against Critical Risks"](#)

- Gartner, February 2014

Cloud security misconceptions



THE PROBLEM: BUSINESSES ARE TAKING LEGACY APPROACHES TO SECURITY WITH THEM TO THE CLOUD

Security measures that are inherited from on-premises deployments are not sufficient and leave your organization open to attack.

This leads to the false conclusion that the cloud isn't safe when the central issue is that businesses aren't reconsidering their security strategies when moving to the cloud.

Gartner suggests starting from scratch when implementing your cloud strategy, focusing in particular on data confidentiality, privacy, service contract commitments and regulatory compliance.

Cloud security misconceptions

THE EVOLUTION OF YOUR DATACENTER BEGINS WITH YOUR DATACENTER SECURITY

Here's a few of the issues that you'll run into when you transplant your on-prem security measures into your cloud:

- Resource overload
- Functionality gaps
- Instant-on gaps
- Always-on gaps
- Management Inefficiencies

Here's a few ways security vendors are responding to legacy approaches:

- Developing and executing a risk assessment
- Externalizing the scan engine
- Intelligent scanning and scheduling
- Managing the visual footprint

BOTTOM LINE: IT'S ABOUT EVOLVING MORE THAN JUST THE TECHNOLOGY, ALSO YOUR PEOPLE AND YOUR PROCESSES.

Cloud security misconceptions



AND THERE'S ANOTHER PROBLEM THAT ORGANIZATIONS RUN INTO WHEN MOVING TO THE CLOUD: THE CONTRACT

In “Predicts 2013: Cloud and Services Security”, Gartner concedes that “there is widespread dissatisfaction with the **relatively scanty and ambiguous contractual language** that cloud services providers typically include in their standard contracts”.

This augments an organization’s hesitation to go cloud because they are, on top of adopting a new way to do business, **being asked to give their trust to the cloud service provider.**

Also, in regards to the contract, Gartner reports that while security is talked about as a top concern for outsourcing, “it is often an afterthought in contract development.”



CHAPTER 4

So, Why Go to the Cloud?

IT is being pressured to save time and money while doing more with less every year. Luckily, the cloud keeps evolving to keep up with demand.

So, why go to the cloud?



Cloud service providers invest in solutions, and new and innovative technologies, that are then delivered in a ready-to-use format that eliminates the need for capital expenditure on the part of the buying organization.



"Customized Security and Risk Attachments in the Cloud Contracts Protect Against Critical Risks"

- Gartner, February 2014

So, why go to the cloud?

DON'T WASTE YOUR TIME AND RESOURCES FIGHTING A TECHNOLOGY THAT SHOULD BE YOUR ADVANTAGE NOT YOUR COMPETITION.

Rather than list out the same cloud advantages you've read and heard in countless blogs and conversations, let's focus instead on a different advantage that cloud service providers have:

The **ability to invest in new security technologies** which can then be delivered directly to the customer's infrastructure, **eliminating the capital expense and training** that would otherwise absorb the time and money of an organization.

BOTTOM LINE: FOR HOSTING PROVIDERS, THE DATACENTER IS THEIR BABY AND, THANKS TO THE SHARED COSTS OF THEIR CUSTOMERS, THAT'S WHERE ALL THE MONEY GOES.



CHAPTER 5

Comparing Public vs. Private Cloud Security

The cloud is making the process easier, but there are still pitfalls along the way, especially in regards to security and compliances.



Cost avoidance is just as important as cost savings.



“Security and Cloud: Private, or Public”
- Aberdeen Group, September 2011

Comparing public vs. private cloud security



THE CLOUD ADVANTAGE CAN QUICKLY BE NEGATED IF YOU LEAVE YOUR ENVIRONMENT OPEN TO ATTACK.

The Aberdeen Group conducted a security study to prove that there is far greater benefit in placing discipline and controls around your environment than just looking for initial cost savings.

Their “Security and Cloud: Private, or Public” research put an entirely new spin on the Public vs. Private Cloud argument.

They introduced the notion that cost avoidance deserves the same attention as cost savings because, due to the higher number of security and compliance related incidents, favoring one over the other will likely eclipse any advantage you see initially.

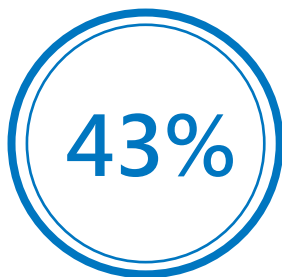
Comparing public vs. private cloud security

PUBLIC CLOUD BY THE NUMBERS

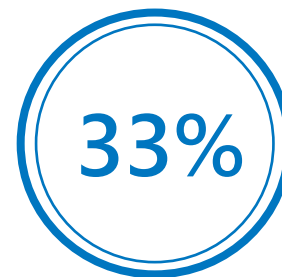
These numbers are compared against a private cloud deployment, unless otherwise noted.



Companies implementing public clouds spent 5% less annually on a per-application basis



Along with a 43% faster deployment time



And 33% less unplanned downtime than on-prem

But the high number of security and compliance incidents quickly put an end to all of the cost savings.



Companies implementing public clouds experienced 3x's more incidents of unauthorized access

Comparing public vs. private cloud security

PRIVATE CLOUD BY THE NUMBERS

These numbers are compared against a public cloud environment.



Companies implementing private clouds incurred 38% fewer costs on a per-application basis related to security and compliance incidents.



The average cost of an incident according to Aberdeen Group's report



Overall, companies deploying a private cloud experienced a combined annual cost advantage of about 12%.

Overall, companies with public clouds spent **5% less** than those implementing private clouds in terms of consistency and efficiency of operations.

However, they spent **63% more** in terms of costs related to security and compliance.



CHAPTER 6

Develop a Risk Assessment for your Organization

Focus on assessing the security and auditing standards/protocols that your business demands. Often you'll find that your organization is flying blind with no clear protocols even in place.

Develop a risk assessment for your organization

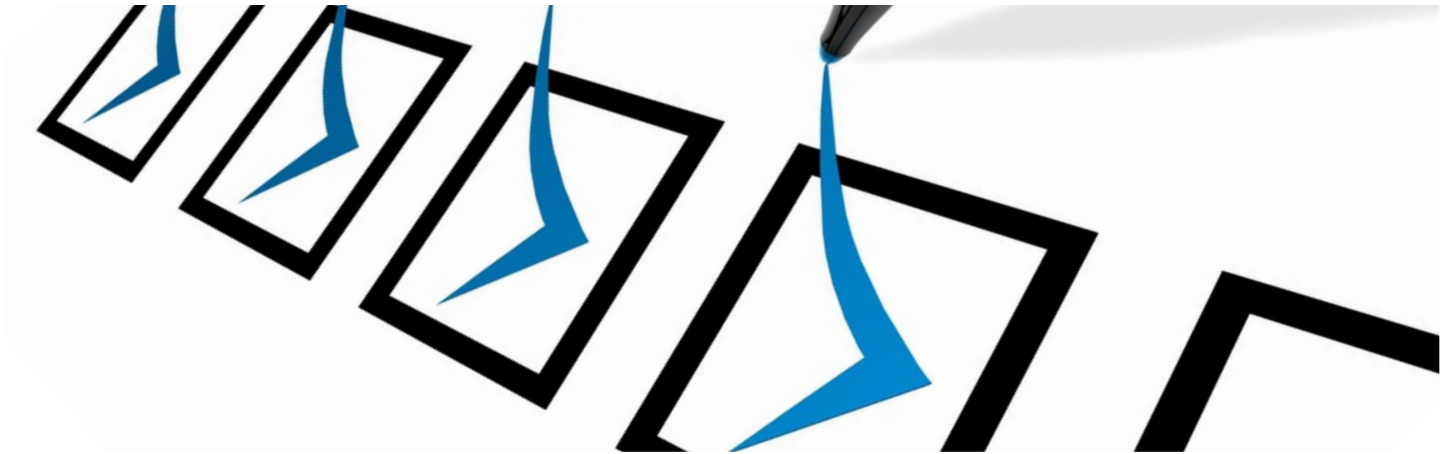


Risk comes from not knowing what you're doing.



-Warren Buffet

Develop a risk assessment for your organization



In order to consider the complete picture and get the most value out of your investment, every organization should do a deep dive into what it takes to protect their business.

Outside of the obvious factors like disaster recovery and compliance within their industry, organizations must focus on **developing and executing their own risk analysis process.**

This should **identify and assess your needs** as they relate to the application or service in question.

Don't be afraid to ask for all the cloud service provider promises to be put in writing. Then thoroughly **review their data center audit** to ensure that what they are saying adds up.

Develop a risk assessment for your organization

SOME KEY WAYS TO ASSESS POTENTIAL SECURITY RISKS:

Evaluate your current mitigation options

Not starting your security strategy from scratch tends to be a problem when moving from on-prem to the cloud.

Enforce data encryption

Organizations often require and implement data encryption. This is driven more by internal policies than by law.

Mask sensitive data

You can keep sensitive data in your own data center. Unlike encryption, which basically blinds the service provider, masking allows limited functionality to continue in the cloud.

Set up backup mechanism in-house

You can leverage additional backup options in-house or have your cloud provider create backup copies at a separate location.

Only allow private cloud

Private cloud usually provides a better level of control for the organization than a public cloud.

Leverage third-party audits for security standards

As security evolves, organizations use external audit companies to test and evaluate the standards from the cloud service provider.

Use secondary cloud provider for storage/backup

In many cases, organizations store their data with multiple cloud providers in order to limit the risk of data loss.

HERE'S YOUR TAKEAWAY:

SECURITY IN THE CLOUD IS MORE COMPLEX THAN JUST 'YES' OR 'NO'...

It's tough to find a proven security solution as the technology it's protecting continues to mature. But these things are certain:

Just because you can see it, doesn't mean it's safe:

Quite the opposite really, as retailers like Target will attest – this factors into how on-prem datacenters typically have less than adequate physical protection. If it's touchable, it's breakable.

The cloud does it better:

The old adage "If you want something done right, do it yourself" won't help you here. You are likely not a data expert, and more importantly, you don't have the budget to protect your infrastructure in the way that it deserves. The private cloud can.

It's not just, 'What am I paying for?' but, more importantly, "What am I NOT paying for?"

Staying compliant in your industry and having your datacenter audited regularly can add up - not to mention training and personnel costs. Remember, one breach could cost you your business.

Do your due diligence:

Identify the best way to move forward with your data and into whose hands you will place it. This will require research, audits and risk analysis to develop the security strategy that fits your business.

Thanks for reading!

Please accept this
Free Cloud Hosting Security Consultation
from **Fpweb.net**

Need help assessing your SharePoint security on-premises or the cloud?

One quick phone call will help you identify the advantages your business can take on when deploying the private cloud to protect your investment.