SOPHOS
Security made simple.

Sophos Best Practices for AWS Cloud Security.

Preparing for the dangers of the public cloud to ensure data security

The public cloud is a veritable data war zone

There are a lot of misconceptions about the cloud and what kind of security and protection you have when you store your data there. One thing you can always count on is that cyber threats are real. Hacker technology continues to improve and cyber attacks increase year over year. In 2015 alone there was a 45% increase in cyber attacks on the public cloud. The fight to protect data becomes increasingly important if you're going to keep your business and data safe.

That's where Sophos comes in. Sophos is an advanced tier AWS technology partner, and our security products are currently used to protect thousands of customer enviornments running on AWS. Based on technical proficiency, adherence to AWS Best Practices, and proven customer success, we've also been awarded the AWS Security Competancy designation. This designation is given to only a handful of companies that match the rigorous security standards outlined by AWS, and also understand how to properly secure Cloud enviornments. We want to share our security best practices with you so you can protect your data. But first, let's define a few things.

What is "the cloud?"

The common belief is that the cloud is something relatively recent. This couldn't be further from the truth. The "cloud" has been around for decades. Essentially, anything hosted and accessed virtually is the cloud – like the entire internet, for instance. Email systems like Gmail are part of "the cloud," social networking sites like Facebook and Twitter are in "the cloud,"

Security best practices checklist

- Understand your data and whether or not that data is appropriate for the public cloud.
- Understand the types of Cloud models in use by your company.
- Research your cloud provider to determine their data security responsibility model and the level of security they provide.
- Determine your organization's security policies – who has access to the data and how they will access it.
- Ensure all data is encrypted in transit and at rest - and determine who is holding the encryption keys.
- Establish the proper layers of protection such as firewall/intrusion protection, gateway antivirus, etc.
- Implement a consistent and secure data backup plan.

Making sense of the cloud

What is recent is labeling the virtual hosting and server infrastructure as the cloud. Calling it the cloud is a coined term to communicate a system of great value to people in non-technical terms. As a result, though, there is a lack of education about what it is and whether or not it's secure.

There are three types of cloud models:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

In the simplest terms, **SaaS** is software designed for end users and accessible via the web. Examples include online applications such as Gmail, Facebook or Uber. For SaaS, security responsibilities are pretty well defined. The application is used for specific purposes and doesn't offer much end user customization, which could lead to exposure. The SaaS provider is responsible for updating and maintaining their system and ensuring the appropriate levels of security in compliance with federal regulations. Though the customer, of course, shares responsibility for things such as proper password management and security of the system used to access the SaaS application.

PaaS provides developers with a platform and the tools needed to build applications, such as those provided via SaaS. PaaS platforms allow developers to quickly and easily create applications without requiring the complexity or cost associated with buying and maintaining the underlying software and hardware. The amount of built-in security provided with PaaS depends on the system and it's components and is usually shared between the PaaS provider and the developer using the platform.

IaaS, provides virtual networking, virtual servers, storage, and the other infrastructure components that both PaaS and SaaS rest on. IaaS security concerns are also shared by both the customer and the IaaS provider. Unlike the other two cloud models though, IaaS offers much more flexibility, which can lead to greater exposure for a customer. This means that IaaS typically requires that the customer pay greater attention to security, and implement additional layers of security and control to protect their assets.

Quick definitions

Making sense of all the different acronyms to define "the cloud" can be difficult. Here's a little key to keep them straight.

SaaS: Software as a Service is a software delivery method that provides access to software and its functions remotely as a Web-based service.

Examples: Gmail, Facebook, Uber

PaaS: Platform as a service is a cloud computing service that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

Examples: AWS Elastic Beanstalk, Force.com, Google App Engine

IaaS: Infrastructure as a Service is a form of cloud computing that provides virtualized computing resources over the Internet – virtual servers, storage, and the infrastructure components that both PaaS and SaaS rest on.

Examples: Amazon Web Services, Azure, Google Compute Engine

So what's the big deal? It's just data

Famous last words. Hackers can do a lot with what they take. The data can be stolen or corrupted. Even if it seems innocuous, these are files you'd never be able to access again unless you've backed them up. For companies, this can result in financial loss and brand recognition damage. In the case of sensitive information requiring privacy compliance, such as medical records or credit card information, data breaches can result in losing customers and major fines from the government.

Individuals can suffer as well. Identity theft and stolen banking information or health records is common, which can ultimately result in bankruptcy or the inability to get a job. One of the most common occurrences is the use of ransomware, a type of software hackers use to hold your data hostage and not release it until you've paid money to get it back. This can affect both organizations and individuals, and is a very real threat that happens more often than people know.

The most important thing to remember is that when you put something in the cloud, it's imperative you understand how it's being protected. You shouldn't assume that security is being taken care of for you.

Cloud security best practices

One of the most common responses to cloud security breaches is that the organization thought they were covered, that their data was secure. Often they're taken off guard, unaware that they were victims of of cyber attack. However, when they go back through a security audit, there are tons of vulnerabilities exposed. For any company, security should be a core functional requirement in order to protect mission-critical information from accidental or deliberate theft, leakage, integrity compromise, and deletion. That's why following this list of security best practices is so crucial.

- Understand the type of data and whether or not that data should be in the cloud in the first place.
- Understand the types of cloud models in use by your company.
- Research the cloud provider to determine the data security responsbility model and the level of security provided.
- Determine your organization's security policies – who has access to the data and how they will access it.
- Ensure all data is encrypted in transit and at rest, and determine who is holding the encryption keys and who has access to the data.
- Establish the proper layers of protection such as firewall/intrusion protection, gateway antivirus, etc.
- Implement a consistent and secure data backup plan.

Different types of cyber threats

To understand what you're up against, it's good to be educated on some of the common cyber threats:

Malware

Malware, short for malicious software, includes viruses, worms, spyware, ransomware, Trojan horse programs, etc. Network traveling worms are one of the biggest threat to cloud security currently.

Phishing

An email or similar message or communication that appears to be from a legitimate source, but sends the user to a hacker site allowing the hacker to collect sensitive data. This is most commonly used with banking info.

Socially Engineered Trojan

An end user browses to a website usually trusted, which prompts him or her to run a Trojan. Most of the time the website is a legitimate, innocent victim that has been temporarily compromised.

The website will inform users they are infected and need to run "antivirus software," or are out of free disk space, or that they must install an otherwise unnecessary program. The user executes the malware, unwittingly falling into the trap.

How to start implementing the security best practices

The best place to start is by understanding your data. Some data is too important to leave to chance without proper protection. Intellectual property, personally identifiable information (PII), credit card info, banking info, or medical records are all examples of data that need high-level security to meet compliance standards and must be properly secured and controlled.

Once you've categorized your data, you need to understand what requirements exist for protecting that data. For instance, does it need to be PCI-DSS compliant because it's credit card or banking data? Is the data required to be HIPAA compliant because it contains medical records? Is it housed within a database accessible through the public cloud? Sensitive data must be encrypted all the way through transit and rest, and some types of data may require mulitple layers of protection, deep packet inspection tools such as Intrusion Protection (IPS) ,multifactor authentication, and detailed real time and historical logging of events and system access.

It's important that you really understand what you're securing. How is that data being used and effected as it travels from system to system? What kind of compliance requirements exist for that data? Not all data is required to be protected in the same way, but some data is required to follow very strict, federally mandated security standards, which can result in major fines if not followed.

You'll want to coincide all this with developing internal policies on how this data is handled. Will everyone in the organization have access to it, or only specific employees? How is the data accessed? Can it only be accessed onsite in a secure environment, or can it be accessed from anywhere? Ensure the data is backed up and implement an automatic and secure backup strategy.

Those that don't take data protection seriously are susceptible to a multitude of risks, so appropriate assessments need to be made to analyze those risks, pain points, and vulnerabilities to ensure that anything exposed is safeguarded. Then, once you've implemented controls, perform ongoing audits to inspect the data and ensure internal practices are being followed. Sometimes protecting the data properly can even require certain types of building security. In those cases, do all employees know they're not supposed to let just anyone in the building?

In order to protect the data and be compliant with security standards, these kinds of policies must be established, evangelized, and adhered to company-wide without exception.

Security standard compliance

HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. It refers to any data that can be categorized as personal health information (PHI). Technical safeguards require authorized access, including using unique user IDs, an emergency access procedure, automatic log off and encryption and decryption. Additionally, network and transmission security are required as well as offsite backup for disaster recovery. Audit reports, or tracking logs, must be implemented to keep records of activity on hardware and software.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards and sensitive customer banking information. Technical safeguards require firewall protection, encryption of customer data, unique user IDs, development and maintenance of secure systems, anti-virus software on all systems, and tracking and monitoring of all system interaction.

What about Amazon Web Services? What kind of security and data protection does it provide?

Amazon Web Services (AWS) developed the shared responsibility model, which means that you're provided with infrastucture-level security (foundation compute, storage, networking and database services), but building the Information Security Management System (ISMS) is your responsbility.

To be more specific, on AWS, you're provided with a global, secure infrastructure that meets specific government, industry, and company security standards and regulations including: ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584), just to name a few. This security covers:

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

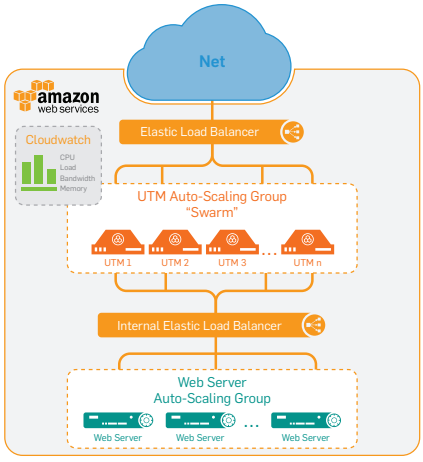
You are responsible for protecting the confidentiality, integrity, and availability of your data in the cloud, and for meeting specific business requirements for information protection.

Think of security in different layers. AWS provides the castle, but you need to provide the moat, the door, the drawbridge, the guards patrolling the watchtowers, and anything else you need in order to ensure that what's inside is kept safe. Different types of data require different types of security against varying levels of threats. AWS's responsbility is to ensure the castle is sound, but they're not responsible for who or what comes in and out of it. Those decisions are entirely left up to you, and without the proper security, all a hacker would need is your IP address and some basic hacking skills to get past infrastructure firewall defenses, and they've got the keys to the kingdom.

At the basic level, AWS provides a secure infrastructure, and you are responsible for secure platforms, operating systems, and data. You have tools as part of the system to enhance security, such as the Identity and Access Management (IAM) service, which allows you to set user permissions. However, in order to really provide your data with the moat, door, drawbridge, and guards, you need layered protection.

AWS partner competency

Sophos is an AWS Security Competency recipient - awarded based on technical proficiency and proven customer success for our UTM with Auto Scaling. To find out more about the AWS Partner Competency Program, click here.



Time to bring in the muscle – Sophos UTM with Auto Scaling

As an advanced tier partner in the AWS Security Competency Program, Sophos is recognized as one of only a handful of companies with long-term success in infrastructure security, reason enough to know your data is safe. It's much more than that, though. Because we use the infrastructure services provided by AWS for deployment, auto scaling, and availability, Sophos UTM with Auto Scaling is compatible with their architecture guidelines. The security is certifiable on the top through UTM and on the bottom through AWS.

It comes standard with an Essential Network Firewall that provides fundamental security like firewalling, networking tools, routing and secure remote access. Plus our modular approach lets you add layers of protection as your needs evolve. Each module also provides detailed real time and historical logging and reporting information to help you better understand the traffic flows and threats your network faces each day.

- Network Protection: stops sophisticated attacks that a firewall alone can't stop via an inline IPS and Advanced Threat Protection
- Web Protection: lets you protect your employees and servers from web threats and control their time online
- Secure Auto Scaling: built to protect your elastic cloud environment
- Inline Network IPS: guard your VPC servers and applications from threats
- Web Application Firewall: secure your web applications against more than 350 attack patterns
- Secure Access VPN: give users secure access to AWS or site-to-site VPN

Sophos UTM with Auto Scaling provides as much or as little security as your data requires, and can help you to meet federal requirements like PCI-DSS and HIPAA compliance. Also, since UTM with Auto Scaling is built specifically for AWS, you get all the infrastructure security benefits within the security system.

Sophos UTM – modular security that auto-scales with AWS cloud.

All the protection your data needs while in the cloud and moving through the network is comprehensively provided through one interconnecting security system that integrates directly with AWS Cloud.

Sophos UTM with Auto Scaling gives you complete security from the network firewall to endpoint antivirus in a single modular system that integrates with the AWS Infrastructure to provide high availability and scalability. It simplifies your IT security and saves money by combining multiple security solutions, and increases visibility through detailed logs and reports.

Try it now for free

Sophos UTM with Auto Scaling or visit us at sophos.com/aws

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2016-04-11 WP-NA (MP)

SOPHOS