What You Need to Know About Cloud Security

ARCTIC WOLF

www.arcticwolf.com

Cloud Is Powering SME Digital Transformation

The competitive advantages of the cloud are fueling a major digital transformation across all segments of the market. The cloud is enabling small to medium sized enterprises (SME) to grow faster yet be nimble and reach more customers anywhere, anytime.

Moving IT infrastructure and applications to the cloud is one of the top 10 technology trends in 2017 for SMEs. Flexibility, reduced cost, speed and ease of deployment are the key drivers. Cloud-based solutions fill the gap, where traditional on-premises systems like ERP, human resources management, real-time collaboration, work flow integration and automation have failed to deliver. With the cloud, customers are being empowered to do business wherever they have an Internet connection.

Why Use Cloud Services?

Cloud services empower SMEs to do more with less. It enables businesses to pay-as-you-go, scale-up or down based on demand, and takes less time to deploy compared to on-premises solutions.

More importantly, the business agility enabled through cloud infrastructure are unparaleled. It used to be that your processes were constrained by your IT capabilities as an organization. Cloud services have fundamentally flipped that logic on its head. Now, your business processes lead the way, and flexible IT infrastructure shapes itself around those needs.

On-Premise		Cloud Computing
Expensive (CapEx)	→	Cost effective (OpEx)
Inflexible (central planning)	→	Agile (business driven)
Manual build/deploy	→	Automated build/deploy
Own infrastructure	→	Shared infrastructure
Manual scale-up	→	Automated scale-out
Manual fault recovery	→	Self-healing

SaaS, PaaS, IaaS:

The three most prominent types of cloud services are: SaaS, PaaS, IaaS.

What cloud service you choose will clearly depend on your business needs, and on how much management of your IT resources you are capable of handling.

SaaS

Software-as-a-Service

Subscription-based web applications that are managed and maintained by a third-party provider.

USED FOR	Turnkey applications that you can rent and customize.
BEST FOR	Commodity applications – Email, CRM, HR, Collaboration tools
SECURITY	Managed by SaaS provider
EXAMPLES	Office365, Salesforce, GoogleApps, Dropbox, Okta

PaaS

Platform-as-a-Service

A pay-as-you-go, remotely managed platform that lets you develop and run your own business applications.

USED FOR	Developer platform that abstracts middle-ware, OS, and infrastructure
BEST FOR	Simple to use applications, don't need control of network topology, OS, or data
SECURITY	Managed by PaaS provider
EXAMPLES	Amazon Elastic Beanstock, Force.com AppExchange, Azure PaaS

IaaS

Infrastructure-as-a-Service

Virtualized computing resources (servers, storage, and networking) are provisioned and paid for monthly.

USED FOR	Developer platform that abstracts middle-ware, OS, and infrastructure
BEST FOR	Variable workloads, need control of compute, storage and networking
SECURITY	Managed by customer
EXAMPLES	Amazon AWS, Microsoft Azure, IBM-Softlayer, Rackspace

Private, Public, Hybrid:

The most common cloud types are private, public and hybrid. The use levels for each among enterprises, as indicated through RightScale’s 2017 State of the Cloud report are as follows:

None:	**1 percent**
Private:	**12 percent**
Public:	**29 percent**
Hybrid:	**58 percent**

The fact that hybrid leads the pack is especially noteworthy. Having unified visibility of segmented infrastructure is not an easy task, as it would require aggregation of log data from the different service architectures. This inherently introduces a layer of complexity best left to a managed security service provider.

Public Cloud	Private Cloud	Hybrid Cloud
Multiple tenant	Single tenants	Private and public combo
Provider owned, leased to multiple customers	Customer owned/leased	Customer owned private, provider owned public-side
Shifts CapEx to OpEx	Leverages existing CapEx	Balances cost between OpEx and CapEx
Customer has complete control over security	Customer has complete control over security	Customer manages security across private and public clouds

What are the cloud security challenges?

Visibility is not the only hurdle associated with cloud adoption. Because cloud computing facilitates anytime, anywhere access, network perimeters are far less rigid. This, paired with hackers' relentless efforts to exploit business in new ways, introduces the following security risks: (See table at left)

With so much that can go wrong, businesses must make cloud security a top priority.

Risk	Description
Data Breaches	Customer sensitive data is more exposed to breaches in the cloud compared to when it resides on-premises
Hijacked Accounts	Stolen credentials can be used to hijack cloud user accounts to steal company data in the cloud
System Vulnerabilities	System vulnerabilities can be exploited by hackers across shared cloud infrastructure
Advanced Malware	Advanced malware can infect files on-premises and then move laterally to the cloud as files are copied over
Insider Theft	Malicious insiders (employees, contractors, partners) can move company sensitive data to unauthorized cloud applications
Shadow IT	Employees can be using unauthorized SaaS applications (e.g. Google Drive) to share company confidential information
Cloud Services Abuse	Cloud services can be commandeered to support nefarious activities, sending spam/phishing email, host malicious content
DDoS Attack	Distributed denial-of-service attacks can be easily launched to make cloud resources unavailable or inaccessible

What are the best practices for security?

Just because a cloud services provider manages the security for its own infrastructure and applications clearly does not mean that your business is safe. To protect your cloud resources against hijacked accounts, insider threats, advanced malware and other cloud-borne cyberthreats, take the following actions: (See table at right)

Best Practice	Details
Access Control	Use strong authentication (multi-factor, certificates) and access control based on user profiles to prevent unauthorized access of cloud resources
Data Loss Prevention	Detect and prevent customer sensitive data from being stored in the clear in the cloud
Vulnerability Assessment	Regularly run vulnerability scans of cloud resources, as you would do for clients/servers, and networks on-premises
Continuous Monitoring	Continuously monitor network traffic in/out of cloud services, as you would on networks on-premises
Log Correlation and Analysis	Collect and correlate log data from virtual machines in IaaS infrastructure, PaaS, and SaaS applications, like you would on-premises
DR and Business Continuity Planning	Put in place a disaster recovery and business continuity plan that includes regular back-up policies

Remember, you have the most to lose from a cyberattack on your cloud resources. Don't sit on your hands where cloud security is concerned.

How can you assess your cloud security needs?

- Are you migrating any applications from on-premises to the cloud (IaaS) to save IT-cost and improve operational efficiencies?
- Are you currently using any cloud-based services such as, Saleforce, Office 365, Google docs, Dropbox?
- Are your employees storing company/customer sensitive data in cloud-based applications?
- Do you lack centralized visibility of user activity across both your on-premises and cloud-based application environments?
- Do you have any regulatory compliance requirements across both your on-premises and cloud-based IT infrastructure?

If you have answered yes to two or more of these, you need a SOC-as-a Service.

Why SOC-as-a-Service is the right choice for Cloud Sercurity

Monitoring and securing all IT resources is challenging, especially in hybrid IT environments that is a combination of on-premises, private and public cloud deployments.

This is where SOC-as-a-Service with managed detection and response (MDR) makes all the difference. Using a cloud-based SIEM that aggregates data flow from your on-premises and cloud infrastructures in a single stream, and includes a dedicated concierge secuirty engineer.

AWN CyberSOC™ supplies all of the above, making it the ideal security service for SMEs that aim to make the most of cloud services securely.

With AWN CyberSOC™, your business evolves securely to the cloud.

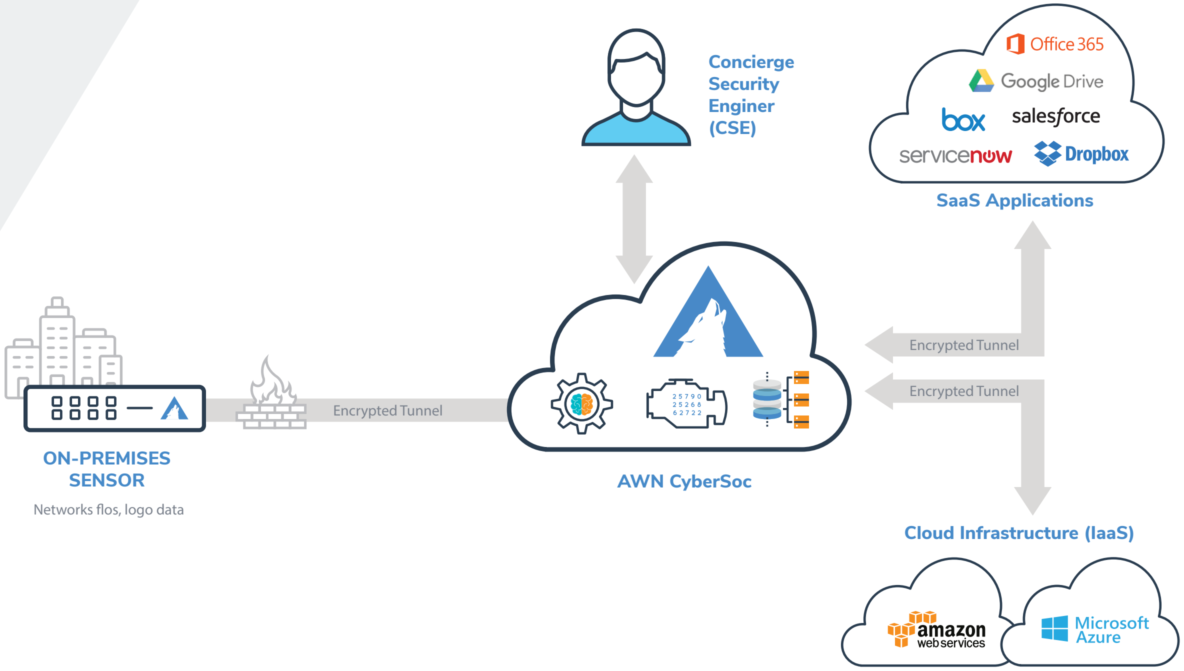
Keys to securing your use of cloud services

01 Monitor both on-premises and cloud resources 24/7

02 Have 360-degree visability into all potential attack surfaces

03 Customize security policies and compliance reports

04 Respond to threats in real time



Protect your applications and data in the cloud with Arctic Wolf Networks

AWN provides SOC-as-a-service that is redefining the economics of security. AWN CyberSOC™ is anchored by Concierge Security Engineers and includes 24×7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required.

For More Information
Call: 1-888-272-8249

Contact us
arcticwolf.com
ask@arcticwolf.com

ARCTIC WOLF

www.arcticwolf.com