NEXOR®

ENABLING SECURE INFORMATION EXCHANGE IN CLOUD ENVIRONMENTS

MARCH 2017

A NEXOR WHITE PAPER

INTRODUCTION

The commercial imperative to use cloud services is ever increasing. Security concerns, once a show stopper, should no longer be the barrier.

It has been reported that 'cloud security' is an oxymoron, a contradiction in terms. How can something that is abstract, ephemeral and cannot be touched by its users be trusted or secure? Of course, the cloud does exist in physical terms. The files, data and information are simply stored, accessed and moved around on other people's computers. Even so, the question remains: can this ever be trusted or secure?

During 2016 and into 2017, people have started to take the opposite view and say that if approached and managed in the right way, the cloud can actually be more secure than conventional file storage, retrieval and management systems.

This paper describes a proven approach based on tried and tested architectural models to enable the use of cloud services for sensitive data.

Globally, use of the cloud is increasing at an incredible rate[1]:

- According to Synergy Research Group, **the worldwide cloud computing market grew 21%** to $110 billion in 2015. That total includes cloud infrastructure services, software services, and hardware.
- According to RightScale's State of the Cloud survey, **17% of enterprises** now run over 1,000 virtual machines (VMs) **in the public cloud**, compared to 13% in 2015.
- According to research firm IDC, worldwide spending on **public cloud services could double** from almost $70 billion in 2015 to over $141 billion in 2019.
- The IaaS/PaaS markets are often dubbed the 'cloud infrastructure' market. According to Forbes, IaaS spending - fuelled by the growing need for remote computing power and storage - could rise from $38 billion this year to **$173 billion in 2026**.
- According to RightScale, **31% of enterprises** run over 1,000 VMs **in the private cloud**, compared to 22% last year. This indicates that this market, which mostly serves larger companies who need to keep their data on-site, is still growing.

This immense growth is driven by bringing lower costs, greater flexibility and wider ranging data availability to any enterprise.

Already the UK government is adopting a cloud-first purchasing policy for public sector IT.

> *'The 'Cloud First' policy will drive wider adoption of cloud computing in the public sector through the government **CloudStore**, the online marketplace for cloud IT services for the public sector. The Cloud First policy will embed the skills a modern civil service needs to meet the demands of 21st-century digital government and help us get ahead in the global race.'* Source: www.gov.uk

1: http://nxr.co/2mJs37n

INTRODUCTION CONT.

The benefits of adopting the Cloud are spread across a range of applications from the business back office functions, through collaboration tools, customer portals and the Internet of Things (IoT) - monitoring as well as command and control. The thing all these applications have in common is the ability to share information much more easily than ever before.

However, myths abound and people hold entrenched views and positions about cloud security. But the take-out from these emerging 'cloud-first' policies is that we have to find a solution. It is no longer acceptable to just say no.

Obviously, traditional online security is based on being able to see and touch controls, know exactly what they do and constantly monitor system performance. However, in the cloud:

- You don't own it;
- You can't touch it;
- Your control is limited to an API;
- It is often shared.

In short, you have to rely on third parties. So how can you turn that reliance into something you can trust?

This paper will argue that it doesn't matter what you are doing. As with conventional online security, if you apply strong principles around secure information exchange - the Cloud Cyber Essentials – solutions will be found.

Some industry experts even argue that the cloud is more secure. Leading organisations are migrating workloads to the cloud to improve the security of critical workloads.

Technology research company Gartner published a report in June 2016 entitled, '*How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center*.' It found that the automation and programmatic infrastructure of top Infrastructure as a Service (IaaS) providers can significantly improve the security protection of public cloud workloads – and if best practices are followed, they can be more secure than those in traditional data centres.

In this paper, we look at the principles behind the cloud that present us with security challenges and explore where responsibility for solving the issues lies. We look at the governance approaches to manage these complex responsibilities, and explore the data lifecycle and core touch points to protect the critical data.

Finally, we will review how the Nexor Secure Information Exchange Architecture can be used to provide data in motion protection.

WHO OWNS THE PROBLEM?

The definition of the cloud as set out by the US National Institute of Standards and Technology (NIST) based in the US is now commonly accepted and used.

NIST define the core characteristics of the cloud as on-demand self-service, broad network access, resource pooling, rapid elasticity and a measured service; from a business perspective, this translates to low-cost service availability and resilience.

NIST also define 4 cloud service delivery models: Private cloud; Community cloud; Public cloud and Hybrid cloud. From a business perspective, this translates to who provides the services, and, as we shall see later, who has responsibility for its secure operation?

Finally, NIST define 3 service models:

Software as a Service (SaaS)
Software as a Service (SaaS) is where the application is defined and managed by the supplier, with little opportunity to change the application behaviours. Beyond simple configuration, it is largely take it or leave it. Examples include Facebook, Google Apps and DropBox.

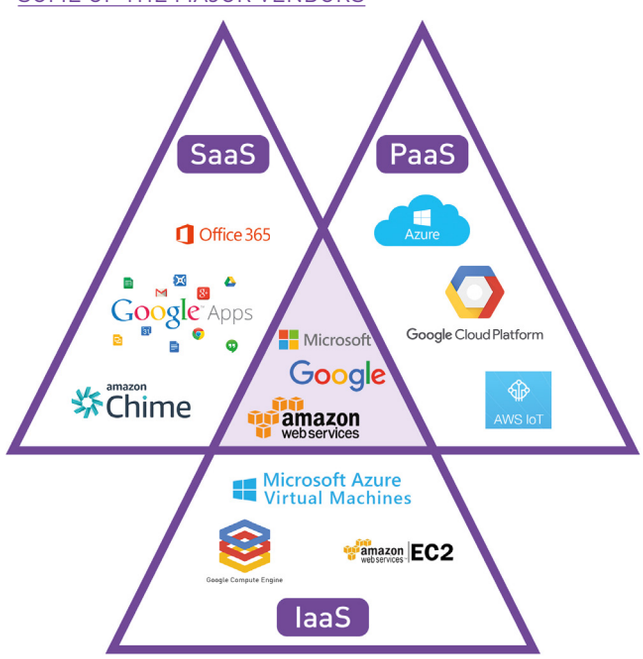
Platform as a Service – PaaS
With Platform as a Service, you are provided with a set of tools which can be used to build your own applications. Examples include Amazon Internet of Things, Windows Azure, Google App Engine.

Infrastructure as a Service – IaaS
Infrastructure as a Service provides compute and storage in the cloud, linked with virtual network services. Essentially you run the OS and applications on the service provider's 'hardware'. Examples include Rackspace, Amazon Web Services (AWS), and Google Compute Engine (GCE).

Figure 1 (above right) gives examples of the cloud platforms provided by a variety of the major vendors.

Whilst the **three definitions (SaaS, PaaS, IaaS)** have stood the test of time so far, the lines are starting to blur with major players like Microsoft, Apple and Google offering services in all three groups. What's more, a full business solution may encompass elements of each service type – a hybrid solution. **So, these distinctions may not really help when we think about security.**

Figure 1
EXAMPLES OF THE CLOUD PLATFORMS PROVIDED BY SOME OF THE MAJOR VENDORS



WHO OWNS THE PROBLEM? CONT.

Who is responsible for what in the cloud?

A different way of looking at this is to examine where the responsibilities lie. To clarify, we can break down a cloud offering into:

- **Governance**: how is it all managed to ensure consistency with corporate policy?
- **Data**: the core asset that the service is managing;
- **Application**: the tools the user interacts with to access and manipulate the data;
- **Platform/operating system**: Windows / Linux / Proprietary developer tools;
- **Communications**: how is access to the application and data achieved through a wide area network, as opposed to a local infrastructure?;
- **Infrastructure**: network switchers, routers, firewalls;
- **Physical**: the hardware it all runs on.

The difference between IaaS, SaaS and PaaS is who is responsible for what: you, the enterprise, the cloud service provider, or is it shared?

See Figure 2 below for a breakdown of responsibilities.

Being responsible for governance and data

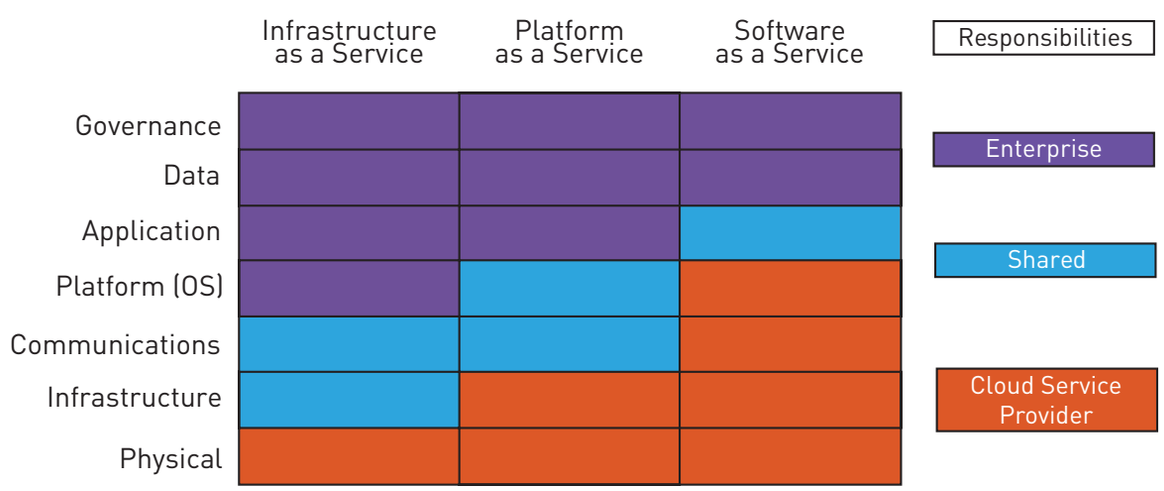
Breaking it down this way, it quickly becomes clear that **you, the enterprise, remain responsible for the governance and data, irrespective of the cloud service model chosen**. Moreover, the choice of service model - IaaS, SaaS or PaaS will depend on how much you want to outsource, and how much you wish to maintain responsibility.

As mentioned previously, in reality, the hybrid service model is used across most businesses, so you have to come at the problem from a governance and data management perspective to ensure a consistent approach.

One crucial point to note, is that even where you outsource as much responsibility as you can, you remain liable for any data security breach, even if you have instructed the cloud service provider to mitigate the risk. Your organisation will receive the regulatory fine, for example under the General Data Protection Regulation (GDPR) - not the cloud service provider.

In the remainder of this paper, we will explore the **governance** and **data layers** of this model. This is not to say you can ignore the other aspects – in fact, we will argue they all fall within the governance model, the difference being how you achieve the governance.

Figure 2
DEFINING RESPONSIBILITIES WITHIN THE CLOUD



GOVERNANCE

As we've already seen, governance of the cloud service model you choose is crucial. To simplify this, we can break the topic down into two parts. The areas you are responsible for and those you have delegated or contracted out.

Governance of your responsibilities

The cloud service provider is only part of the story. This will need to be incorporated into the business's overall governance environment.

Internal governance is not the focus of this paper, and there are many approaches that can be used. At Nexor we prefer the ENISA Security Framework for Government Clouds[2] which is based around the Plan-Do-Check-Act cycle embedded in the ISO management standards.

Governance of the cloud service provider's responsibilities

As we've mentioned previously, you can't duck liability, so where you've used a Cloud Service Provider (CSP), your governance programme has to validate that the CSP provides an adequate environment.

The National Cyber Security Centre has set out a framework of "*14 Security Principles*" that you need to consider when procuring a cloud service, summarised in Figure 3. As part of your procurement process, you should assess the proposed services against these principles to ensure you are being offered the security controls your business needs.

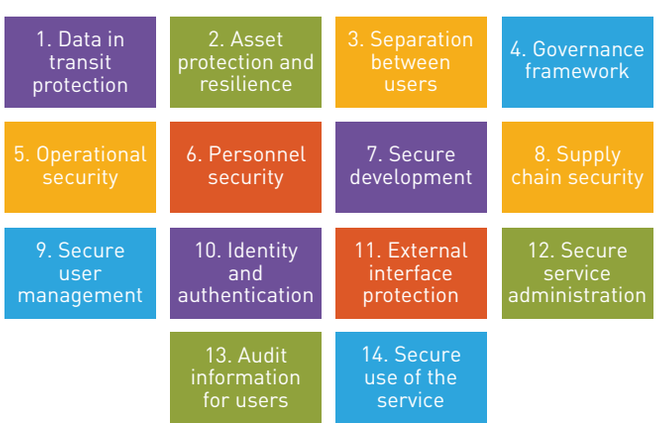
Added to this, is the Cloud Security Alliance's "*Security, Trust & Assurance Registry (STAR)*", which contains both a more detailed controls framework and a registry of how CSPs implement the controls.

Both of these frameworks (NCSC and CSA) cover governance. The STAR registry contains details of the governance processes the CSP implements, and details of the audit reports that are made available for you to obtain confidence they are doing what they claim to be doing.

Using these tools, you can establish what security controls the CSP has implemented, their governance mechanisms, including audit regime, to enable you to come to a risk judgement of the viability of the environment.

Having identified a suitable cloud service, you will also need to establish the policies and operational procedures for ongoing service management. This will include how you provide internal audit of cloud usage – this can be tricky as the information needed is not always readily available.

Figure 3
THE FOURTEEN SECURITY PRINCIPLES WHEN PROCURING A CLOUD SERVICE (SOURCE: NCSC)



2: http://nxr.co/2miqVdB

GOVERNANCE CONT.

SecDevOps

If your implementation uses IaaS or PaaS, you will need to build a robust methodology for the development and deployment of the application and the underlying IaaS and PaaS services they use.

This is often referred to as DevOps - a set of practices that emphasise the collaboration and communication of both software developers and information technology (IT) professionals whilst automating the process of software delivery and infrastructure changes.

Nexor take the view that DevOps does not go far enough. Security must be integrated, and not bolted on, a process referred to SecDevOps. The key features of SecDevOps are:

- **Managed Roll-out** – how the new capabilities are managed through the development lifecycle into deployment;
- **Operational Monitoring** – how the live service is monitored to ensure it maintains a live service in line with any service level agreements;
- **Security Monitoring** – how the system security is monitored to eliminate new vulnerabilities and enable early detection of intrusion;
- **Remediation** – how the service reacts when operational or security issues are discovered, and how the issues are addressed automatically.

It is via SecDevOps the Gartner claim of "*if best practices are followed, they [clouds] can be more secure than those in traditional data centers*" can be realised.

THE DATA LIFECYCLE

We've looked at governance responsibilities for each of the three cloud service models IaaS, PaaS and SaaS. Now we need to examine data responsibilities.

When using any of the three cloud service models IaaS, PaaS or SaaS, we should consider the data lifecycle when assessing security requirements and controls.

This is because it is always applied, and remains the area your business is liable for, regardless of where you have outsourced responsibility.

The lifecycle includes six phases from creation to destruction.

Although we show it as a linear progression, once created, data can bounce between the different phases without restriction, and may not pass through all stages; for example, not all data is eventually destroyed.

- **Create** – data can be created both in or outside of the cloud, and can be human or machine generated. Attesting the data integrity before 'accepting' it is a key challenge.
- **Store** – where and how is the data stored? What controls are applied to ensure only authorised access in later stages of the lifecycle?
- **Use** – providing access to the data in the cloud can be a human user, or machine analytics. Core controls are about ensuring only authorised access.
- **Share** – making the data available to others to copy outside of the specific cloud environment. Core controls are about ensuring only authorised access.
- **Archive** – effectively sharing the data with longer term storage, occasionally offline.
- **Destroy** – knowing where the data is and how you can erase it is important in the cloud, so you have to consider this upfront. Cryptography, perhaps, has a strong role, but if you don't encrypt in the first place this could be a challenge.

Figure 4
THE DATA LIFECYCLE (SOURCE: SECUROSIS)

Data Protection

Having looked at the data lifecycle, there are three different occasions when data is exposed and therefore at risk:

Data at Rest - The problem is protecting data where it is stored. This can be achieved by access control and encryption. This topic is outside the scope of this paper.

Data in Motion - How do you protect data when it is being moved between systems (into, out of and between clouds), and how do you protect systems from rogue data? There are a number of solutions including encryption - application, data or transport layer considerations, data transformation and data validation. This is Nexor's area of expertise and the **focus of this paper**. Nexor has developed SIXA, based on NCSC architectural models, which is all about the protection of data in motion.

Data in Use - Finally, how do you protect data when it is being used by cloud services - man and machine. This can be achieved by access control and identity management. This is outside the scope of this paper, but there is a strong link with Nexor's Data in Motion controls.

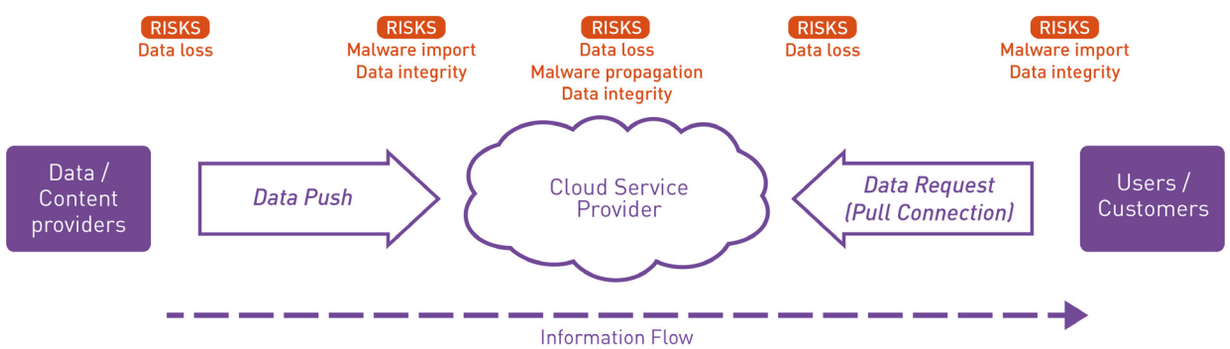
DATA IN MOTION

Nexor is a secure information exchange specialist. Our core mission is to help organisations get information into and out of secure networks. Our information exchange solutions have particular relevance to the Data in Motion aspect of the data lifecycle.

Data in Motion generally follows three paths:

1.	**Data export to the cloud either by organisation or user**	• Risks (to data owner): unauthorised data loss. • Risks (to cloud): malware import, data integrity.
2.	**Data import from the cloud to organisation, user or partner**	• Risks (to cloud): unauthorised data loss. • Risks (to data user): malware import, data integrity.
3.	**Data migration within the cloud**	• Risks: unauthorised data loss, malware propagation, data integrity.

Figure 5
DATA IN MOTION



Introducing SIXA

For all three of these Data in Motion paths, Nexor has developed SIXA, which is based on National Cyber Security Centre architectural models and is all about the protection of data in motion. Nexor can apply the proven methodologies of SIXA to protect these three motion paths.

SIXA is an acronym meaning Secure Information Exchange Architecture (SIXA). As part of our specialisation in addressing secure information exchange challenges, we have developed our own modular architecture. It consists of a number of configurable building blocks that follow best practice design patterns from the National Cyber Security Centre (NCSC, formerly CESG), the UK National Technical Authority, for the import and export of data across security domain boundaries.

The three building blocks at the heart of SIXA are:

Transform - Modify the content or protocol for interoperability or security purposes. Sometimes referred to as a gateway.

Flow Control - Ensure data only flows in the direction required to support the business process. Often delivered by a firewall (two-way data flow) or a data diode (one-way data flow).

Validate - Ensure the content (and in some cases protocol) conform to the security policy. Sometimes referred to as a guard.

DATA IN MOTION CONT.

Using the **Transform** and **Validate** modules in particular, SIXA can be used quite simply to manage the import and export of data to the cloud, as well as data flow within the cloud. This is the exact use case set out in National Cyber Security Centre design patterns.

A key difference when implemented in the cloud environment is that when SIXA is located on site it has physical attributes – you can touch it and see it, and you know where the wires come in and go out. In essence, you manage what is connected to what. This gives a layer of physical control missing in the cloud, so the risk needs to be mitigated in other ways.

One of the additional controls used to manage this risk is **Identity**. We can't control who has access based on where the wires go, so we need to provide assurance that we know who we are communicating with.

Therefore, we have enhanced the SIXA model, when used in the cloud, to add Identity. The identity controls are used to enable the cloud service to ensure the connecting user or systems is who they claim to be, and they are permitted to use the service.

This also applies the other way around – the connecting service validates it is connecting to the genuine cloud service, and not a rouge phishing site (for example).

With on-site deployments, you can easily add **Flow Control** elements, such as data diodes, to enforce one way data flows. It might seem that this is not possible in the cloud. However, some of the software-defined network controls enable 'virtual diode' capabilities. This means that flow control is equally possible in the cloud – arguably with greater flexibility.

Cloud SIXA

The movement of data within the cloud is more of a challenge. The concept of a network separation by use of a physical device does not apply; however, the concept of virtual private clouds (VPCs) can be used to separate services.

By breaking the National Cyber Security Centre architecture down to its fundamental components, which include transformation and verification, and by looking at the communication paths in the cloud, it becomes apparent that the SIXA architecture still very much applies – it just needs to be deployed differently.

With Cloud SIXA we use virtual private clouds to segregate cloud services and deploy SIXA components to manage the data in motion between the VPCs.

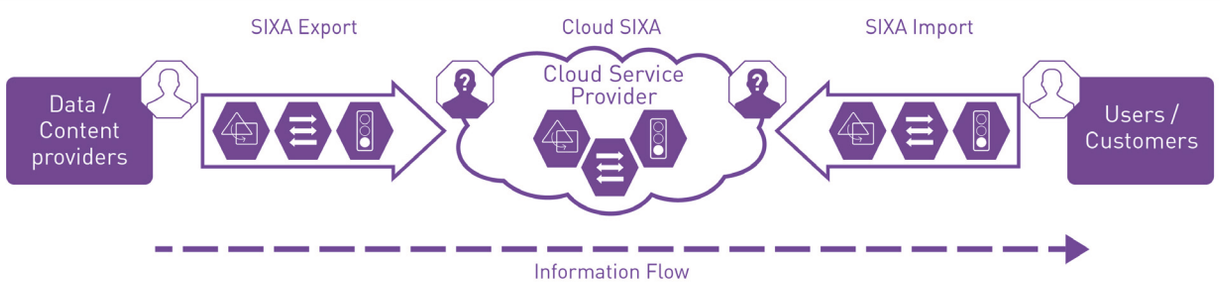
Persistence

There is a core feature of the cloud that can fundamentally change the Physical SIXA deployments from Cloud SIXA deployments: **Persistence**.

When integrating a SIXA component such as a verification guard, a key challenge is to ensure that malware-infected protocol or data cannot adversely affect the operation of the guard itself.

Advanced Persistent Threats (APTs) are a major threat that the platform needs to protect itself against, and companies like Nexor put a great deal of effort into platform protection. APTs are coordinated cyber activities usually deployed not to bring down a business, but to stay embedded within its systems and extract information at a slow and undetected pace.

Figure 6
SIXA APPLIED TO THE CLOUD



DATA IN MOTION CONT.

The Cloud offers a use-model that is of significant benefit here – non-persistence or transience. Careful system engineering enables us to build transformation, verification and flow control modules that are transient – they are created for the sole purpose of a single instance of a data flow, perform their task, and disappear.

This means that even if there are content-based APTs that attack the checking tool, the attack disappears after the verification or transformation, so the threat will find it significantly harder to persist.

This 'APT resilience' is a perfect example of how a cloud engineered solution can actually be more secure than a traditional physical platform.

Example Cloud SIXA solution

To bring these concepts together, consider the following scenario. A government department wishes to obtain information for a citizen, by way of a PDF file. There is a risk the PDF file contains malware, a risk that needs to be managed. The SIXA model is to transform the PDF into a new format and verify its structure, then create a new clean PDF.

Deploying this in the cloud using Amazon Web Services could be implemented as below in Figure 7.

An AWS CloudFront PaaS with non-persistence and auto-scaling is used to create a web front end, ensuring it is able to meet peaks of demand, elastically. This provides the user capability to upload a file. The file is placed in an S3 bucket.

A non-persistent AWS Lambda function notices the file upload, performs the transformation and verification, and copies the clean file to a new S3 bucket, where it can be used by the government user or application with confidence that the risk has been mitigated.

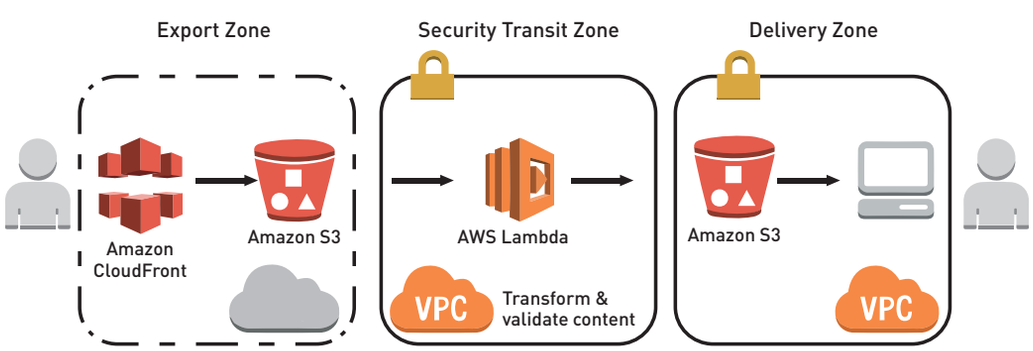
The SIXA components are split between three different management domains; the key feature is the Lambda function runs in its own VPC, with the only connection via S3 buckets (and the management interface), thus hard to attack.

Any content-based attacks affecting the Lambda function will be unlikely to gain a foothold, as a new instance of the Lambda function is created every time.

In this example, we have shown how traditional, tried, tested and assured Nexor SIXA concepts can be applied in cloud environment, where the security characteristics of the cloud (non-persistence) are used to provide additional security controls, which traditional solutions find hard to achieve.

This is just one example – the Cloud SIXA concept can be applied as widely and flexibly as traditional SIXA.

Figure 7
CLOUD SIXA DEPLOYED IN AMAZON WEB SERVICES (AWS)



IN CONCLUSION

This paper has shown that with appropriate governance and data lifecycle controls, the Cloud can be more secure than traditional IT solutions.

To make this case we show that no matter what model is used to adopt cloud services, the adopting organisation remains responsible for the data. If the data is lost, the adopting organisation must deal with the consequences - be it loss of business through to regulatory sanctions.

Different cloud models provide you with differing options in terms of the security controls that are available and the level of configuration of these controls. Implementing a strong SecDevOps and governance model can lead to the cloud being mode secure – as presented by Gartner (see below).

Gartner: 'How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center'

The automation and programmatic infrastructure of leading IaaS providers enables enterprises to significantly improve the security protection of public cloud workloads to the extent that, if best practices are followed, they can be more secure than those in traditional data centers.

Strategic Planning Assumptions

- *Through 2020, workloads that exploit public cloud IaaS capabilities to improve security protection will suffer at least 60% fewer security incidents than those in traditional data centers.*
- *Through 2020, 95% of cloud security failures will be the customer's fault.*
- *Through 2020, 99% of vulnerabilities exploited will continue to be ones known of by security and IT professionals for at least one year.*

This is not the whole story; the data is your responsibility too. As such understanding the data lifecycle is crucial – this will drive an understanding of where the data flows, and where the relevant data controls be implemented. We describe how Nexor's tried and tested SIXA architecture can be applied to cloud environments to ensure the security of the data flows, maximising an organisation's ability to protect the data.

The commercial imperative to use cloud services is ever increasing. Security concerns are no longer the barrier – perceptions are!

WHY NEXOR?

Nexor is an expert in developing world-class secure information exchange capabilities that protect data in motion in mission critical systems. With our heritage in research, we continue to innovate and apply this approach to create high integrity, cross-domain solutions in hostile environments like the unprotected cloud.

Our innovative secure information exchange systems have created competitive advantage for our customers, and on several occasions Nexor has produced an innovation that proves to be a technological first.

Our solutions are based on our industry-leading SIXA technology portfolio, which has a modular architectural design that offers both security and flexibility. Combined with our technology integration and software engineering capabilities, this ensures that we can provide deployments for an extensive range of secure information exchange scenarios, including use of the Cloud.

At Nexor, we believe a solution can only be a success if the business context and problem space are properly understood.

To enable us to do this, we developed CyberShield Secure, a consultative delivery methodology for working with our customers. It has been designed to put the customer's business requirements and security constraints at the heart of any engagement and is based on industry best practice for secure engineering.

The Cloud is here to stay, it will not evaporate; it is a technical innovation that enables new business models and is driving down cost. Secure information exchange into and out of cloud environments will continue to be a requirement.

The body of knowledge on how to build secure systems has evolved over decades as processes and technologies have matured. The lessons from these traditional computing paradigms are embodied in SIXA and have now been applied to ensuring data in the cloud is secure too.

CONTACT DETAILS

Nexor Limited, 8 The Triangle, Enterprise Way
ng2 Business Park, Nottingham, NG2 1AE, UK

+44 (0)115 952 0500
info@nexor.com
www.nexor.com