Cloud Security Services

Secura delivers world-class security assessment services. Naturally, these also include cloud security services. Whether you simply utilise virtualised servers at a provider, or have built your entire workload in the cloud using microservices, in all cases your security is still your own responsibility in the end. Secura can help you gain insight into the threats to, and security status of all your cloud-connected and cloud-dwelling applications and data.

What Is the Cloud Really, Anyway?

According to the well-known trope, "There is no cloud, it's just someone else's computer". And to an extent that is true. It certainly embodies the notion that you don't control everything as you would in an on-premise situation with hardware that you own. However it fails to address where exactly this split in responsibilities is made. Commonly, several cloud deployment models are distinguished:

- **IaaS: Infrastructure-as-a-service.** In this model the user is presented with visualized instances of various hardware components such as servers, storage, routers or firewalls. The user is largely responsible for installing software and OS updates.
- **PaaS: Platform-as-a-service.** In this model, the software platform is also visualized and presented to the user as if they ran the software on their own installation. This model is often used for CSMs, or business-connectors such as Biztalk, and a large number of specific services within AWS and Azure follow the Paas model, as do many DevOps-related services such as Kubernetes, Jenkins and others.
- **SaaS: Software-as-a-service.** Here, the whole application is offered in a managed contract to the user. You share all underlying components, except your data. Office365 is a common example of a SaaS service, as is SalesForce.
- **FaaS: Functions-as-a-service.** For small, automatable tasks that need to scale, it is not practical to utilize any of the above-mentioned models. Therefore the major cloud providers also have a model where users can provide code for a specific function (in many popular languages such as Java, Python, PHP and others) and run it on demand. The application owner is only responsible for providing the code. Azure Microservices and AWS Lambda functions are the most common offerings.

From On-Premise to SaaS

On-Premise	IaaS	CaaS	PaaS	FaaS	SaaS
Data	Data	Data	Data	Data	Data
Application Code	Application Code	Application Code	Application Code	Application Code	Application Code
Data Store	Data Store	Data Store	Data Store	Data Store	Data Store
Runtime / Middleware	Runtime / Middleware	Runtime / Middleware	Runtime / Middleware	Runtime / Middleware	Runtime / Middleware
Containers	Containers	Containers	Containers	Containers	Containers
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Hardware	Hardware	Hardware	Hardware	Hardware	Hardware

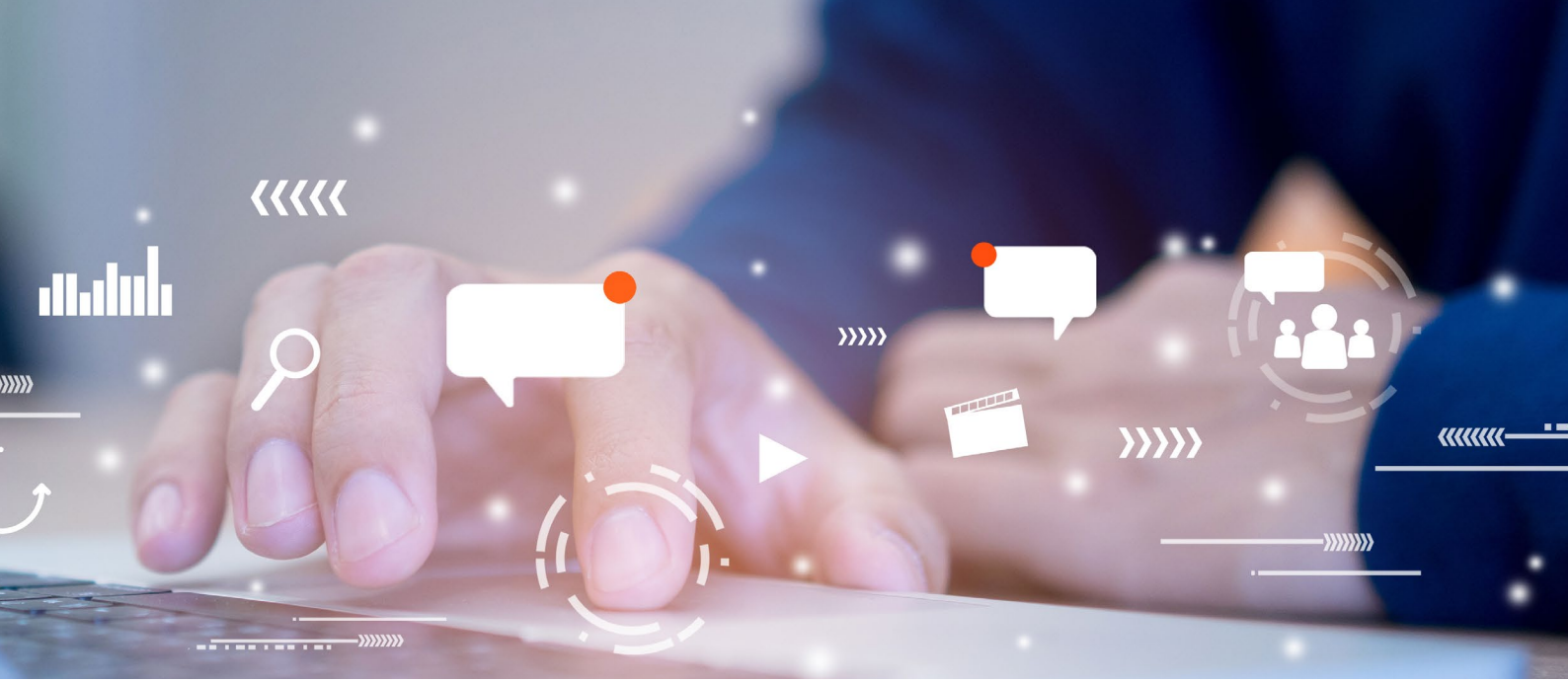
Cloud Service Customers CSCs) *Cloud Service Providers (CSPs)*

It is entirely possible to specify 'anything'-as-a-service and many other concepts exist as a result, including DaaS (Data-as-a-service, or Desktop-as-a-service), DBaaS (for Databases) and CaaS (specifically for containers such as Docker and related products such as Kubernetes). The biggest difference with traditional models of course is the shared control aspect. In an on-premise situation you have control over all aspects. In the IaaS model, you still control everything, except the hardware. And on the other side of the spectrum, with the FaaS-model, you only control the actual code that runs and nothing else.

The varying scopes of control can make it very difficult to describe and implement security measures and many projects make (incorrect) assumptions about who controls what, and who is ultimately responsible for security. And indeed, while you don't have to worry about patching software, servers and operating systems when using a Saas-provider, you as data owner are still responsible for many choices that govern data security.

Secura currently offers a number of services that relate to cloud deployment models. Some are virtually the same as the non-cloud versions: a grey-box application vulnerability assessment (see our Vulnerability Analysis and Penetration Testing services brochure) will not differ much when performed on an IaaS-hosted application, as compared to a fully on-premise installation. However for PaaS and SaaS models, they can differ significantly in focus and execution. The same goes for infrastructure vulnerability assessments.

For this reason, Secura has developed a number of cloud-specific service offerings that augment the existing application and infrastructure assessments and assurance services that we have always performed.



Crystal-Box Cloud (CBC) Assessment for Cloud Service Customers (CSCs)

As customer of a Cloud Service Provider (CSP), you must trust that the cloud foundation is in order, but you have few possibilities of actually verifying that. Moreover, many CSPs are themselves also customers of other CSPs and wish to provide transparent assurance on security to their customers. In the shared responsibility model, there are important aspects that the cloud service providers control, that a customer cannot see or influence. In most cases a CSP provides assurance about these aspects through certification and compliance schemes such as the Cloud Control Matrix (CCM). If not, Secura can provide assurances for service providers on these aspects (see below for our Cloud Controls Matrix offering). In many cases Secura can build on existing CCM assurance reports (although we always double check).

In our security assessments for Cloud Service Customers (CSC) we focus on what lies within the sphere of control of the CSC. Analogous to a crystal-box (or white-box) application security assessment, the Crystal-box Cloud assessment (CBC) is performed with as much information available to the testers as possible. This enables the most in-depth testing to take place, and provides insight into detailed configuration settings and authorizations. In a purely application-focused assessment, this usually means that the source code is available to the testers so that complex and hard-to-find vulnerabilities can be identified. In the cloud, in addition to the source code of an application, Secura can identify weakness by examining the actual cloud configuration settings.

The following topics will be addressed in such an assessment:

- **Data Protection**
  - Unintended exposure of data
  - Encryption of data storage (S3 buckets or otherwise)
  - Key Management (such as CloudHSM or Keyvault)
  - Credential management
  - Data Loss Prevention (DLP) settings
- **Identity and Access Management**
  - User groups and permissions
  - Service authentication settings
  - Account Policies
  - Synchronization and Identity Federation settings
- **Logging and Monitoring**
  - Log service usage
  - Regional settings
  - Log file encryption
  - Workload monitoring
- **Network Security**
  - API Management
  - VPNs
  - Network access controls such as VPC, SG, NSG and VNet security settings
  - TLS certificate and Public Key Infrastructure usage

Secura begins by using an authorization key (that you supply) for your cloud accounts that allows Secura to access the configuration settings in your account (read-only). First, Secura uses a cloud-scanner to read out these settings, and will also compare them best practices (CIS baselines). This first

step provides Secura with the insights needed to dig deeper and perform manual checks that go further than tool-based, automated checks. Then, as a second step, Secura will search for flaws in business logic and application logic: for instance, conflicting roles and authorizations will be found, as well as potential misconfigurations of interfaces to the outside world. All these tests and checks result in a written report that clearly describes the weaknesses in your cloud configuration, as well as the risks identified. Clear, actionable recommendations for improvement are also included so that it is possible to remediate all our findings efficiently.

Note that though such a crystal-box-cloud assessment can be performed on its own, it is usually executed in conjunction with an application or infrastructure security assessment (black, grey- or crystal-box) to provide you with an unprecedented security 'x-ray' of your cloud-dwelling application landscape. However it is equally possible to perform the assessment on the cloud configuration only. Secura often performs such assessments together with configuration reviews of the relevant application environment, including operating system hardening (mainly for IaaS customers). This is especially important where it concerns DevOps and Container orchestration, using Docker and Kubernetes for instance. Such tests are quite specific, looking at segmentation and hardening of container clusters, updates and network policies and Kubernetes pod security policies. This also includes testing from the vantage point of a compromised pod or Docker container, deploying rogue pods, and lateral movement between nodes or namespaces.

All our cloud assessment services, whether application security, cloud configuration or DevOps orchestration in the cloud, are vendor-agnostic. Secura has intimate knowledge of the major cloud providers obviously including Microsoft Azure, Amazon AWS and Google Cloud. And Secura regularly tests environments in other vendor-specific (PaaS and SaaS) contexts such as the SAP Cloud, Oracle Cloud or Mendix Cloud and can also help your organization stay secure when moving to the cloud from an on-premise situation.

CCM Compliance Audits for Cloud Service Providers (CSPs)

Whereas Secura's CBC assessment services focus on directly helping customers of cloud service providers, Secura also has the knowledge and qualified auditors to assist Cloud Service Providers (CSPs) with providing assurance and guidance to their customers. While larger vendors have already gained the trust of the industries and markets, smaller vendors or CSPs that offer cloud-based SaaS and PaaS services are often asked to provide assurance on their control of data security for their customers. An ISO27001 certification is of course a good starting point but fails to include cloud-specific controls and compliance aspects. For this reason, there exists an extension to the ISO27002 standard, specifically for cloud providers (ISO27017), and also an extension for personally identifiable information (PII) in the cloud (ISO27018). Furthermore, the Cloud Security Alliance (CSA) specifically developed the Cloud Controls Matrix (CCM) framework as a stand-alone framework addressing a full gamut of controls with regards to cloud security.

The CCM is by now of course a well-known standard when it comes to assessing CSPs. It is specifically designed to provide fundamental security principles to guide CSPs and to assist (prospective) cloud customers in assessing the overall security risk of a cloud provider. It has a tight relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI and NIST.

While the CCM standard is positioned to be used by cloud consumers, it is clear from the standard that a significant number of controls cannot be directly checked by a CSP. Instead, what is needed is for an auditor to audit the CSP against this framework, for instance using the International Standard on Audit Engagements 3000 (ISAE 3000) assurance standard. This then enables the CSP to prove to the (prospective) customer that an independent auditor has verified adherence to the CCM.

As you can expect from a professional services organization such as Secura, we provide such ISAE3000 assurance audits for CSPs and their customers. Our certified and registered IT-Auditors (Register EDP-auditor, or RE in Dutch) are qualified and Secura's audit process is efficient and modern, supported by various tools and fully compliant with modern audit standards. What's more, they can build on the knowledge and experience of our technical experts who perform cloud security assessments for our customers.

The CCM assurance engagement starts with defining of the scope of the audit. Based on the cloud architecture

and service descriptions, Secura determines the subject of the audit and the controls (objectives) that need to be assessed. Moreover we identify the relevant stakeholders. After understanding the services and architecture we assess the risks involved and plan the audit work.

The findings from our audit will be verified with the auditee before they are reported. After receiving conformation of the findings we issue the final Assurance Report including our opinion. The Assurance Report is produced in line with internationally recognized assurance standards, offering you an independently attained, qualified opinion for proving your cloud security according to internationally accepted audit standards.

With our audit report, CSPs can provide their customers assurance on the quality of controls in their organization, while the customers have a qualified opinion on the control level of the service provider they are dependent on. Additionally the report provides a list of specific user controls that customers need to implement themselves to stay in control.

The audit report can be a considerable step forward, also to other certifications and recognized schemes such as the Cloud Security Alliance STAR Certification.

Conclusion

Secura aims to be the best security partner for her customers, and that is no different when it comes to broad coverage of technology stacks and cloud computing. If you have any questions regarding this offering or any other service offered by us, please do not hesitate to contact your account manager or Secura's offices directly.

Interested?

Would you like to learn more about our services? Contact us today:

Follow us:

+31 88 888 31 00

info@secura.com

secura.com