KuppingerCole Report

WHITEPAPER

by Alexei Balaganski | September 2020

Safeguarding Your Most Valuable Data: Five Key Criteria to Assess Cloud Provider Security

This whitepaper focuses on defining the key security-focused selection criteria to help your company choose a secure platform for current and future cloud projects.

by **Alexei Balaganski**
ab@kuppingercole.com
September 2020

Commissioned by Oracle

Content

Related Research

Leadership Compass: Infrastructure as a Service – Global Providers – 80035

Advisory Note: Security Organization Governance and the Cloud – 72564

Advisory Note: Cloud Services and Security – 72561

Advisory Note: How to Assure Cloud Services – 72563

Executive View: Oracle Identity Cloud Service – 80156

Executive View: Oracle Database Security Assessment – 70965

1 Introduction

Digital Transformation has profoundly changed our entire society, especially in the last decade. The world today is quickly growing more digitalized, interconnected, and complex.

Most companies seem to intuitively understand the cloud's operational benefits such as elastic scale, reducing costs, automation, and even security. Yet some see risks such as added network latency, potential availability problems, or the risk of cloud vendor or platform lock-in.

A surprising majority of IT specialists see the cloud as a more secure alternative to their existing on-premises infrastructure. This can be especially true for smaller companies with limited IT security staff. All Cloud Service Providers (CSPs) invest heavily in the security and compliance of their infrastructure and gladly offer their customers a large portfolio of security solutions and services.

Cloud provider selection and assurance should be a major part of every organization's IT governance. Otherwise, security can devolve into a "cargo cult", its only purpose being another checkbox in a compliance audit form.

However, many companies are still struggling with identifying the basic criteria for selecting the right cloud provider for their business needs, security policies and compliance requirements. This whitepaper focuses on defining five key security-focused selection criteria to help you with this choice.

2 Key Challenges

Information technology and the digitalization of our society have promised to make our lives (and our businesses) better and more efficient. To be fair, the sheer number of new opportunities they have unlocked for organizations is astonishing.

These new opportunities have brought new risks and challenges, and perhaps the most obvious of them is complexity. The explosive growth of digital information and its barely controlled sprawl across multiple environments, platforms, and silos can leave IT operations and security teams overwhelmed.

Compliance can be a major roadblock for companies operating in highly regulated industries or dealing with sensitive information like personal data covered by regulations such as EU GDPR. All these difficulties effectively force the majority of modern businesses, with the exception of a relatively small percentage of "100% cloud-native" startups, to operate their IT in a hybrid model, making it even harder to maintain consistent data protection policies across on-premises and cloud environments.

It is therefore unsurprising that a large number of security incidents can be directly traced to incorrect deployments, configuration errors, missing patches, and other human mistakes. Unfortunately, humans continue to be the weakest link in the chain of IT security, and this does not apply just to administrators.

Whether an action of a malicious insider like a rogue admin or disgruntled employee leaving the company or a simple case of negligence – in an increasingly digital company these errors can lead to a massive data breach.

Additionally, when sensitive data is stored in the cloud, the circle of malicious "insiders" can increase unexpectedly, now including not only your own employees, but the service provider's administrators and support technicians, and even other customers sharing the cloud infrastructure with you. With multiple known exploits that affect multi-tenant environments typical for public clouds – the Meltdown and Specter vulnerabilities in Intel processors perhaps the most well-known – the problem of "nosy neighbors" obtaining illegal access to your sensitive data is a risk.

A 2019 study by Ponemon Institute has established that the global average cost of a data breach has increased to $3.92 million dollars, with smaller companies hit proportionately harder. While system vulnerabilities and human error are still the largest direct contributors, third party breaches and cloud adoption are substantial risk multipliers.

More importantly, however, the total cost of most data breaches often does not include indirect business losses caused by the erosion of customer trust, negative effect on brand reputation, etc. These factors have a long-lasting effect, continuing to impact a company's business even years after the initial breach report. Such consequences cannot be mitigated by any technical means, although proactive investments in a proper incident response management plan can be recommended to any company, regardless of its size or industry.

Last but by no means the least are the fines for compliance violations imposed on the corporate victims of data breaches by regulatory authorities. GDPR fines are perhaps the most well-publicized at the moment, with massive amounts imposed on companies that suffered large-scale personal data breaches. The current GDPR fine record holder is British Airways with a $230 million fine issued last year. However, other, less publicized industry-specific fines like PCI DSS violations for companies dealing with credit card transactions can quickly pile up, since they are applied each month until the company returns to a compliant state.

It is also worth stressing that if a data breach happens in the cloud, the cloud service provider will not likely be held responsible for losses. According to the widely adopted shared responsibility model, the responsibility for security and compliance is split between the cloud service provider and the customer. The actual division varies between IaaS, PaaS, and SaaS models, but responsibility for the data stored in the cloud always remains with the customer: from sensitive data discovery and classification, to access governance and activity monitoring, to user risk assessment and management.

The best way to deal with these challenges is to avoid them altogether by having proactive security controls in place to minimize the risk of a data breach, this is true for on-premises and cloud. In the next section, we'll look at some of the most important things to consider when choosing a cloud service provider.

3 Five Key Security Criteria to Build Trusted Platforms

When organizations deliver IT services from their own data centers, they can maintain tight control over the security and compliance. The growing demand for distributed and highly scalable, yet affordable computing, is driving organizations to adopt cloud services, possibly even from multiple providers. While these services are a major enabler of digital transformation and provide greater flexibility as well as lower costs, concerns over compliance and security remain.

When companies decide to replace parts of their own, on-premises IT infrastructure with cloud-based services, they inevitably face a trade-off between outsourcing a large part of operational costs and management effort to an arguably more qualified third party service provider and giving up control and even further reducing visibility into the operations of that provider's cloud infrastructure. Thus, though migrating to the cloud can make a company more secure, this does not happen automatically, contrary to a popular misconception. There are important security criteria that must be considered when selecting a cloud service provider.

Key Criteria #1: Security Capabilities that Support Shared Responsibility Model

For Infrastructure-as-a-Service (IaaS), the cloud service provider has no control over how the service is being used by the customer and is responsible for securing the physical infrastructure used to provide the service. The customer is responsible for security from the operating system upwards. For Platform-as-a-Service (PaaS), which often includes managed middleware such as databases, the CSP is responsible for the security of the physical infrastructure, operating systems, and the managed middleware. The customer is responsible for the security of how they use these managed services and data therein. For Software-as-a-Service (SaaS) offerings, the CSP is responsible for the security of the infrastructure, operating systems, middleware, and applications.

Thus, regardless of the consumption model chosen by a customer, they still retain responsibility for the security and compliance of the data processed in cloud services. In terms of the GDPR, for example, this means that the customer retains the role of Data Controller even when their users' personal data is stored in the cloud and processed by a CSP. The customer will also bear all the consequences of a data breach caused by a misconfiguration of a cloud service, lack of data encryption in transit or at rest, or for any other missing or misconfigured security control, even those which are provided by the CSP. Naturally, this makes the process of evaluating the existing security capabilities of a cloud platform a key factor in any organization's governance, risk, and compliance processes.

Key Criteria #2: Cloud Security Controls for Defense in Depth

With such a broad range of risks influencing the sensitive data in the cloud, ranging from compliance and business continuity issues to cybersecurity (such as infrastructure attacks, account hijacking, privilege abuse, or platform vulnerabilities) and data security (such as improper classification and encryption, key management, or isolation failures) risks, the task of securing it properly and reliably

cannot be solved at a single “security perimeter”. Instead, a multitude of security controls deployed at every level of the cloud application architecture is required.

This approach predates the cloud and has long been known as “defense in depth”, where multiple physical, technical, and administrative controls are deployed to ensure that every risk is covered by several mitigation measures at different locations. Of course, every CSP has a broad range of tools and services either deployed and managed by themselves or offered to their customers.

The first and foremost challenge is to ensure that the security controls at all levels, from the hardware powering the cloud infrastructure all the way up to the applications and data sources, are operating in accord despite the fact that they are managed by different parties. Each component should be properly monitored and configured for quick remediation. Second, all these controls must be set up for redundancy to ensure that if some fail, others will be there to compensate. This is especially crucial to protect against insider threats, where some of the security controls can be manipulated by rogue administrators.

Finally, the resulting security architecture must be able to provide uniform and consistent visibility into all security events, provide a foundation for IT governance, and allow for quick response and remediation of detected threats. In theory, every cloud service provider should be able to provide this level of defense in depth to all their customers.

Key Criteria #3: Secure by Design

Most cloud service provider security tools are still just tools and add complexity. When a security feature is implemented as an optional add-on to a business-relevant product or service, someone still has to know that it exists to deploy and configure it properly. Then the security tool must be monitored continuously. Security alerts have to be investigated and acted upon. Security tools also require periodic bug fixes themselves, and they receive new features from time to time. CSP customers must utilize the latest best practices for these tools.

Security by design as a principle defines inherent security as one key requirement for the specification of software and systems. This results in software that has been designed and implemented to be thoroughly secure. Security by design can be understood as the integration of strong security requirements and relevant security aspects into all phases of the software development process starting from the requirements analysis through the development of testing and on to the deployment.

When these principles are applied on a larger scale to cloud environments, we again expect them to influence the design and operations of every layer of the whole platform: security controls must be designed as integral parts of the underlying hardware, networking stack, storage facilities and so on, all the way up to the application logic and activity monitoring. Unfortunately, for all cloud service providers this is not necessarily the case.

The first public cloud service providers appeared over 15 years ago, and back then security was not the first priority in their platform design. Threat landscapes, business requirements, and compliance regulations have changed considerably since those times.

In fact, it is the newer players in this market that have a unique opportunity. Instead of catching up with the veterans' efforts, they can benefit from early mistakes and focus on embedding security into their infrastructure from the design phase and build a future-proof, next-generation cloud architecture to meet current needs and anticipate future customer challenges.

Key Criteria #4: Secure by Default

One of the primary reasons for not doing security properly (which in the worst cases degenerates into a cargo cult mentioned earlier) is insufficient guidance and a lack of widely accepted best practices in every area of cybersecurity. The best security controls do not work if their existence is not communicated to users and if they are not enabled.

Of course, every IT expert is supposed to know better and never make dangerous mistakes. Unfortunately, not every company can afford to have a team of such experts. The notorious skills gap is real – only the largest enterprises can afford to hire enough real pros, and for smaller companies, managed security services are perhaps the only viable (yet still costly) alternative. And remember that even those experts can turn rogue and become malicious insider actors themselves.

For software, the "secure by default" principle means that the default configuration settings are the most secure settings possible, even at the expense of flexibility or user-friendliness. For large cloud environments, this introduces numerous challenges: how to ensure these settings are consistent across multiple infrastructure layers and services, how to keep them up to date with changing best practices, how to apply them to existing customers without breaking existing functionality, etc.

Key Criteria #5: Automated Security

As companies are dealing with growing volumes of digital information that powers their key business processes and often becomes their most prized asset, storing, analyzing, and properly securing this information is becoming increasingly complicated. Although outsourcing these activities to a qualified third party like an MSSP or a cloud service provider is one of the most popular solutions for companies, in the long term this approach is just as unsustainable, since those providers end up experiencing the same "skills gap" problems with alert fatigue and lack of qualified personnel to operate their own infrastructures.

Automating the largely repetitive and manual jobs of administrators and security analysts has been a popular trend in recent years: from configuration management and orchestration to security event correlation and behavior analytics powered by machine learning – the market offers a plethora of tools to improve the productivity of human experts. However, the ultimate holy grail for automating cybersecurity nowadays, at least according to the press, is Artificial Intelligence.

Having AI as a potential replacement for overworked humans to ensure that threats and breaches are detected and mitigated in real time without any manual forensic analysis and decision-making – that has been a dream for both security experts and the general public.

Cloud service providers have always been at the forefront of modern AI technology developments. Large-scale hardware reserves combined with massive amounts of security telemetry they are collecting from their infrastructure and services give them a strong competitive advantage.

Still, it must be stressed that artificial intelligence, at least in its practical definition, was never intended to replace humans, but rather to augment their powers by automating the most tedious and boring parts of their jobs and leaving more time for creative and productive tasks. And with several technological challenges specific to the field of cybersecurity, such as the availability of quality training data for ML models, insufficient formal verification and testing of those models, and the need to constantly adapt to new threats, making strategic decisions based on overblown expectations could be a risky move.

Unfortunately, at least until the arrival of General Artificial Intelligence, these challenges cannot be addressed by automation alone, even if it is based on AI/ML technologies. Ensuring that all management controls to an IT system are sealed and all human access to it is eliminated – that is the distinction of "autonomous" solutions as opposed to more traditional "automated" ones.

There is however another, an arguably more important aspect of security automation to consider, especially for cloud environments: elimination of the human factor. To err is human, and human mistakes (service misconfigurations, improper access, or just plain negligence) account for the majority of data breaches. In the next section, we will have a closer look at the latest security-related developments Oracle now has to offer its existing and future cloud customers.

4 Oracle's Security-First Approach

Oracle Corporation is a multinational technology company headquartered in Redwood City, California. Founded as a relational database vendor, Oracle has grown into one of the largest companies in the software industry. The Oracle Cloud offers a complete suite of integrated applications for Sales, Service, Marketing, Human Resources, Finance, Supply Chain and Manufacturing, plus Highly Automated and Secure Generation 2 Infrastructure featuring the Oracle Autonomous Database.

In recent years, Oracle has established itself as a prominent cloud service provider. It was only a couple of years ago when the company pursued a new strategy that instead focuses on their unique differentiators and their added value for cloud customers. Some of those differentiators are fairly obvious and well known to anyone familiar with the company: among them are Oracle's industry-leading database technology, the most secure database, a highly-optimized Exadata computing platform, rich analytics capabilities directly tied to the company's business applications and so on. Somewhat less obvious but arguably more critical for a modern cloud platform is Oracle's strategic approach towards information security.

4.1 **"Security Vendor" vs "Secure Vendor"**

The public perception of Oracle has not been associated with being a cybersecurity vendor: very few people would call it a "security vendor". In fact, even though Oracle has been investing in security for decades and has a broad portfolio of relevant products and services, the company does not position itself as one, too. The company's strategy has always been to offer security capabilities integrated directly into their flagship products like databases, business applications, and more recently, cloud infrastructure. In this sense, Oracle is rather a "secure vendor".

This subtle distinction is crucial: instead of offering customers an overwhelming number of security tools to choose from (and we have already established that this approach only works for a small slice of companies with expert security teams and highly motivated modern developers), Oracle is focusing on its key expertise of managing their customers' most sensitive data at scale and ensuring that security is implemented as an integral part of this process at every layer of IT architectures, not as an afterthought driven by compliance alone.

Oracle had a unique opportunity to learn from the mistakes of other major cloud service providers and design its "second-generation cloud" infrastructure with a much higher level of security by design. Incorporating such features as advanced tenant- and resource-level isolation, off-box network virtualization, and least privilege access, it can ensure that customers' sensitive data is kept off-limits not just from "nosy neighbors" but from Oracle's own administrators as well. Ubiquitous encryption, strong identity management, and fine-grained access controls guarantee data integrity and confidentiality across its full life cycle.

The autonomous capabilities that Oracle has pioneered with the Autonomous Database are now being extended to its cloud infrastructure as well. A range of security services for cloud applications, APIs, databases, and other potential attack surfaces is available for customers as well, enabling them to fulfill their part of the shared responsibility for cloud data protection.

4.2 Oracle's Security-First Approach

As mentioned earlier, Oracle has a vision to offer organizations comprehensive protection using layered security that spans infrastructure, applications, and users, enabling trusted interactions with their data and actively defending against attack attempts.

Oracle has taken a security-first approach that unifies three foundational components to enable comprehensive data protection, and serve as a business enabler, not merely a checkbox in a compliance report.

First and foremost, security must be built-in throughout the entire cloud architecture, providing multiple layers of security controls at every level: from hardware infrastructure across networks, servers, applications, and users. This approach closely follows the secure-by-design principle described in an earlier section.

Second, security can only be a true business enabler if it removes complexity and is highly automated, freeing IT specialists from tedious manual labor and allowing them to concentrate on more creative and productive tasks. Eliminating the human factor from cloud operations massively reduces the exposed attack surface and minimizes the effect of potential mistakes and negligence. For cloud services, it also greatly improves governance and compliance by ensuring customers that their sensitive data cannot be accessed by unauthorized third parties (including Oracle itself).

Last but not least, security is only efficient when it's always-on. As mentioned earlier, security controls offered as optional tools for customers to choose from fail to provide sufficient protection in most cases. Only when every cloud service is tuned according to the latest security best practices and any configuration drift is detected and corrected early, can the customers be sure that their data is properly protected.

5 Summary and Recommendations

If you're only looking for a single takeaway from this paper, let it be the following: even though outsourcing IT infrastructures to a cloud service provider helps organizations minimize their operational costs, reduce administrative efforts and address the skills gap challenge, it is critical to evaluate the cloud providers security principles and architectural choices that they have made.

According to the shared responsibility model, cloud customers retain responsibility for protecting their sensitive information in the cloud and will bear full consequences of a data breach. Although each cloud service provider can offer its customers a broad selection of security tools, doing it without a clear strategy, guidance, and education won't magically address your security and compliance challenges. In

the end, you should consider the distinction between a security vendor and a secure one and evaluate a CSP as the latter.

As we have established earlier, there are several key principles that a cloud service provider should adhere to in order to be considered a truly secure vendor. First, security must be treated as an integral and indispensable component of every layer of a cloud platform. This involves making security always-on – not just configured according to the current best practices out-of-the-box, but continuously monitored and updated as new threats emerge. Finally, the scale and complexity of the modern threat landscape requires a high degree of automation for security, not just augmenting human analysts but removing them from decision-making and operations completely.

Oracle had a unique opportunity to learn from cloud provider mistakes and avoid repeating them. By focusing on its unique expertise and making security more autonomous and the foundation of its development strategy, Oracle is now able to quickly grow its own cloud infrastructure not just in scale (by mid-2020 Oracle Cloud already has as many regions as AWS), but in the level of security and compliance it provides to its customers.

Even though Oracle never positioned itself as a security vendor, security is core to everything the company does for its customers as every truly secure cloud vendor should.

Finally, it's worth reiterating that when looking for a cloud service provider for your future projects, you should always look behind labels and never assume that a CSP will enable your security and compliance strategy by default. Instead, focus on critical security architectural choices and capabilities, evaluate services, and ask the vendor explicit questions about them.

6 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com