v1.1 | 10 09 2019

# Key Cloud Principles

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

# INDEX

## SUMMARY

With over 10 million active users in the US, Netherlands, UK, Germany, and France, Tools4ever is an Identity and Access Management market leader. We serve a wide range of organizations across all industries and varying in size from 300 to more than 200,000 user accounts.

Recently, Tools4ever migrated its HelloID offering from a hybrid model – that had incorporated private cloud and on-premise deployments - towards a cloud-only solution running on Microsoft's Azure cloud infrastructure. It is a major step in our roadmap towards becoming a cloud-only solution provider.

In this document we explain the drivers behind this migration, our approach and how customers benefit.

## Drivers for the cloud-only migration

Cloud technology – specifically Tools4ever's Infrastructure-as-a-Service (IaaS) suite – has reached maturity. Gartner positions IaaS very close to the final "plateau of productivity" stage on their cloud computing technologies "hype cycle", which interprets the timelines of industry expectations for a given technology breakthrough. Cloud surveys from RightScale illustrate that 96% of companies already use the cloud today – 92% of which already use public cloud infrastructure. On average, organizations make use of 4.8 different cloud offerings over the full range of private, hybrid and public services.

Tools4ever's customers have been rapidly migrating their IT landscapes to the cloud. The key driver behind cloud migrations has been a need for greater flexibility and adaptation. Additionally, cloud technologies provide organizations a cost-efficient method to focus on optimizing core business operations. As part of these widespread migration strategies, our customers also demand our Identity and Access Management solutions to be cloud-based. We are listening.

## IaaS offerings offer advanced capabilities

Given these demands and our firm belief in cloud technology, we started adapting our Identity Governance & Administration solutions from on-premise towards a cloud-enabled portfolio. Our first implementation of a “cloud-only product”, HelloID, is fully designed, developed and tested for public cloud deployment – a milestone for Tools4ever.

Until recently, we supported HelloID for on-premise and private cloud installations. However, our Azure public cloud facilities have increasingly outgrown today’s on-premise and private cloud capabilities. Maintaining a combined on-premise and public cloud offering is no longer a sustainable option from either our professional solution management or our customers’ point of view. Therefore, we decided to discontinue the on-premise and private cloud offerings to focus all our expertise on accelerating the public cloud roadmap for HelloID.

## Are public cloud solutions reliable and secure?


Although the cloud is widely adopted, it is still worthwhile to reconfirm its current maturity level with respect to availability, reliability, security and data protection. Our cloud partner, Microsoft Azure, is internationally recognized as a global market leader and has deployed a cloud infrastructure that fully covers global and local demands. By leveraging their leading and well-structured topology of Geographies, Regions and Availability Zones, we can guarantee our customers the highest levels of data resilience. Today, the Azure public cloud is already used for many business-critical solutions, such as core banking applications.

## Certified and verified solutions

Tools4ever and Microsoft Azure's compliance with international standards are documented where possible with the applicable certifications. Equally important is our strict verification policy. Tools4ever considers the pro-active and frequent testing of our security solutions a cornerstone of our success.

We run an in-house program in which our own solutions are frequently tested on potential security flaws by our own experts. However, that is only our first line of prevention. We also have our software solutions tested twice a year by the top-class, external and ethical hackers of Deloitte – the international market leader in information security. These external tests keep us sharp, prevent the occurrence of blind spots and provide us with an extra pair of eyes. The external, ethical hackers look at IT systems from the point of view of experienced cybercriminals to recognize vulnerabilities others might overlook. For example, Deloitte's hackers utilize the NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

## About this white paper

In this whitepaper, we discuss our cloud strategy in more detail. We explain our vision on cloud maturity and security and how we have translated that vision into the design, development and deployment of our solutions. Specific details about the architecture and design of individual solutions – like HelloID – will be addressed in separate security white papers per solution.

In this white paper we explore 4 questions:

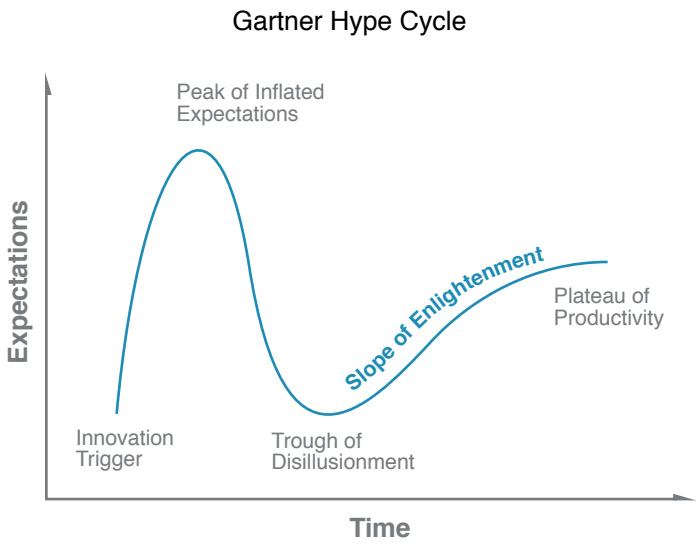
1. What is the state of the cloud? How mature is the technology and what is the adoption level of cloud solutions?
2. How does our Infrastructure-as-a-Service cloud provider (Microsoft Azure) guarantee business critical requirements in areas like reliability, security and data protection?
3. What design, development and operational principles does Tools4ever follow to guarantee optimized reliability, security and data protection for our IDaaS offerings that run on Azure?
4. How are Tools4ever and Azure certified for quality and verified by independent parties in the market?

# CURRENT STATE OF THE CLOUD

Cloud infrastructure provides today's main IT deployment method. Despite such, executives still harbor some understandable concerns. Confronting your organization's transformative migration of its IT landscape from on-premise to an external environment can be daunting. An external IT environment managed by external staff will reduce parallel IT workloads within your organization. However, cloud concerns include vulnerabilities in security and the closely related data management field. Vendor management also raises concerns. To address these concerns, let us start with summarizing the current 'state of the cloud', as well as the main challenges that customers experience and foresee.

## Current cloud adoption

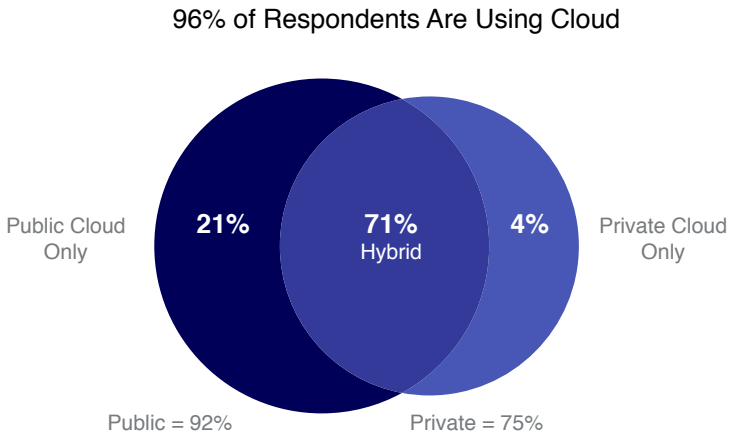
One of the most commonly used indicators to define the 'maturity' of a new technology is the Gartner Hype Cycle (see below). This model shows the development path of technologies through several well-defined stages, progressing from the trigger and phase of innovation to the peak of inflated expectations, then falling to a subsequent disillusionment period. Finally, the technology reaches the "plateau of productivity" phase in which it is widely accepted and delivering all promises. In the most recent Gartner Hype Cycle for cloud computing [1], the Infrastructure as a Service (IaaS) technology we use to deploy our security solutions sits on the precipice of the plateau of productivity.



RightScale's annual State of the Cloud Report [2] quantitatively backs this analysis of current cloud deployments. Researchers surveyed 997 technical professionals across a broad cross-section of organizations about their adoption of cloud computing. The main conclusion is not so much if companies are adopting cloud, but how many cloud solutions they will use in parallel.

96% of RightScale's respondents indicated that their organization makes use of cloud services – whether private clouds, public clouds or hybrid deployments in which both types are combined. Public cloud adoption increased over 92% and private cloud adoption increased to 75% compared to prior reports. Many respondents indicated that their public cloud strategy is their top priority.

This is not restricted to specific niche applications or basic tools with limited integration demands, like email or storage. Today, core business applications with substantial integration requirements such as complex ERP and CRM solutions are delivered from the cloud.



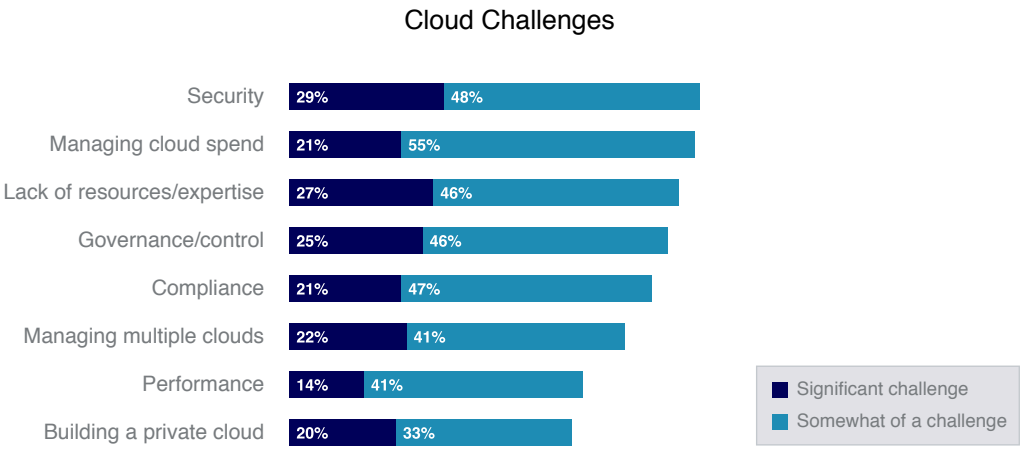

Source: RightScale 2018 State of the Cloud Report

## From single cloud to multi-cloud

In 2019, the question is not whether the market will adopt the cloud, but how many cloud services are already in-use. According to the RightScale's survey, organizations leverage 4.8 clouds on average across both public and private infrastructures. The average company requires 3.1 cloud environments to run its applications while experimenting with the remaining 1.7.

## Key challenges for cloud deployment

Just because the cloud is now widely adopted does not mean that cloud migrations are without challenges.




Source: RightScale 2018 State of the Cloud Report

As expected, security is a top challenge for the respondents of the survey. There is, however, an important observation: although security and other topics are mentioned as challenges, the majority sees them as 'somewhat of a challenge,' not a 'significant challenge.' The security challenges regarding cloud computing technologies are considered manageable hurdles. As businesses and employees develop experience with cloud security, particularly with early adopters and already-more-familiar larger organizations, this concern requires less concern moving forward than cost-management and resourcing.

## An expert view on cloud security

In Gartner's expert opinion on security practices, issues with respect to cloud services have mainly to do with the human processes around them:

> *"The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user — not the cloud provider — who fails to manage the controls used to protect an organization's data"* [3]

Gartner even quantifies this by stating that they expect at least 95% of cloud security failures will be the customer's (i.e. the customer of the cloud provider) fault through 2022. Despite this, they also claim that public cloud Infrastructure as a Service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers through 2020. Reporting similar reliability, the McAfee Cloud Security Survey [4] revealed that 83% of the 1400 interviewed IT decision makers confirmed that they already store sensitive data in the public cloud.

Tools4ever's industry expertise corroborates Gartner's assertions. For example, systems managers have high-level authority, they have the technical knowledge and they even know the technical access details like the IP address of SQL clusters. The impact of a simple mistake or a vindictive ex-employee could be disastrous. Cloud service providers are generally better prepared than in-house IT departments for these types of vulnerabilities.

## Security services are moving to the cloud

During Gartner's Security and Risk Management Summit in June 2018, Gartner research vice president Peter Firstbrook discussed several security trends regarding the delivery of security services from the cloud [5]. One of the trends highlighted was the fact that security itself is moving to the cloud. Firstbrook explained that enterprise security organizations are overloaded by the maintenance burden of legacy security solutions. At the same time, cloud-based security products appear to be more agile. They can adopt new detection methods and security services faster than on-premise solutions.

Tools4ever experienced this first-hand in our co-operation with our cloud infrastructure partner Microsoft Azure. We recently supported HelloID for on-premise and private cloud installations, but our Azure public cloud facilities increasingly outgrow today's on-premise and private cloud capabilities. Maintaining a combined on-premise and public cloud offering is no longer a sustainable option from either a professional solution management or customer point of view. Therefore, we decided to discontinue the on-premise and private cloud offerings to focus all our expertise on accelerating the public cloud roadmap for HelloID.

## Conclusions

If one message is clear from the market, it is that the cloud already passed the phase of inflated expectations and unproven claims years ago. Cloud services have reached maturity and are used for mission critical IT services. While executives defined topics like security as challenges, they are certainly not showstoppers. The migration of applications towards the cloud is – in other words – not an Elon Musk-esque journey to Mars, but that of a skilled driver weaving through Europe's winding mountain roads: it certainly requires the right materials, the right skills and the right planning, but given these preparations, it is one of the most reliable journeys on earth.

## TOOLS4EVER CLOUD PARTNER: MICROSOFT AZURE

HelloID is hosted on Microsoft's Azure cloud computing platform. This platform can be used to host many types of services including webservers, databases, virtual machines and many more. Tools4ever has a long-standing Microsoft Gold Partnership and has built up specific security experience working with the Microsoft product suite. Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world.

### Microsoft Azure positioned as a Cloud Infrastructure worldwide market leader

Under the leadership of Satya Nadella, Microsoft has made an impressive transformation towards a leading cloud player. In the most recent Gartner Magic Quadrant for Cloud Infrastructure-as-a-Service, Microsoft is listed for the 5th consecutive year as one of the worldwide market leaders along with AWS and 'new entrant' Google [6]. Today, 90% of Fortune 500 companies make use of Microsoft's Cloud for not just O365, but business-critical applications.

An example of a company transferring their business-critical assets to Azure is Geneva-based Temenos AG [7]. Temenos provides banking software to 3,000 firms across the globe, including 41 of the top 50 banks, and processes transactions of more than 500 million banking customers daily. Temenos was listed in July 2017 as a Market Leader in the Magic Quadrant for Global Retail Core Banking. The banking industry's strict security and compliance requirements regulating operations and data are well known. The Temenos chief enterprise architect John Schlesinger explains:

> *"This is a traditionally on-premises industry in terms of core banking applications, but our view is that by 2020, all new core banking projects will be on infrastructure-as-a-service (IaaS) platforms, if not software-as-a-service platforms."*

He also confirms that, from a security and compliance perspective, Azure is fully equipped for extremely demanding financial businesses processes:

> *"From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters," and "From the compliance point of view, we already have the regulators in Europe allowing core banking on the Dublin datacenter."*

## Microsoft Azure global infrastructure and cloud security

Security is built into the Microsoft Cloud from the ground up starting with the Security Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process. The Microsoft Cloud is protected at the physical, network, host, application, and data layers so that their online services are resilient to attack. Continuous proactive monitoring, penetration testing, and the application of rigorous security guidelines and operational processes further increase the level of detection and protection throughout the Microsoft Cloud.

'International topology' is essential to the Azure cloud. Microsoft organizes Azure into **Geographies**, each of which consists of two or more Regions. Each Geography is a discrete market that preserves data residency and compliance boundaries (e.g. GDPR). Thus, customers with specific data-residency and compliance needs can keep their data and applications close. Microsoft may replicate data to other Regions within that Geography for data resiliency but will not replicate or move customer data outside that Geography.

**Geographies** are not just defined at the supra-national level; there are also smaller, independent Geographies defined according to specific countries. For North and South America, the United States, Canada and Brazil all exist as separate Geographies along with a distinct, Government-specific iteration. For Europe, Germany, France, the United Kingdom, Switzerland, and Norway exist as separate Geographies within the Azure hierarchy. Azure Germany is a so-called sovereign offering: a physically and logically instance of services with a dedicated network between German datacenters. It is designed to meet the strictest EU data protection laws, under control of a German Data Trustee (T-Systems International GmbH, a subsidiary of Deutsche Telecom) and is only available to customers and partners in the EU and the European Free Trade Assembly (EFTA). In the France Geography, the availability, resiliency and business continuity are fully organized within France, using 2 Regions (France Central and France South). Azure provides a number of Geographies defined under Asia Pacific as well as Middle East and Africa.

Within a Geography, a **Region** is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Most Azure services enable customers to specify the Region where their customer data will be stored. Microsoft may replicate this data to other Regions within the same Geography for data resiliency. As such, Geographies are fault-tolerant to withstand complete region failure through their connection via the dedicated high-capacity networking infrastructure.

54 regions worldwide

140 available in 140 countries


* Two Azure Government Secret region locations undisclosed

Finally, some regions (West Europe, North Europe and France Central) contain multiple **Availability Zones**. Availability Zones are physically separate locations and made up of one or more datacenters equipped with independent power, cooling, and networking. Availability Zones allow customers to run mission-critical applications with high availability and low-latency replication. For example, the France Central Region offers three availability zones.

Tools4ever offers its services via two Geographies by default: US and Europe. Other Geographies are available on request.

## TOOLS4EVER SECURE CLOUD DEVELOPMENT AND OPERATIONS

Cloud technology is mature and fully deployed at most businesses in the United States and Europe, often for business-critical applications including security and identity solutions. Cloud services deliver levels of security and maturity today that, most of the time, is in better hands with cloud providers than with an isolated security team.

By partnering with Microsoft, we can leverage the top-ranked capabilities of a partner that meets the highest standards for cloud services, security and data protection. However, utilizing Azure datacenters does not mean that we can sit on our hands when it comes to our Identity-as-a-Service offerings. Implementing our solution at the heart of the customer's IT landscape forces us to ensure Tools4ever's security design, development and deployment meet the most demanding standards.

In this chapter we explain which key principles we used by designing, developing and operating our IDaaS propositions.

### The Tools4ever security design, development and deployment principles

The way we design, develop and maintain our solutions is based on a set of key principles described below. The Security by Design Principles as defined by OWASP forms our approach's foundation.

| | | |
|---|---|---|
| 1 | **Minimize attack surface area** | Our aim for secure development is to reduce the overall risk by reducing the so called 'attack surface area'. Every feature added to an application adds a certain amount of risk to the overall application. |
| 2 | **Establish secure defaults** | By default, we deliver a maximally secure user experience. It is up to the application user – within his or her mandate - to reduce the default level of security as configured in our applications. |
| 3 | **Principle of least privilege** | Accounts by default have the minimal privileges required to perform the necessary business processes. This covers not just user rights but also resource permissions like CPU limits, memory, network, and file system permissions. |
| 4 | **Principle of defense in depth** | Even when one control would be reasonable, we prefer more controls in order to approach risks in different fashions. This principle can make severe vulnerabilities extraordinarily difficult to exploit and, thus, less likely to occur. |
| 5 | **Fail securely** | An application may fail to process transactions for a variety of reasons. However, the result of such a fail determines whether an application is secure or not. If a user authorization check fails, but as a result assigns admin rights to that user, this is an example of unsecure failing. |
| 6 | **Don't trust services by default** | Third party partners will typically have different security policies and procedures than we do. Therefore, we do not use implicit trust of externally run systems and treat all external systems in a similar fashion. |
| 7 | **Separation of duties** | This is an essential fraud control part of the implemented solutions' process flows. For example, administrators should not typically be users of the application. |
| 8 | **No security by obscurity** | In our vision, security of key systems should not just rely on hiding details. We consider this a weak security control. |
| 9 | **We keep security simple** | Our approach favors straightforward and simple code instead of overly complex approaches: no double negatives or complex architecture are used unless absolutely necessary. |
| 10 | **Fix security issues correctly** | Once a security issue has been identified, it is important to develop a test for it and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all code bases, so developing the right fix without introducing regressions is essential. |

Your organization's experts can review how we implement these principles in the security white papers for each individual solution. The foundation outlined in this section provides Tools4ever with a consistent basis across all solutions.

We are extremely proud that our efforts to design, develop and deploy truly secure solutions are recognized by peer industry experts. In 2017, Tools4ever won the Cybersecurity Excellence Awards in the Network Access Control category. Holger Schulze, founder of the 350,000-member Information Security Community on LinkedIn, which organizes the awards program explained:

> *"With more than 450 entries, the 2017 awards are highly competitive. All winners and finalists reflect the very best in leadership, excellence and innovation in today's cybersecurity industry."*

Our solutions are also tested twice a year by the security experts of Deloitte, as described in the next chapter.


## Security and privacy. By design and by default

For many customers, a migration to the cloud does not only mean a move from an existing, trusted on-premise deployment to a new, shared environment that they have to 'learn to trust'. It also means adapting to changes in the way they work. In the on-premise scenario, staff often had direct access to the solution database.

At Tools4ever, we often receive questions and requests covering the comprehensive spectrum of scenarios. Some customers are concerned with what happens if an unauthorized person could access the database (For example: "can someone access my cloud data and reset or export it using a Powershell script?"). We also receive the converse request to provide direct customer access to cloud data and functionality.

We deal with these mixed demands in the following way, according to our key design principles:

- We only open access to those functions and data which are indeed relevant for our customers (we 'minimize the attack surface').
- We offer a highly secured API for customers who need direct access. Some solution providers do not offer API's for security reasons, but the simple truth is that every company may sooner or later be in the position where an API is required to support their business processes. The question for Tools4ever is not if we offer an API (we do), but how we protect this API.
- By default, all security levels are set at their highest while the least necessary privileges are established. Further, in-depth security mechanisms support two-factor authentication (2FA) and restricting access to business-critical functions by specific IP addresses among others configurable policies.
- With respect to access procedures, Tools4ever internally maintains a strict separation of duties. We also advise this approach to our customers.

No one can guarantee that a solution is 100% safe. Such a guarantee would only be a proof of incompetence in an era where even security and intelligence organizations suffer from security breaches. What we can guarantee is that we leveraged Microsoft Azure's powerful arsenal of security tools to provide our customers with an optimal, reliable and secure identity solution.

# CLOUD SERVICE VERIFICATION AND CERTIFICATION

The deployment of secure cloud solutions starts with using the right principles, technologies and partners as we addressed in the previous chapters. The means providing our customers with as much continual verification and certification as possible that our cloud solutions are independently tested against clear security requirements and compliant with relevant standards. Verification and certification are, therefore, important elements of the Tools4ever cloud security policy.

## Deloitte Security Scan

At Tools4ever, we consider proactive and frequent testing of our security solutions a cornerstone of our success. Since we develop advanced Identity & Access Management solutions, we have a large number of security experts within our own ranks. They are not only active in developing our security solutions and products; we also run an in-house program in which our own solutions are tested on potential security flaws by our own experts on a regular basis.

However, that in-house testing is only our first line of prevention. We also have our software solutions tested twice a year by top-class external ethical hackers of Deloitte. By selecting Deloitte for this, we have opted for the guaranteed, independent and highly qualified security expertise of the market leader in information security. Gartner positioned Deloitte first in global Security Consulting Services for the sixth consecutive year in its July 2018 report titled 'Market Share: Security Consulting Services, Worldwide, 2017' [8].

These external tests keep us sharp, prevent the occurrence of blind spots and provide us with an extra pair of eyes.

The test consists of a large number of attempts by professional, ethical hackers to attack the HelloID solution. These ethical hackers have been trained to look at IT systems from the point of view of an experienced cybercriminal to recognize vulnerabilities that others might overlook. For example, they utilize NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

The tests cover the full range of potential vulnerabilities: from system reports providing too many details to the presence of cross-site scripting (XSS) vulnerabilities. Besides the well-known black box tests, the testers go further and execute so-called grey box tests. A grey box test looks for security weaknesses in specific parts of HelloID using inside information about the design and operation of the software. Finally, we look at the possibilities for authorized users within the system. Do they have 'unintended' possibilities which go beyond what's necessary for their role? This is critical because fraud and cybercrime have been determined to take place most often from within organizations.

## Certification

A crucial element in cloud services is the compliance with international standards because of their global reach. This element ensures both the correct integration with IT systems in other domains as well as that the latest developments in security, privacy and availability are adopted.

Tools4ever has an active compliance and certification policy. A recent example is our HelloID OpenID certification. This certification confirms the high quality of the OpenID Connect implementation as part of our HelloID Identity-as-a-Service solution, further reinforcing our customers' confidence in the quality of our services.

Our cloud IaaS provider Microsoft Azure maintains the largest compliance portfolio [9] in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). Compliance covers major, globally applicable standards and certifications. In addition, Microsoft offers compliance to both industry specific and region/country specific standards and certifications.

# SOURCES


| | |
|---|---|
| 1 | **Gartner**, “Hype Cycle for Cloud Computing,” August 2017. [Online]. Available: https://www.gartner.com/doc/3772110/hype-cycle-cloud-computing-. |
| 2 | **RightScale**, “State of the Cloud 2018,” 2018. |
| 3 | **Gartner**, “Is the cloud secure,” March 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/. |
| 4 | **McAfee**, "Navigating a Cloudy Sky; Practical Guidance and State of the Cloud Security," April 2018. [Online]. Available: https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html. |
| 5 | **Gartner**, "Gartner Top 6 Security and Risk Management Trends For 2018," 4 Juni 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-5-security-and-risk-management-trends/. |
| 6 | **Gartner**, May 2018. [Online]. Available: https://azure.microsoft.com/en-us/resources/gartner-iaas-magic-quadrant/. |
| 7 | **Microsoft Azure**, "Core Banking Software Provider Moves Flagship Offering to the Cloud and Opens New Markets," September 2017. [Online]. Available: https://customers.microsoft.com/en-us/story/core-banking-software-provider-moves-flagship-offering. |
| 8 | **Deloitte**, "Deloitte positioned first by Gartner in market share for Security Consulting Services worldwide for sixth consecutive year," 5 october 2018. [Online]. Available: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-ranked-1-gartner-in-security-consulting-for-5th-consecutive-year.html. |
| 9 | **Microsoft**, “Microsoft Azure compliance offerings,” 29 october 2018. [Online]. Available: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942. |

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION


TOOLS4EVER NEW YORK

Address 300 Merrick Road, Suite 310
Lynbrook NY 11563
USA

General +1 866 482 4414
Support +1 516 482 7525
FAX +1 516 825 3018

Information nainfo@tools4ever.com
Sales nasales@tools4ever.com
Support support@tools4ever.com