Monitizer® | GLOBAL cloud security FAQs

Monitizer® | GLOBAL is a digital platform that lets you monitor your foundry data in real-time from anywhere at any time. It does this by using cloud technology.

Cloud applications are now mainstream, with 77% of enterprises hosting at least one application or a portion of their enterprise computing infrastructure in the cloud (2018 IDG Cloud Computing Study).

Monitizer® | GLOBAL is hosted in the Amazon Web Services (AWS) public cloud which offers numerous benefits like easy global access, high security and instant scalability.

The cloud offers huge advantages for foundries, opening up new possibilities for turning data into value and managing operations in a smarter way. Almost all of our customers recognize this, but many also have some remaining questions and concerns about the technology – especially with regard to security.

These Frequently Asked Questions cover some common concerns and misconceptions about public cloud technology and how Monitizer® | GLOBAL makes use of it.

1. Is the public cloud "open" to the public?

Although the word "public" conjures up an image of data sitting unguarded for all to see, the public cloud really isn't public at all in that sense. It just means that it uses shared cloud infrastructure that anybody could pay to use.

Every client's ("tenant's") application and data is securely walled off from everyone else's.

If managed by experts, modern public cloud infrastructure offers the strongest cybersecurity in the world.

2. Will anyone else be able to see our data and applications in the cloud?

Though shared infrastructure is what gives the cloud its enormous scalability and cost advantages, robust "tenant" isolation separates different users' hardware, operating systems, data and applications. No unauthorised person can access your information at any time.

3. Could Norican analyse our data and use the results for its own benefit?

End-to-end encryption protects all data in transit and in storage. As customers control their own encryption keys, neither Norican nor the cloud provider can read your files unless you give them permission. You are in total control, granting and limiting access for different users, deciding what they can see and do depending on their roles.

DISA
A Norican Technology

Monitizer® | GLOBAL cloud security FAQs

4. How can data and applications in a remote cloud data centre be safer than our locked-down, firewalled in-house data centre and computing network?

Physical computer security alone is insufficient. Safeguarding digital access is the vital part. Keeping up to date and staying cybersecure requires specialist experience and deep pockets.

The leading cloud infrastructure providers like Google, Microsoft and AWS have invested far more in security resources and expertise than any foundry IT department could ever afford.

Some examples:

- Multiple layers of different encryption with different keys.
- Proprietary super-secure servers, software and network equipment.
- Layered physical security at data centres. Huge range of safeguards, from custom-designed electronic access cards to metal detectors, biometrics, and laser beam intrusion detection. Super-secure process for hardware destruction.
- Extensive enterprise security certifications, with regular audits to prove compliance: SSAE16, ISO 27017, ISO 27018, PCI, and HIPAA. Adhere to strict ISO and SOC standards.
- The leading providers invest millions of dollars incentivising independent researchers to report potential vulnerabilities.
- Multiple specialist teams constantly scan for security threats using monitoring tools, review internal precautions and audit compliance with stringent standards.

In comparison, private and on-premise data centres are seen as far softer targets by hackers. Global research firm Gartner predicted in 2017 that, "Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centres."

5. So are there any cloud vulnerabilities?

Responsibility for data and application security in the cloud is shared jointly between customer, application provider (Norican) and cloud platform host (AWS).

The greatest vulnerability on the customer side is inadequate user management. "Through 2025, 99% of cloud security failures will be the customer's fault." Gartner, 2019.

Meanwhile, it's Norican's/DISA's responsibility to ensure our applications are secure and free from loopholes a hacker could exploit. Knowing our customers' operating environments intimately helps us "design in" security in a way generalist providers could not.

For the reasons listed above, security breaches due to a fault with cloud hosting infrastructure are exceptionally rare.

6. Is Norican's cloud application thoroughly tested and approved?

Yes. Norican's security accreditations from trusted organisations like Germany's TÜV prove its software is thoroughly security tested and is ultra secure. Security upgrades and patches are applied centrally and swiftly.

DISA
A Norican Technology

Monitizer® | GLOBAL cloud security FAQs

7. Is managing user access done differently in the cloud?

Carefully managing each user's individual identity – their log-in information, plus the resources they can work with and what they can do with them – is vital to avoid unauthorised access, for example, by an unhappy ex-employee. That applies to any business software application, whether cloud or on-premise.

The User Management module within the Norican Hub is simple to set up and offers centralised control of identity and access permissions. Optional Multi-Factor Authentication (MFA) makes weak single passwords a thing of the past. Entering a system with MFA requires at least two pieces of independent identity evidence, helping to guard against common threats like phishing.

If your company currently has a well-defined and executed security strategy, staying safe in the cloud won't require any major changes. In fact, the same amount of effort will deliver a safer system.

8. Could a hacker intercept my data on its way to the cloud? Or break into and damage my foundry systems?

NoriGate collects sensor data from machines, stores it locally and streams it to the Norican Hub in the cloud. All the data collected via NoriGate hardware is encrypted using TLS 1.2 (which is standard encryption used today) immediately and sent via secure (https) connections.

This is best practice security, as used for online banking transactions. TÜV has penetration-tested the entire data collection chain from NoriGate in the foundry to Norican Hub in the cloud, and was unable to hack or copy data from it.

By design, Monitizer® | GLOBAL only uses outgoing ports to stream data away from the machine. Because the connection is one-way and only collects data, no-one can use this solution to interfere with machine controls.

9. What if I want to switch to another public cloud hosting provider or move my Monitizer® | GLOBAL implementation into a private cloud?

As standard, Monitizer® | GLOBAL is hosted in the AWS public cloud. But because it is a "containerised" application, it can be run in any cloud environment: private, public or hybrid. Switching to a different hosting environment will incur extra costs.

Public cloud benefits

Scalability: extra storage and processing power on demand

Cost: no initial or ongoing capital investment required, just sign up, switch on and pay for what you use. No in-house data centre reduces staff and energy costs.

Predictable budgeting: a fixed monthly fee with no surprises

Minimal management: outsourced hosting and SaaS apps slash the management time needed for IT

Global collaboration: easy worldwide access for global teams via a browser interface

Best, most up-to-date cyber security: Big cloud vendors attract the world's most talented engineers, spend the most money on security, and constantly innovate to improve it.

Modern integration: cloud integration tools make it quicker and easier to gather data from other foundry systems or to integrate Monitizer® | GLOBAL with existing systems and portals. NoriGate can also collect data from non-Norican machines.

If you have any further questions, your local DISA or Wheelabrator sales representative will be delighted to help.

DISA
A Norican Technology