Reimagining the Cloud

Alexander Sokol

Executive Chairman and
Head of Quant Research
CompatibL

Alexander Sokol is the founder, Executive Chairman, and Head of Quant Research at CompatibL, a trading and risk technology company. He is also the co-founder of Numerix, where he served as CTO from 1996 to 2003, and the co-founder of Duality Group, where he served as CTO from 2017 to 2020.

Alexander won the Quant of the Year Award in 2018 together with Leif Andersen and Michael Pykhtin, for their joint work revealing the true scale of the settlement gap risk that remains even in the presence of initial margin. Alexander's other notable research contributions include systemic wrong-way risk (with Michael Pykhtin, Risk Magazine), joint measure models, and the local price of risk (with John Hull and Alan White, Risk Magazine), and mean reversion skew (Risk Books, 2014).

Alexander earned his BA from the Moscow Institute of Physics and Technology at the age of 18, and a PhD from the L. D. Landau Institute for Theoretical Physics at the age of 22. He was the winner of the USSR Academy of Sciences Medal for Best Student Research of the Year in 1988.

Q&A

with Alexander Sokol

Alexander Sokol took part in a Q&A session on cloud computing in finance. Below are the key takeaways from the discussion.

The questions touched on how remote working has affected the use of cloud computing during the Covid-19 crisis, how companies can reduce costs with cloud transition, cloud security risks, and the main cloud migration challenges the financial sector is still facing.

Has remote working/hybrid working changed the way cloud computing solutions operate?

Alexander Sokol: Remote working going mainstream during the pandemic dismantled the "everything has to be in-house" mentality. Executives and management boards have come to realize that cloud applications can be more resilient to unexpected changes in business environments and can provide easier disaster recovery processes.

While many firms with on-premises equipment had to keep some of the IT staff on site, whose who were 100% in the cloud were able to go full remote-working. With the majority of employees working remotely, it has also become easier for IT managers to secure and audit corporate environments in the cloud than to secure and audit on-premises networks.

What are the benefits of using a cloud solution vs. continued use of a local or on-premises system?

Alexander Sokol: An optimally running cloud solution reduces cybersecurity risks through the use of a standard set of cloud services and technologies, which present less penetration risk than non-standard on-premises or hybrid networks.

As cloud costs include a high degree of redundancy, and even further redundancy can be achieved by using a different geographic region as a hot standby, this leads to significant cost savings compared to deploying an on-premises application at a disaster recovery side.

Many cloud solutions also use the "pay-per-use" billing model, which eliminates the costs of one of the most significant cost drivers—the idle time of powerful on-premises servers that are underutilized for the majority of the time. Many functions performed by the in-house IT department for on-premises networks are now also the responsibility of the firm's cloud infrastructure provider.

What are the cybersecurity risks in the cloud?

Alexander Sokol: While cybersecurity risks exist in either on-premises or cloud environments, cloud systems are better protected from the cybersecurity perspective than on-premises or data center deployments. It is notable that many of the recent major hacks occurred in on-premises networks or hybrid environments rather than pure cloud systems.

Working with on-premises deployment creates a false sense of security because of the perception that the network perimeter itself has physical protection. However, only the most sensitive networks operate in the air-gap mode without any outside access. Of course, providing remote access opens systems up to certain cybersecurity risks, but there is also less risk of misconfiguration in the cloud, and all those risks are more easily mitigated in the cloud by using standard security infrastructure and features and standard security audit tools.

If a company has some niche needs/ software, how does that translate to the cloud?

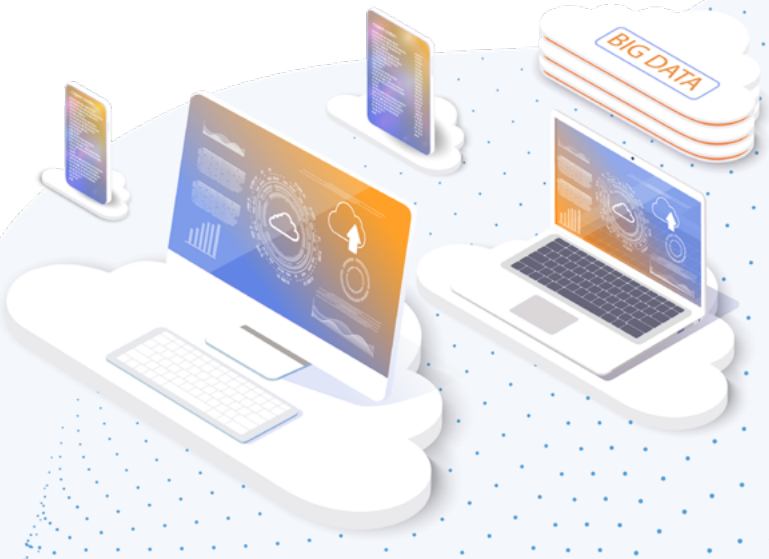
Alexander Sokol: Many firms rely on internal or vendor software solutions that are highly specialized and developed for one firm or a small number of firms.

With these solutions, it may be especially challenging to migrate to the cloud because of the significant development and IT expenses involved relative to the small development budget. Sometimes these solutions were developed years ago and there is no ongoing budget for their development. Despite often being based on outdated technologies, such solutions contain important know-how and address highly specialized needs that cannot be solved by off-the-shelf cloud-based systems.

Firms must develop a process and secure funding for migrating such niche solutions to the cloud without starting from scratch, involving their business and IT or software developers to ensure unique functionality is not lost during cloud transition.

As a living example, CompatibL recently worked with a Swiss bank whose regulator required them to use a national cloud provider hosting the bank's data in an account under the bank's direct control. The CompatibL team was able to deploy CompatibL Cloud with the new (to us) provider within days and became the winning bidder, while no other vendors were able to meet this regulatory requirement.

It is also worth noting that many banks and



asset managers are subject to data custody regulations and fiduciary responsibilities that must be specifically addressed by cloud solutions.

What is the transition from on-premises to a cloud solution like?

Alexander Sokol: Working in the cloud is still a new paradigm for software vendors and internal software developers, IT departments, and end users. Initially, it may be jarring for an IT engineer to realize that there is no "server" to update, replicate, or troubleshoot for application issues, as the "server" is replaced by an interconnected mesh of cloud services. Software developers and IT departments must adapt their established practices of deploying, monitoring, and troubleshooting when their "server" is replaced by a collection of cloud services that are maintained by a cloud infrastructure provider such as AWS or Azure.

For the end users, it may be equally jarring to realize there is no longer a machine where the front end is running, which changes workflows that previously relied on copying files from one application to another.

Many users developed a sense of comfort when they could save their files and data locally on their desktop or VDI. They will need to develop a new sense of comfort that their files and data are not leaving the cloud, and this transition should be supported by software developers, who will need to add software features to replace what was previously done by working with files on the local machine, e.g., a revision history, archives, or sandbox functions.

What are the major barriers to transitioning to cloud services?

Alexander Sokol: First of all, transition to the cloud can be difficult because of proprietary monolithic applications and applications that use outdated technologies but perform a critical business function that cannot be easily migrated to the cloud. Secondly, retraining IT specialists to deploy, maintain, and monitor cloud applications can be tough. And lastly, it is difficult to address all regulatory and data custody concerns.

More financial institutions are providing API access to data. How can firms tap into these vis-à-vis the cloud?

Alexander Sokol: Moving applications to the cloud enhances the ability to leverage data in new ways without the barriers created by incompatible databases and isolated networks. For example, cloud APIs that use standards-based RESTful service conventions can be integrated easily. On the other hand, SAML and other security technologies provide the ability to access any data made available in the cloud through RESTful APIs.

What are the future trends/ developments of the cloud and the SaaS model in financial services?

Alexander Sokol: The most important is the ability to use the client's preferred cloud infrastructure provider—each with its own unique set of technologies—which will simplify procurement, reduce IT costs, and resolve many of the regulatory and operational issues.

Sales
+1 (609) 436 5074
+44 (20) 3882 4203
sales@compatibl.com

Princeton
CompatibL Technologies LLC
100 Overlook Center
Second Floor
Princeton, NJ 08540, USA
+1 (609) 919 0939

London
CompatibL Technologies Ltd
The Clubhouse
8 St. James's Square
London, SW1Y 4JU
+44 (20) 3743 8800

Singapore
CompatibL Pte. Ltd.
30 Cecil Street
19-08 Prudential Tower
Singapore, 049712, Singapore
+65 6813 2067

Warsaw
CompatibL Sp. z o.o.
Prosta 32, Second Floor
Warsaw, 00-838
Poland
+48 (22) 110 8005