Cloud-Native Security Using Zero Trust

For most organizations, cloud usage is now the norm. Much like the adoption path of many technologies, the road to cloud normalization started with an initial reluctance and has only recently begun to gain wider acceptance. More specifically, many organizations had initial reservations about cloud, in large part based around security and privacy concerns. Almost a decade later, cloud is not only prevalent but, arguably, ubiquitous: According to data from IDG,[1] nearly all (92 percent) organizations employ some level of cloud in support of their technology strategy.

This widespread adoption does not mean that security and privacy concerns around cloud have been entirely eliminated—in fact, the reality is far from it. Specifically, for security and assurance practitioners, discussions around cloud are still a bit nuanced. Why? Because even though cloud usage is the norm, many practitioners still have lingering questions about the security of cloud services. Likewise, because cloud purposefully abstracts elements of the underlying technology stack (i.e., those elements below the level of the cloud service model the customer employs), it necessarily means organizations *de facto* cede some degree of direct operational control over those elements to service providers.

But just as cloud can be scary for organizations, so, too, can it be harnessed as a source of strength that bolsters security goals rather than acts in detriment to them. Therefore, it is worth investigating one such organization that has adopted cloud as a critical element of its security strategy. Specifically, it is useful to consider what organizational, cultural and business context elements helped it leverage the cloud to achieve security goals, the processes it employed to do so, and the challenges that it encountered along the way. EvolutionIQ, a cloud-native start-up, is one organization that has designed, built and optimized its security program around cloud.

As a service provider within the insurance vertical, EvolutionIQ has made cloud a foundational element of its security strategy, both for the applications it builds and for the critical business applications that it employs to keep the enterprise running. As a lean organization and one that seeks to rapidly build on and expand the services it offers, one challenge for EvolutionIQ is the need for flexibility while still maintaining controls that satisfy its conservative, risk-savvy and highly regulated customers. Building a 24/7 security operations center (SOC) would prove prohibitively expensive, particularly given the volume of changes the organization routinely makes and the need to constantly expand its service offerings. However, EvolutionIQ's customers very much expect 24/7 coverage for security monitoring. How can it achieve this? One strategy: cloud offerings.

The organization uses two elements in tandem to achieve its strategy: risk-aware adoption of security services offered by cloud providers and a zero trust approach to the enterprise's technology footprint more generally. Both elements are important to EvolutionIQ's technology usage and its overall approach to security. It is worth examining how the organization did this, why and how it was done and what challenges it overcame in doing so.

As a start-up software company that provides a specialized predictive analytics platform to the insurance industry, EvolutionIQ's main value proposition is to help organizations detect, investigate and, ultimately,

ED MOYLE | CCSK, CISSP

Is director, Systems and Software Security at Drake Software. Previously, he was a software security principal with Adaptive Adaptive Biotechnologies. He is also a partner with Security Curve. In his more than 20 years in information security, he has held numerous positions including director of thought leadership and research for ISACA®, senior security strategist with Savvis, senior manager with CTG, and vice president and information security officer for Merrill Lynch Investment Managers. Moyle is coauthor of *Cryptographic Libraries for Developers and Practical Cybersecurity Architecture*. He is a frequent contributor to the information security industry as an author, public speaker and analyst.

minimize insurance fraud. Founded in 2018 as DeepFraud AI,[2] the enterprise subsequently changed its name to EvolutionIQ in 2019. It is headquartered in New York, USA, and funded with US$5 million in venture capital from First Round Capital, Foundation Capital, FirstMark, and Plug and Play.

In terms of the technology that drives the services EvolutionIQ provides, it has cloud—and cloud security—written into its very DNA. Cofounder Tomas Vykruta is a former Google AI engineer, and cofounder Michael Saltzman is a former algorithmic investor from Bridgewater Associates. The lead security engineer, Stanley Yang, also a former Google engineer, helped build some of the very security services (e.g., Google's Chronicle[3] project) that now form the backbone of the EvolutionIQ security approach. They subscribe to Google's BeyondCorp security philosophy, which itself is entirely predicated on a zero trust security architecture model.[4]

Since the organization was founded, key decision makers at EvolutionIQ already had detailed background knowledge about, implicit trust in and extensive knowledge of the cloud services available to customers through the Google Cloud Platform (GCP). As could be expected, the company employs almost entirely Google cloud services within the operations of its business and to form the technical substrate upon which its products are built and delivered. Communication and collaboration for the organization happen over Google's suite of business tools (i.e., the G-suite), while technology offerings including big data and artificial intelligence (AI) tools are created, deployed and maintained within GCP.

"In terms of the technology that drives the services EvolutionIQ provides, it has cloud—and cloud security—written into its very DNA."

Security services in use are a blend of native Google capabilities and more niche (and always cloud-based) technical services. In short, EvolutionIQ—and the entirety of its security approach—is cloud native. The ceding of direct operational control that results from implementing cloud security means that some critical and foundational elements of the technology ecosystem—and thereby the security model for that ecosystem—are outside of the organization's direct control. For customers who have high-risk usage, specific regulatory obligations or a mature security program, it raises many questions, such as:

- How does the organization know that the cloud provider is going to secure its data (or its customer's data) appropriately?
- Will the cloud provider employ the same diligence the organization would in securing its assets?
- Will the organization have leverage to push back on a provider if it does something with which the organization does not agree?
- How and under what circumstances will the provider notify the organization of breaches or security issues?
- Will the organization be alerted to security events and/or changes that impact from security to the company's risk posture?

This list of questions is just a starting point. In reality, the list goes on and on.

Even when practitioners can get answers to those questions—and even when those answers sound good on paper—it can be hard for customers (especially very risk-averse customers) to have full confidence in them. This is true for at least two reasons. First, there can be a perception that providers will be less than fully transparent about their security practices and incidents. This is to be expected since cloud providers, like any other organization, are in the business of being profitable. Because a security incident has the potential to undermine customer confidence and, thereby, drive customers to competitors. This, in turn, creates an economic incentive for a cloud provider to present all aspects of its service (including the security of that

service) in the best, most favorable light. So even if a cloud provider does everything perfectly from a security point of view, the financial and economic realities can make it difficult for practitioners to trust that this is the case.

Second, cloud providers seek to differentiate themselves from one another not only in terms of factors such as price, but also features, including security features. This means that the security services (e.g., security features, operational security practices and, to a lesser extent, the provider's security model itself) can be moving targets. Even if one asks and receives answers to security-relevant questions today, there is no guarantee that the answers will be equally true tomorrow, as service providers are continuously optimizing existing capabilities, adding new ones and seeking to compete with other cloud providers.

> "One strategy organizations can employ to do this is to embrace cloud as a purposeful strategy to safeguard security and reduce risk."

With that backdrop in mind, it is understandable that many practitioners feel that cloud can weaken security. Even when a cloud provider includes robust security features, provides assurance in the form of third-party attestation, and is transparent about its operations and operational metrics, practitioners can still sometimes feel as though moving to cloud is a "step down" security-wise.

Looking at the data, this perception is arguably somewhat entrenched. For example, data from IDG's *2020 Cloud Computing Study*[5] listed security and privacy challenges as the second highest concern among potential adopters (with 38 percent of respondents citing these as the biggest challenge or obstacle to public cloud). This negative perception can cause practitioners to miss out on many potential security advantages that strategic, disciplined and risk-aware cloud adoption can provide.

Only very rarely in technology, however, is something solely beneficial or solely detrimental from a risk and security perspective. As is common knowledge, usage and context play a major role in whether (and how) risk scenarios increase or decrease in severity. For example, consider a technology such as email. Does the existence of email in an organization increase risk? On the surface, it would seem, yes. After all, it does enable attack paths that would not otherwise be there. And, as is well known, there are widespread issues that arise from email, such as phishing, email-borne malware, business email compromise (BEC) and others. That said, there is also risk associated with not employing email. It is difficult to imagine an enterprise being successful in today's landscape without using email or some other electronic communication method. Such an organization would certainly find itself hampered in communicating with customers and suppliers, communicating effectively internally, and in myriad other ways. Meaning, though technical risk might decrease by foregoing the use of email, business risk would increase by at least as much.

Just like every other technology, cloud usage has two sides when it comes to risk: It has the potential to increase risk in some areas but can decrease risk in others. Practitioners' duties are to optimize risk—to help the organization safely take on the risk factors that make sense and manage or mitigate those that do not. One strategy organizations can employ to do this is to embrace cloud as a purposeful strategy to safeguard security and reduce risk. By combining a zero trust viewpoint with increased reliance on security services offered by cloud providers, organizations can leverage the properties of cloud that bolster their overall security postures while simultaneously controlling the properties that, if left unchecked, would add risk.

"Cloud-Forward" Security

Most practitioners are familiar with the shared responsibility models for cloud that are highlighted by cloud service providers. These are essentially formalizations of security models whereby cloud customers and cloud providers share responsibility for the operational side of security. In most models, management and oversight of lower-level operational tasks shift to the cloud provider (rather than being performed by the organization internally). This includes tasks such as ensuring the reliability of the underlying network, ensuring that virtual workloads run on a hardened hypervisor and enforcing segmentation boundaries between customers (e.g., between virtual

LOOKING FOR MORE?

- Read *Beating the Adversary at Their Own Game With Zero Trust. www.isaca.org/zero-trust*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

workloads on the same hypervisor). Higher levels of the technology stack (e.g., ensuring the security of business applications running on a virtual machine, patching of the guest operating system [OS] in a virtual machine context, monitoring user behavior) remain the responsibility of the customer. The specifics of what is the customer's responsibility and what is in the hands of the provider vary depending on the specific service and the cloud model in use (e.g., Platform as a Service [PaaS], Software as a Service [SaaS] or Infrastructure as a Service [IaaS]).

From the point of view of the customer, there can be security advantages to this sharing of security responsibility. If this sounds anathema, consider that smaller organizations are often limited in how much they can spend on security and the specialized skills that they can afford to retain on staff. Likewise, they may find a large capital outlay for security controls to be cost-prohibitive. By sharing responsibility with a larger, more technologically mature organization, they can often gain the benefit of resources (e.g., tools, expertise, processes) that would be challenging to acquire directly. For a smaller organization, benefits of using a cloud provider such as more specialized security staff or enhanced controls can be compelling compared to trying to build everything from the ground up.

By contrast, the volume of cloud customers provides economies of scale for cloud providers. This means that they can afford to maintain teams of staff—some with very niche technical skills. One initial promise of cloud was a more efficient and cost-effective method of acquiring underlying important operational elements. This is true both of security and of other operational aspects of the underlying technology ecosystem. While the small organization might not be able to afford certain security or operational capabilities on its own, a larger customer can realize the same benefits potentially more cost effectively as providers scale their operations to realize efficiencies that are emergent only at very highly concentrated and high-volume usage levels.

For example, the costs associated with building and staffing a large-scale security operation center (SOC) are considerable. For a mid-market organization, this investment would likely be cost-prohibitive—at minimum, from a staffing perspective. Full-time security operations resources, specialized resources such as identity management experts and staff with specialization in particular tools might cost more to maintain than an organization can reasonably invest. This leaves the organization with two choices:

1. Do without
2. Cobble together some level of operational capability within the confines of existing staff

"The smaller organization, by virtue of employing the cloud service, can derive the benefit of these things without the large up-front investment."

This is just staffing resources. One must also consider the monitoring tools that might be used within that SOC. A full suite of monitoring tools also might be out of financial and logistical reach for a mid-market organization, let alone acquisition of the technical staff required for such an investment. For a large cloud provider, such a capability is almost a given by virtue of the scale at which it operates. This means that the smaller organization, by virtue of employing the cloud service, can derive the benefit of these things without the large up-front investment.

Because of these dynamics, a smaller organization can—by aligning its architectures with the shared services model of its cloud provider and by making use, selectively (and based on risk), of the security features within their cloud providers—gain access to capabilities that it would not be able to otherwise. This means that a smaller organization, particularly one that services a large, mature and compliance/security-conscious customer base, can provide more and better security controls by leveraging cloud services compared to what it would otherwise be able to do on its own.

Cloud Native Meets Zero Trust at EvolutionIQ

The Cloud Native Computing Foundation (CNCF) definition of cloud native includes technologies that

> *...[E]mpower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid*

> *clouds… that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.*[6]

While this is a somewhat broad definition, effectively it refers to organizations that engineer for cloud and employ it as the foundation for most (if not all) of their technology and infrastructure; in short, the 9 percent of organizations that IDG referenced in its cloud usage survey as 100 percent externalized (i.e., those that use almost entirely cloud to operate).[7]

EvolutionIQ has always combined a cloud-native philosophy with zero trust in much the same manner as outlined by Google in its BeyondCorp reference architecture.[8] While the term "zero trust" has been used to mean different things over time, in this context, zero trust means that the enterprise subscribes to the architectural philosophy of zero trust. Namely, the philosophy whereby it considers all networks, users and devices to be inherently and explicitly untrusted. Information is always encrypted in transit and decrypted at trusted endpoints. Employee endpoints are only considered trusted when they are continuously monitored and kept updated. Even with a trusted endpoint, access is prohibited until the user or service can prove their identity.

While EvolutionIQ is by no means unique in its all-in approach to cloud or use of zero trust architecture, what differentiates it in large part is its customer base. EvolutionIQ's customers exist at the intersection of two highly regulated industries: insurance and healthcare. Since the organization specializes in insurance fraud prevention, its business involves analyzing information about insurance claims, most of which contain health information such as diagnostic information, which is itself also personally identifiable. The enterprise's clientele consists mainly of large, highly regulated organizations with mature, sophisticated security programs. Given that these customer organizations are almost always larger and more mature, they are also more likely to employ on-premises technology approaches (e.g., on-premises data centers, traditional colocation, hybrid cloud) and less likely to be cloud native in the same way than is EvolutionIQ.

Regulatory compliance and risk management are key drivers in the insurance vertical. Acceptance of the security of cloud services is by no means ubiquitous in that space; for example, Accenture's *Cloud Readiness Report—Insurance*, June 2019, found that only 42 percent of insurers cited security as a benefit of cloud adoption.[9] While some view security as a potential upside of cloud use, these data suggest that the majority do not.

Given the background and profile of EvolutionIQ's customers, choosing a security model that draws heavily on cloud services was not a consequence-free decision. The model gives the organization security capabilities that would be unattainable otherwise, but it involves continuously educating customers about the enterprise's security model and overcoming the public's natural concern about cloud-based risk. It also means that conducting due diligence activities with potential customers during the sales cycle can be more harrowing than would otherwise be the case, potentially leading to increased scrutiny during presales vetting activities performed by customers.

There are both advantages and disadvantages of this approach.

Advantages of Cloud Security

"We were built as a cloud-native company. Because of that, cloud security, and the benefits that we can draw from that as a cloud customer, is a huge part of our strategy…" EvolutionIQ Lead Security Engineer Stanley Yang explained what drove the enterprise's decision-making process.

"For example, since we don't own the physical server or network hardware supporting our production environments, we spend less time dealing with low-level operational issues," he explained. "Because we don't trust employee endpoints, we purposefully limit where data are stored, transmitted, or processed. You can't lose what you never have in the first place, so we limit where customer information can go and enforce that rigorously."

Yang describes five main benefits to using cloud in this way:

1. Opportunity cost optimization
2. Availability advantages
3. Security decision transparency
4. Breadth of services
5. Logistical benefits

Each of these benefits is worth further examination.

Opportunity Cost

The first benefit Yang described is one whereby resources conserved through this architectural and philosophical approach allows the enterprise to shift resources to its benefit. In essence, what he described were opportunity costs related to security. As a small and relatively new start-up, he explained that it does not have infinite resources to spend on security activities. Therefore, every security decision the organization makes comes at the cost of what it could have done instead with those same resources. If the enterprise can gain efficiencies in one area, it can directly bolster security in different areas. If it does something inefficiently in one place, it has less resources to spend on other areas.

> "Every security decision the organization makes comes at the cost of what it could have done instead with those same resources."

"Cloud frees us to better protect and secure devices and, most important, our application. Every dollar we save by drawing on services cloud providers supply means a dollar that we can put to better use elsewhere." He went on to describe security capabilities that the organization was able to implement specifically because it uses cloud: The organization conducted pre-release application penetration testing, engaged consultants to help with application threat modeling, and implemented improvements to identity management and authentication.

"It's more than just cost efficiencies too," Yang went on to say. "There's also the time investment to consider. As a young company, our limiting factor is almost always time. Time spent on operations is less time available to review source code or available during design in evaluating, and preventing, how the application can be attacked."

Availability

"Availability is a huge consideration for us as well. Cloud services let us easily scale up or down depending on what we need and in response to customer demand," Yang said. "We can add capacity if we need to and can take advantage of availability zones to ensure that a localized disruption doesn't impact our capacity to deliver services to customers."

This point is one with which most cloud customers will be familiar. Namely, that cloud providers offer capabilities that can be scaled as needed and utilize data centers in different geographic regions. Taking advantage of these requires more than just using a cloud provider; it also requires architecting the application in such a way as to realize those benefits and configuring the usage of those cloud services in such a way that the benefits can be realized. However, the capacity to do so is available to the cloud customer.

Transparency

Yang also highlighted advantages in the transparency of security decisions and the operational side of security. "As a smaller company and one that is in a regulated industry, we not only need to provide a secure service, but we need to be able to prove to others—for example, customers and potentially even regulators—that we are doing so," Yang continued. "Cloud services let us easily capture and report on the configuration of devices in those cloud environments."

"For our own internal testing, we can give read-only access to trained security assessors to review configuration decisions and, with customers or auditors, we can export configurations if needed to provide full transparency into how workloads are configured," Yang explained. This means that customers can have better and more transparent assurance about the services being provided.

Breadth of Services

Most cloud providers offer a breadth of different security capabilities. There are not only stock, built-in capabilities (e.g., Amazon Web Services [AWS] GuardDuty, Microsoft Azure Defender), but more enhanced security services that provide enhanced monitoring, audit and technical capabilities. These vary by service provider but can provide an immediate security capability that eliminates the requirement for a large initial investment in favor of a monthly cost model.

Logistical Benefits

The last advantage Yang described is an advantage to EvolutionIQ and an illustration of how entrenched

cloud usage is in the enterprise's culture. Specifically, he said that Google's features allow the organization to separate customers internally, within their own environment. "One huge benefit we have noticed with GCP is their projects architecture," Yang said. "By simply putting a customer into their own GCP project, we can easily silo all resources related to it—from storage buckets to serving infrastructure—and also easily grant limited access via identity and access management (IAM). This has enabled us to work with several customers without any fear of mixing their data and limiting access only to employees who are actively working with those clients. Scaling this is also straightforward using tools such as Terraform to consistently stamp out a new project for a new client."

What is particularly interesting about this benefit is that the projects used by GCP are not in and of themselves a security feature, but they have been adapted by EvolutionIQ in furtherance of its security goals.

Disadvantages of Cloud Security

The preceding are, of course, only some of the potential advantages that such services offer; others will depend on a given organization's context, business model and the types of products/services it supplies. However, there are also drawbacks and disadvantages. Yang said that the primary downsides were less about the technology itself and more about the perception of the approach from customers, two of which he noted:

1. **Modern customers**—Make heavy use of cloud and understand its potential advantages
2. **Traditional customers**—Come from organizations with large internal technology footprints that are accustomed to racks of equipment and on-premises data centers

This, he says, can lead to assurance challenges. "We are a vendor to them so they understandably want to validate our control environment. But our control environment is architected in a much different way than they expect. It's not that we don't have the controls they're looking for, it's just that the implementation is outside what they're accustomed to," he explained.

"For example, they might ask about network IDS on our internal network." He qualified, "We consider that network untrusted and have built in protections to keep important data off it. For us, a physical office serves as a place to meet, to provide Internet and to supply snacks." He explains that his team would much rather invest the same dollars in monitoring the production network in the cloud (where the data actually reside) and hardening employee endpoints (where data can be viewed). "But from their point of view, they might see it as a missing control."

He also said it is possible that the services and capabilities that the enterprise consumes from cloud providers might, over the long term, cost it more than if they are implemented internally. He explained that when setting up a new security capability, if one does it themselves, it front loads the cost while the ongoing support and maintenance allow one to potentially recoup that investment over time. By contrast, with cloud pricing, a pay-as-you-go model exists in the form of a monthly service provider charge. These dynamics do not always mean that cloud is the cheapest way to acquire such capabilities. Over the long term, EvolutionIQ may consider moving some of these capabilities internally if the economics and purchasing dynamics make sense.

> "The primary downsides were less about the technology itself and more about the perception of the approach from customers."

Results

Specific metrics can be challenging to quantify when it comes to the performance of an approach such as this. After all, EvolutionIQ was built from the ground up to be cloud native, so drawing a direct comparison between the performance of its architectural approach relative to another model would be difficult. That said, the enterprise has anecdotally cited positive security outcomes such as:

- **Negligible malware impact**—The organization has made a conscious decision to standardize on Mac for employee endpoints, enabling it to enforce robust security configuration via a third-party tool. To date, EvolutionIQ has not had any malware or ransomware impacts on business operations.

- **Technical security review**—The enterprise has been able to conduct both first-party and third-party security reviews of its cloud configuration, which would have been more difficult without the ability to export cloud security configuration or allow read-only access to assessors.
- **Compliance management**—By leveraging environments that are designed to be compliant with a number of existing regulatory requirements, the organization can more easily track compliance with those regulations in the portions of its processes in its scope of responsibility.
- **Availability**—EvolutionIQ has received capacity and availability advantages through this approach. It can more easily test availability and scale up nodes for additional capacity when needed.
- **Time to market**—While hard to quantify, the enterprise cites more rapid time to market for new services using this model. This also is true of development activities, which allow it to develop and test with security controls enabled to the rapid integration of new security features such as new identity providers and multifactor authentication.
- **Customer transparency**—As more and more of EvolutionIQ's customers are themselves using cloud extensively, conversations about the security of underlying services (e.g., physical data center security) can be shortened (or in some cases obviated entirely when customers are already familiar with a given provider), allowing the focus of customer reviews to be the security features of its applications and the operational security tasks for which those customers are directly responsible.

Considerations

Yang was asked what factors he would encourage others considering this model to evaluate. Meaning, for practitioners who wish to employ a similar architectural and operational strategy, what factors would he recommend that they evaluate before doing so to save themselves time, expense and hassle? He pointed to several things that should be considered, including:

- **Stakeholder reaction**—Of particular import is the reaction of stakeholders in the vertical market in which the organization operates. In EvolutionIQ's case, customer perception is paramount. However, depending on business context, these stakeholders could be partners, regulators, customers, end users or any number of other individuals. For example, one of the disadvantages to EvolutionIQ's strategy involved the need to continuously educate potential customers on its security model to allow them to validate EvolutionIQ's security appropriately. This is an important factor to consider. In EvolutionIQ's case, it needs sales staff who are capable of understanding the technology so that they can speak directly—and early on—to customer concerns. For another organization, this might be different. Thus, understanding which stakeholders need to be involved and to what degree this strategy impacts them is paramount.
- **Understand costs and pricing structures**—The economic dynamics of cloud services differ. How customized security operations are and an organization's risk profile will impact the degree to which it can use a cloud service provider's security tools and products out of the box. If extensive customizations, staff time or other organization-specific elements are required, it can very well impact whether the services offered by a cloud provider can be profitably leveraged. Organizations should fully evaluate and understand the potential costs and perform an economic analysis beforehand and validate spend in real time.
- **Organizational readiness**—It helps when the whole organization is on board with this type of model. If there are elements of the organization that are not, for example, individual business units or departments with specific requirements that are incompatible with either zero trust or a cloud-forward security architecture, trying to shoehorn a model such as this into an enterprise may be infeasible or generate friction internally.
- **Legacy applications and environments**—For the approach to work well, it needs to truly embrace zero trust. Accomplishing that with an extensive legacy footprint is challenging because these applications often were not created with zero trust in mind. This means that for the approach to work, extensive workarounds and customizations for

"By leveraging environments that are designed to be compliant with a number of existing regulatory requirements, the organization can more easily track compliance with those regulations."

those legacy elements may be needed. Having an extensive legacy footprint can significantly increase the time requirements and complexity and reduce some of the security value.

- **Understand what the cloud provider offers**—To operate effectively, it must be clear what exactly the service provider is offering. This requires constant education on the part of the cloud customer since services change over time and new capabilities are added.

Conclusion

There is a new paradigm for security operations that has potential for organizations. Just as cloud native enterprises such as EvolutionIQ fold the security features of their cloud providers into their security programs, so, too, can organizations make the choice to bolster their operational capabilities with services offered by providers. The advantage of this is that economies of scale allow organizations to gain access to skills, products and capabilities that might otherwise be out of reach. The disadvantage is that they may have to undertake some level of customer education and work together with customers to help bring them to a level of comfortable transparency and trust in the supporting operational processes.

Endnotes

1 Knorr, E.; *The 2020 IDG Cloud Computing Survey, InfoWorld*, 8 June 2020, *https://www.infoworld.com/article/3561269/the-2020-idg-cloud-computing-survey.html*

2 DeepFraud, "DeepFraud AI, a Recent Google Spinout Company, Named to Insurance CIO Outlook's Top 10 Artificial Intelligence Solution Providers," PR Newswire, 24 September 2019, *https://www.prnewswire.com/news-releases/deepfraud-ai-a-recent-google-spinout-company-named-to-insurance-cio-outlooks-top-10-artificial-intelligence-solution-providers--2019-300923550.html*

3 Chronicle, *https://chronicle.security/*

4 BeyondCorp, *https://beyondcorp.com/*

5 IDG, *2020 Cloud Computing Study*, USA, 8 June 2020, *https://www.idg.com/tools-for-marketers/2020-cloud-computing-study/*

6 Cloud Native Computing Foundation (CNCF), *CNCF Annual Report 2018*, USA, 2018, *https://www.cncf.io/cncf-annual-report-2018*

7 *Op cit* IDG

8 *Opcit* BeyondCorp

9 Dague, D.; "How Insurers Can Boost Their Readiness for Cloud Adoption," Accenture, 22 August 2019, *https://insuranceblog.accenture.com/how-insurers-can-boost-their-readiness-for-cloud-adoption*

> "Having an extensive legacy footprint can significantly increase the time requirements and complexity and reduce some of the security value."