Cyber Security Month
October 2021

THE IMPACT OF CLOUD MIGRATION ON CYBERSECURITY AND DIGITAL TRANSFORMATION

FIND YOUR BLIND SPOT

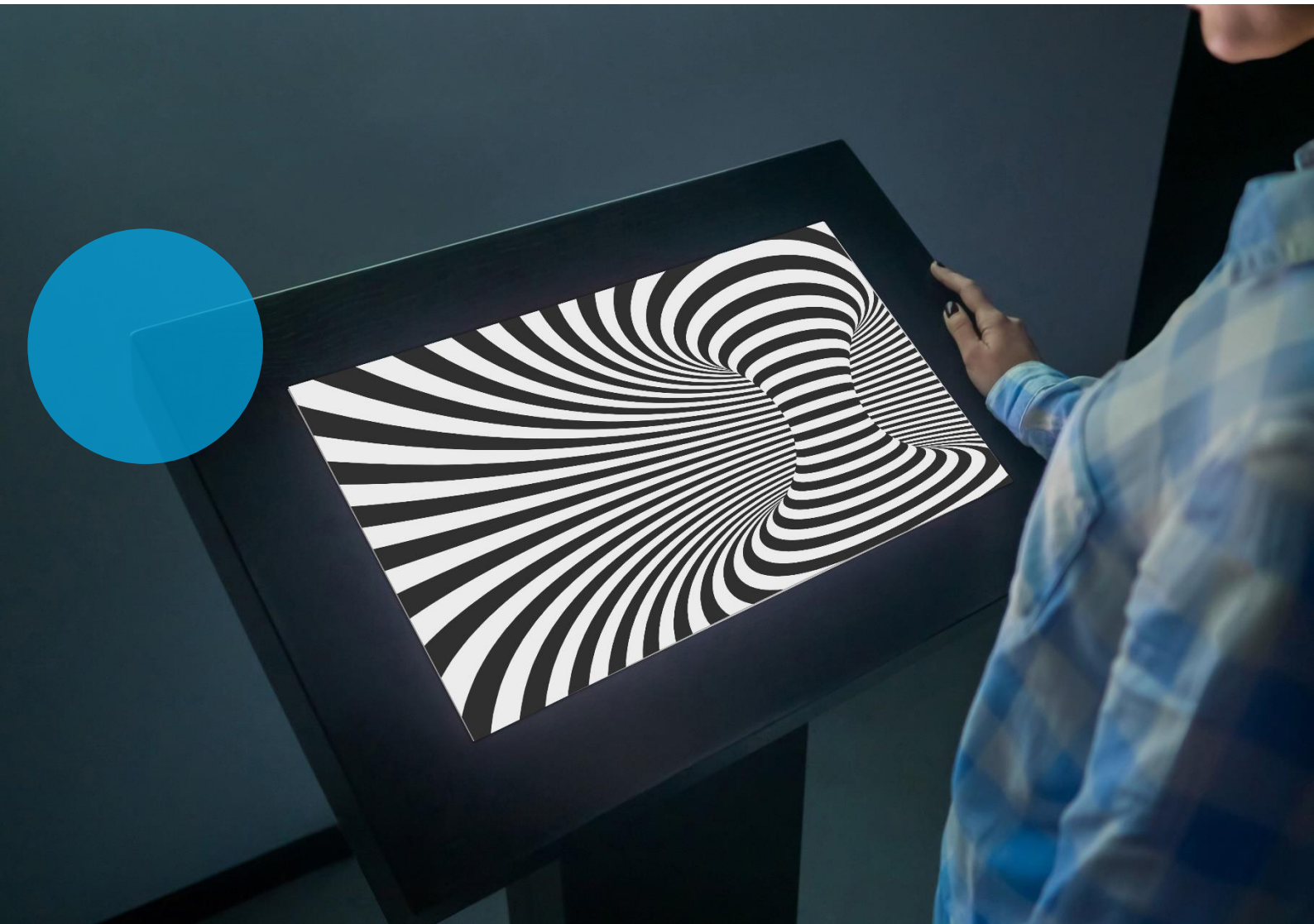
BDO

ABSTRACT

Cloud computing is a major contributor to digital transformation. The COVID-19 pandemic and resulting economic downturn have further accelerated the shift to cloud computing in many organisations while modern services continuously require acquisition and analysis of huge volumes of data and its translation into actionable insight. Cloud computing is a crucial part of the equation that enables servicing and securing this data, which could be challenging.

Just a few years ago, customers were struggling to become deeply involved in developing in-house applications and integrating the various platforms that refuse to communicate with each other. Many standards have been developed in recent decades with the aim of defining a "common security language" to enable easy integration of different services. This includes protocols in domains such as access control, authentication and authorisation, central security auditing, and many more.

The rise of cloud computing enabled a paradigm shift in the manner of which such protocols are implemented. Various cloud-based services can "talk" with one another using these standard protocols. Furthermore, these protocols allow major vendors to offer central security capabilities as a service, eliminating the need for developing such capabilities separately. This development reduced the time and effort required to develop, implement and maintain new functional services while ensuring a better and improved security posture.



PART 1: DIGITAL TRANSFORMATION AS A CLOUD GROWTH ACCELERATOR

ADVANTAGES OF THE CLOUD AS AN INFRASTRUCTURE FOR DIGITAL TRANSFORMATION

Digital transformation is defined as a "process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies". [1]

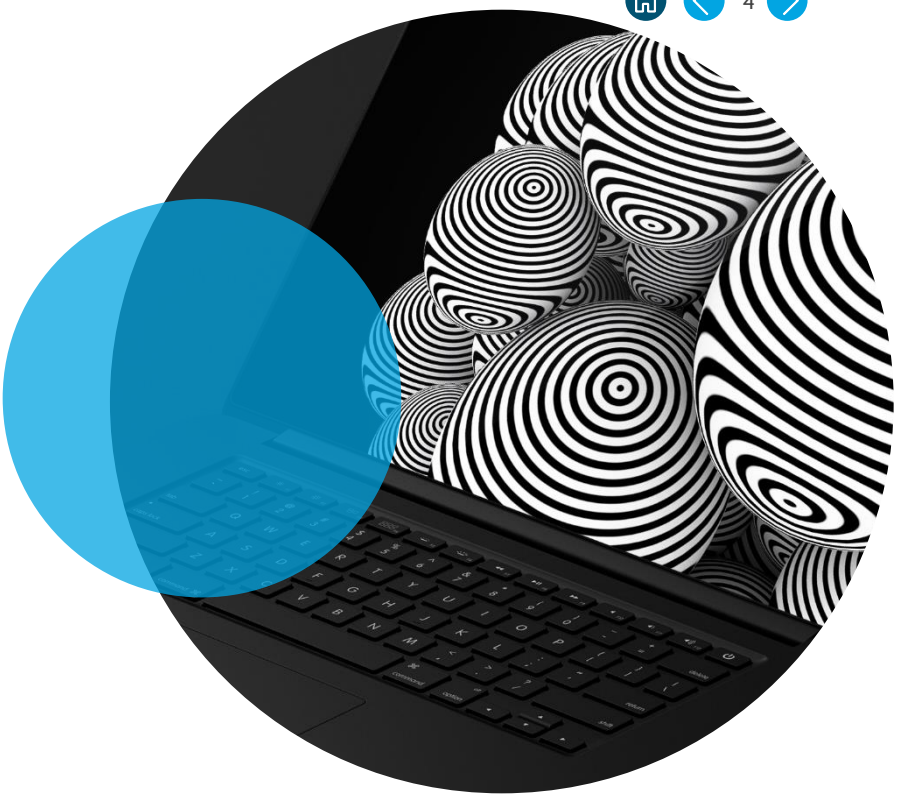
Digital transformation is impacting many areas of our lives, e.g., government interaction has dramatically shifted by going paperless; the music and visual arts industries have changed, as artists are now publishing their creations directly via social media and streaming services, healthcare now offers "conversation with a doctor" applications and initial patient diagnosis can be done remotely while scientific research runs incredibly complex simulations in an effort to assess potential COVID-19 treatments[2] by combining millions of home computers resources into the largest civilian computing greed in existence.

Cloud computing is a major contributor to digital transformation. It enables automation of the business processes that make such transformations possible. Rather than maintaining its own cumbersome data centres and expensive infrastructure, an enterprise can leverage cloud computing resources to plug into enormous, on-demand computing power, data-analysis, and other capabilities at a lower total cost of ownership compared to traditional computing architectures. This is not to say that the cloud is necessarily cheaper, but that the total cost of ownership is extensive and needs to take into consideration activities in R&D, Technical Support, Project Management, Software Lifecycle and many more in addition to hardware and data center costs (depending on the cloud strategy that is utilised – further elaborated below).

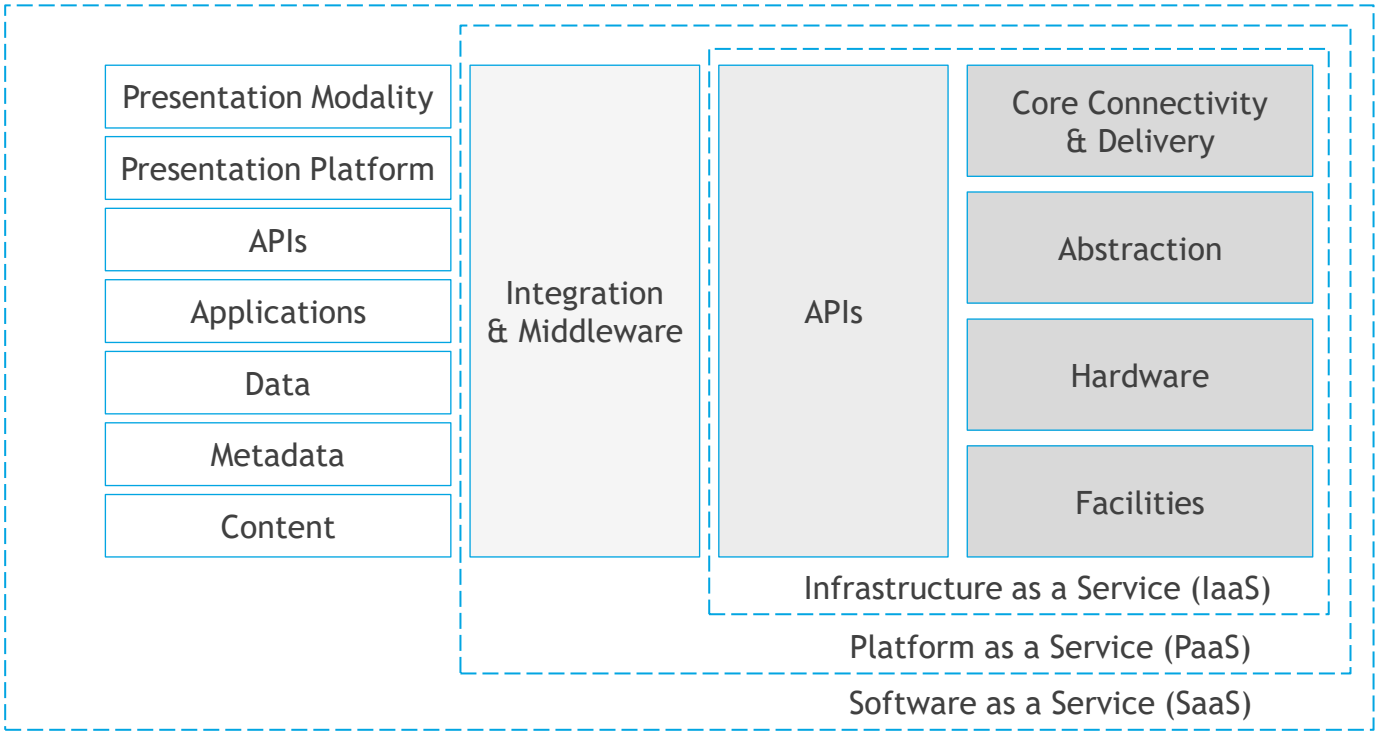
Cloud computing is the foundation of well-established companies such as Amazon, Uber, Spotify, Airbnb, and Netflix. These organisations have used the cloud to build disruptive business models, taking advantage of its flexibility, scalability, and affordability. At the same time, small-scale startups, established by entrepreneurs in their garage, can quickly ramp-up their ventures using the capabilities offered by the cloud.

Cloud computing provides several benefits that traditional networks have difficulty competing with, ranging from minimum to no on-prem server maintenance, faster deployment times and less infrastructure overhead and complexity.

1 Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. 2013. "Using grounded theory as a method for rigorously reviewing literature," European Journal of Information Systems (22:1), pp. 45-55.
2 Folding@Home project: https://foldingathome.org/



One way of looking at cloud computing is as a stack where Software as a Service (SaaS) is built on Platform as a Service (PaaS), which in turn built upon Infrastructure as a Service (IaaS).[3]



3 Cloud Security Alliance Guidance - https://github.com/cloudsecurityalliance/CSA-Guidance/blob/master/Domain%201-%20Cloud%20Computing%20Concepts%20and%20Architectures.md

Here is a short description of each layer, as defined by the Cloud Security Alliance:

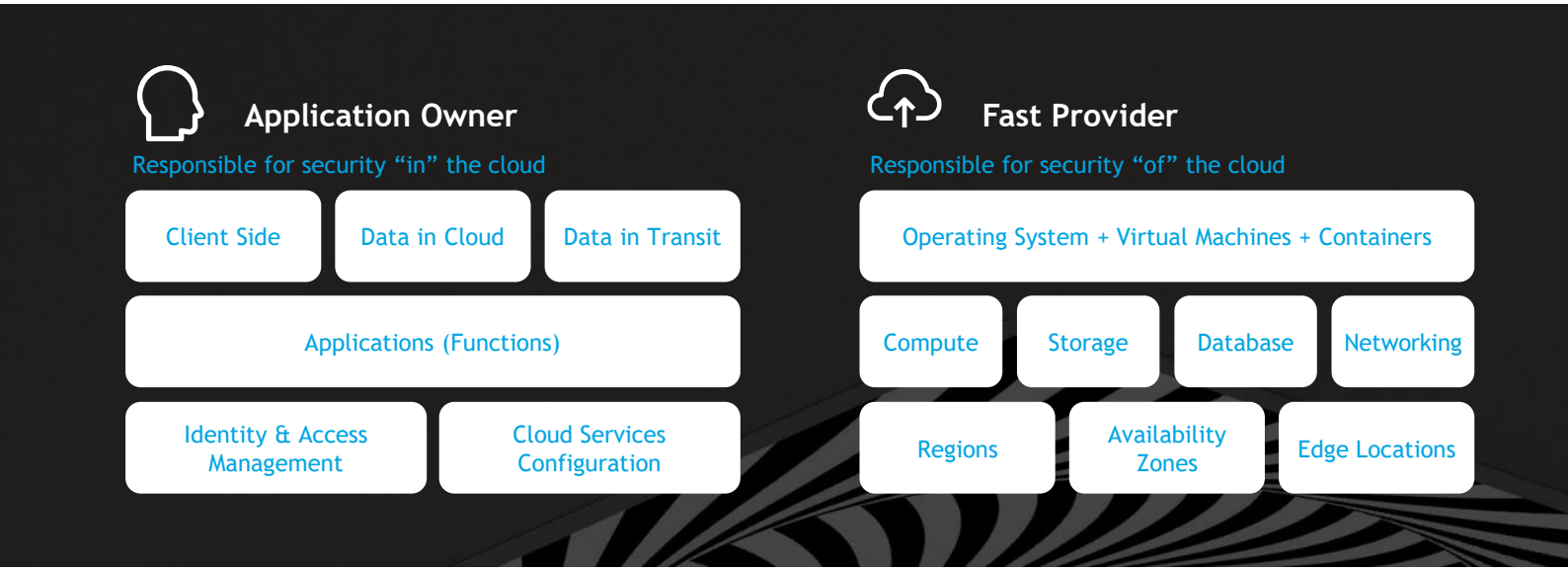
Infrastructure as a Service (IaaS): With cloud computing, we abstract and pool these resources but, at the most basic level, we always require physical hardware, networks and storage to build upon. These resources are pooled using abstraction and orchestration. Abstraction, often via virtualisation, frees resources from their physical constraints to enable pooling. Then, a set of core connectivity and delivery tools (orchestration) ties these abstracted resources together, creates the pools, and provides automation to deliver them to customers.

Platform as a Service (PaaS) adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing. Such services allow developers to develop applications on the platform using the stack-supported programming languages and tools.

Software as a Service: SaaS services are full, multitenant applications with all the architectural complexities of any large software platform. Many SaaS providers build on top of IaaS and PaaS due to the increased agility, resilience, and (potential) economic benefits.

Most modern cloud applications use a combination of IaaS and PaaS, sometimes across different cloud providers.

Function as a Service is a novel concept, commonly described as being the upper layer of the stack. Serverless architectures (also known as "FaaS" or Function as a Service) enable organisations to build and deploy software and services without maintaining or provisioning any physical or virtual servers. Applications made using Serverless architectures are suitable for a wide range of services and can scale elastically as cloud workloads grow. From a software development perspective, organisations adopting Serverless architectures can focus on core product functionality and completely disregard the underlying operating system, application server or software runtime environment. By developing applications using Serverless architectures, users relieve themselves from the daunting task of continually applying security patches to the underlying OS and application servers. Instead, such tasks are now under the responsibility of the Serverless architecture provider. The image below demonstrates the shared security responsibilities model, adapted to Serverless architectures.[4]



4 Cloud Security Alliance, The 12 Most Critical Risks for Serverless Applications

COVID-19 CRISIS AS A CATALYST FOR CLOUD MIGRATION

According to IDC,[5] 30% of European organisations are planning an aggressive migration to the cloud as part of their long-term IT strategy. This alone demonstrates the pivotal role of cloud services that drive the development of new business cross-industry models.

Then came COVID-19, a pandemic that turned the world upside down and changed business practices forever, relocating the workplace from traditionally centralised offices to their own personal home offices. The state of affairs caused by the pandemic has proven to be an accelerant of some trends that were already identified, and some that were already underway.

A study conducted by LogicMonitor[6] revealed that 87% of IT decision makers cite COVID-19 as the reason for future increase in cloud migration. Nearly three-quarters of respondents believe that within the next five years, 95% of all workloads will run on cloud environments.

The study marks a dramatic shift from a 2017 study in which LogicMonitor conducted a similar survey with only 13% of all respondents stating they did not think the shift to cloud migration would ever happen; 62% believed 95% of workloads would run on cloud environments within five or more years.

5 IDC, COVID-19 Tech Impact in Europe: The Journey to Recovery - Analyzing 3 Waves of Sentiment Survey Data. https://www.idc.com/getdoc.jsp?containerId=EUR146296920

6 Logic Monitor, Cloud 2025: The future of workloads in a cloud-first, post-COVID-19 world. https://www.logicmonitor.com/resource/cloud-2025

THE EXPONENTIAL VALUE AND VOLUME OF DATA

In Big Data, a Revolution[7], the authors offer insights as to why dataset size matters, and what it can be used for: 'The ability of society to harness information in novel ways to produce useful insights or goods and services of significant value', and '... things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value'

The nature of big data is commonly described using the following characteristics ('5 Vs'):

- **Volume** - the volume of data that companies manage skyrocketed around 2012 when organisations began to collect more than three million pieces of data per day. Since then, the volume doubles nearly every 40 months!
- **Velocity** - in addition to managing data, organisations are often measured by their ability to deliver data quickly - as close to real-time as possible. Velocity can rJ be more important than volume as it can give organisations a bigger competitive advantage.
- **Variety** - a company can obtain data from many different sources: from in-house devices to smartphone GPS technology, or using what people say on social media. The importance of these sources of information varies depending on the nature of the business, with data points often increasing exponentially over time.
- **Veracity** - veracity in this context is equivalent to 5 quality. We have all the data, but could we be missing something? Is the data "clean" and accurate? Does it amount to useful insights?
- **Value** - the value sits at the top of the Big Data pyramid, referring to the ability to transform a tsunami of data into a valuable business asset.

The acquisition and analysis of such huge amounts of data and its transformation into actionable insights extend well beyond the traditional data center, to the edge and into the cloud as a seamless hybrid environment. The utilisation of edge devices, centralised storage and analysis, along with deep learning methodologies which accelerate data processing at scale, require a new technological approach.

A study conducted by Splunk[8] notes that two-thirds of participating organisations expect the sheer quantity of data to grow nearly five times by 2025. The survey included more than 2.000 global business and IT managers from the US, Europe, China. Australia and Japan.

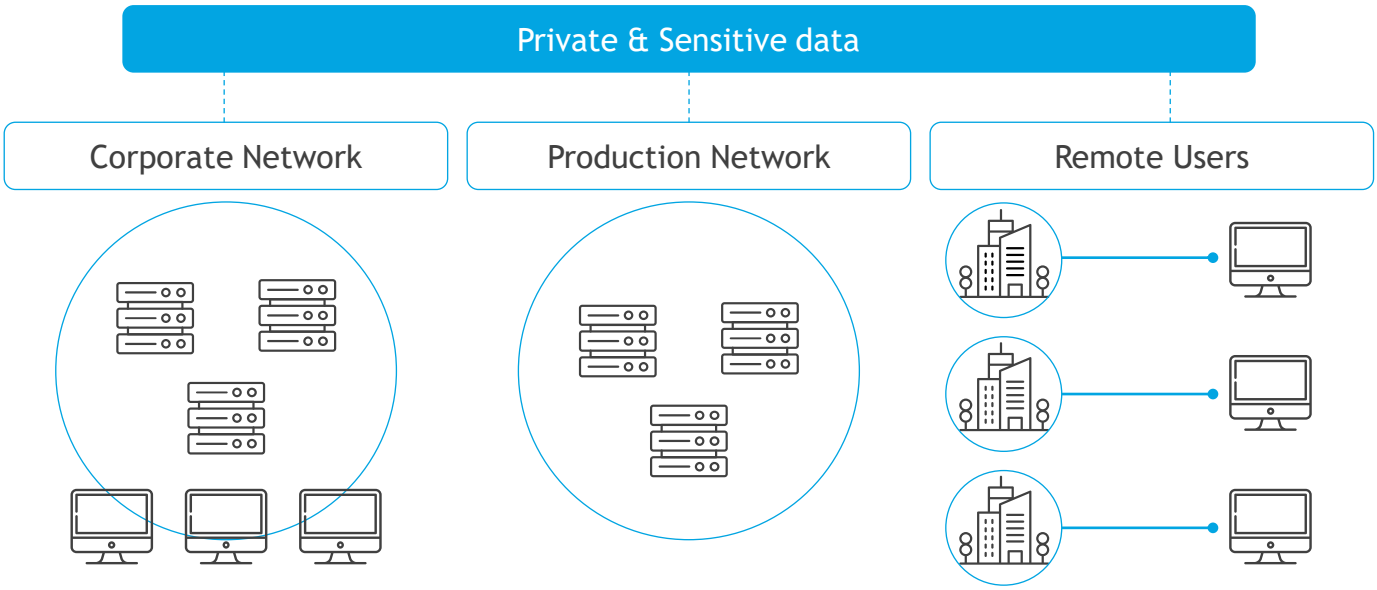
To thrive in this new age, every organisation needs a complete overview of its data - a real-time insights panel with the capability of taking action in real-time. The study quantifies the emergence of a Data Age and the realisation that organisations still have a lot of work to do in order to use data effectively and be successful. The main insights cri expressed by the study participants include:

- 57% say the volume of data is growing faster than their organisational ability to accommodate it.
- 47% acknowledge that their organisations will fall behind when faced with rapid data volume growth.
- Data is extremely valuable to organisations in terms of overall success (81%), innovation (75%) and cybersecurity (78%).
- 66% of IT and business managers report that half or more of their organisational data is dark (untapped, unknown, unused) - a 10% increase over the previous year.

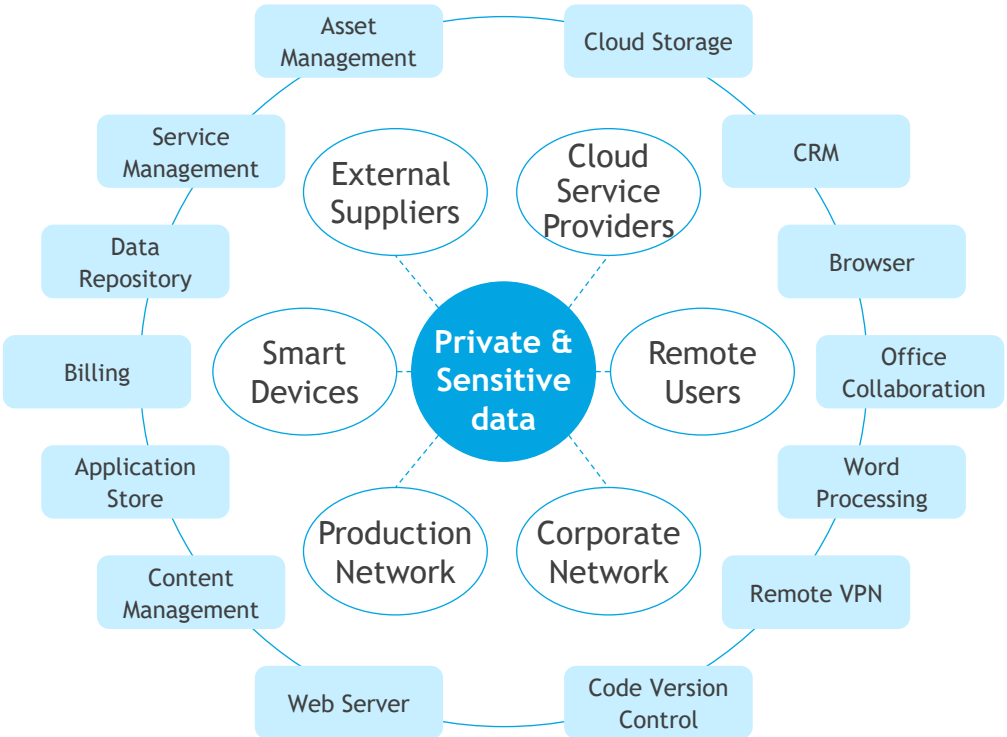
7 Mayer-Schönberger, V., & Cukier, K. (2014). Big Data: A Revolution that Will Transform How We Live. Work, and Think, 2.
8 Splunk. The data age is here. Are you ready? https://www.splunk.com/en_us/campaigns/data-age.html

OLD FRONTIER VS. NEW FRONTIER

Back in the day, organisations used to be comprised of an external perimeter with trusted internal network and some satellite environments (side offices and remote users). The border between the trusted internal and untrusted external networks was very clear. All data resided within the organisational perimeter, in locked and secure data centres. The following chart shows what a typical organisational network architecture would look like:



Nowadays, modern organisations are comprised of hybrid environments with applications and services often spanning cloud, on-prem, edge and endpoint resources. This means information security risks can equally originate in every part of the organisational network, blurring the lines between internal and external security controls. as seen in the chart:



Cloud Security Alliance (CSA) mapped the op Threats to Cloud Computing. [9] The latest report highlights the Egregious Eleven, ranked in order of significance according to the survey results:

1. **Data Breaches** - Cyber attackers are after your data - particularly personal information - and data accessible via the internet is most vulnerable and easiest to exploit when misconfigured. As more data shifts to the cloud, effective risk mitigation often begins with the question, "Who can access to this?"
2. **Misconfiguration and Inadequate Change Control** - Misconfigurations - including granting excessive permissions or unchanged default credentials - occur when computing assets and access are set up incorrectly. Misconfiguration of cloud resources is a leading cause of data breaches and can result in deleted or modified resources, and service interruptions. The dynamic nature of the cloud makes traditional control change approaches for proper configuration extremely difficult.
3. **Lack of Cloud Security Architecture and Strategy** - Worldwide, organisations are migrating portions of their IT infrastructure to public clouds. One of the biggest challenges during this migration is the implementation of appropriate security architecture to withstand cyberattacks. Unfortunately, this process is still a mystery for many organisations. Entire datasets are being exposed to various threats when organisations assume that cloud migration is a "lift-and-shift" endeavor of simply porting their existing IT stack and security controls into a cloud environment. The lack of understanding of the shared security responsibility model is another contributing factor.
4. **Insufficient Identity, Credential, Access and Key Management** - The cloud introduces a host of changes and challenges related to identity and access management (IAM) and particularly to privileged access management (PAM), since privileged credentials associated with human users as well as applications and machine identities are exceptionally powerful and highly susceptible to compromise in cloud environments.
5. **Account Hijacking** - Using phishing methods, vulnerability exploitation or stolen credentials, malicious attackers are on the hunt for effective means to access highly privileged accounts in the cloud, e.g., cloud service accounts or subscriptions. Account and service hijacking means full compromise: control of the account, its services and the data within. The fallout from such compromises can be severe - from significant operational and business disruptions to complete elimination of organisational assets, data and capabilities.
6. **Insider Threat** - Malicious insiders can be current or former employees, contractors or other trusted third parties who use their access to act in a way that could negatively affect the organisation. Since insiders have legitimate access, pinpointing potential security issues can be extremely difficult and often involve a costly remediation process.
7. **Insecure Interfaces and APIs** - Cloud computing providers expose a set of software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are often dependent on the security level and maturity of such APIs.

9 CSA. Top Threats to Cloud Computing: The egregious 11 https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

8. **Weak Control Plane** - Migrating from data centres to the cloud poses some challenges for creating a sufficient data storage and protection program. Users must now develop new processes for data duplication, migration and storage and - when using multi-cloud - another layer of complexity is added. A well-defined control layer should be the solution for these problems, as it enables the security and integrity that are needed to complement the stability and runtime of the data layer.
9. **Meta-structure and Appli-structure Failures** - Cloud service providers routinely reveal operations and security protections that are necessary to implement and protect their systems successfully. Typically, API calls disclose this information, and the protections are incorporated in the meta-structure layer for the CSP. The meta-structure is considered the CSP/customer line of demarcation - also known as the waterline.
10. **Limited Cloud Usage Visibility** - Limited cloud usage visibility occurs when an organisation does not possess the ability to visualise & analyse whether cloud service use within the organisation is safe or malicious.
11. **Abuse and Nefarious Use of Cloud Services** - Malicious actors may leverage cloud computing resources to target users, organisations or other cloud providers. Malicious attackers can also host malware on cloud services. Cloud services that host malware can appear more legitimate because the malware uses the CSP domain. Furthermore, cloud-hosted malware can use cloud-sharing tools as an attack vector to further propagate itself.

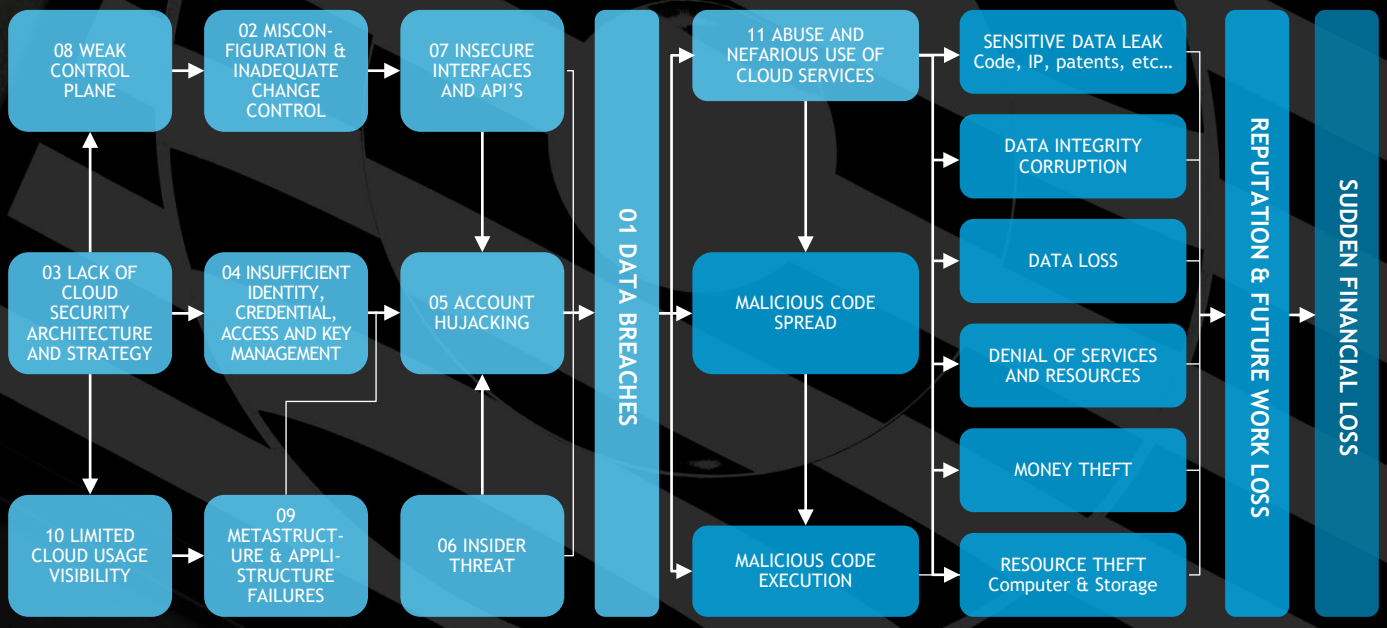
Most "Egregious Eleven" threats presented above can result in the following risk scenarios:

- **Malicious Code Spread** - Whether in a single virtual machine or an entire environment, the spread of malicious code is a power multiplier in any cyber-attack.
- **Malicious Code Execution** - The execution of malicious code by an attacker in a real-world security incident.

Both risk scenarios can be further mapped into the following real-world incidents:

- Sensitive Data Leak;
- Data Integrity Corruption;
- Data Loss;
- Denial of Services and Resources;
- Money Theft;
- Resource Theft.

The following chart maps the "Egregious Eleven" threats and their cascading implication on the state of information security:



PART 2: CLOUD-DRIVEN STANDARDISATION

FROM DIGITAL TRANSFORMATION TO CLOUD-DRIVEN CUSTOMISATION

As discussed in previous chapters, the old frontiers of on-premise computing which uses limited computing power and storage capacity, are gone. Today, most organisations are looking for flexible storage and computing power, which can scale and grow with the organisation while enabling the acquisition and analysis of huge amounts of data and transforming it into actionable insights. The "Big-data" scene is here to stay, with cloud computing supplying all its needs.

With cloud migration, a new problem arises: The organisation does not control its applications and the way they communicate with each other. Surprisingly enough, this problem turnout to be a great opportunity: In order to succeed and sell cloud solutions, Cloud Service Providers had to look for a common language, which would otherwise result in a modern-day Tower of Babel.

Luckily, many of those standards already existed when the CSPs became prominent. Those standards were waiting out there for years, some of them even decades, until the industry united in adopting them, making the cloud shift the right thing in the right time. The long leaving standards found their rightful place in history.

HYBRID ARCHITECTURE AS A CATALYST FOR CYBER SECURITY INVESTMENT

The vast adoption of cloud-based platforms is generating a significant shift in the manner by which infrastructure technologies and business applications are being approached.

In today's new reality, there are no more huge technical integrations and most data-related projects can be considered customisation projects, with integration done in the background by Cloud Service Providers; in order to implement a new business solution, the organisation is only required to manage and implement organisational changes.

RESPONSIBILITY SHIFTS

As previously described, there are four models of cloud architecture: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Function as a Service (FaaS). Each model distributes responsibility differently between Cloud Service Consumer (CSC) and Cloud Service Provider (CSP).[10]

The Infrastructure as a Service (IaaS) model offers physical security, hardware and virtualisation management as a service, however, the customer is still required to perform all necessary security configuration, management tasks and component overhead. Customers who deploy virtual hosts are responsible for managing the guest OS, including OS updates, third-party patching, configuration hardening, network security hardening and secure configuration of any applications and utilities installed on the instances. It is important to realise that this model is remarkably close to the old model in which customers were required to handle security on-prem. Do not be confused, a breach cause by server misconfiguration in this model is under the full responsibility of the customer.

Platform as a Service (PaaS) offers abstracted services, e.g., database as a service, queuing mechanisms and hundreds of additional services. For such services, the CSP operates the infrastructure layer, OS and platforms while customers are responsible for managing their own data, classifying assets, applying appropriate permissions and adhere to organisational encryption policy.

The underlining security mechanisms of Software as a Service (SaaS) are theoretically under the full responsibility of the CSP.

The shared responsibility model also extends to IT controls. Just as responsibility for operating the IT environment is shared between the CSP and its customers, so do the management, operation and verification of shared IT controls.

For the IaaS and PaaS environments, vendors are offering a comprehensive set of modules and tools, either as integral part of the service or as a third-party integration available at the CSP marketplace. These services can secure the cloud-based environment and/or other environments.

Below is a representation of the Shared Responsibility Model, inspired by CIS:

Responsibility	Data Classification and Accountability	Client and End-Point Protection	Identity and Access Management	Application-Level Controls	Network Controls	Host Infrastructure	Physical security
On-premises	●	●	●	●	●	●	●
IaaS	●	●	●	●	◑	◑	◎
PaaS	●	●	◑	●	◎	◎	◎
SaaS	●	◑	◑	●	◎	◎	◎
FaaS	●	◑	◑	●	◎	◎	◎

● Cloud Customer ◎ Cloud Provider

10 As a reference, see AWS' explanation of their shared responsibility mode here https://aws.amazon.com/compliance/shared-responsibility-model/

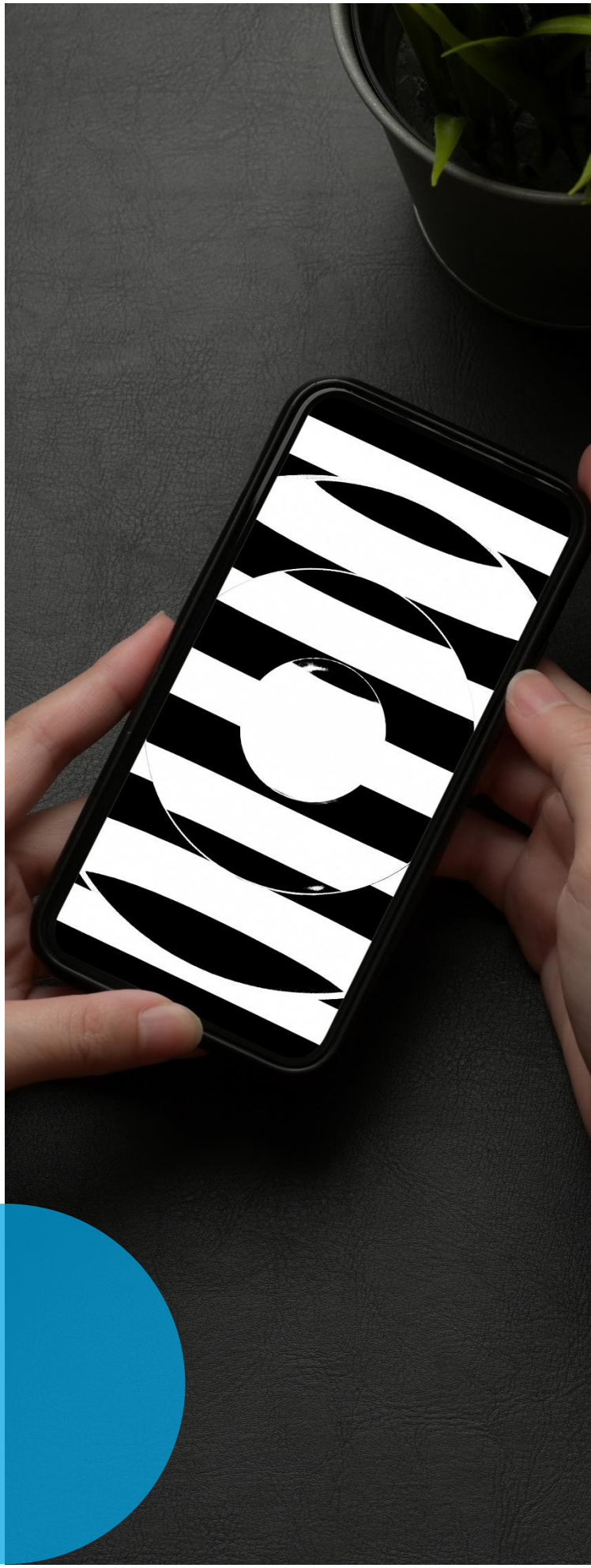
CLOUD SERVICES INTEGRATION - THE NEW IT STANDARD

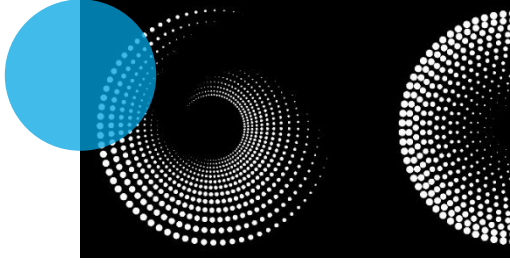
Just a few years ago, software and hardware were increasingly being acquired and used for stand-alone operation. Customers where struggling and becoming deeply involved in developing in-house applications and integrating various platforms that refuse to “talk” with each other.

Recognising the potential of this new paradigm shift, consumers of IT technologies and services began demanding standards to assist in their transition to Cloud Computing. These include foundational concepts and technologies, operational issue troubleshooting and interactions among cloud computing environments and other distributed systems.

On the CSP side, vendors realised that openness is the name of the game. CSPs began promoting standardisation of Identity Management, CRM, SIEM and other services of note. The impact of this standardisation is undeniable and has made cybersecurity investments much safer.

In the on-prem era, integrating in-house and off-the-shelf applications required tremendous effort. It is particularly complex when considering integrating two or more different components into the same security architecture, with each using different protocols, many of which were undocumented and kept as a secret inside the developer’s head, making the task a near impossibility. Cloud computing is changing all that.





CLOUD SERVICES INTEGRATION – A PARADIGM SHIFT FOR INFORMATION SECURITY

Cloud security protects information stored, accessed, and shared in the cloud. It is different from network security, mainly due to the fact that the cloud sits outside the traditional organisational network.

Using cloud environments allows IT teams to outsource infrastructure security and maintenance. Cloud computing is built atop a new model, enabling applications both in the cloud or on-prem. With cloud-based security solutions, it is now possible to separate security functionality from application logic using common, proven and centrally managed components. Such components are called Security as a Service (SecaaS)[11]. A few examples of common security services offered by various CSPs include:

- **Identity and Access Management (IAM)** platforms let IT departments ensure that cloud, on-prem and hybrid environments provide the correct level of access to the right roles and individuals at the right time. IAM solutions are used to manage access to enterprise resources by assuring that the identity of an entity is verified and granted the correct level of access based on such assured identity. Identity and Access Management can be centrally managed using a cloud-based solution (**IDaaS**). This approach bypasses many of the complexities and potential security gaps by creating connections to SaaS vendors for authentication and account management. Some of these services can also act as a bridge to on-prem identity management or access management tools. As a result, many of those adopting IDaaS will use it to replace on-prem IAM. **Single sign-on (SSO)** is usually combined with IDaaS solutions. Such services give users the ability to access all of their enterprise cloud apps as well as some of their on-prem applications using a single set of login credentials. SSO also gives IT and network admins better capabilities to monitor access and accounts.

  With the rise of standard authentication protocols, e.g., SAML, OATH 2, Radius and Kerberos, integration of various applications has become a smooth and easy process. It should be noted that these protocols existed way before the notion of the cloud was even conceived. However, they are now widely adopted.

  Using these open protocols, solutions of different vendors can be smoothly integrated. For example: Oracle Cloud Infrastructure can be federated with Azure Active Directory (AD) by setting up Oracle Cloud Infrastructure as a basic SAML single sign-on application in Azure AD. [12]

- **Data Loss Prevention (DLP)** are solutions that monitor, protect, and verify the security of data at rest, in motion and in use, both in the cloud and on-prem. On-prem data protection solutions don't have visibility into data in cloud services like Office 365 and can't control collaboration or sharing within the cloud. Many organisations are considering the addition of a separate data protection solution for their cloud environment, but in doing so, they fragment their policies, reporting mechanisms, and incident response. This results in increased operational overhead and inconsistent data protection across devices, networks, and cloud services. **Cloud-based DLP** solutions provide unified data protection across endpoints, networks, and the cloud by offering unified data protection experience, and by minimising data loss risk while maximizing operational efficiency. Such solutions are offered by numerous vendors, e.g., Checkpoint, Code42, Digital Guardian, Fidelis, Forcepoint, McAfee, Proofpoint and Trend Micro.[13]

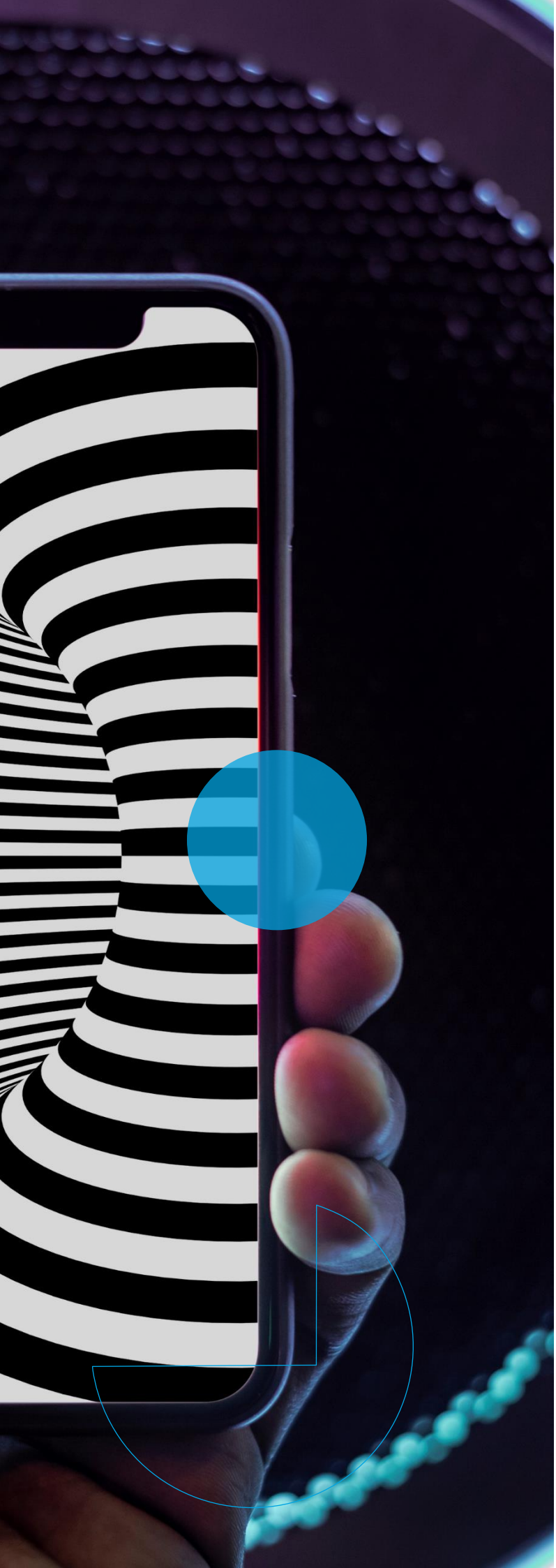
11 Cloud Security Alliance, Defined Categories of Service, https://s3.amazonaws.com/content-production.cloudsecurityalliance/dKyC3pQhxEsiXZjhVMcGWffg?response-content-disposition=inline%3B%20filename%3D%22SecaaS_V1_0.pdf%22%3B%20filename%2A%3DUTF-8%27%27SecaaS_V1_0.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20201101%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20201101T171650Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=eedabcd1087cc9e54977a0892410d96d0072a5095fc1505462717b49e09ff75f

12 https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/federatingADFSazure.htm

13 https://www.esecurityplanet.com/products/top-dlp-solutions.html

- **Web Security** is a real-time protection that is offered either on-prem via software/appliance installation or on the cloud via proxying or redirecting web traffic to the cloud provider. This provides an added layer of protection on top of solutions like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable can also be enforced via these technologies. **Cloud Web Gateways** are centrally managed through the cloud by redirecting Web through the solution provider. They protect businesses by blocking online viruses and filtering dangerous web sites. They also provide reports of online user behaviour. There is a variety of web filtering platforms out there to suit a variety of use cases. Some examples of vendors offering Cloud Web Gateway include Zscaler, Symantec, Forcepoint, and MacAfee.[14]
- **Email Security** provides control over inbound and outbound email, thereby protecting the organisation against phishing and malicious attachments, enforcing corporate polices such as acceptable use and spam, and providing business continuity options. Furthermore, the solution allows for policy-based e-mail encryption and integration with various email server solutions. Digital signatures enabling identification and non-repudiation are also features of numerous email security solutions. Some of the Web Gateways vendors mentioned below also offer **Cloud Based Email Security** as part of their gateway bundle.
- **Security Information and Event Management (SIEM)** systems accept (via push or pull mechanisms) log and event information. This information is then correlated and analysed to provide real-time reporting and alerts on incidents/events that may require intervention. The logs are likely to be kept in a manner that prevents tampering, to enable their use as evidence in any investigations. **Cloud-based SIEM** (also referred to as **SIEM-as-a-Service**) is providing IT teams with greater comfort, flexibility, and power when managing threats across multiple environments - both on-prem and in the cloud. Cloud-based SIEM provides an effective and efficient way to constantly monitor all devices, servers, applications, users, and infrastructure components on the network as well as on the cloud, all from one central cloud-based dashboard. With a cloud-based SIEM platform, one can:
  - Monitor systems, applications, and workloads, whether physical or virtual, anywhere in your network, whether in your data center, in a private cloud, or across one or more public clouds;
  - Get real-time alerts on security incidents;
  - Serve as the basis for risk analysis and audits;
  - Consolidate and manage security and event log data;
  - Automate compliance reporting.
- **Cloud access security brokerages (CASBs)** are an integrated suite that provides a range of services designed to help protect cloud infrastructure. CASBs sit between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications. These tools monitor and act as security for all of a company's cloud applications. CASBs have four key advantages, which Gartner calls the "Four Pillars of Functionality":
  - **Visibility:** CASBs centralise cloud security control and allow security personnel to monitor all cloud activity, inside and outside the organisational network, including shadow IT applications and access by remote workers.
  - **Compliance:** CASBs can control user activity to ensure compliance with industry regulatory requirements, e.g., HIPAA and PCI, and detect whether cloud usage poses a threat to compliance.
  - **Data security:** CASBs enforce internal security policies regarding encryption, tokenisation, and access to sensitive data without interfering with application features, such as search capabilities. Most CASB solutions can also prevent data leakage by labeling certain data as sensitive, preventing its download, or redacting it. They may also provide templates to organisations that currently have no DLP policies to identify sensitive data.
  - **Threat protection:** CASBs prevent unauthorised users and devices from accessing corporate cloud services and protect against malware, provide threat intelligence, and detect anomalies.

14 https://www.expertinsights.com/insights/the-top-5-cloud-web-gateways-for-businesses/



SUMMARY AND CONCLUSIONS

In this chapter, we reviewed the impact of digital transformation on the proliferation of cloud computing and on establishing standard interfaces and services, thereby enabling rapid integration among services while maintaining a high level of security.

Cloud computing permits the collection and processing of enormous data to further process it using virtually unlimited resources. While this reveals endless new possibilities, it also raises information security concerns. These include, among others, data breaches due to internet exposure, lack of secure architecture and insufficient Identity and Access controls which, in turn, may lead to sensitive information leaks, corruption of data integrity, data loss, and theft of funds and/or resources. All of the above may further result in loss of reputation, which may cause significant financial losses.

However, with proper security awareness, best security practices and novel technologies, cloud computing can be as secure as on-prem service and, in many cases, even more secure.

The standards for security protocols evolved during the last decade. One example is SAML - Security Assertion Markup Language, developed by OASIS in 2002. With the increased adoption of cloud-based services, such protocols are widely being ‘let out’ to address their original intention - building a common language for security services.

These standards enable a rapid, easy, and secure method for services to communicate one with one another. Furthermore, they permit the complete separation of security components from the application, and offer external services for secure authentication, e.g., Single Sign On, Web security and security auditing.

We believe that a combination of well-defined standards, together with novel, modern and innovative services, can facilitate the rapid introduction of these services without the need to reinvent security components, while maintaining a high level of security.

OPHIR ZILBIGER

Global Cyber Leader
Partner, Head of Cybersecurity Center
BDO Israel
OphirZ@bdo.co.il

GILAD YARON

Director
Head of Privacy & GRC Division
BDO Cybersecurity Center, Israel
GiladY@bdo.co.il