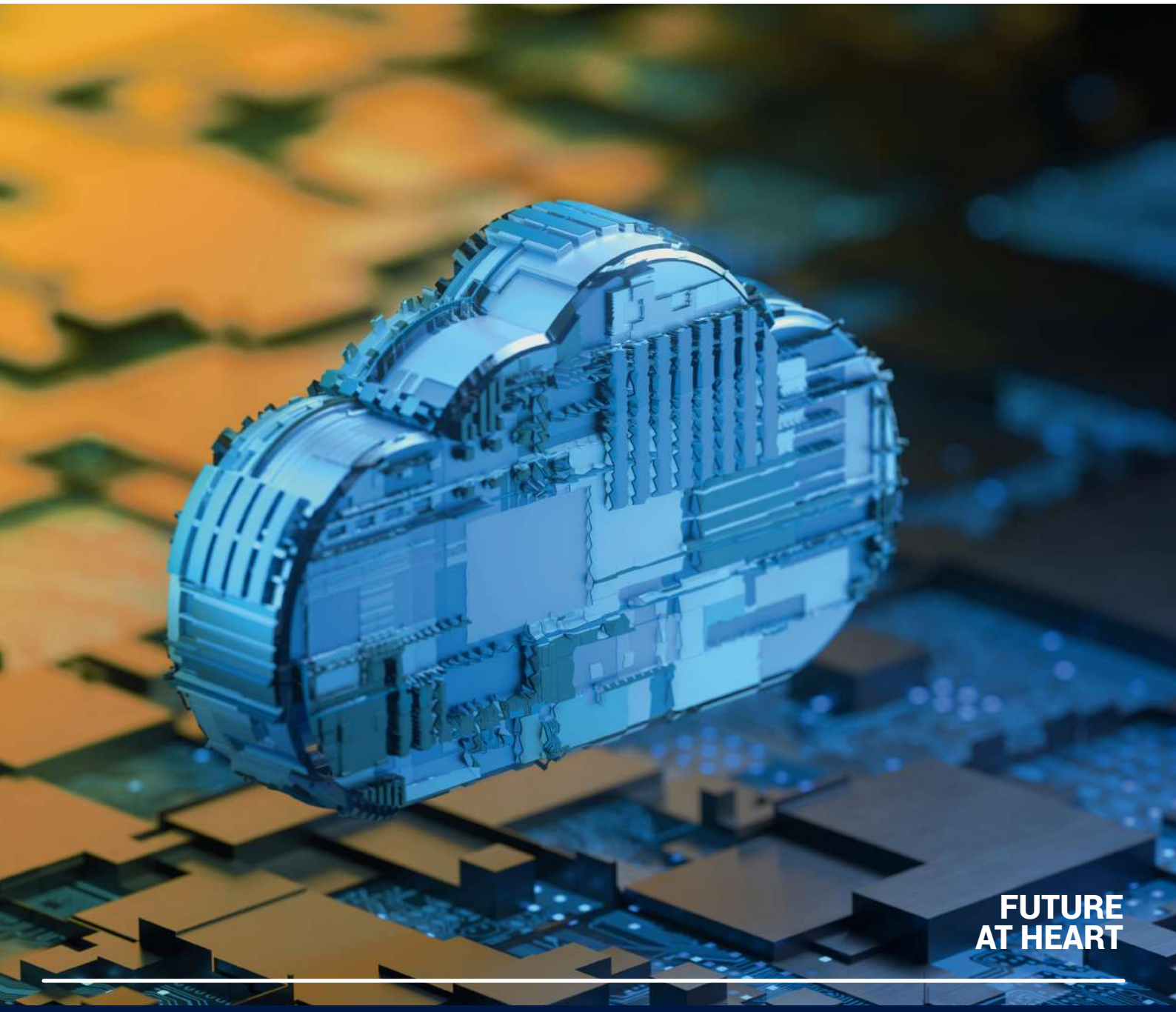
NTT DATA



WHITE PAPER

DYNAMIC CHANGE, UNCOMPROMISING SECURITY

HOW TO MAKE THE CLOUDA SAFE SPACE FOR INNOVATION AND GROWTH

MOVING TO CLOUD: FAST AND SECURE

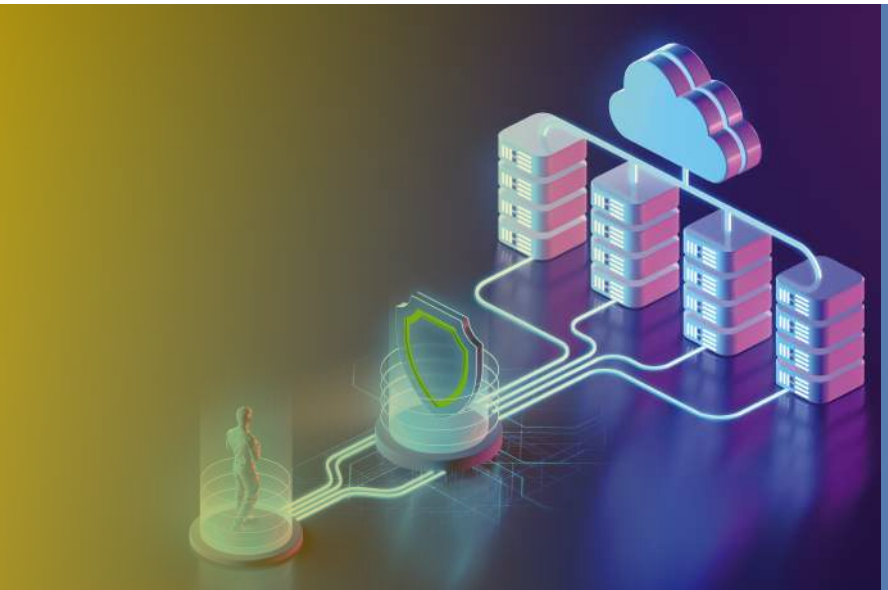
Enterprises see Cloud-based operations as not simply desirable but essential for their long-term viability. Many of them, however, still have work to do in order to understand just how challenging and different cyber-security requirements will be. In this paper we will explore some of these differences, though it is important to say clearly that security issues do not affect the essential logic for Cloud.

Yet these issues do exist, need to be analyzed and must be dealt with effectively to ensure that enterprises gain the benefits of Cloud, without negative impacts to their business activities.

Most large enterprises and other organizations are moving to Cloud as fast as they can: The reasons for this are well known and are covered in depth within the NTT DATA white paper: **The Evolving Enterprise: *How new generation Cloud drives change, growth and value***.

In headline terms, Cloud offers rapid scalability, enabling infrastructure to match demand at all times; cost reduction, as capital investment is replaced by a "pay for what you use" approach; agility, through IT environments that flex to meet unpredictable changes and are always kept at best practice level by external partners; and innovation capability, as Cloud reduces project risk and enables more flexible ecosystem working (with access to innovation from external partners).

With potentially very attractive reductions in fixed costs on offer from just moving to Cloud (some estimates make this as high as 31%), it is clear that no business operating in cost-competitive markets (which means all of them) can afford NOT to make this change. Cloud is now business as usual. All we need to discuss are the details of preparing, migrating and maximizing the potential that Cloud offers.



CLOUD OFFERS RAPID SCALABILITY, ENABLING INFRASTRUCTURE TO MATCH DEMAND AT ALL TIMES; COST REDUCTION, AGILITY AND INNOVATION CAPABILITY.

A STAGED APPROACH

Moving to Cloud can be seen as a major Change program, involving migration from a legacy IT environment to a virtual location, normally hosted by one or more of the major hyperscale providers.

In this paradigm, the change involved is equivalent to any large migration from one corporate platform to another. It is disruptive and costly, involves all the well-known risks associated with large-scale change and, most frustrating, does not usually enable enterprises to "bank" the cost benefits of Cloud until the end of the process.

That's because cost reduction does not take full effect until legacy systems are closed down. This cannot happen until migration is complete. Up to this point, costs are likely to be higher than normal, as the business will have to support the legacy platforms as usual, invest in the new Target Operating Model, and also enable interoperability between the two. Ensuring that the entire hybrid environment stays secure during transition is also a major cost- one that should not be under-estimated.

This explains why businesses try to manage their journey to Cloud on a step by step, rather than "big bang" basis. This reduces risk and makes it easier to start monetizing Cloud by identifying "quick wins" early, using profit gains from these to pay for the other changes taking place.

We support this approach as a matter of principle and give a top-level analysis of how organizations can prepare for and carry out this strategic move in our eBook: ***guide to a successful, collaborative journey to Cloud.***

Yet there is a major issue with any radical change of this kind, and it is a topic we need to understand in depth and manage with care. That issue is Cyber-Security.

MANAGING COMPLEXITY

Most large enterprises adopt a variety of methods for their moves to Cloud. They attempt to gain quick wins by identifying "doable actions": practical steps that appear to have low inherent risk and hold out the prospect of rapid pay-back. Given the complexity of such activities (there may be many of them taking place right across the business), they try to manage them through a single, strategic program. This is not the same as an old-fashioned comprehensive migration, but rather a light touch oversight and monitoring program.

We strongly believe in strategic oversight, but most of the Cloud adoption programs we have seen run the risk of allowing inconsistencies to build up between different elements of the overall change activity. This is where security weaknesses can develop, leading to opportunity for cyber criminals and potential for problems caused by human error. Most enterprises use one or more of these three approaches:

SaaS

Large organizations are using business Commercial Off The Shelf (COTS) software and solution packages to accelerate access to the advantages of Cloud. To be clear where we stand, we believe this can be an extremely rational and useful way to deliver competitively prices services, delivered intuitively to end users, and to use Cloud as a source of competitive advantage.

This approach takes many different forms:

- Large-scale systems of record, such as ERP and CRM, have been adopting Cloud-based delivery methods for nearly a decade now. This makes it unnecessary to invest in and migrate to the latest "release" of SAP, Oracle, Salesforce, or another major equivalent. Instead, enterprises access a continuously evolving platform, which evolves and becomes more capable through time. Major software companies, such as SAP, are now competing to become even more important strategic partners. The significance of this development needs to be understood and factored into Cloud planning.

- Software platforms, targeted at specific industries and customizable for individual customers, are now a vital part of Cloud strategies. We at NTT DATA have developed our own portfolio of vertical and horizontal offers designed to accelerate time to market and time to profit for large enterprises in multiple sectors. Adopting a cloud-native platform (such as Platea, our own core banking platform), enables enterprises to start profiting from Cloud long before a conventional migration project could be complete.

- Some organizations are using aspects of consumer SaaS to develop customer-facing services, delivered via portals, while others are using consumer practices to enable their own employee and ecosystem communities to adopt self-service methods for provisioning their own business environments. These methods are generally reliable and stable, but in many cases, they do not meet the highest corporate security standards for operations.

APPLICATIONS MIGRATION

The top priority for a successful, rapid move to Cloud is to transfer the complete applications portfolio and turn it into a true cloud-native resource.

To do this, enterprises will:

- Audit the current portfolio to decide what applications they can terminate or move from a license model to SaaS.
- Define how to repurpose, where possible, and replace, where necessary.
- Streamline the entire portfolio, which is an essential exercise in enhancing operational efficiency.

The most important goal here is to build an environment that optimizes (or makes it possible to optimize) business operations, leading to long-term competitive advantage. This will involve a combination of applications migration, re-engineering, replacement and closure: which is in itself a major change activity.

Inevitably the process of migration and optimization will involve moving applications to a range of dockers and containers, or Kubernetes, which are designed for working across clusters. The issues arising from extensive use of containers should be obvious.

CLOUD-BASED DEVOPS

One of the most critical potential advantages of becoming truly Cloud Native is to gain rapid access to innovation through more agile and open ecosystem working.
This delivers key advantages through rapid reconfiguration of development teams, the ability to develop on near production platforms, use of rapid testing and scenario or Digital Twin options, leading to more stable, advanced, and innovative outcomes.

One possible downside for this approach is the need to accept a certain loss in the centralized control that is normal for large enterprise environments. Enterprises are attempting to address this issue through the evolution of DevOps (development and operations in the same process) into DevSecOps (which includes security as a fundamental part of each team member's own responsibilities).

The security aspect of this approach is critically important and needs to be further tested and managed to ensure that agility across corporate boundaries does not lead to ambiguity about who owns what, who does what and who is accountable for what.

» MAJOR CLOUD-BASED THREATS

Some of the potential threats associated with Cloud are well understood, but others may not be. Here is a brief assessment of the issues that every major organization needs to identify and manage as part of their journey to Cloud.

Summary

Moving step by step to Cloud makes excellent sense and we certainly do not want to oppose it or undermine it in any way. We do want everyone to be aware of the additional complexity it brings into our strategic planning and execution. Each new step towards Cloud realization has implications for security, and each of these must be clearly understood, without ambiguity, and effectively managed.

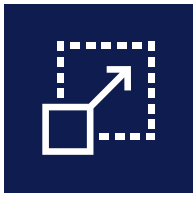
Data. This is probably the best-known risk of Cloud transformation, thanks to an intensive focus on this issue by governments and regulatory bodies. Data Sovereignty requirements, combined with GDPR and related requirements mean that organizations are aware of the need to define the locations of data, together with how this is stored, accessed, and used.

It remains a complex area, however, and new technologies (such as data sharding) are coming to market now precisely because of the need to manage this strategically vital subject more effectively. Data loss caused by human error has impacted on many if not most large enterprises and continues to do so.

Identity Management. Every organization now understands the critical need to define data access in terms of roles, responsibilities and privileges. This means that "starter and leaver" processes have become more robust, and levels of authentication are also far more restrictive than in the past.

As we become habituated to Cloud working, however, we need to understand that the complexity of Identity and Access Management (IAM) will become greater, and the need for Cloud native solutions will grow. Security of personal or corporate credentials is a matter of extreme concern today, as failures in this area represent the single most effective way for infiltration by malicious actors.

Our experience is that many enterprises do not yet fully understand why IAM in the Cloud is not the same as for single enterprise-only solutions. A lot of education and engineering work needs to be done in this area.



Interfaces. We are now gradually moving from Cloud as virtual Datacenter to Cloud as Intelligent, Programmable Network. Convergence of technologies, such as low latency connectivity (enabled by 5G), collaborative work platforms and new generation interfaces (including XR), continue to drive this new Cloud revolution.

This also highlights the role of Open APIs in enabling scalable, multi-dimensional and highly flexible interface solutions, which are critical to operation of customizable business platforms and shared environments more generally.

APIs enable configurable services to be delivered to a vast number of different interest groups via a shared portal. They are now being targeted as a potential area of weakness in this complex service landscape. Access to core code by increasingly dedicated and sophisticated malicious actors can give them easy access to services and customer data.

Networking and Sharing. We identify two different, though related issues under this heading:

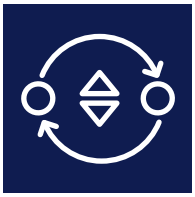
- Reliance on shared technologies brings huge advantages in terms of cost reduction, stability and development speed. On the other hand, a single fault, which may have been a relatively minor concern to a single enterprise in the past, can now lead to similar problems across all those businesses using the same software.

- The rise of agile, cross corporate boundary teamworking is another factor that drives access to innovation, operational efficiency, and other benefits. It also requires tighter control on IAM, scrutiny of more credentials and more disciplined management of the shared environment, to ensure that fluid and agile collaborative working does not happen at the cost of additional security failures.

Malicious Attacks. We are all becoming hardened to the idea of malicious action by a range of bad actors, but it is still worth asking why it is that companies we all depend on, such as healthcare and energy providers, are relentlessly attacked by criminal gangs and state actors. In reality, this threat is here to stay for three main reasons:

- Online crime, using crypto currency from (relatively) safe havens has a fast and high level ROI. If you are a criminal, it is worth investing in sophisticated capabilities as this is now the safest way available for organized criminals to make a good living.
- Attacks on critical infrastructure enable states with hostile intentions to test competitors' defenses and carry out aggressive acts without the need for military action.
- Unhappy and disaffected employees and partners can do damage to an organization they have come to dislike easily and at low risk.

As long as these factors remain in place, attacks will continue, and security structures will be challenged.



Organizational Transformation. This is a top-level term for a very big issue, and cyber-security is a critical part of this. All major change activities come with security concerns, and these have to be understood, quantified and mitigated as a basic part of the transformation strategy.

We need to understand that it is possible to migrate from on-premises IT infrastructures to Cloud as virtual datacenter without transforming your business practices or organizational structures. To maximize the potential of next generation, "networked" Cloud, however, will require re-engineering of workforce, culture, processes, and operations at a profound level.

All of these changes will lead to potential openings for security problems, so security procedures and capabilities will need to be examined and updated rigorously as part of this transformation process.

» MANAGING HYBRID ENVIRONMENTS

As large organizations of every kind commit fully to Cloud enabled and delivered solutions, it is completely normal and inevitable that they will operate within complex, hybrid technology and operational environments. They will certainly work with multiple Cloud providers, and the complexity of their Cloud landscape will grow as their own business develops. To enter new geographical markets, for example, it may be necessary to establish communication links via any suitable regional Internet provider, and to connect locally situated Edge devices (or IoT assets, or sensor arrays or all of these at once).

Summary

Most security issues that relate to Cloud adoption are well known, with many of them being subject to public discussion and government action. We believe that many of the large organizations moving to Cloud right now may still not have the kind of focused, well-resourced management strategies in place needed to handle these threats successfully in an integrated, effective manner.

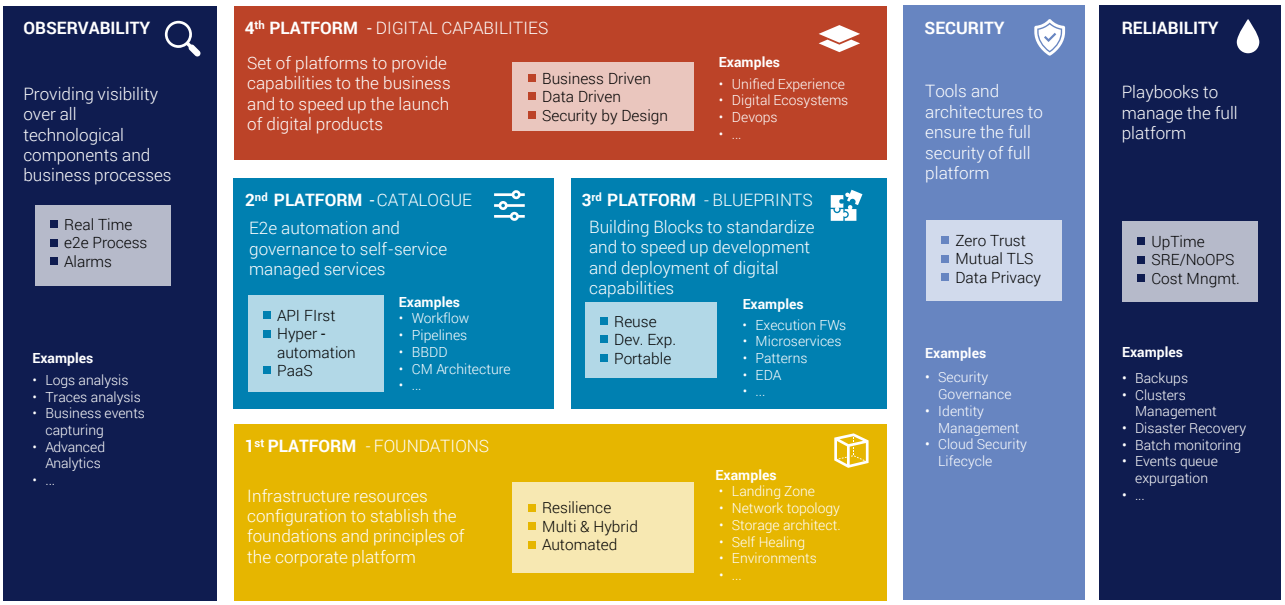
This is especially true of all those organizations handling the very complex environments that are encountered at points along the journey from entirely in-house environments to Cloud native, as shown below.

This will inevitably mean that some services and processes are delivered and managed via datacenters, Cloud providers and networks that flex, scale and develop in step with the organization, itself.

In the same way, new services, new operational centers and new data hosting locations will be needed both to serve local market demand and to satisfy the requirements of regional, national and pan-national regulators. The logic of Cloud demands that agility, speed to market and cost-efficiency should be prioritized. The outer edge of the corporate environment will therefore be flexible and even fluid in nature. That means living with and managing complexity.

So, what does this mean for security management? The graphic below gives an idea, at a very top level, of the non-negotiable, basic security requirements that hybrid, networked Cloud requires:

CORPORATE PLATFORMS



The basic features of this architecture include:

Four interconnected, focused operational platforms. These include resources and capabilities that may be hosted by a range of Cloud providers and in many different locations. The key requirement is to ensure full inter operability to deliver Cloud native speed and efficiency. The four platforms are:

01 Foundation, containing the resources needed to define and deliver the core principles of the corporate operating environment and related services. This includes network topology, storage architecture and basic management systems.

02 Catalogue, designed to locate, name, manage and deliver individual resources to users according to underlying business rules, with a strong emphasis on secure self-service.

03 Blueprints, providing the standard “blocks” of resources needed to accelerate development and deployment of services, again as defined by business rules.

04 Digital capabilities, the top-level interface layer, which provides access to the core development resources and speed up launch of new services. This will include unified experiences, collaborative work environments, DevOps and other key user capabilities.

These platforms can be (in fact, will be) logically disaggregated and may be geographically distributed. There is no security issue about this, as long as the core management and security capabilities are in place. This is where the challenges start to mount up. Our reference architecture includes three cross-platform management disciplines:

Observation. This provides a comprehensive, top to bottom, end to end monitoring capability over all assets, resources, and capabilities within or interfacing with this core architecture. This is where we establish systems to analyses and report on all operational parameters and events, together with alerts and alarms.

Reliability. This is where we locate all systems and disciplines related to Business Continuity and Disaster Recovery (BCDR), including backups, batch monitoring and cluster management. Resources here will include physical locations for BCDR, redundancy in networks and communication, rapid escalation and managing of major events.

Security. Of course, the two topics above form part of an integrated security strategy, so here we focus on the governance and core management factors needed to keep the entire environment secure. This includes Identity and Access Management, strategies for managing the entire cloud security lifecycle and the vital procedures for governance of the entire, complex landscape.

Summary. Complexity along the journey to Cloud is inevitable and we would even say necessary. Cloud provides freedom to evolve, change direction fast and scale as demand develops. Structures cannot be set in stone, so we need to accept and work with a certain level of unpredictability.

Yet this means, of course, that our underlying management and security principles need to be all the more secure, precisely because we cannot depend on fixed structures, working methods and operational "habits" to do the work for us. Security procedures must be dynamic and flexible in the way they operate, while being completely uncompromising about the principles they enforce. That is the key to an effective Cloud security approach.

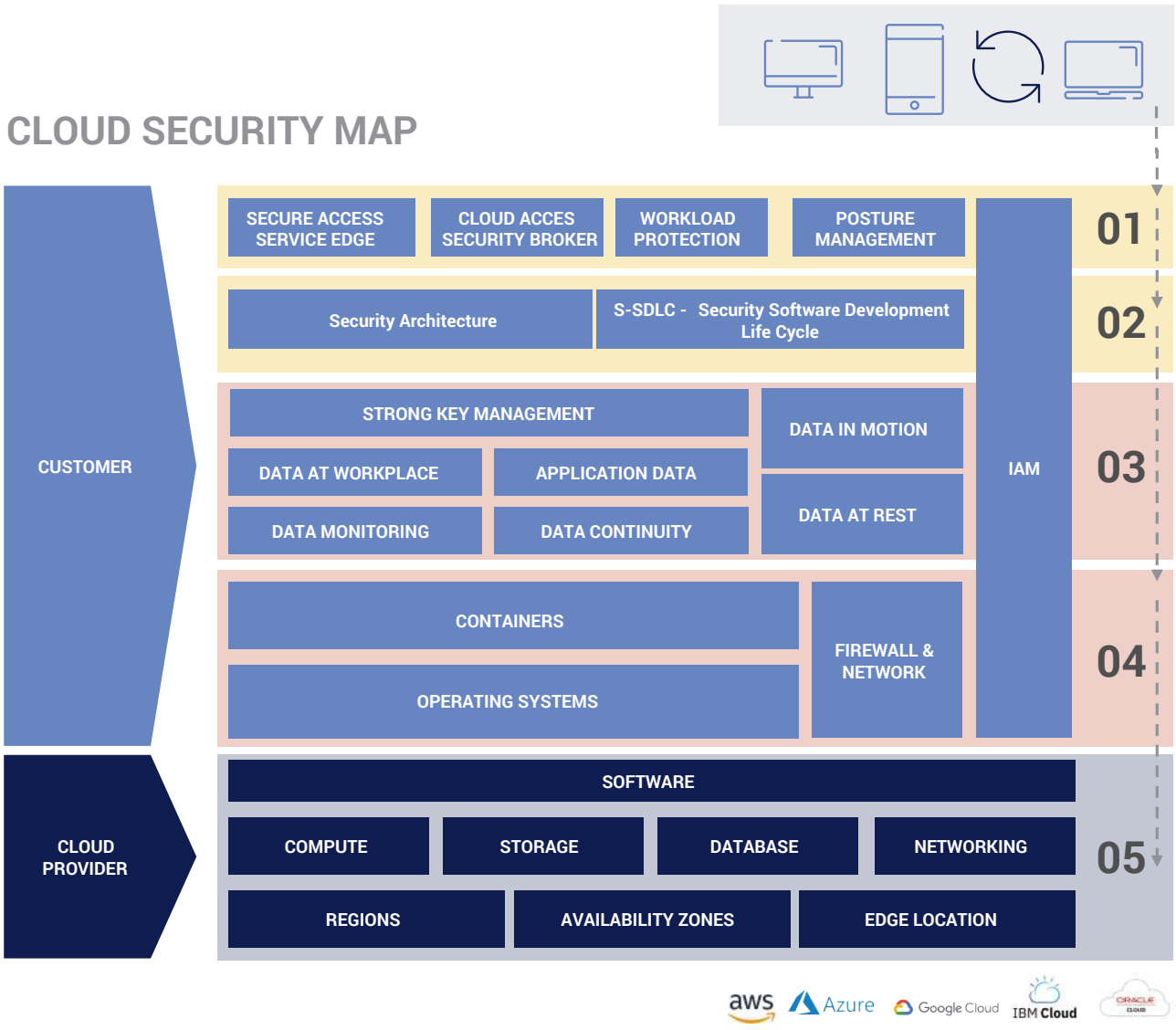
BUILDING AN EFFECTIVE CLOUD CYBER SECURITY STRATEGY

In the Cloud, and especially in the evolving world of Next Generation Networked Cloud, old-fashioned thinking about security will not be relevant or effective. For on-premise environments, it was entirely appropriate to seek ways to total secure: to adopt the "fortress" concept, with walls high enough and thick enough to prevent an enemy from breaking in.

When Cloud is network and network is Cloud, this approach does not work. By definition, we are all working inside the Cloud, now, so keeping enemies out simply is not possible. Instead, we need to safeguard our own assets, our own data, our own connections, people, customers, processes, wherever they may be and whoever they may be working with at any given moment.

This is a much more flexible concept, and one that reflects the continuous variations in Cloud scope and scale that take place as a matter of course, second by second and minute by minute. The space our business affairs inhabits will change constantly, after all, depending on customer contacts, levels of interaction across our ecosystems and balance between locally managed actions and those that require connectivity across different locations and across different operational boundaries.

The layout and structure of this new approach can be seen in the graphic below:



01 Cloud Access Protection & Identity Management

02 Software Protection

03 Data Protection

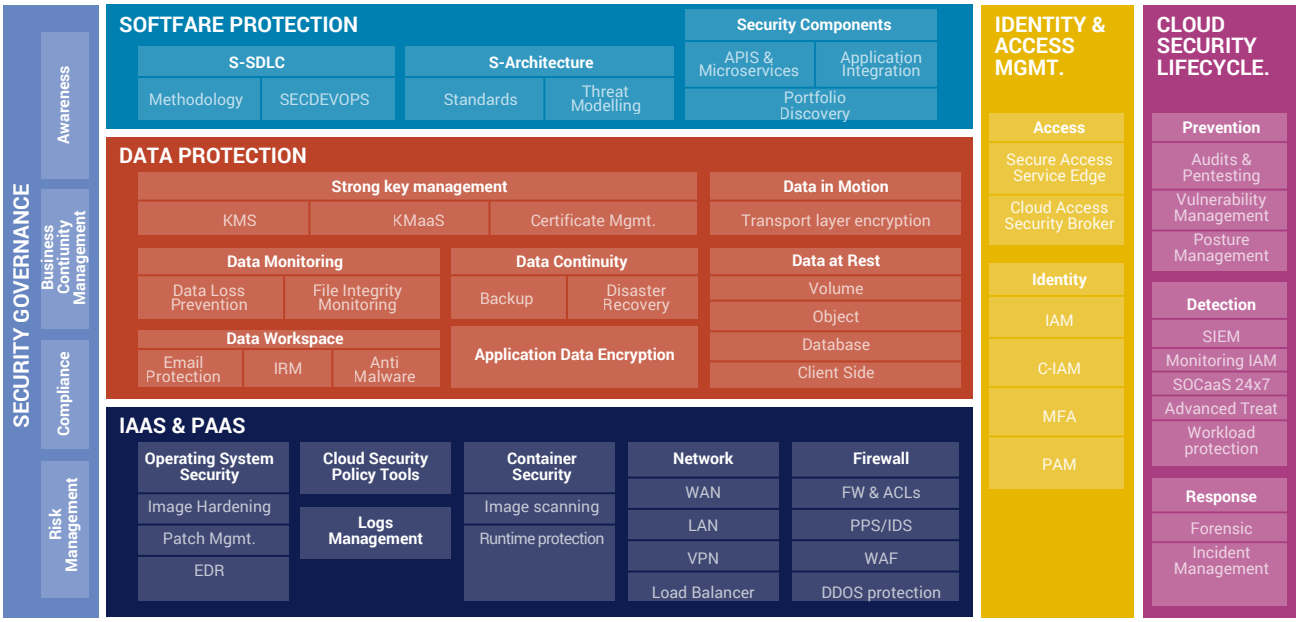
04 IaaS and PaaS workloads

05 Global Infrastructure

For an efective cloud cyber security strategy, we need to safeguard our own assets, data, connections, people, customers and processes.

CLOUD SECURITY MAP

Reference Model



In this operational structure, we build on the four platforms established in our digital architecture and apply security measures to every part of these platforms.

- **Foundation:** IaaS and PaaS, where we deploy specific solutions focused on policy, network and firewall integrity, operating systems and containers.
- **Catalogues and Blueprints:** focusing on all aspects of data. This covers data in motion and at rest, monitoring, continuity, data sharing in the workplace, all secured through strong key management.
- **Digital Capabilities:** protecting software at development stage, through an effective SecDevOps process, with strong security architecture to identify and manage threats, supported by continuous review and securing of components.

These policies, solutions, processes and methodologies apply to every part of the corporate and ecosystem Cloud native environment, and are entirely location and technology agnostic.

As the boundaries of Cloud flex with demand and work priorities, so the scope of the security environment will scale up and down to keep step with the business and its evolution.

Around the entire virtual environment, the three core components of security management continue to operate efficiently and relentlessly, systematically enforcing:

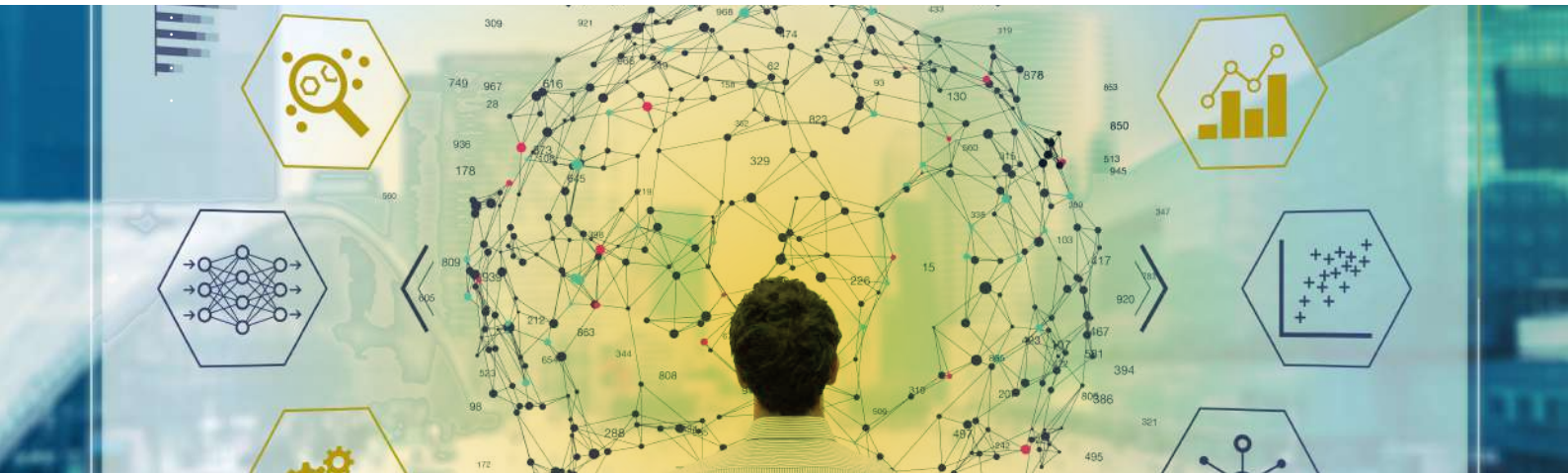
- Consistent, efficient **governance**, that applies to every asset, datapoint, process and location that ever comes into the scope of the enterprise Cloud environment.
- Uncompromising **Identity and Access Management**, applied at every point of contact, on-premise or remote, at the Cloud Edge, via secure tunnels and other connections, all managed to the most rigorous access standards.
- Continuously updated methodologies and practices for the **Cloud Security Lifecycle**, focusing on best practice prevention, detection, response and continuity capabilities.

In the Cloud, security provisions will be dynamic and agile, yet at the same time, security provisions will remain more consistent and inflexible than ever, precisely because the Cloud is now such an unpredictable environment.

This connects with our earlier statement, that it is possible to move to Cloud-as-Datacenter without organizational transformation, applying the old “walled garden” security thinking as well to private spaces in a virtual datacenter as to an on-premise environment. We cannot move to the newer forms of next generation networked Cloud, however, without substantially re-engineering security provisions.

From now on, it is not enough to secure the location where assets are hosted, we need to secure each individual asset, wherever it may be, together with the temporary connections between them, entry points for a growing number of ecosystem partners, and the standard components used to build our customized solutions.

This is conceptually more complex, which is why Cloud security must begin in the mind first of all, before being executed and operationalized.



INTEGRATION AND AUTOMATION

In the Cloud, enterprises of every size will necessarily build, run and manage hybrid environments, with some assets under their direct control and many others that are not. Smaller businesses and Cloud native organizations are likely to inhabit Cloud entirely, while larger bodies may maintain some on-premise systems, and are also likely to depend on growing numbers of Edge or IoT devices at distributed locations.

In all cases, we will require a certain level of security automation to deliver the consistency required, no matter how complex the operational environment may be. Suitable solutions now exist to enable efficient, automated monitoring and management of security across the most complex environments, although here, as in all forms of Cyber-Security, a continuous battle is taking place to stay ahead of threats and to cope with growing complexity.

KEY SOLUTIONS:

Infrastructure as Code (IAC). This enables security policies to be coded automatically and applied across all activities, as a basic obligation (you cannot carry out your tasks without applying the defined security policies).

This approach is ideal for a growing range of businesses that are becoming truly Cloud native in their approach, with all assets in the Cloud. It provides visibility, centralized control, and automated enforcement, even for businesses with very small IT functions.

Cloud Security Posture Management (CSPM). This approach is especially suitable for businesses delivering services across multiple jurisdictions, and managing variable inputs and partnerships (consumer goods businesses being a relevant example).

CSPM defines and imposes a consistent set of policies and procedures on all activities and connections, while automating the identification and remediation of risks across every part of the wider Cloud touched by a particular organization. The solution provides a single point of visibility across multiple Cloud environments and vendors, consolidating alerts and optimizing the efficiency of Security Operations Centers (SOCs).

Cloud Workload Protection Platforms. This is a class of solutions targeted at security of specific workloads held in multiple Cloud environments or in the networked Cloud. This concept has been developed to manage the new emerging reality, in which workloads are divided between Containers and Kubernetes on many different platforms.

It can now be extremely hard for conventional management systems to keep track of where different assets and resources, related to content or software in development, might be at any given moment or to identify issues and threats that could compromise the organization as a result of failures in any one of these multiple points of presence.

Summary. Tools are now being developed that are designed to automate, integrate and enhance security performance across environments provided by multiple Cloud vendors, and networked between different locations and organizations. We expect this kind of development work to accelerate in the future, as opportunities and threats continue to grow.

THE NTT DATA VISION

Staying secure in the Next Generation Cloud environments that are now evolving is a quite different challenge, when compared with on-premise security (which has in the past proved to be challenging enough, after all). There is an urgent need for a new set of attitudes, new organizational disciplines, procedures, methods and systems that enables businesses of every kind to maximize the benefits of Cloud, while managing and minimizing risks.

NTT DATA have a strong affinity with and commitment to the development of Next Generation Networked Cloud. Our long heritage in telecommunications and leadership in low latency connectivity (enabled by 5G) enables us to see Cloud as something quite different from the "virtual datacenter" concept that drove the first "Cloud Revolution".

In the near future, the boundaries between "Cloud" and "Network" will blur to the point where such a division becomes meaningless. Cloud will be redefined as Intelligent Programmable Networks, with full disaggregation of assets and fully distributed locations. This is a very dynamic environment, in which connections are negotiated, made and dropped moment by moment between millions of assets, often in highly unpredictable ways.

All data, IP, processes and other assets must remain secure and uncompromised at all times in this shapeshifting, variable geometry environment. You will not be able to apply the same security protocols that worked well enough in on-premise infrastructure to this different kind of environment. Yet it is not possible to maximize the almost unlimited potential of Cloud without appropriate security management solutions.

NTT DATA is one of the emerging architects of Networked Cloud, and understands it at a profound level. We will apply best practice thinking and management practice to ensuring that the Journey to Cloud for every enterprise is not only profitable but safe.