Shaping the future of digital business

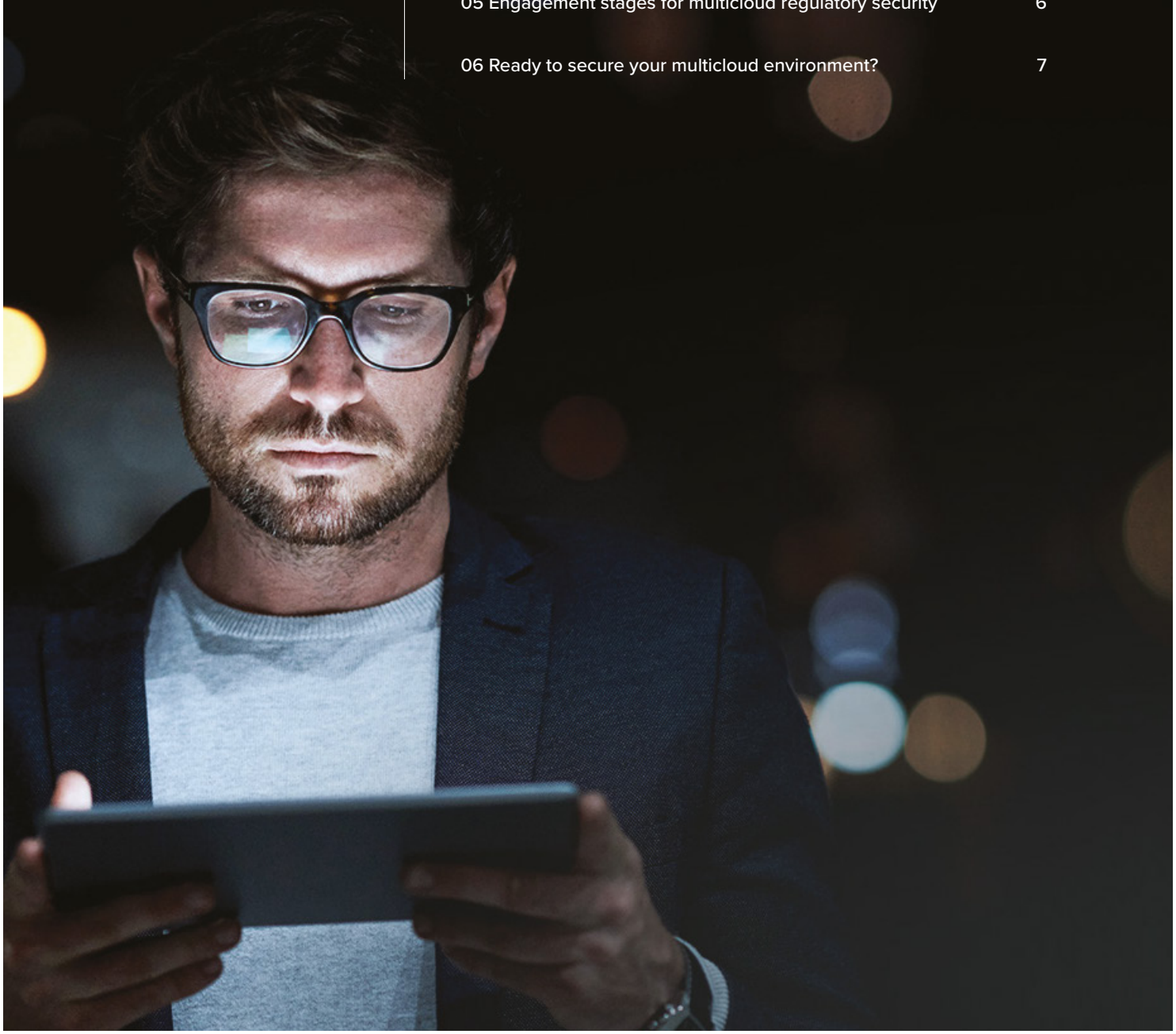
Cloud Security

Whitepaper

GFT

Upgrading your security posture for a multicloud future

Table of contents



01
The challenges of security in a multicloud environment

Over the last few years, many organisations have made a move from private cloud-based environments, such as virtual platforms or mainframes, to public cloud-based platforms. Cloud platforms have many advantages, including a reduced spend on integration of solution components, elastic scale, focused cost control measures and improved monitoring and security solutions. Although these tools are all available, not every consumer of cloud platforms makes good use of native cloud controls and tools or may even mis-use them.

01.1

When the security perimeter shifts from being solely on-premise to a shared platform, a different mindset is required. Although businesses may no longer be responsible for the hardware or the nuts and bolts of the IT infrastructure, data and applications hosted on external cloud platforms are still the responsibility of the business. Thorough consideration must be made to protect data and plan for ways to safely make full use of cloud resources.

As businesses move to a multicloud environment, maybe due to a regulatory requirement or pressures to reduce shadow IT, maintaining a positive security posture can become complex and expensive. When moving to a multicloud environment, the following risks are amplified:

- **Data leakage** - with more external connections and environments, businesses are more susceptible to outside actors influencing the system, accidental data exposure and more risk from insider threats
- **Compliance** - always challenging, moving to multicloud amplifies the difficulty of maintaining the necessary compliance with data privacy laws and regulations associated with their industry and geographic region
- **Misconfiguration** - cloud platforms can be misconfigured, thereby allowing unforeseen exposures; this risk grows as complex multicloud environments are utilised.

> **Adoption of next-generation solutions are almost always 'cloud-enhanced' solutions, meaning they build on the strengths of a cloud platform to deliver digital business capabilities.**
>
> Sid Nag, Research Vice President at Gartner[1]

01.2
Is your security posture keeping up with your multicloud strategy?

Data continues to move from traditional on-premise datacentres to software-as-a-service (SAAS) and public cloud services. Users are accessing data from both traditional offices and non-traditional hybrid working environments, from multiple devices. Phishing and other security threats are on the rise once again. A multicloud environment adds additional layers of complexity, and that complexity is creating greater risk. Ensuring that common security controls are enforced over multiple clouds can become time-consuming and expensive.

Additional tooling, such as cloud access security brokers (CASB), web-based proxies and cloud provider security tooling, require additional people with new skills or the training of existing people, which can be an unexpected cost when moving to a multicloud / multi-SAAS environment.

Through 2025, 99% of cloud security failures will be the customer's fault[2]

Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data[2]

Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks[2]

63% of organizations find security analytics and operations more difficult than they did two years ago[3]

02
Common multicloud security issues

Based on our experience with many client projects, some common security issues can arise when moving to a multicloud environment. Common security themes include:

Over-permissioned users

Many companies provide too many permissions to users when establishing a multicloud environment. This may be due to the initial set up of an environment, transitioning from a development environment or sandbox to a production system, or a lack of headcount. It is important that permission reviews are completed regularly to mitigate this risk.

Internet-exposed cloud resources

When companies move from one cloud provider to another, common settings around network traffic can differ between cloud providers. This can lead to cloud resources becoming exposed to the internet with little to no protection. Common security measures such as web application firewalls and traditional firewalls can be implemented incorrectly, allowing unforeseen access.

Logging and monitoring

When moving to a multicloud environment, logging and monitoring is another topic that may be misunderstood. In some cases, businesses may not have sufficient logging turned on, but more often than not, there are just too many logs from applications which then leads to ‘log fatigue’. Making sense of the large volume of log data is a key capability that needs to be built into the new environment.

Data sovereignty and exposure

Where data resides is becoming increasingly important due to regulatory concerns. Many multinational companies are subject to laws restricting where data can be stored and processed. Ensuring data stays within a geographical area is a concern when dealing with multicloud workloads. On top of this, ensuring that users and developers are responsible when placing data into the cloud has become a greater concern over recent years. Since all cloud storage is accessible via the internet, it is imperative that access is restricted to only people that require it.

Cloud encryption and key management

Ensuring data is encrypted on a multicloud platform is imperative and many cloud platforms now encrypt data by default. Many companies now use their own encryption keys, ensuring that their data is safe from external access and access by the cloud providers themselves. Ensuring these encryption keys are kept secure has become imperative, as well as rotating these keys in a timely manner to ensure that companies are not locked out of their own data.

Complex security governance

Providing a consistent set of security controls across multiple cloud platforms and SaaS providers has become an increasing challenge. It takes time to understand a single cloud platform and build security around it. It becomes even more complex to have multiple cloud environments and SaaS providers.

Key management and secret keeping

As previously highlighted, mismanagement of keys can result in loss of access to data or improper access to data if keys are compromised. Passwords and secrets are equally at risk in a multicloud / multi-application environment. Ensuring there is a consistent policy when working with passwords and secrets is vital.

Compliance and control violations

Monitoring compliance and control violations within a multicloud environment is a time-consuming and daunting task. Many cloud platforms now offer industry standard control sets that will allow alerting when violations occur. However, this can lead to alert fatigue and prevent important actions being taken in a timely manner to remediate risks.

Alert fatigue

Alert fatigue occurs when there are too many alerts occurring, with no way to filter relevant alerts from the noise of day-to-day logging and monitoring. Ensuring the correct alerts are being given attention requires the fine tuning of logging and monitoring systems.

Zero trust

A zero trust architecture ensures that users and applications have the appropriate access permissions and no more. It also limits network traffic to application requirements, which helps to reduce an internet-exposed attack surface. If applications are not limited in this way, attackers have a large attack surface to exploit.

03
What is a cloud security posture?

A cloud security posture refers to the overall security status of an organisation for public and private cloud, including applications, user access, data security and network security. It is essentially a 'report card' on the ability of the organisation to prevent, detect and remediate security threats across all these domains for a multicloud environment as quickly and thoroughly as possible, in order to minimise risk and impact.

The cloud security posture of any organisation is enhanced by a solid combination of working on a trusted cloud platform and correctly leveraging the platform tools available. When working with multiple cloud providers, a third-party tool can accelerate the process of securing all cloud environments to a similar security standard.

Making use of a third-party security tool helps to simplify the process; from analysing the different cloud platforms, putting in place consistent tooling to prevent attacks from happening, detecting them when they do happen, and responding to them to resolve the situation. They allow a business to create a single set of controls within the tool and then apply them to multiple cloud environments.

Prevent
Preventative controls put the guardrails in place to prevent problems from happening in the first place.

Example
Preventative controls limit the things you allow people to do, such as what applications or data they can access or edit.

Detect
Detection provides the visibility and alerts to bring attention to a potential problem somewhere in your environment. This can include real-time monitoring of a live attack.

Example
Detection controls can create an alert when someone makes a change to their own permissions.

Respond
Response can come in different forms, from isolating suspected compromised infrastructure, to disabling suspect user accounts.

Example
Response can be an alert that is triggered or an automated playbook, to remediate any problems that may occur.

04
GFT regulatory security for multicloud environments

GFT's regulatory security services for multicloud environments are designed to help enterprises implement a common set of controls across multiple cloud platforms within their technology estate. We leverage best practice control sets, such as CIS, ISO and NIST, as well as building custom control sets for clients to assist in preventing common attacks.

We work together with customers to implement a cloud security posture management platform which enables a 'single pane of glass' view across multiple cloud platforms. This enables us to correct any short-term cloud misconfigurations and provide a longer term roadmap, in order to maintain a high level of security and reduce overall risk in leveraging the cloud.

With a single pane of glass across multiple clouds, alerts can be picked up easily and measures put in place to prevent alert fatigue. Having an aggregated log and cloud configuration view across multiple clouds allows businesses to prevent misconfigurations and pick up any actions performed. This can assist in reducing risk from both insider and external threats.

- Accelerate outcomes and close security gaps faster
- Reduce risk of incident occurrence and severity
- Get security configurations and controls right first time
- Achieve more sustainable results

05
Engagement stages for multicloud regulatory security

1 Plan

Phase 1: : Plan

Discovery
Discovery of the client environment builds the understanding of the key requirements for multicloud security, covering current pain points and challenges, as well as future plans that may affect the overall security posture.

Design
Utilising Prisma Cloud from Palo Alto Networks, GFT ensures best practices are followed to architect solutions and recommend models to address security requirements and mitigate issues across any multicloud scenario. Being aware that security budgets are not unlimited, solutions are designed to be cost-effective, with high degrees of automation and filtering, ensuring security teams get the prioritised information they need, when they need it.

2 Build

Phase 2: Build
The build out of the platform includes: integration of multiple cloud platforms, implementation of infrastructure as code scanning, build out of custom policies, implementation of out-of-the-box policies such as PCI DSS, ISO270001 etc, implementation of cloud workload protection, and any other solutions agreed to in the Plan phase.

3 Operate

Phase 3: Operate
Operational handover is the key part of this phase. This includes informal training on use of the platform, a handover of an operational guide and guidance around formal training provided by the chosen vendor. GFT works with customers to ensure that the deployment of Prisma Cloud is smooth and sustainable.

06
Ready to secure your multicloud environment?

Cloud is the foundation for digital transformation, enabling business agility, application modernisation and more. However, the cloud of today has become a vast and complex landscape, with security teams struggling to keep up. Properly assessing and strengthening the cloud security posture can create additional benefits, but often requires outside guidance.

GFT has broad security expertise, plus deep experience with GCP, AWS and Azure security, and hands-on experience of solving enterprise security challenges across industries. GFT is here to help you achieve your secure cloud vision.

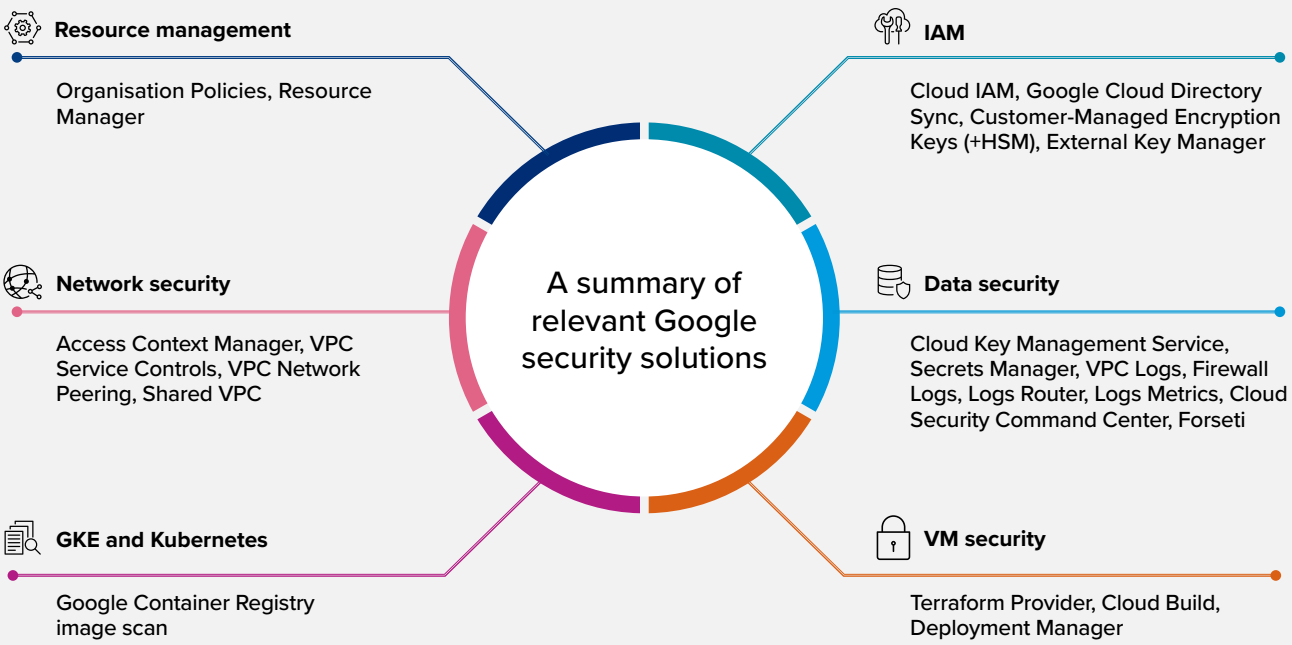
For more information on GFT and our **regulatory security for multicloud environments**, please visit gft.com.

To arrange an initial discussion with our security specialists, email businessmarketing@gft.com.

Sources:

1. Gartner, “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020,” Nov 2019
2. Gartner, “Is the Cloud Secure?” Oct 2019
3. ESG, “The Rise of Cloud-Based Security Analytics and Operations Technologies,” Oct 2019
4. Forrester, Predictions 2021: Accelerating out of the Crisis

06.1
A summary of relevant Google security solutions



07
The complete solution for security in a multicloud environment

GFT and Palo Alto Networks offer security capabilities with hundreds of built-in policies spanning more than 20 different industry-standard compliance rulesets.

At GFT, we have Palo Alto certified experts with hands-on experience of delivering and integrating Prisma Cloud into regulated enterprise environments across multiple cloud providers. Partnering with the three major cloud providers (AWS, Azure, GCP) we have constant and consistent communication channels with all suppliers to ensure implementations meet industry standards and best practice.

We are excited about our partnership with Palo Alto as it enables us to combine GFT's deep engineering expertise across the financial services industry with Palo Alto's cutting-edge multicloud security offerings. Working together, we provide our clients with peace-of-mind, enabled by best-in-class cloud security.

paloalto NETWORKS

08
Our success story – Salt Bank ushers in a new era of digital banking in Romania

Salt

GFT and Engine by Starling enable the launch of Romania's first neobank, successfully delivering for customers in under 12 months.

Salt Bank, a new digital bank in Romania's financial landscape, has launched less than one year after the project was kicked off. Salt Bank is the first neobank using Engine by Starling's core banking system outside of the vendor's parent company, Starling Bank. It was implemented in partnership between GFT, Salt Bank and Engine by Starling. This continues a transformative trend GFT sees in financial services and beyond. Organisations are reinventing their technology capabilities, adopting a 'platform of platforms' approach. This involves consuming ready-made capabilities from the wider industry.

GFT was engaged to provide overall design and integration services, relying on their deep expertise. For Salt Bank, security was a cornerstone, not an add-on. Our goal was to set a new benchmark for security and scalablilty and to build customer-centric, cloud-first solutions where speed and responsiveness were imperative. To enable this, we implemented Palo Alto's Prisma Cloud; an industry-leading, cloud native application protection platform (CNAPP), to provide a 'single pane of glass' view of the entire IT estate as it was built.

Our experts

Dean Clark
Chief Technology Officer at GFT UK
dean.clark@gft.com

Dean is responsible for the technology strategy for GFT, with a heavy focus on cloud and new innovative technologies. His focus is on identifying areas of customer business that can be improved via transformation or rationalisation.

Dean's experience has seen him work on complete cloud migrations for a UK retail bank, Head of Web Engineering for an investment bank, and Head of Technology for a managed hosting provider. This varied experience brought him to GFT where his combination of banking, insurance and IT leadership has been perfectly placed.

Dean is passionate about growing the business and in addition to his day to day responsibilities, was the founder of our graduate intake programme, which trains new starters on a variety of cloud infrastructure and coding skills.

About GFT - Shaping the future of digital business

GFT is driving the digital transformation of the world's leading companies in the financial and insurance sectors, as well as in the manufacturing industry. As an IT services and software engineering provider, GFT offers strong consulting and development skills across all aspects of pioneering technologies, such as cloud engineering, artificial intelligence, mainframe modernisation and the Internet of Things for Industry 4.0.

With its in-depth technological expertise, profound market know-how and strong partnerships, GFT implements scalable IT solutions to increase productivity. This provides clients with faster access to new IT applications and innovative business models, while also reducing risk.

Founded in 1987 and located in more than 20+ countries to ensure close proximity to its clients, GFT employs 12,000+ people. GFT provides them with career opportunities in all areas of software engineering and innovation. The GFT Technologies SE share is listed in the Prime Standard segment of the Frankfurt Stock Exchange (ticker: GFT-XE).

12,000+
specialists worldwide

20+
markets worldwide operating from 40+ physical locations

35+
years' experience

blog.gft.com
twitter.com/gft_en
linkedin.com/company/gft-group
›gft.com

For more information please visit › gft.com