

Deloitte.



Unlocking the Business Case for Cloud Security:

**Make better risk informed design decisions with
Deloitte and Google Cloud**

Google Cloud | **Deloitte.**



The Reality of **Cyber Attacks**: Key Statistics

63% of incidents were notified by external entities.¹

In 2023, the most targeted cloud environments were Software-as-a-Service (SaaS) **39%**, and cloud-based storage services **36%**.²

These attacks often lead to data breaches, impacting **39%** of businesses that experienced cloud-based targeting.²

Deloitte CTI observed threat actors increasing their use of valid accounts used to gain initial access in **43%** of cloud intrusions.²



(M-Trends 2023¹)

(Deloitte Global Cyber Threat Intelligence – Annual Trends 2024²)

With the high volume of misconfigured and vulnerable platforms exploited across all industries, companies using cloud are continuously exposed to the real risks of data loss and financial penalties. Google Cloud is one of the fastest growing cloud services and as such, businesses need to get a handle on cyber risks and threats. These challenges aren't easy to grasp given the following trends we are seeing in secure cloud transformations and migrations.

- Increased proliferation of threats due to global tensions and organisation security challenges
- Identifying the right balance between security protections and business goals for your specific circumstances across the Google Cloud ecosystem
- Organisational security risks aren't always considered in design decisions during Google Cloud transformations and migrations
- Releasing budget to secure your Google Cloud ecosystem requires critical analysis to measure risk burndown against capex and opex spend

A range of opportunities can be unlocked to reduce risk and improve agility when consuming Google Cloud.

To reduce the likelihood of cyber risks and threats materialising in your ecosystem, Deloitte and Google Cloud have developed a proven approach, which will help you achieve security in your cloud transformations and migrations.





Dive into the Google
Cloud ecosystem of
security resources



What's available?

Google Cloud is continuing to publish new security frameworks and blueprints that support design decisions on your Google Cloud environment, rest assured you're in good hands. Those that we notice that are of high relevance to organisations are:

- **Enterprise foundations:** a blueprint of recommended products and security capabilities for organisations to achieve a robust security posture and protections across their environment. This is Google's foundational baseline, providing key recommendations for your cloud ecosystem.
- **Software delivery shield:** a software supply chain security solution that provides a modular set of capabilities and tools across Google Cloud products to improve software supply chain security. This has been created for organisations developing applications on Google Cloud.
- **Security artificial intelligence framework:** security best practices that apply to AI systems risks. A risk based framework from which to safely design and create AI systems.

Why is it so important now?

Cloud native recommendations are dependent on the services you build and your business environment. Changes in the external business environment makes cloud security even more complex:

- Geopolitical tension, coupled with advances in AI, have led to an increased threat landscape across all industries. Both targeted and supply chain attacks are now easier to fulfil, more sophisticated and more prevalent.
- Regulatory expectations are increasing, with new standards and acts (e.g. EU AI Act, Telecommunications Security Act, DORA) coming into force. While good for the industry it adds pressure for security teams to do more.
- Digital business requirements are increasing with pressures to ship more features, faster. Security teams have to work at the same pace.
- Global economic conditions have put cost reduction high on the agenda for organisations, with appetite to spend less on security. This creates additional pressure for how companies effectively manage risk. Security teams may be expected to do more with less resource.



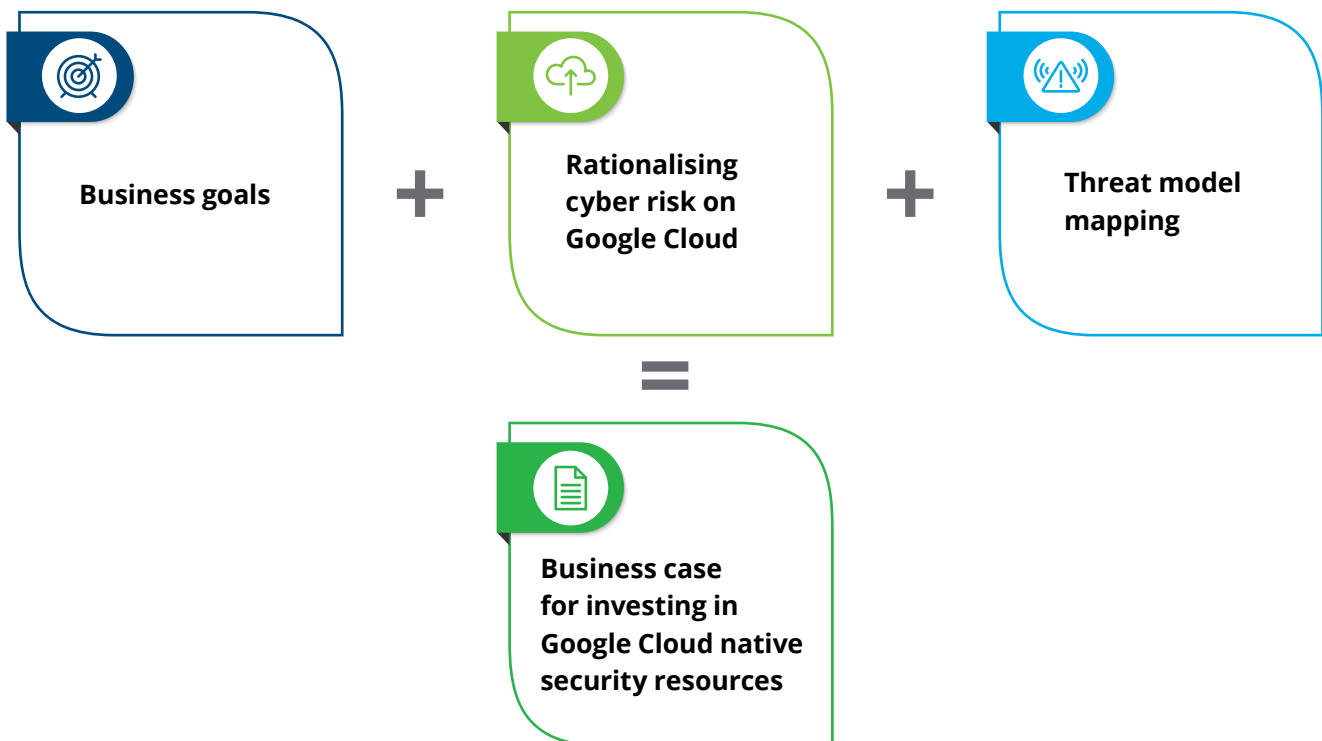
The consumption challenge and how our method unlocks the **security business case**

Where we see organisations get stuck

We see companies (across all industries) fall into three categories when consuming frameworks during a transformation or migration. We outline these below:

- 1 Enable everything:** Google Cloud is the primary business driver and they have allocated enough budget to procure the entire Enterprise Foundations stack.
- 2 Do nothing:** Struggling to realise the return on investment and build a business case for additional budget required for cloud security.
- 3 Stuck in the middle:** Already have existing security tooling in place before Google Cloud transformation/migration. Companies are grasping with organisational cyber risk management on Google Cloud and don't know which Google Cloud native security resources to procure for their specific needs.

Category two and three are more common. If your organisation is in one of these categories then the challenge is going to be around rationalising focus areas to release budget. To support with this, Deloitte and Google Cloud have created an approach, which we cover in more detail below.



Business goals

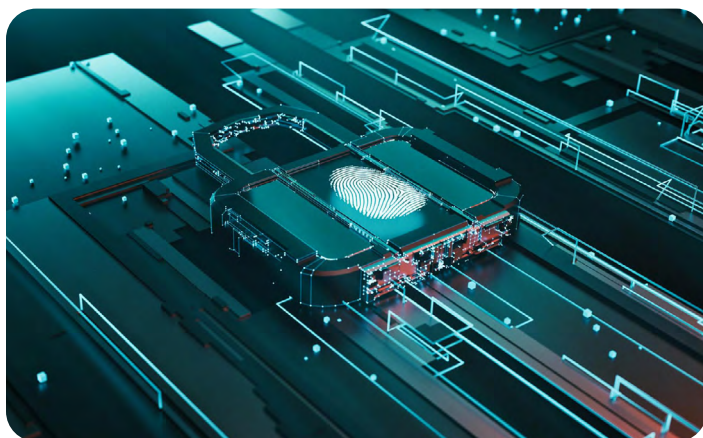
Many of us are familiar with the concept that security should facilitate business goals, highlighting the importance of understanding the objectives for a transformation or migration. It may be gaining new market share, scaling to end-user demands, introducing new product offerings, or reducing infrastructure cost. These business goals can be mapped against a transformation or migration to compliment risk remediation, and to create a more effective business case for budget holders.

Rationalising cyber risk on Google Cloud

Arguably the most important part. We find that business risks informed by technical threats foster better decision making. The business risks should be consistent across your organisation and mappable to goals. These risks at a very high level can look like:

- Avoid loss of business critical services.
- Prevent data leakage of sensitive data that could lead to regulatory fines.
- Non-compliance to regulation and loss of cyber accreditation due to poor security posture.

Business risk statements and corresponding registers are common and most organisations already have these.



Threat model mapping

Threat use cases are more nuanced and provide the technical detail that helps describe the attack profile, tactic and technique. This follows a one-to-many relationship where multiple threats inform a single risk statement.

Your threat statements read something like "An attacker spoofs the identity of a legitimate user to upload malicious content (e.g. malicious files, injection attacks)". It's a technical, descriptive statement of how we hypothetically reverse engineer or abuse a service.

Threat modeling requires us to decompose your Google Cloud solution design to identify entry points, targets and control failure opportunities. At Deloitte, when we run our threat models we often find that we have anywhere up to 60 threats identified across several themes:

- **External attack:** an internet based attack to an exposed field or entry point (e.g. injection or cross site scripting to an application/ cloud resource)
- **Compromised cloud resource:** a threat actor that already has access and is trying to maintain foothold or laterally move to other resources
- **Distributed Denial of Service (DDOS):** inbound traffic of significantly high volume from multiple sources designed to render a cloud service unavailable
- **Malicious event:** general malicious activity and lateral movement across the cloud environment
- **Data leak:** cloud storage (database, storage bucket, source code repository) data exposed to a public domain
- **Vulnerability exploited:** vulnerable resources exposed to the internet enabling an attacker to exploit and cause harm

We map threats back to your business /cyber risk statements to inform risk prevalence and exposure. Which in turn helps prioritise where effort and budget requires additional focus.

Recommendations to each threat are tailored to native security changes. In most cases a single control/capability will address multiple threats. The cross reference of one recommendation to multiple threats inform the measurement of return on investment.



Make better risk informed design decisions with Deloitte and Google Cloud

Business case for investing on Google Cloud native security resources

Deloitte unlocked a business case recently with a large European client on a Google Cloud transformation project. They already had some Security Foundations services enabled so we weren't starting from zero.

We ran the threat model and mapped several threats with mitigating measures. Google Cloud's frameworks provided a blueprint for cloud native recommendations. Deloitte and Google Cloud worked together to develop a bespoke approach with proven methods. Together we formulated a view on prioritisation and effort.

The capability that had addressed the most threats and helped provide, detect and response capabilities was Security Command Centre Premium (SCCP). The organisation was able to articulate the return on investment and burndown of risk from SCCP, request budget and manage findings and control recommendations SCCP provided across its Google Cloud estate. All achieved by unlocking the Deloitte and Google Cloud alliance and following our formulated approach.



Accelerate safer cloud consumption

The Deloitte and Google Cloud alliance offers a collaborative approach to work with you to securely architect your Google Cloud ecosystem. We will:

- Empower you to make better decisions cloud transformations and migrations.
- Reconcile organisational security concerns/risks to your Google Cloud transformations and migration efforts.
- Address tooling spend and focus on yielding a higher return on investment on cloud security investments.
- Engineer sustainable long-lasting benefits and protective measures.



Authors



Roupe Sahans
Cyber Security
Senior Manager,
Deloitte
rsahans@deloitte.co.uk



Omar Saenz
Security Specialist,
Google
osaenz@google.com

Contacts



Susan Sharawi
Cyber Security
Partner,
Deloitte
ssharawi@deloitte.co.uk



Reto Haeni
Cyber Security
Partner
Deloitte
rhaeni@deloitte.ch



Ashish Gupta
Cyber Security
Director
Deloitte
asgupta@deloitte.ch

References

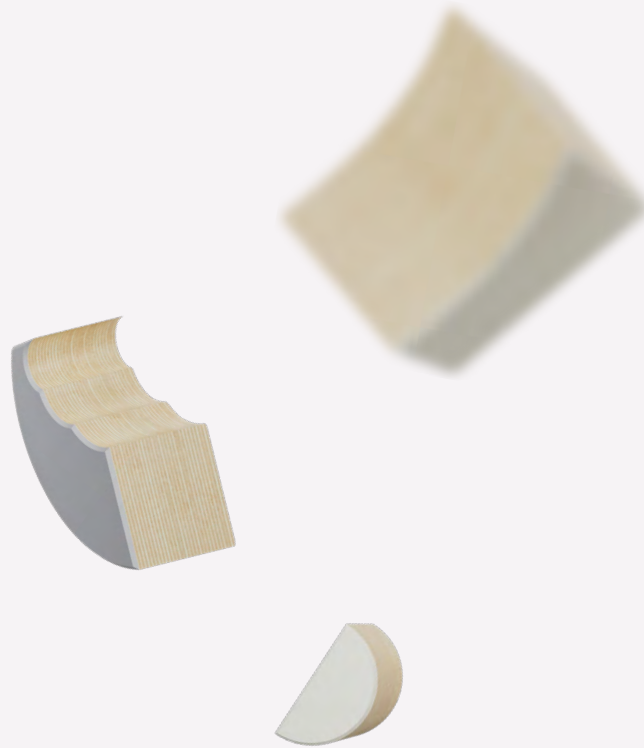
¹ <https://www.mandiant.com/threat-detection-and-response-are-you-compromised>

² <https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2024.html>

Reinvent the game.

Become the architect of your future. Connect the innovation of the Global Google Cloud ecosystem to unlock outsized business value and new competitive opportunities. When you have the power of Deloitte + Google Cloud at your fingertips, you can reinvent the game, set the rules and win.

Learn more at deloitte.com/googlecloud



Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/aboutto learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and the unrelated entities, are legally separate and independent entities.

©2024. For information, contact Deloitte Global.

Designed by CoRe Creative Services. RITM177722