Deloitte. | Google Cloud

CYBER SERVICES

Cyber threats are in constant evolution, presenting new security challenges every day. With Deloitte's integrated security approach and suite of broad, end-to-end solutions, paired with Google Cloud's leading security technology, your organization can protect what matters. Let us be your trusted, committed confidants to keep you running at full speed, no matter what the world throws at you.

Deloitte's Google Cloud Cyber Capabilities

Cloud Security

- *Secure Cloud Foundations, Landing Zone, and Migrations*
- *Cloud-Native DevSecOps, CNAPP: Security Command Center Enterprise (SCCE) Implementation and Managed Service*
- *FedRAMP Compliance and Assured Workloads*
- *Cyber Cloud Managed Services (CCMS)*

Security Operations

- *SecOps Modernization Strategy and Roadmap*
- *SecOps Deployment and Support*
- *SecOps Managed Security Service*
- *Managed Extended Detection and Response (MXDR)*
- *Mandiant Incident Response*

Secure Browsing

- *Secure Enterprise Browser Strategy and Roadmap*
- *Chrome Enterprise Premium Implementation, Optimization, and Support*

Secure AI

- *Security of Generative AI (GenAI) Models*
- *Force Multiplying SecOps with GenAI*
- *AI-Driven Security Operations*

Market trends

- Attack surface expansion
- Security tools consolidation
- Digital supply chain risk
- Engineering trust with cloud-native controls

Common business challenges

Cyber as a catalyst to empower your organization

C-SUITE

- Regulatory adherence and compliance
- Business agility, customer experience, and trust

1. Software development lifecycle (SDLC), DevSecOps, tools, and governance
2. Secure digital transformation, secure solutions, and better user experience

VP/DIRECTOR/MANAGER

- Transformation and operating advancement
- Technology shift, modernization, and cost

3. Adoption of new technologies and next-gen cyber products
4. Next-gen cyber transformation of people, process, technology, and automation

ANALYST/ENGINEER

- Shortage of skilled resources
- Lack of industry and business case knowledge and exposure

5. Upskilling and technology adoption, Infrastructure-as-Code (IaC), Policy-as-Code (PaC), and automation for cybersecurity
6. Cyber standard operating procedures, playbooks, templates
7. Use of artificial intelligence, machine learning, user and entity behavior analytics, and advanced toolsets

Why Deloitte and Google Cloud

In 2025, Deloitte's strong collaboration with Google Cloud was recognized with four Partner of the Year awards, including accolades in the security domain: Global Security Partner of the Year and EMEA Security Partner of the Year. These awards underscore Deloitte's commitment to delivering cutting-edge security solutions and reflect our deep understanding of the evolving cybersecurity landscape.

This recognition builds upon a consistent record of success. Deloitte was also named Google Cloud Security Partner of the Year for Security Specialization in 2024 and has received numerous other Partner of the Year awards and acknowledgments from 2017 to 2023. This long-standing achievement highlights Deloitte's proven ability to deliver innovative Google Cloud solutions that address the increasingly complex security challenges faced by clients.

Google Cloud
Security Specialization

Google Cloud's
most capable SecOps service delivery partner

5,800+
Google Cloud Certified Professionals
Including architects, security engineers, and developers

Spotlight: *Deloitte engagements*

CLIENT:
MAJOR BANK

Background:
Deloitte assisted a bank in building a secure and resilient Google Cloud environment for migrations over a multi-year period.

Solution:
Deloitte developed secure Cloud Foundations and compliance automation to accelerate application migration and deployment into Google Cloud.

Impact/Outcome:
Secure and resilient network structure that enables minimal latency and maximum security. Securely migrating over 700 applications to Google Cloud enabling the bank to exit the data center.

CLIENT:
GLOBAL INVESTMENT BANK

Background:
The client aimed to enhance their cloud security while establishing foundational capabilities for the large-scale development of new products and market offerings in the cloud.

Solution:
Deloitte developed and automated security guidelines for use of Google Cloud services, assisted with cloud security design reviews, developed threat models in conjunction with client tech risk personnel, and developed Open Policy Agent (OPA) policies to help enforce PaC for Google Cloud's Kubernetes Config Connector (KCC)-based IaC deployments across the client's Google Cloud environment and implement into development process with Continuous Integration and Continuous Delivery (CI/CD) pipelines.

Impact/Outcome:
Ability to shift left in cloud development with automated preventative guardrails confirming Google Cloud resource configuration even before deployment.

CLIENT:
GLOBAL FAST-FOOD CORPORATION

Background:
Global fast-food client faced challenges in scaling its legacy cybersecurity systems to match its rapid digital growth and outpace continually evolving threats. As part of their security strategy, the client needed a comprehensive solution to monitor, detect, investigate, and respond to cyber-attacks, while safeguarding their data.

Solution:
Google Cloud Security and Deloitte collaborated to provide an intelligence-driven security solution for the fast-food client's global cyber security operations. Deloitte designed a comprehensive security logging framework mapped to industry best practices and implemented Google's Security Operations platform for scalable, intelligence-driven threat detection and proactive response.

Impact/Outcome:
Through an accelerated journey from initial development to full-scale global adoption with standard security operations across markets, the client achieved increased visibility of threats and their associated level of risk and a reduction in threat actor dwell time through prioritized and proactive response actions thereby reducing business risk throughout their global enterprise environment.

CLIENT:
NATIONAL CONVENIENCE STORE CORPORATION

Background:
The client sought to upgrade their SIEM platform to a cloud-native detection and response tool but faced challenges due to a limited budget and resources, leading to restricted data ingestion and reduced environment visibility.

Solution:
Deloitte and Google Cloud Security collaborated to deliver an accelerated migration to Google SecOps.

Impact/Outcome:
Client's SOC was operational in 60 days and achieved significant cost reductions while increasing visibility and gaining a larger lookback period.

Start the conversation

Mark Nicholson
Google Cloud Cyber Lead
Alliance Partner
Deloitte & Touche LLP
manicholson@deloitte.com

Chris Trollo
Lead Sales Executive
Deloitte & Touche LLP
ctrollo@deloitte.com

Ryan Lee
Deloitte Security Alliance Manager
Google LLC
rryanlee@google.com

Jason Tarlton
Deloitte Security Alliance Manager
Google LLC
jtarlton@google.com