

# ***BANKING ON CYBER***

*How Deloitte and Google Cloud can help fortify your financial services IT infrastructure*

Across the financial services industry, organizations face new cyber security challenges in the cloud from increased regulatory pressure and multi-cloud design patterns. ***Combined with the increasing cost of cyber incidents, these challenges make threat detection, prevention, and cyber resilience board-level issues, including:***

**Global cyber talent shortages:**

The scarcity of cyber professionals, especially those in specialized fields such as Cloud Security Engineering and SecOps, can hinder an organization's efforts to build and maintain robust cybersecurity measures, which can lead to development delays.

**Multi-cloud control inconsistencies:**

Inconsistencies in controls across cloud and on-premises environments can create vulnerabilities and complicate efforts to maintain a unified security posture. These inconsistencies can also frustrate developers, who must navigate varying requirements, development complexity, and inconsistent experiences while working with different environments or teams.

**Mergers and acquisitions integration:**

Integrating newly acquired environments imposes a significant burden on cyber teams, as they work to evaluate security posture, harmonize controls, and integrate or migrate security tool stacks—all while avoiding cyber-related delays and improving operational synergies.

**Regulatory pressure:**

Increased regulatory scrutiny across the cloud and IT landscape can impact development velocity as organizations must prioritize remediating regulatory findings over developing new solutions.

**Legacy security tooling:**

As data volumes increase, maintaining legacy security information and event management systems (SIEMs) is increasingly challenging and costly. But as organizations migrate to modern SIEMs that better support evolving needs, they must address data migration, integration with existing systems, and configuration and customization challenges.

## ***Tackle today's security challenges with integrated cyber solutions that scale for the future***

Depending on specific application needs and cybersecurity goals, organizations can address and fortify their security posture by building cloud-based and on-premises solutions that combine Google Cloud cybersecurity technologies with specially designed solution accelerators, services, and support from Deloitte. ***These integrated solutions include:***

**Google SecOps SIEM/SOAR:**

Modernize your security operations center (SOC) with Deloitte Cyber Google SecOps, a service offering that helps design, deploy, and configure Google SecOps implementation, including data collection and ingestion, data normalization, and detection and analytic enablement.

**Cyber Cloud Managed Services (CCMS):**

Accelerate your digital transformation journey on Google Cloud with Deloitte CCMS, a cloud security service that provides 24/7 security monitoring and protection for essential resources. Gain peace of mind with security built in from day one, empowering faster cloud migration.

**Secure Cloud Deployment (DevSecOps):**

Secure your cloud deployments with automated guardrails that leverage Deloitte's extensive cloud Policy-as-Code (PaC) accelerator library, which can be tuned to your specific requirements using Deloitte AI Assist for PaC. These guardrails are put in place to help reduce the burden of manual control validation and remediation while accelerating cloud deployment velocity.

**Security Command Center Enterprise (SCCE):**

Monitor and protect your multi-cloud environment with Google SCCE, operationalized with enterprise security tools and IT Service Management (ITSM) system integrations and tuned using Deloitte's curated library of Custom Security Health Analytics (SHA) Modules, IaC posture policies, and custom organization policies.

## Additional benefits of deploying integrated solutions:



### Build a secure landing zone:

Accelerate cloud adoption and migration with the Deloitte Google Cloud Accelerator, which allows for the rapid creation of secure landing zones with integrated capabilities across major Cyber domains such as Access Management, Network Security, Application Security, and Cloud Native Application Protection Platforms (CNAPP).



### Improve and secure the developer experience:

Empower your development teams to focus on core development activities with "ready-to-go" secure deployment architectures, easily accessible and consistent security requirements, Infrastructure-as-Code (IaC) security scanning that's directly integrated into deployment pipelines, and enablement of secure integrated development environment (IDE) tools.



### Simplify regulatory readiness:

Prepare for major regulatory reviews and reduce delays from unexpected findings by working with Deloitte cloud security practitioners to identify control gaps, remediate findings, design compliant architectures, and document relevant control evidence to help provide a smooth review process.



### Establish secure enterprise browsing:

Secure and protect enterprise endpoints from browser threats while also protecting enterprise data with Google Chrome Enterprise Premium (CEP), configured to meet enterprise users' unique needs and operationalized with Deloitte's experienced security engineers. CEP protections are also enhanced with threat detections and custom detection rules enabled by Google SecOps integration.

## Why Deloitte?

In addition to Deloitte's comprehensive experience in the financial services sector, we've also been recognized as a Google Cloud Global Services Partner for four consecutive years, including being named Global Security Partner of the Year in 2025. These accolades demonstrate our consistency and reliability in delivering trusted service and support for financial services clients, while creating a more cohesive security posture using enhanced Google Cloud solutions.

## Take the next step

To learn how Deloitte can help your financial services organization build a more resilient, scalable, and secure cyber infrastructure using Google Cloud solutions, get in touch with a Deloitte specialist today.



### Mark Nicholson

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



### Pradeep Sandhu

Google Cloud Cyber FSI Partner  
Deloitte & Touche LLP  
prsandhu@deloitte.com



### Vivek Saxena

Google Cloud Cyber FSI Senior Manager  
Deloitte & Touche LLP  
vivsaxena@deloitte.com



### Chris Trollo

Google Cloud Cyber Sales Lead  
Deloitte & Touche LLP  
ctrollo@deloitte.com



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see <http://www.deloitte.com/us/about> for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved.