Enterprise Strategy Group™

Mitigate Risk While Improving Cybersecurity Efficacy and Efficiency

Accelerate Time to Value With Google Cloud Solutions and Foresite Catalyst

Tony Palmer | Practice Director
Justin Boyer | Senior Analyst

ENTERPRISE STRATEGY GROUP

NOVEMBER 2025

This Enterprise Strategy Group eBook was commissioned by Foresite and is distributed under license from TechTarget, Inc.

"This eBook explores how to **modernize** security operations using the rich capabilities of Google Cloud and and its partnership with Foresite."

Tony Palmer | Practice Director
ENTERPRISE STRATEGY GROUP

Introduction

The cybersecurity skills shortage is not improving, and organizations impacted by it are experiencing serious ramifications.

Organizations reported multiple areas of impact from the cybersecurity skills shortage, including increased staff workload, unfilled open security positions, high burnout rates, and attrition. Working as a cybersecurity professional continues to become more difficult. Increasing cybersecurity complexity and workloads, increased threats due to a growing attack surface, staffing issues, and cybersecurity budget pressures are all contributors.

This eBook explores how to modernize security operations using the rich capabilities of Google Cloud and its partnership with Foresite. Modernizing security in this way enables organizations to effectively build their security strategies to protect their business and drive growth with greater security, agility, and resilience, while minimizing impact to the business.

CONTENTS

Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals,* November 2024 . All Enterprise Strategy Group research references and charts in this eBook are from this research report.

Back to Contents

Chapter 1:
Persistent Security Challenges

The cybersecurity chain is only as strong as its weakest link.

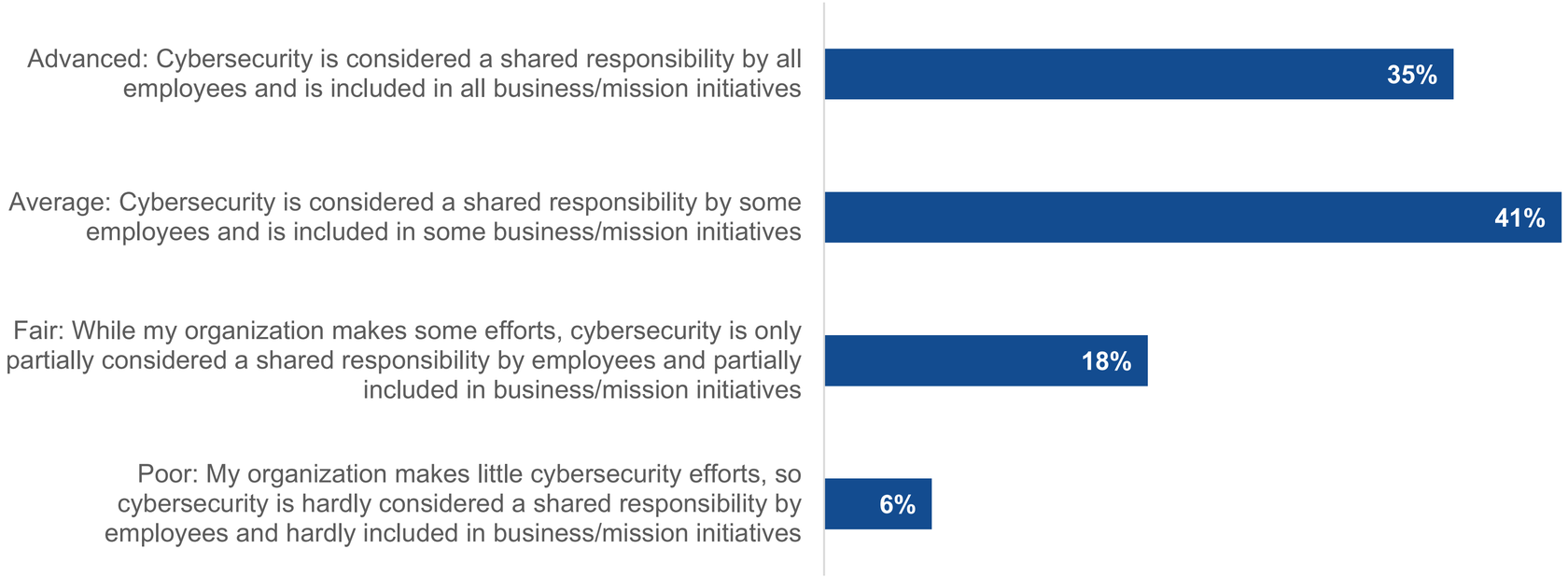
An average cybersecurity culture, where cybersecurity is considered a shared responsibility by some employees and is included in some business initiatives, suggests that other employees and business initiatives ignore or minimize cybersecurity.

This leaves ample room for misconfigured systems, vulnerable software, and uninformed employees, creating avoidable cyber-risks throughout the enterprise.

65%

of cybersecurity professionals indicated that their **organization's cybersecurity culture is "average" or worse.**

How would you characterize the cybersecurity culture at your organization?



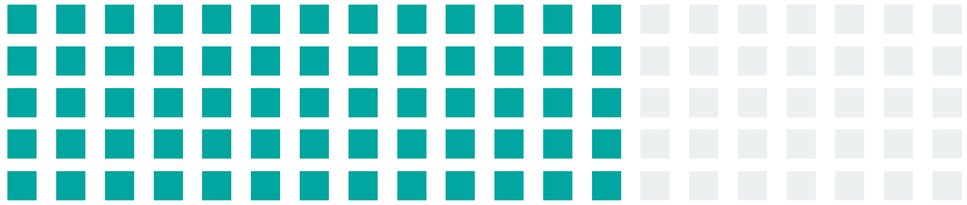
Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals*, November 2024 .
All Enterprise Strategy Group research references and charts in this eBook are from this research report.

Back to Contents

The Cybersecurity Skills Gap

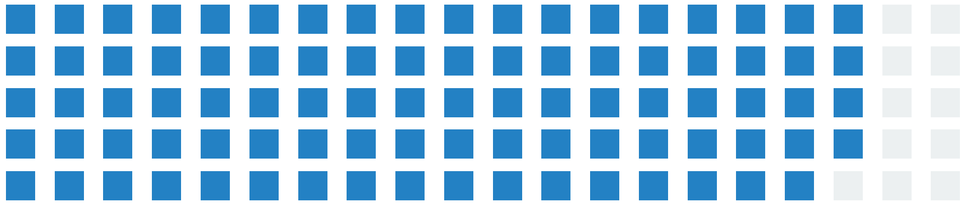
65%

of organizations claimed to be impacted **by the cybersecurity skills shortage.**



89%

said the impact is the same or has gotten **worse over the previous two years.**



Persistent skills shortages have numerous implications **that ultimately increase risks to the business**.

Back to Contents

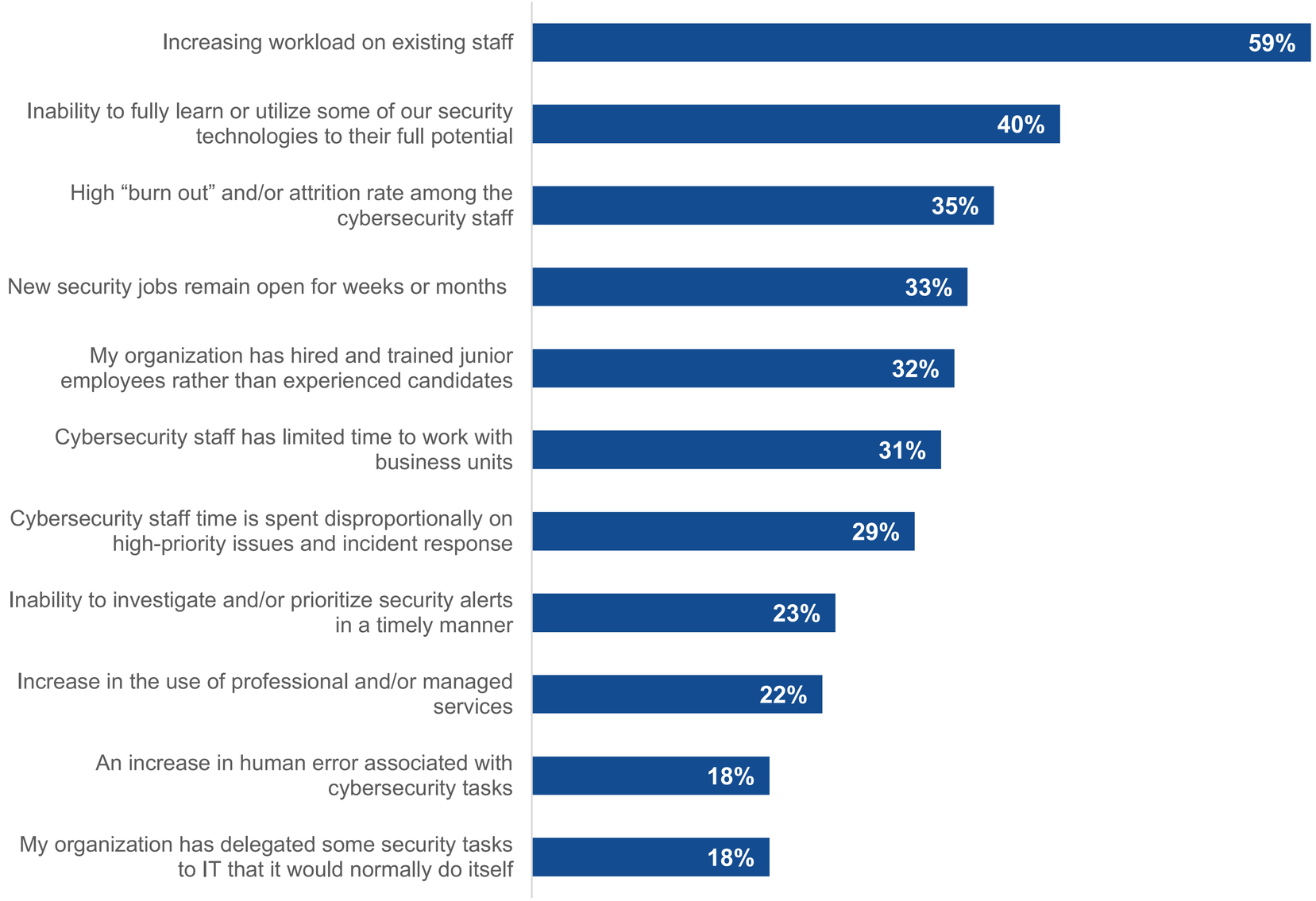
Impacts of the Skills Gap

Of those organizations impacted, 59% said the skills shortage has increased workloads on existing staff, while 40% claimed that the skills shortage has led to an inability to fully learn or utilize some of their security technologies to their full potential.

Other issues include high rates of employee burnout, jobs remaining open for lengthy periods, and the need to hire and train junior—rather than experienced—cybersecurity professionals.

Organizations should be alarmed by this data and consider supplementing technology and staff with services to address these challenges.

What type of impact do you believe the global cybersecurity skills shortage has had on your organization?



Back to Contents

The Need for Effective Security That Supports Scale

It's clear that technology alone can't rectify this situation. When organizations struggle to learn and utilize security technologies to their full potential, it's no surprise that organizations are finding it challenging to maintain their own security operations center (SOC) in the face of rapidly changing technologies and threats, which can lead to gaps in security posture.

Organizations are finding it challenging to hire and retain the experienced cybersecurity professionals needed to fully protect highly complex hybrid and/or multi-cloud environments. An MSSP, such as Foresite, can help close the gap, guiding organizations in the selection and effective operationalization of the right combination of technology and services.

Back to Contents

Chapter 2:

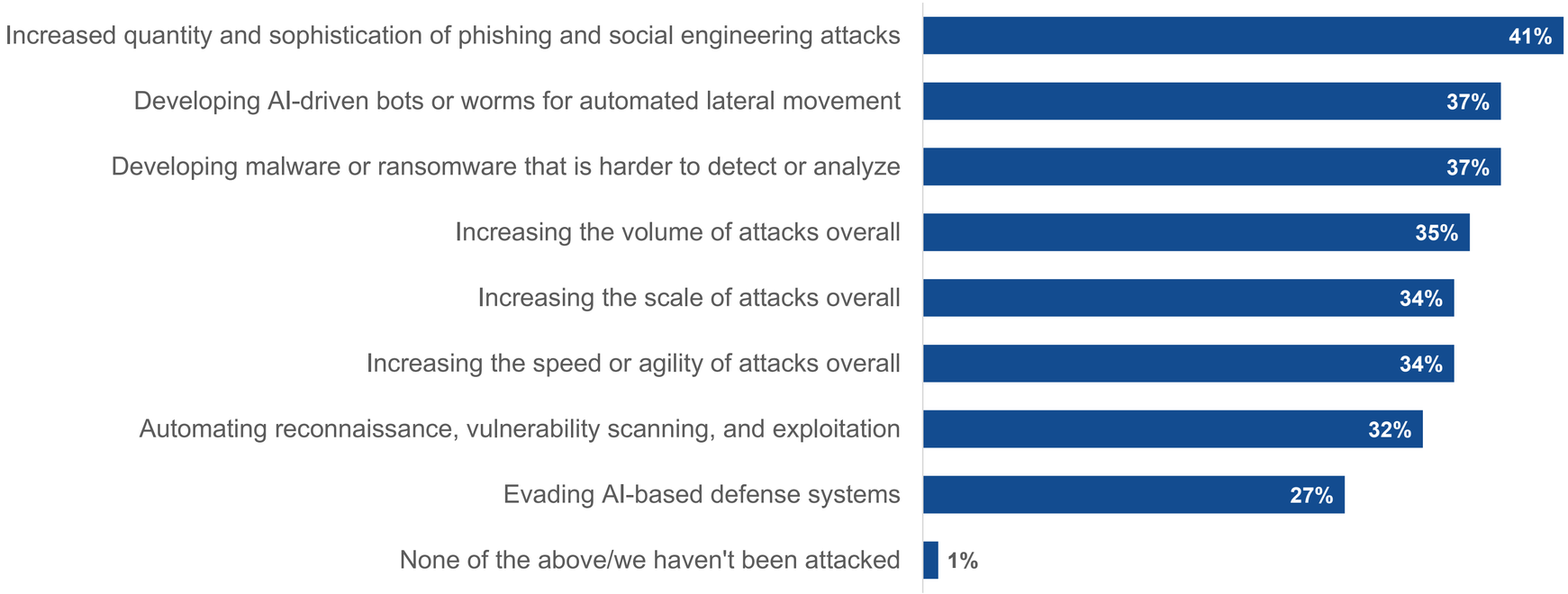
Foresite Catalyst: Bespoke Security Solutions With Google Security Operations

Organizations face a host of challenges in the current modern security environment. According to Enterprise Strategy Group research, 63% of survey respondents believed that security operations are more difficult than they were two years ago. The rise of AI-based attacks has contributed to the increase in security operations challenges. Organizations are seeing AI used in several types of attacks, including phishing and social engineering attacks, advanced worms for lateral movement, and in making malware and ransomware that is harder to detect. As more attackers use AI, organizations must adapt and begin to use AI to defend themselves.

However, if organizations desire to quickly and effectively employ AI to combat advanced attackers, they might need the help of an experienced extension of their team to operationalize AI-enabled security operations using Google Security Operations (SecOps).

Foresite is an MSSP partner that delivers 24/7 security services built with Google SecOps. Google SecOps forms the backbone of Foresite's service, used in conjunction with its vast experience helping to evaluate and improve an organization's security program while providing around-the-clock threat detection and response. Foresite Catalyst is a modularized security program built on Google Cloud. Catalyst aligns these modules with the functions and domains within a SOC, enabling Foresite to create bespoke solutions for any customer and at any level of security maturity.

With respect to end users and their devices, how has your organization observed AI being used by attackers?



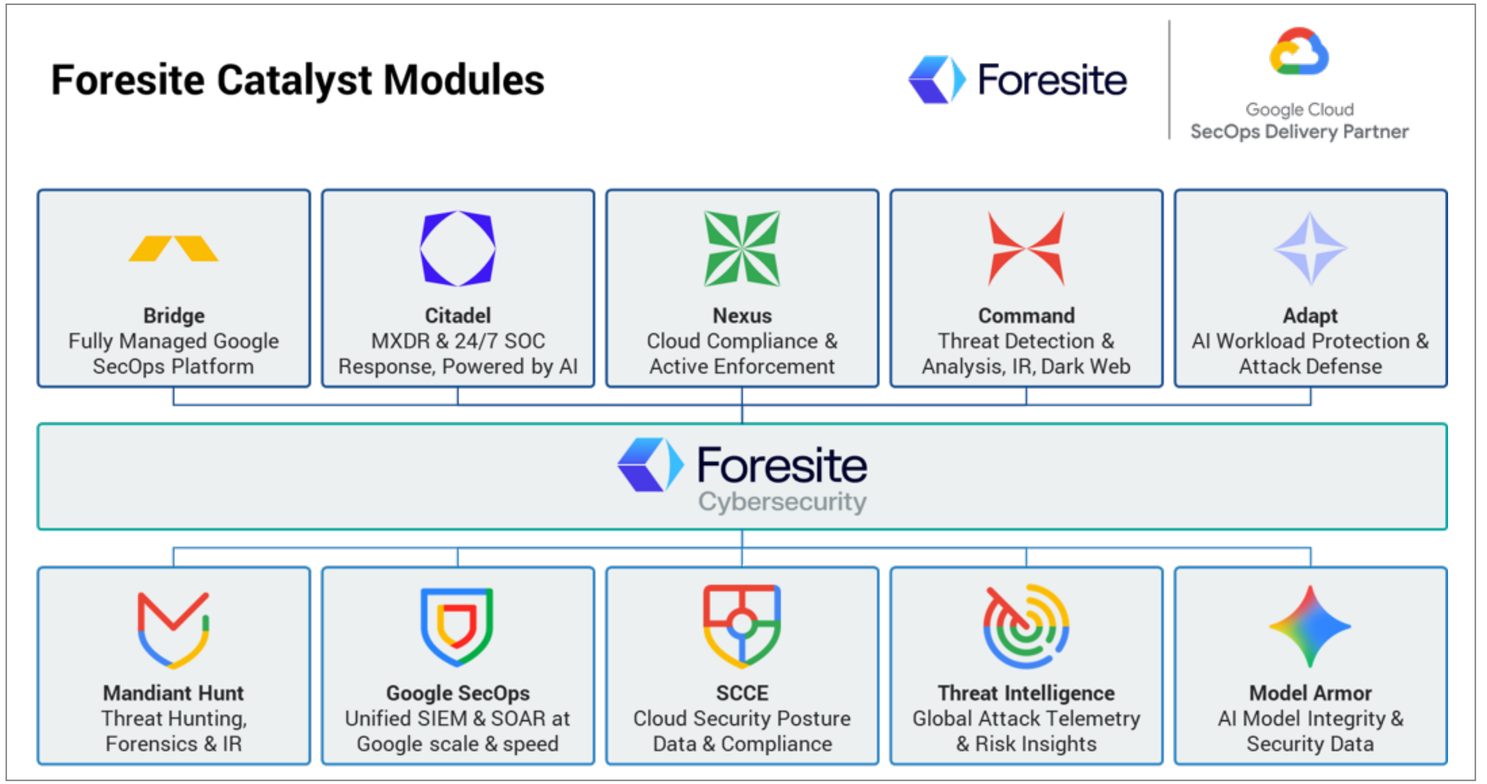
Back to Contents

Foresite Catalyst: Bespoke Security Solutions With Google Security Operations

Foresite Catalyst enables a fast path to security maturity at Google scale and speed. Catalyst arrays to each technical component of the Google Cloud Security technology stack to enable bespoke configurations of people, process, and technology for any organization.

Catalyst integrates Google Cloud technologies such as Google SecOps, Security Command Center Enterprise, and Google Threat Intelligence into a cohesive proactive cyber defense system.

Catalyst Citadel provides complete security coverage with 24/7 monitoring and managed detection and response. Organizations can take advantage of Citadel with the platform management presented in the Bridge offering as the foundation. Citadel provides around-the-clock security monitoring and threat hunting with rapid incident response, leveraging AI-powered detection and automated workflows.



Foresite offers several specialized services to better accommodate clients with different needs. Nexus provides multi-cloud compliance and GRC automation services with Google Cloud's Security Command Center Enterprise. Command provides AI-powered threat intelligence by integrating directly with Google Threat Intelligence to ingest and correlate emerging threat intel feeds. Adapt integrates with Model Armor and Google Cloud AI tools to monitor AI pipelines for malicious inputs and anomalies and enforce model validation and runtime integrity policies.

Back to Contents

Chapter 3:
The Google Cloud MSSP Ecosystem

Google Cloud works with a select group of MSSPs that offer customers the managed security services they need to scale and modernize their SOC functions and ensure end-to-end cybersecurity.

Security is fundamental to everything Google Cloud does. Google Cloud protects billions of end users daily from every service threat, including within Chrome and Gmail. This experience has led to deep and broad security expertise that can benefit Google Cloud's MSSP partners and their customers regardless of their current cloud platform.

Google Cloud layers on security controls to enable MSSPs and their customers to meet their own policy, regulatory, and business objectives. Google's cloud infrastructure doesn't rely on any single technology to make it secure.

MSSP Partner Ecosystem	Infrastructure security	Data protection	Scanning, logging, and monitoring	Configuration, vulnerability and governance, risk management, and compliance	Identity and endpoint protection
Google Cloud Open Solutions	Data Cloud		Modern Infrastructure Cloud		Security Cloud
Google Cloud Core Infrastructure	Hardened, custom-designed hardware and components		Zero-trust applications and services		Highly provisioned, low-latency private global network

Back to Contents

Defense-in-depth Approach to Cloud Security

The Google Cloud stack builds security through progressive layers designed to deliver true defense in depth and at scale. Google Cloud aligns with the needs of MSSPs and helps them deliver better, more capable offerings to their customers:

- Google Cloud hardware infrastructure is designed, built, controlled, secured, and hardened by Google.
- Google Cloud infrastructure—designed from the ground up to be multi-tenant—uses a zero-trust model for applications and services, with multiple mechanisms to establish and maintain trust. This means that only specifically authorized services can run, and only specifically authorized users and processes can access the services.
- Data is automatically encrypted at rest and in transit and is distributed for availability and reliability to help protect against unauthorized access and service interruptions.
- Strong authentication protects access to sensitive data with advanced tools such as phishing-resistant security keys to verify identities, users, and services.
- Google Cloud network and infrastructure have multiple layers of protection that guard customers against denial-of-service attacks.
- At the top of the stack, Google Cloud develops and deploys infrastructure software using rigorous security practices, employing around-the-clock operations teams to detect and respond to threats to the infrastructure from both internal and external threat actors.

The Google MSSP Partner Program

Google Cloud and its MSSP partners recognize that every customer is unique. MSSPs provide various solutions to meet an organization's specific requirements to defend its data, applications, and users, combining Google Cloud's security technology with human expertise and experience to provide the right solution for organizations' diverse needs.

Visibility

Detection

Context

Assisted Response

Back to Contents

Keys to Efficient and Effective Security With MSSPs

There are several key areas where Google Cloud offers differentiated technology and services for MSSPs and their customers.

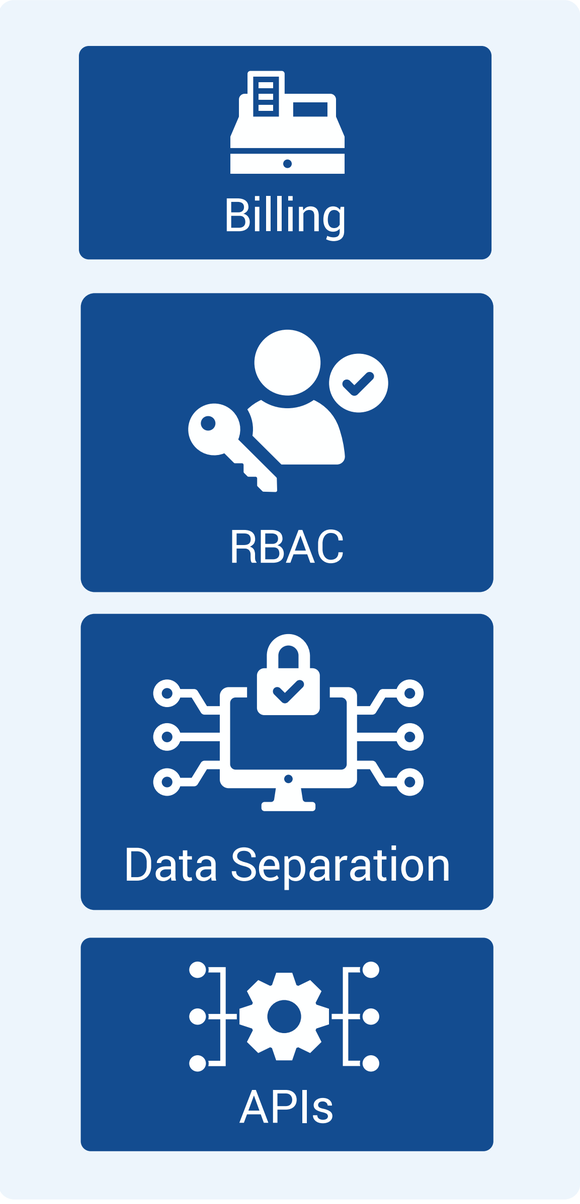
- **Robust and secure multi-tenancy.** Google Cloud's approach provides robust multi-tenancy for MSSPs and their clients.

  - **Billing.** Google Cloud simplifies how MSSPs bill each of their clients individually for precisely the services they are using.

  - **Role-based access control (RBAC).** MSSPs can provide granular access to specific roles to both their SOC support personnel and to their clients. A strict separation of duties is applied to SOC analysts and client team members; access to client information is restricted based on roles and responsibilities.

  - **Data separation.** While Google Cloud leverages all ingested data to identify and respond to threats, data access and visibility is strictly controlled so that each MSSP and each of its clients can only access the data that is appropriate to them. Every client's data is air-gapped from other clients to ensure complete isolation and prevent unauthorized access or cross-contamination.

  - **Partner management APIs.** These APIs enable MSSPs to provision and manage distributed instances for multiple customers.



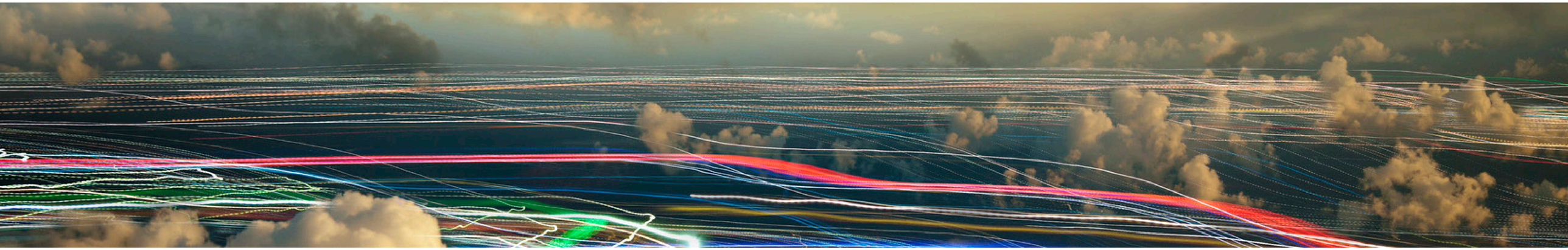
Back to Contents

Keys to Efficient and Effective Security With MSSPs (Continued)

- **Ingestion.** Google Cloud leverages the scale and speed of zero day and fully manages data ingest end to end, providing cost-effective efficiency and the ability to query across all data. Security Operations retains hot data for 12 months by default, with the option to extend retention.

- **Resourcing.** Google's MSSP partners tell them that Google Cloud makes their SOC analysts more effective and efficient with quicker time to mitigation/ resolution and supports cost-effective implementation with fewer administrators.

- **Threat Intelligence.** Google's broad and deep visibility into the internet, protecting billions of devices and mailboxes, combined with Mandiant's frontline incident response expertise and the global reach of the VirusTotal community, is infused into Google Threat Intelligence. By understanding the threat actors' tactics, techniques, and procedures, security teams can take a more proactive approach to security with strategic planning and informed prioritization. Google Threat Intelligence helps security teams stay ahead of threats by focusing on those that are most relevant to them and enabling them to respond quickly when needed. The entire corpus of VirusTotal metadata is available for use as threat detection, giving MSSPs access to petabytes of threat data. This enables more than just automation of complex analyst activities like escalation decisions. Google Threat Intelligence enables behavioral detection with metrics like prevalences on activity to help organizations move beyond signature-based detection. This enables detection and quick action to neutralize fileless and zero-day attacks.



Back to Contents

Keys to Efficient and Effective Security With MSSPs (Continued)

- **AI.** AI empowers SOC personnel to operate at a more sophisticated level by augmenting their capabilities in threat detection and response. Gemini in Security Operations enables analysts to use natural language queries, summarize and cluster alerts to reduce alert fatigue, and automate complex tasks such as threat hunting and playbook creation.

  - Google Cloud is the only company Enterprise Strategy Group has evaluated that is implementing generative AI across the full stack, from the infrastructure through the foundation model, to the applications. Google Cloud's large language model for security is fine-tuned on its own security data set. This gives Google Cloud complete control over what goes into the training data, unlike other companies that are using public models such as OpenAI. This, combined with the deep integration into Google Cloud's applications, enhances both the quality and capabilities that Google Cloud can provide.

  - Organizations can leverage pre-trained models accessed via APIs and low-code custom training to solve real-world problems quickly with integrated analytics and an AI platform, BigQuery ML. Machine learning (ML) model development and experimentation is fast-tracked with Vertex AI, Google Cloud's end-to-end ML platform.

  - AI can be leveraged to automate grouping of alerts in the SIEM to reduce noise and consolidate the view of threats in the top-level view for analysts in the security orchestration, automation, and response platform while amplifying analysts' actions via automated response.

Back to Contents

Foresite Catalyst: Bespoke Security Solutions With Google Security Operations – Why It Matters

Google Cloud provides world-class security tools, but turning them into consistent, 24/7 outcomes can be complex and time-consuming. Most organizations struggle with integration, hiring expert staff, and alert fatigue. Foresite empowers enterprises with tactics, techniques, and procedures honed through years of real-world defense experience using Google Cloud security.

Foresite uses Google SecOps to defend itself and its clients with a keen focus on using the best of Google Cloud security to provide complete security coverage against known and unknown threats.

Foresite is a Google Cloud Premier Partner with Security Services Specialization and deep Google SecOps Delivery expertise. Foresite's people, practices, and AI-enabled tools help clients make the best use of Google's security tool set; execute an agile, automated threat management process; and reduce response time from hours to seconds. Foresite meets clients where they are and helps them accelerate their security journey to deliver Google-native security at speed and scale. Foresite transforms Google Cloud infrastructure into an actionable, always-on defense, helping organizations grow their security team's maturity while protecting valuable assets.

Foresite

LEARN MORE

Back to Contents

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.