Enterprise Strategy Group™ by TechTarget

Secure Cloud Adoption to Enable Business Growth

Leveraging the Google Cloud Platform, Its Partner Ecosystem, and Fortinet FortiXDR for Secure Digital Transformation

Melinda Marks, Practice Director, Cybersecurity

AUGUST 2024

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

TABLE OF **CONTENTS**

CLICK TO FOLLOW

INTRODUCTION

PAGE 3

CHAPTER 1:

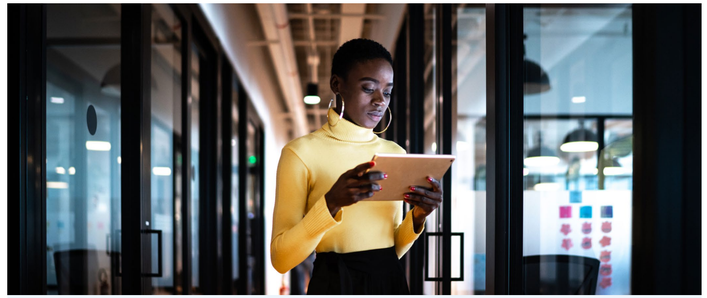
Security Challenges With Digital Transformation

PAGE 4

CHAPTER 2:

Modernizing Security With Google Cloud

PAGE 10



CHAPTER 3:

Optimizing Security Control With Google Cloud Partners

PAGE 16

Introduction

Organizations are using state-of-the-art cloud services to digitally transform their businesses and optimize productivity and innovation. These services enable them to efficiently use their resources and staff for faster software development cycles, giving them a competitive advantage and driving better business results.

However, as cloud services enable organizations to scale to efficiently deliver applications and services to customers, partners, and employees, security teams need to ensure they can protect their business-critical applications across cloud environments. They need effective solutions in place to meet the challenges of faster development cycles, the dynamic and ephemeral nature of cloud workloads and their associated resources, the expanding attack surface, and a rapidly evolving threat landscape.

This eBook explores how to modernize security for digital transformation using the rich capabilities of Google Cloud and its ecosystem of partners. Modernizing security in this way enables organizations to effectively build their security strategies to protect their software applications and drive business growth with greater security, agility, and resilience, while achieving cost savings.

BACK TO CONTENTS

CHAPTER 1:

Security Challenges With Digital Transformation

Organizations are under pressure to increase productivity and drive innovation to best serve their customers.

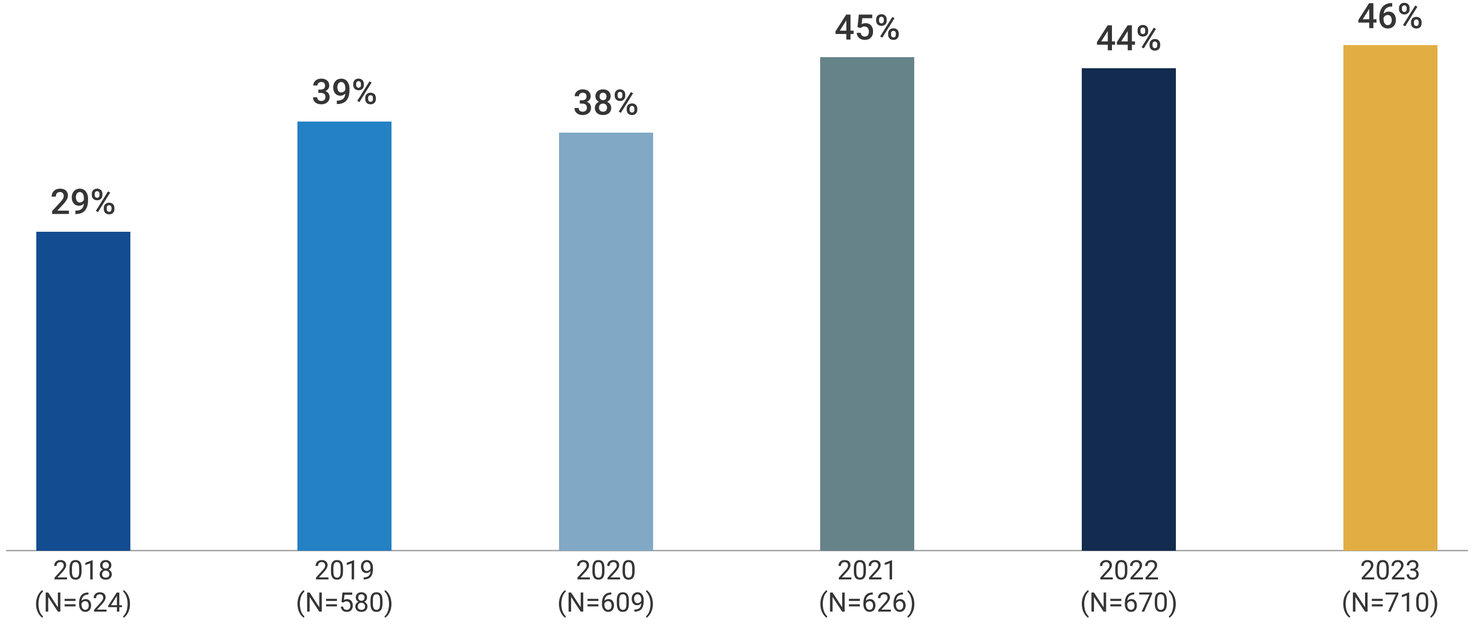
To meet the demand and gain a competitive advantage, organizations are leveraging cloud service providers (CSPs) for their state-of-the-art platforms. This enables organizations to efficiently develop and deploy their applications to the cloud, making them available to better serve their employees, partners, and customers.

Organizations don't have to worry about the underlying infrastructure or maintenance, while benefiting from economies of scale with pay-as-you-go models.

86%

of organizations **run production workloads** in public cloud infrastructure/platforms.

Organizations are increasingly adopting a cloud-first policy



Cloud-first policy, i.e., we deploy a new application using public cloud services unless someone makes a compelling case to deploy it using on-premises resources

BACK TO CONTENTS

Scaling Development With Optimized Efficiency

Cloud services enable teams to modernize their application development processes for greater operational efficiency. This helps them meet their digital transformation objectives, which include operational efficiency, improved product development, and better customer experiences. As a result, organizations report greater efficiency in development processes with faster releases and better collaboration.

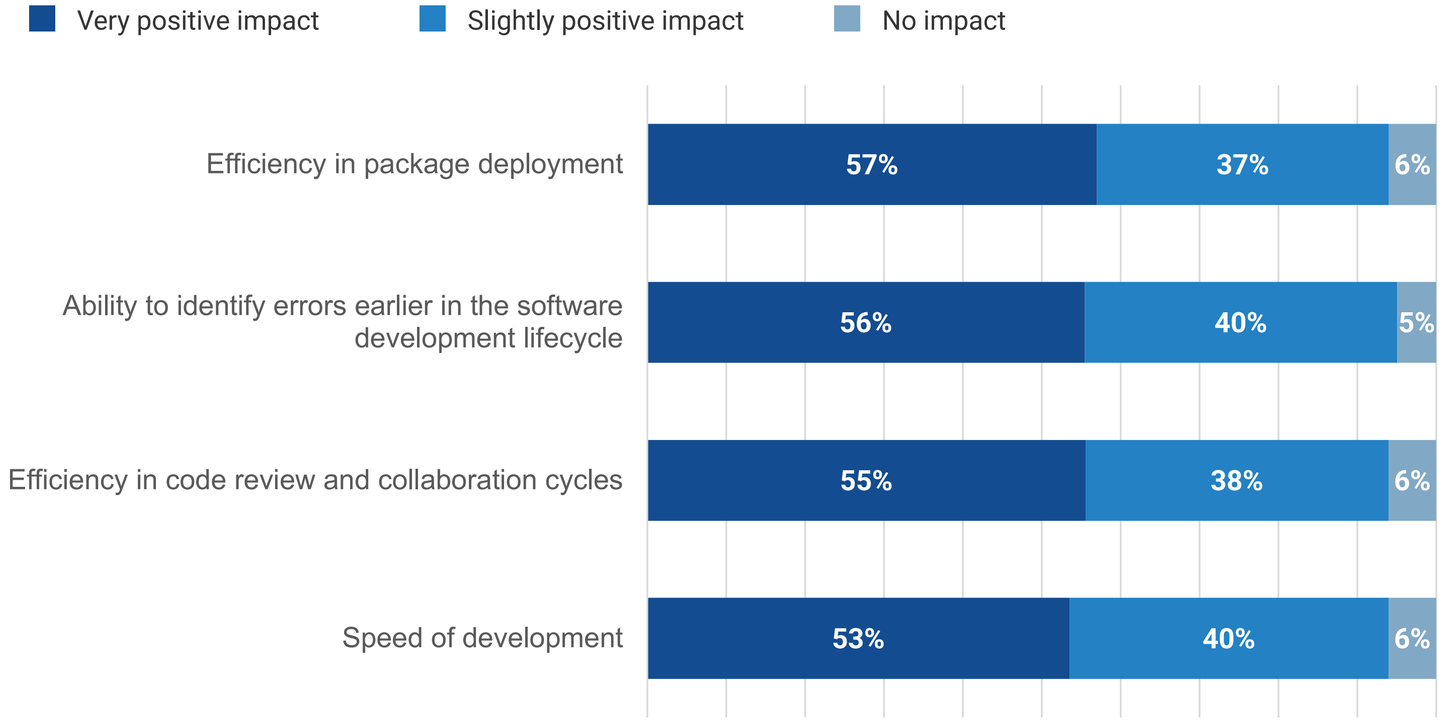
Top 3 digital transformation objectives

54%
Become more operationally efficient

47%
Develop new data-centric products and services

45%
Provide better and more differentiated customer experience

Impacts of cloud-native application development



BACK TO CONTENTS

The Need for Security That Supports Scale

Before the availability of cloud services, security programs were aligned with infrastructure provisioning processes. An application developer would file a ticket, wait for someone from the IT or operations teams to provision a server, work to release software, and then issue updates over periods of months or even yearly. For security teams, it was a matter of running vulnerability scans and impact assessments at set points along the development process, as well as ensuring the physical security of the data center.

Top 5 challenges for cloud-native applications

34%
Security

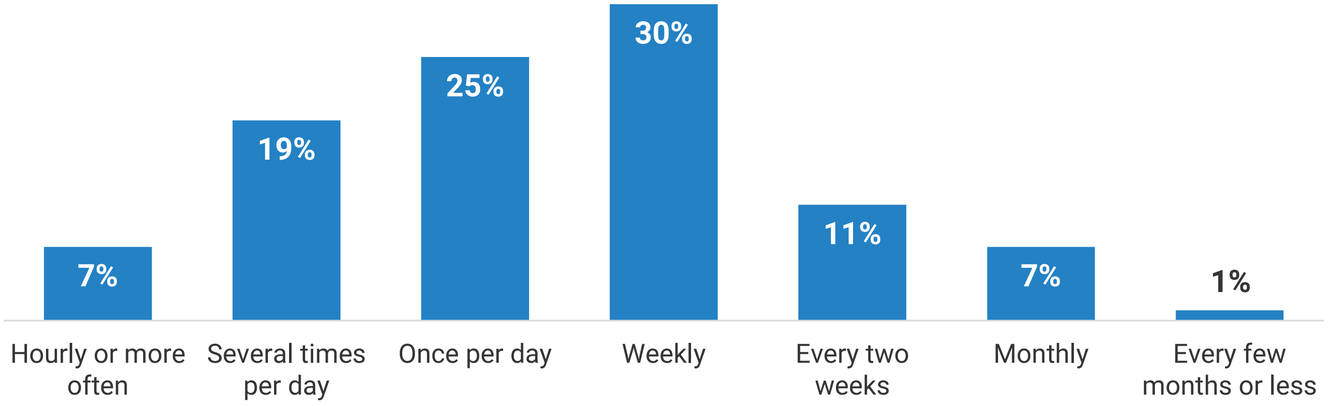
30%
Meeting and maintaining compliance requirements

29%
Lack of performance monitoring/observability

29%
Services purchased outside the purview of IT or other authorized decision makers

27%
Retaining full-featured functionality and capabilities

Frequency of new code releases



Today, by leveraging cloud services and cloud-native development processes, developers are empowered to provision their own infrastructure, build their applications, and deploy the applications to the cloud using continuous integration and continuous deployment pipelines for rapid software releases and updates. Although the CSP takes care of securing the platform, security teams are challenged keeping up with the speed of cloud-native development. Most organizations are deploying new code to production on a daily basis. As a result, the top challenges for cloud-native applications are security and maintaining compliance.

BACK TO CONTENTS

The Complexity of the Cloud Threat Landscape

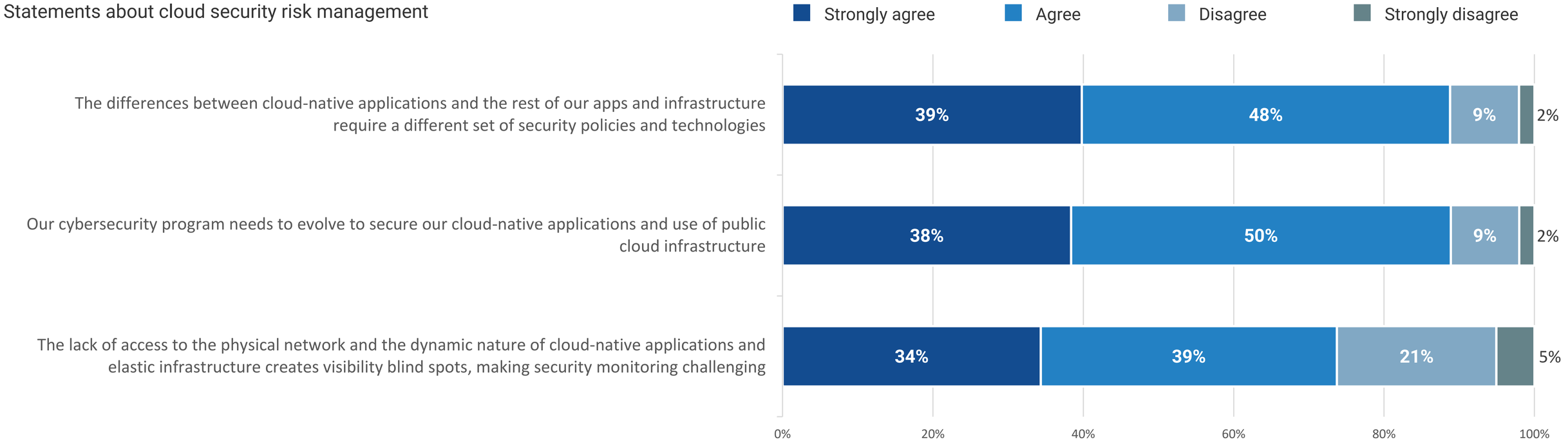
In addition to keeping up with the faster speed of development, organizations are challenged with the fact that the threat landscape in the cloud is more complex. Developers can easily deploy their applications to the cloud to make them available to users, but that means more exposure with access through the internet.

Microservices architectures mean that applications are using dynamic and ephemeral infrastructure and resources that are being spun up and spun down. The evolving attack surface cannot be controlled by setting up a perimeter. Also, each cloud provider implements services differently, creating uniqueness in the attack surface and threat exposure.

88%

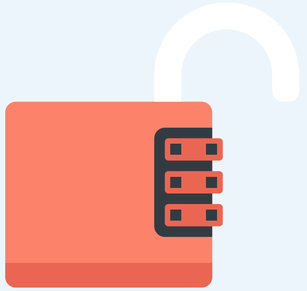
of respondents believe their cybersecurity program needs to evolve to secure their cloud-native applications and use of public infrastructure.

Statements about cloud security risk management



 Source: Enterprise Strategy Group Research Report, The Maturation of Cloud-native Security, May 2021.

BACK TO CONTENTS



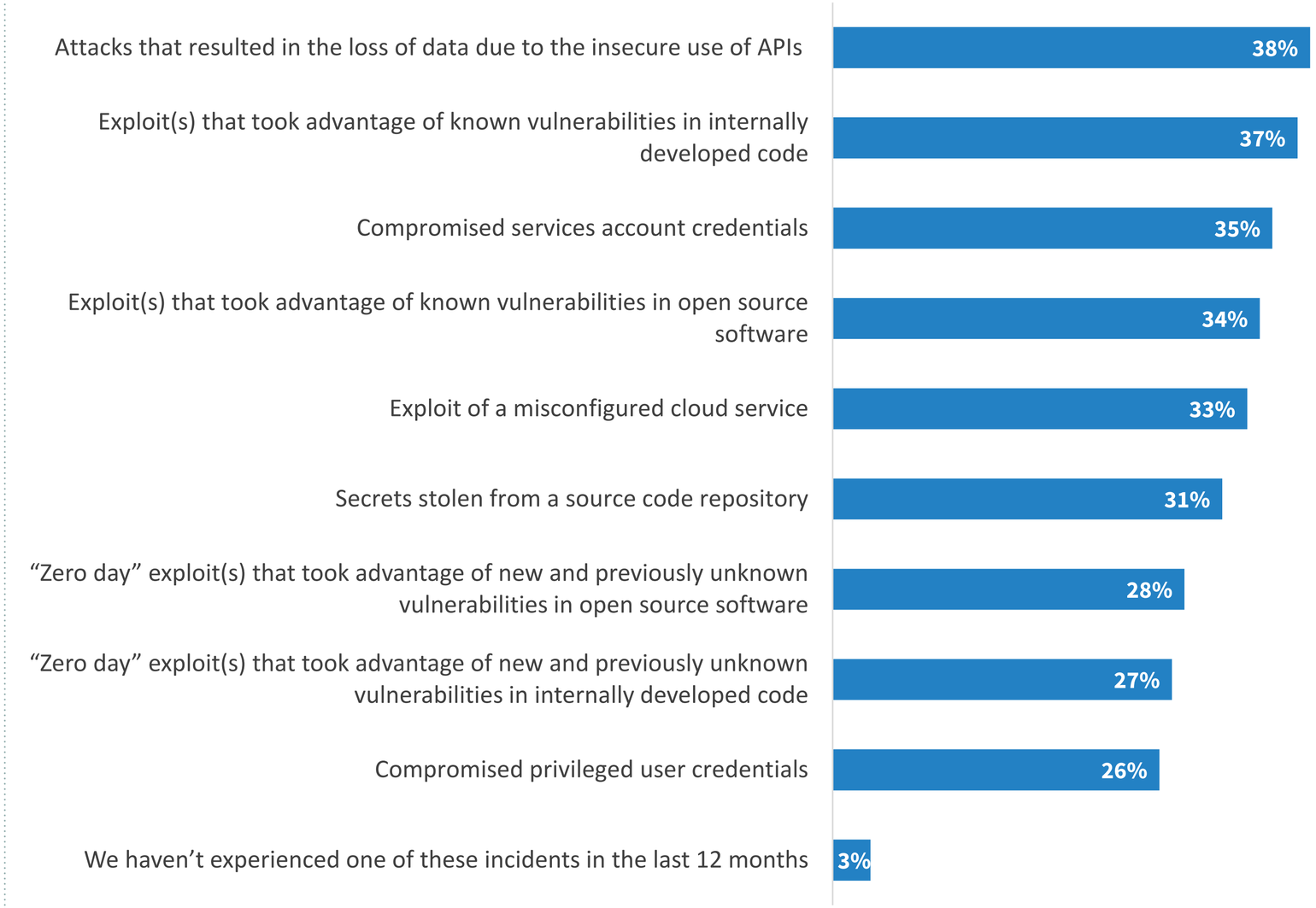
97%

of organizations **experienced security incidents** with their cloud-native applications in the past year.

Security Incidents in Cloud Environments

Organizations have faced a wide range of attacks on their cloud applications, making it clear that they need to take steps to reduce their security risk. Many of the incidents are caused by mistakes or coding issues, such as insecure usage of APIs, exploits taking advantage of vulnerabilities, access issues, and misconfigurations, which are preventable with the right security processes and policies in place.

Cybersecurity incidents on cloud-native applications and infrastructure



 Source: Enterprise Strategy Group Research Report, Walking the Line: Shift Left and GitOps Security, November 2022.

BACK TO CONTENTS

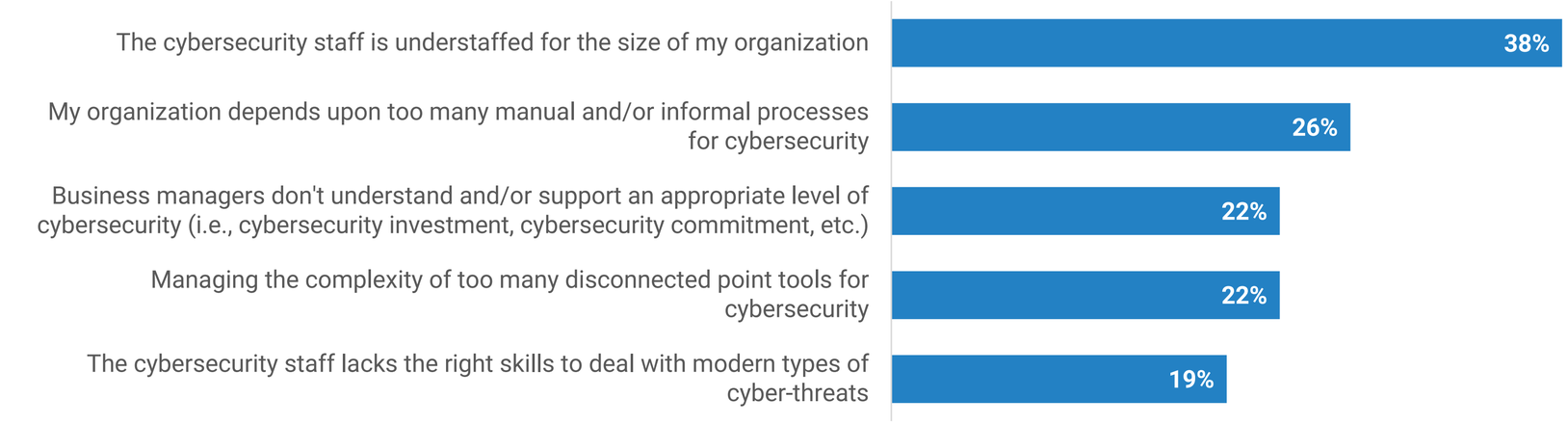
The Need for Effective, Efficient Security

Security teams face challenges ensuring that their teams can scale to support digital transformation. They face cloud security skills gaps and are often understaffed. They need the right tools in place to help them scale—tools that reduce manual, tedious tasks so they can focus on higher value work.

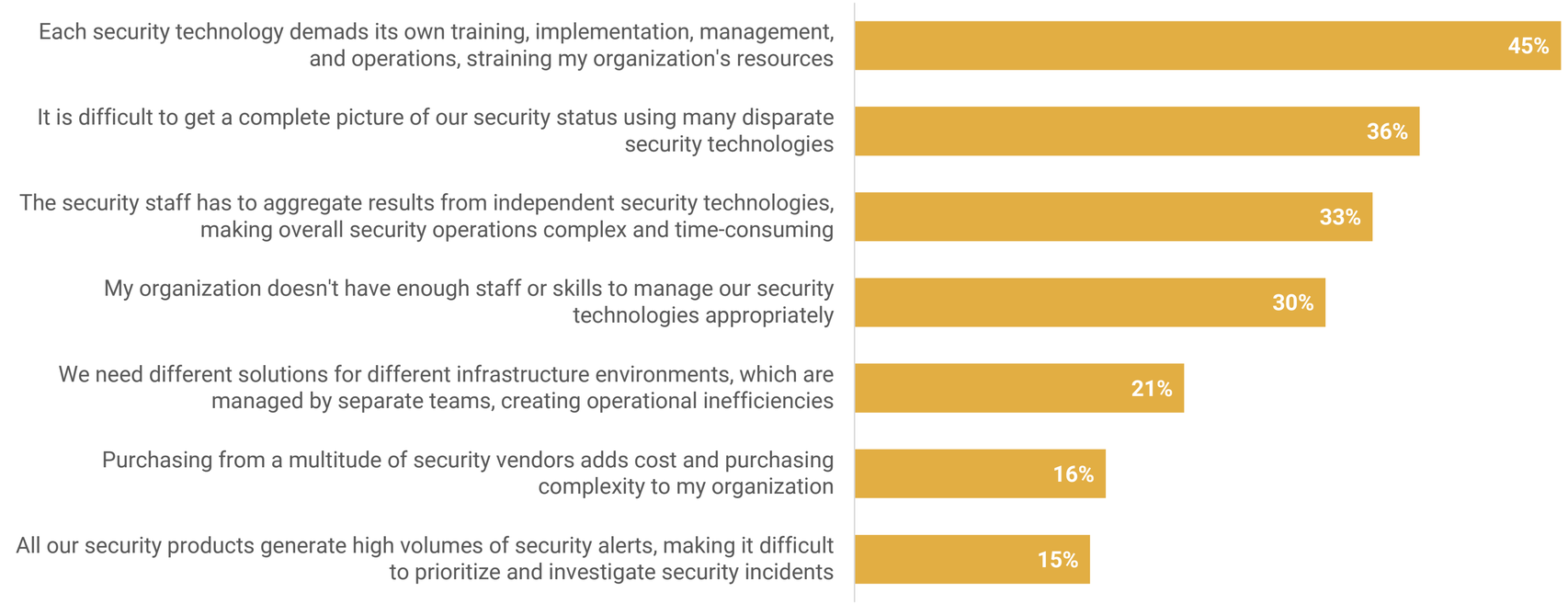
They also face challenges with their usage of multiple security tools from different vendors. Research from TechTarget's Enterprise Strategy Group shows that 70% of organizations use more than 10 application security tools, with 58% using tools from more than five vendors. Each solution takes time to deploy and manage. The solutions are siloed and often built differently and in different languages, creating more work with separate alerts and requiring time to aggregate findings.

Organizations need consolidated solutions that provide context to drive efficient actions that are impactful in reducing risk to help them stay ahead of attacks.

Top 5 cybersecurity challenges



Challenges managing multiple security products from different vendors



 Source: ESG Complete Survey Results: ESG/ISSA Cybersecurity Process and Technology Survey

BACK TO CONTENTS

CHAPTER 2:

Modernizing Security With Google Cloud

It is important to understand and leverage CSP-native security features and offerings, especially as many features are built into the cloud architecture in ways that provide security benefits without performance or efficiency impacts.

CSPs operate with shared responsibility models for security, delineating that they are responsible for securing the underlying infrastructure security while the customer is responsible for securing the workloads they move into the cloud. CSPs also offer extra features and services to help customers secure their workloads because of the importance of security to their customers.

Google Cloud helps customers protect their workloads, going one step further with its “shared fate” approach. This breaks down the delineation in the shared responsibility model to enable CSPs to serve as active partners and fully support customers to secure their cloud workloads so they can deploy securely on Google Cloud.

Google Cloud Shared Fate Model

BACK TO CONTENTS

Defense-in-depth Approach to Cloud Security

Google Cloud is designed, built, and operated with security as a primary design principle to help protect its customers against threats in their environments. Securing more than three billion users globally, Google's cloud infrastructure stack builds security through progressive layers designed to deliver true defense in depth and at scale.

Google Cloud's hardware infrastructure is designed, built, controlled, secured, and hardened by Google.

Google Cloud's 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.

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 like phishing-resistant security keys to verify identities, users, and services.

The multiple layers of protection that Google's network and infrastructure provide to guard customers against denial-of-service attacks and communications over the internet to its public cloud services are encrypted in transit.

At the top of the stack, Google 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.

BACK TO CONTENTS

Secure Foundation on Google Cloud Hardware Infrastructure

Google Cloud hardware infrastructure is custom-designed by Google to precisely meet stringent requirements, including security. Its servers are custom-built and don't include unnecessary components that can introduce vulnerabilities. The same philosophy is imbued in Google's approach to software, including low-level software and its operating system, which is a stripped-down, hardened version of Linux.

Google designs and includes hardware specifically for security. For example, Titan, its custom security chip, is purpose-built to establish a hardware root of trust in its servers and peripherals. Google also builds its own network hardware and software to optimize performance and security. Finally, Google's custom data center designs include multiple layers of physical and logical protection.

Owning the full stack enables Google to control the underpinnings of its security posture with far greater precision than is possible with third-party products and designs. Google can take steps immediately to develop and roll out fixes for vulnerabilities without waiting for another vendor to issue a patch or other remediation, greatly reducing exposure for Google and its customers.

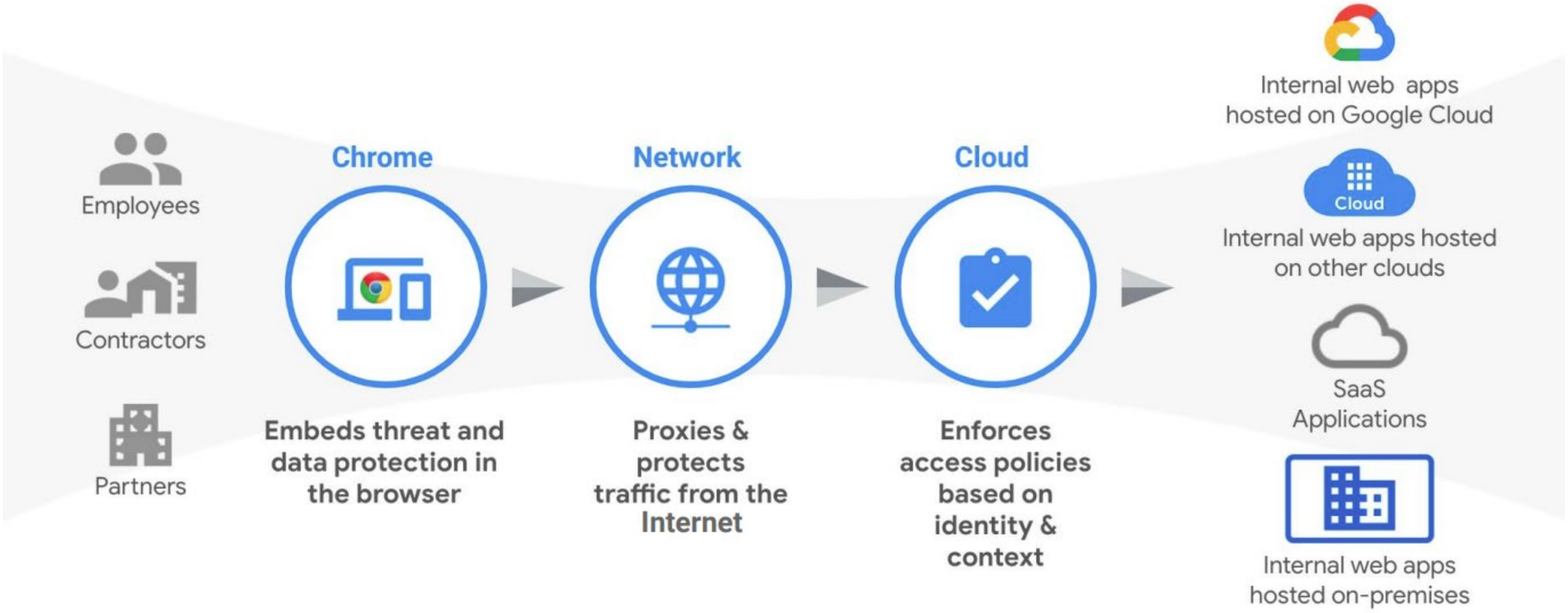
BACK TO CONTENTS

Enabling Zero Trust to Protect Applications

Organizations are challenged adapting their security strategies to the cloud because a perimeter defense does not work for applications deployed to the cloud. In the cloud, a zero trust approach is needed to protect applications by ensuring that all users, whether inside or outside the organization's network, are authenticated, authorized, and continuously validated.

Google was an early proponent, designer, and practitioner of zero trust computing, developing the concepts that underpin zero trust architectures with its BeyondCorp and BeyondProd models. Operating this way has helped to protect its internal operations over the last decade. Google's zero trust architecture ensures that only the individual with the correct identity is able to access only the machines specifically authorized by the correct code and only the data they are authorized to access, in the correct context. BeyondProd uses these core principles to enable partners and Google Cloud customers to protect their operations in the same way.

Google Cloud Beyond Corp Enterprise



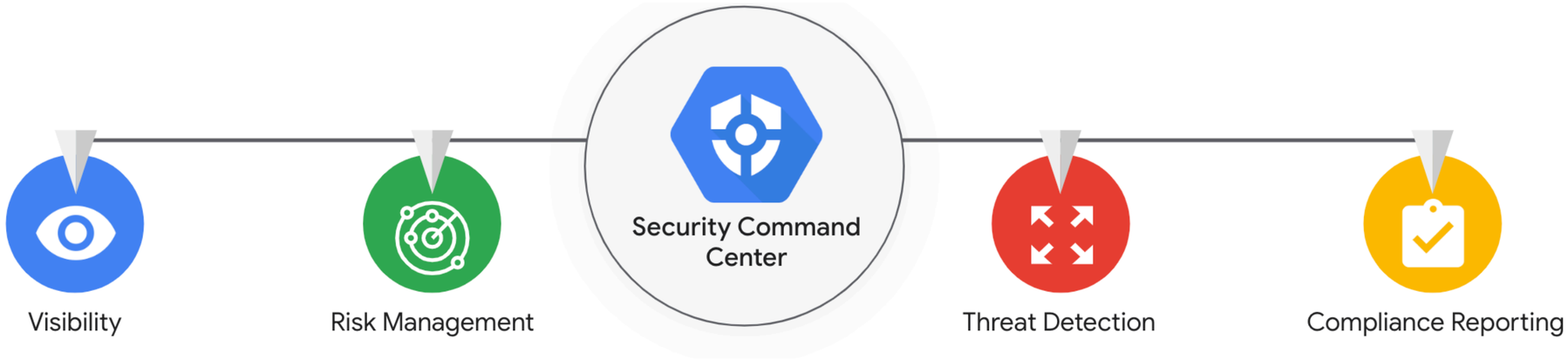
BACK TO CONTENTS

Centralized Visibility and Control

In order to scale with the speed of cloud-native development, security teams need full visibility of their assets, as well as control to implement the needed security processes and policies to effectively manage security risk. They need the right solutions to help them prioritize taking the right actions that reduce their risk and exposure to attacks.

The Google Cloud Security Command Center provides:

- A complete view into Google Cloud resources and their policies.
- Notifications about findings associated with critical assets.
- Near-real-time visibility into any changes in asset history.
- Risk scores and attack path simulation for prioritizing needed remediation actions.

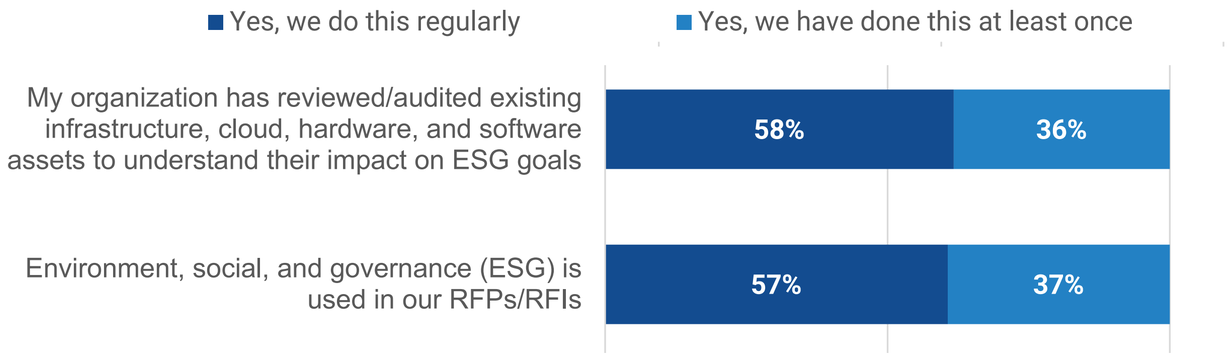


BACK TO CONTENTS

The Sustainability Advantage

Enterprise Strategy Group research shows the importance of environmental, social, and governance (ESG) initiatives for technology adoption and resilience. Google Cloud helps organizations build and work sustainably, operating the cleanest cloud in the industry, with data centers that are twice as energy efficient as a typical enterprise data center, helping customers reduce their IT-related carbon footprints.

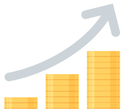
The importance of ESG in evaluating technologies



Areas impacted by ESG goals

Top 5 benefits of ESG

46%
Improved brand development



41%
Increased profitability

40%
Improved staff retention

39%
Compliance with government mandates

35%
Increased goodwill

Google also matches 100% of the electricity that powers cloud workloads with renewable energy to mitigate the annual operational carbon footprint of its customers' digital applications and infrastructure.

It also provides insights to increase climate resilience with Earth Engine, BigQuery, Maps, and Google Cloud compute and AI tools that predict climate risk, increase supply chain visibility, and help organizations source materials responsibly.

BACK TO CONTENTS

CHAPTER 3:

Optimizing Security Control With Google Cloud Partners

With the portability of modern software components, organizations typically utilize platform services from multiple CSPs, often with a mix of applications in private data centers as well as public clouds.

This presents a market opportunity for cybersecurity independent software vendors (ISVs) to develop and deliver solutions to help customers efficiently manage risk and protect their business applications with the move to the cloud.

Google Cloud works closely with security ISVs to provide integrated solutions to optimize security control, helping customers meet stringent security, sovereignty, and compliance needs.

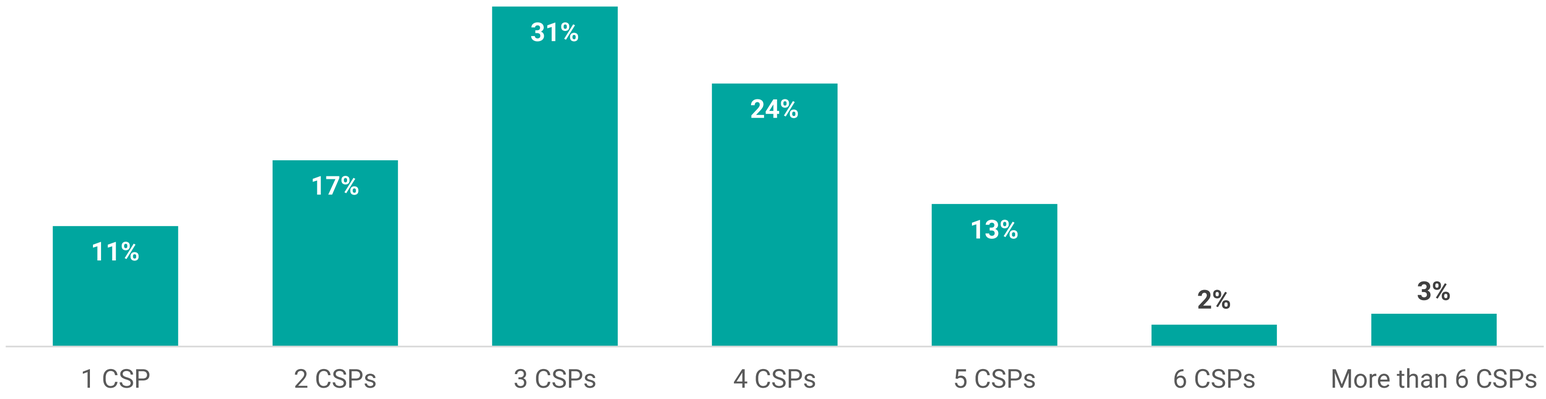
Application portability provides deployment flexibility

14% Our cloud-native applications are/will be deployed in a **public cloud environment** only (including edge locations)

25% Our cloud-native applications are/will be deployed in an **on-premises data center or co-location** facility managed by our organization only

30% Our cloud-native applications are/will be deployed **in a combination of public cloud platforms (including edge locations) and private data centers**

Organizations most often use multiple CSPs



BACK TO CONTENTS

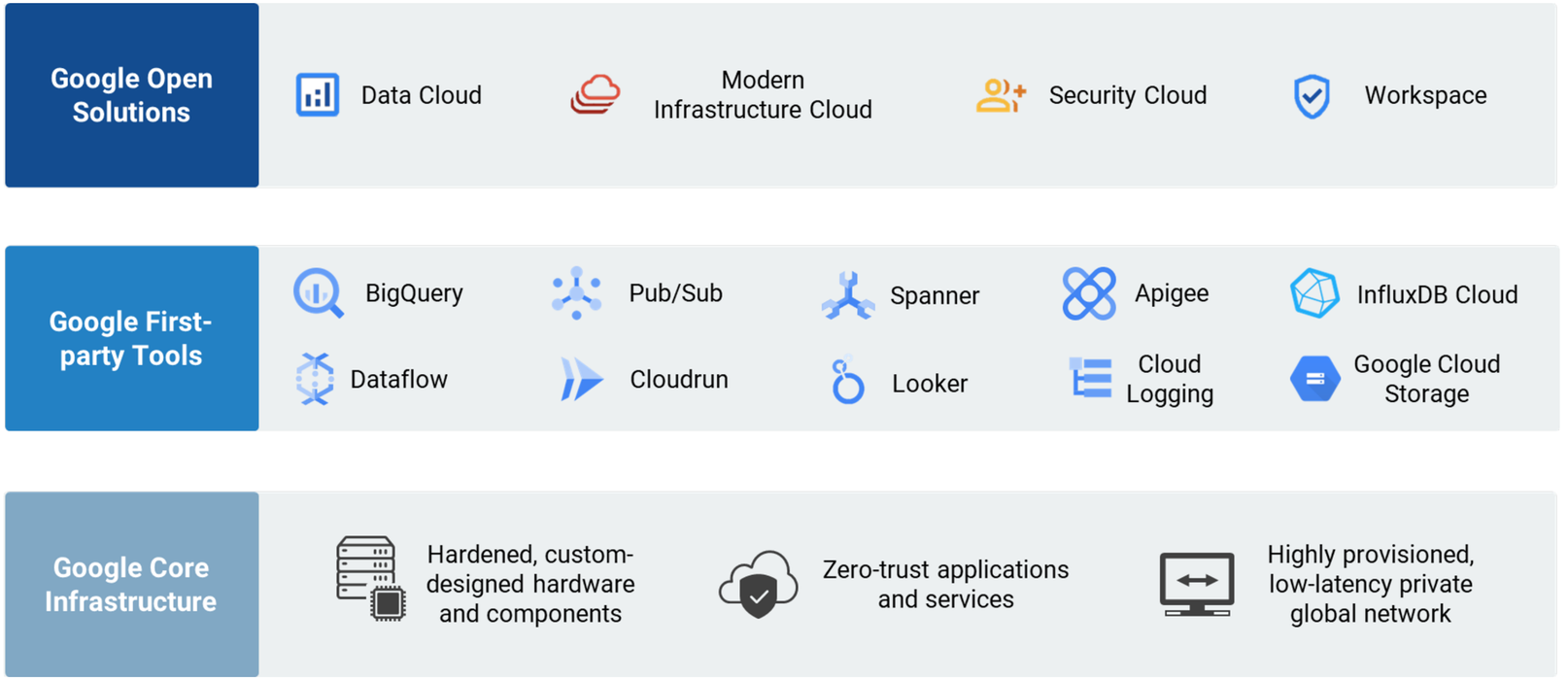
The Google Security Ecosystem

Google aligns with the needs of security ISVs to help them deliver better, more capable offerings faster. It offers economies of scale, software-defined infrastructure, simplicity, automation, and global-reach help. ISVs accelerate time to market and optimize delivery of new products, enhancements, and updates.

Google Cloud provides tools and technologies for partners to fully leverage the elements from its secure foundation, eliminating the need for ISVs to build duplicate security features so they can focus on augmenting their capabilities.

Google Cloud provides tools and technologies for its partners—which they traditionally had to build in house—to augment their capabilities. The Security Ecosystem uses Google Cloud capabilities to provide trusted security in the cloud, on premises, at the edge, and everywhere in between.

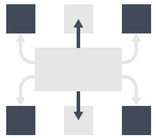
Google Cloud Ecosystem Overview



BACK TO CONTENTS

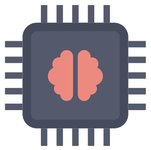
Unified, Open Intelligent Data Cloud Platform

Google's Data Cloud enables organizations to digitally transform with a unified, open, and intelligent data cloud platform.



Data Cloud enables organizations to manage every stage of the data lifecycle, including databases, business intelligence, data warehouses, data lakes, and streaming on a unified data platform.

Data Cloud is open and standards-based for portability and flexibility with an extensive partner ecosystem, designed for multi-cloud environments.



Data Cloud incorporates built-in intelligence and AI/ML, with comprehensive tools and processes. Organizations can leverage pre-trained models accessed via APIs and low-code custom training and solve real-world problems quickly with integrated analytics and an AI platform, BigQuery ML. ML model development and experimentation is fast-tracked with Vertex AI, an end-to-end ML platform.

Security AI Workbench provides generative AI for security solutions. Security AI Workbench is a platform that enables security partners to extend generative AI to their products, bringing threat intelligence, workflows, and other critical functionality to customers, while retaining enterprise-grade data protection and sovereignty.

BACK TO CONTENTS

Modern Infrastructure Cloud Platform

Google's Modern Infrastructure Cloud gives partners and customers the freedom to securely innovate and scale across data centers, edge locations, and the cloud on a transformative, open platform designed to be easy:

- Google has a long history of leadership in open source, including projects like Kubernetes, TensorFlow, and others. Open source gives organizations the flexibility to deploy—and, if necessary, migrate—critical workloads across or off, public cloud platforms.
- Google Modern Infrastructure Cloud gives organizations the flexibility to build and run apps anywhere. Anthos, the modern application platform that extends Google Cloud services and engineering practices to hybrid and multi-cloud environments, delivers portability that helps teams modernize apps faster and establish operational consistency across them.
- Modern Infrastructure Cloud provides autonomy and control over infrastructure and data, enabling organizations to manage all their apps—both legacy and cloud-native—while meeting sovereignty, regulatory, and policy requirements.

BACK TO CONTENTS

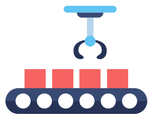
Security Cloud With Data Protection

Data protection is core to everything Google does. Security Cloud helps partners and customers protect what's important with advanced security tools:

The Google Cybersecurity Action Team is Google's security advisory team. Its singular mission is to support the security and digital transformation of governments, critical infrastructure, enterprises, and small businesses.

Google BeyondProd helps create trust between microservices—beyond what is possible with traditional network perimeter protections like firewalls—using characteristics such as code provenance, service identities, and trusted hardware. This trust extends to software that runs in Google Cloud and software that Google Cloud customers deploy and access.

Google has produced numerous foundational innovations. Google invented now-standard technologies, such as Kubernetes, and was an early proponent, designer, and practitioner of zero-trust computing.



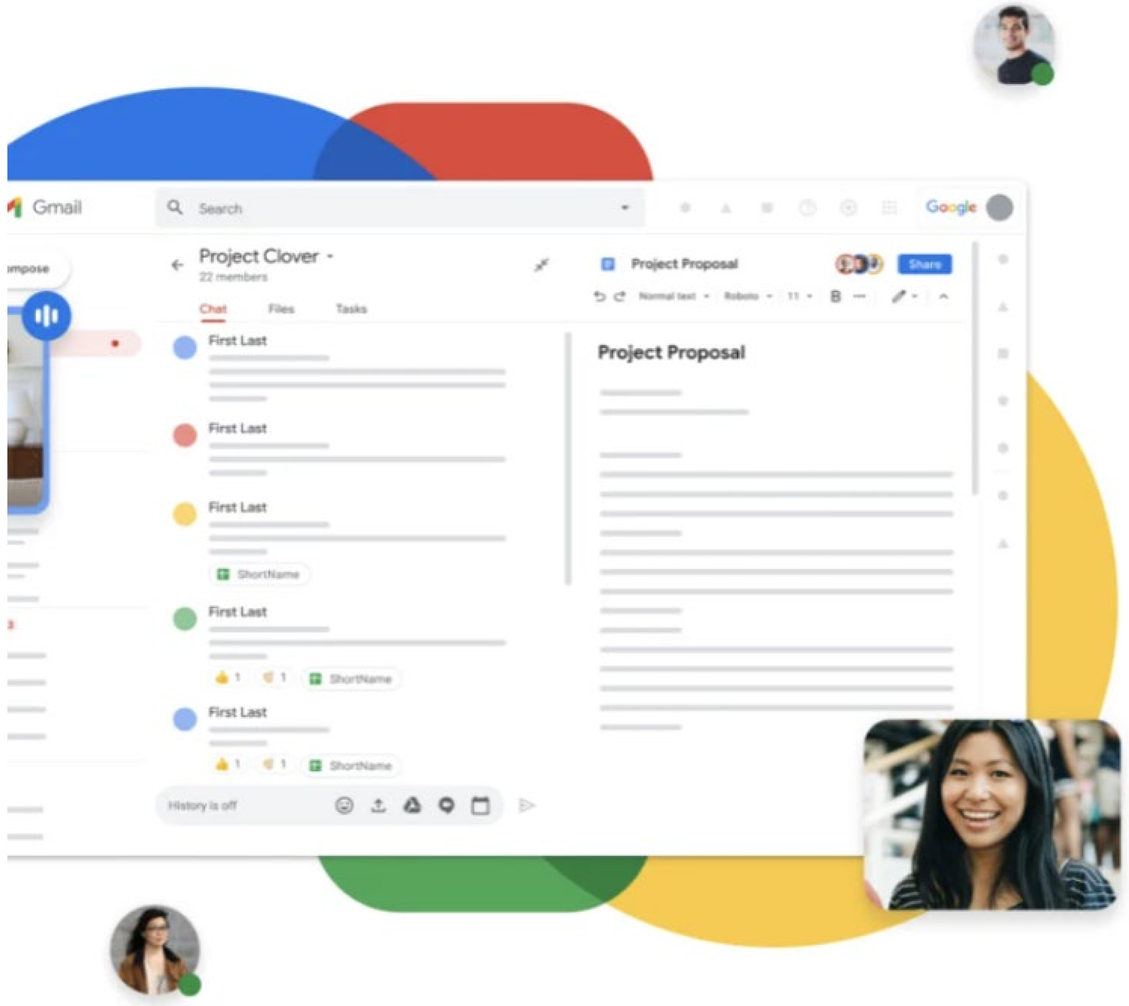
Security Cloud supports DevSecOps, including secure software supply chain.

BACK TO CONTENTS

Google Workspace

Google Workspace offers an ecosystem of cybersecurity partners to extend its native security capabilities, building a strong security foundation for Workspace with Google Cloud.

Google Cloud is committed to helping customers achieve their security and risk-mitigation goals, while enabling partners to deliver applications and capabilities that give customers greater security, agility, and resilience, all with significant cost savings. Google Cloud's best practice guidance and tools help ISVs deliver their products securely and at scale.

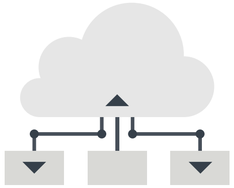


BACK TO CONTENTS

Driving Efficiency and Cost Savings

Google and its Cloud Ecosystem help customers address their top cloud security challenges using the full capabilities of Google Cloud. Working with a Google Cloud Ecosystem ISV provides benefits, including:

Minimized attack surface that avoids extra service accounts or agents, which add more technical components that can increase exposure to risk



Integration with the cloud core to detect threats to production workloads in as near-real time as possible, without adding operational or performance overhead

Minimized exposure window aligned with development and release cycles to provide coverage of applications across cloud environments

Visibility of assets and access points for greater control and information needed for context to accurately determine risk of security threats

Control optimization by maximizing operational efficiency and lowering expenses, including API, compute, storage, and egress costs

BACK TO CONTENTS

Google Cloud Partner Advantage

Google Cloud's security partners augment its platform security features to holistically meet the security needs of organizations using GCP.

LEARN MORE

BACK TO CONTENTS

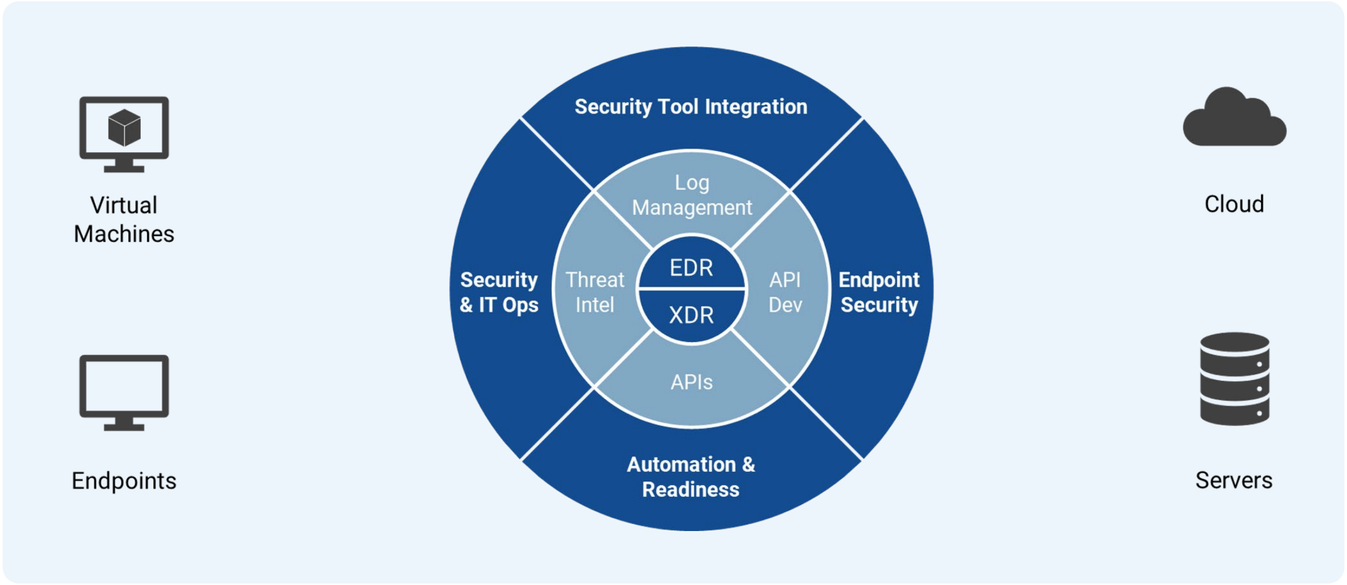
Google Cloud With Fortinet

Fortinet FortiXDR is a cloud-native endpoint security platform, built on top of FortiEDR, that protects endpoints from compromise, working in conjunction with Fortinet Security Fabric and Google Cloud Security Command Center (SCC). It features a lightweight, kernel-based agent that provides visibility into potential attack paths with threat hunting from the workstation to the cloud workload and resistance against malware evasion tactics.

The FortiXDR platform incorporates automated response capabilities driven by analytics an organization's data lake architecture provides as well as by Google Cloud. It can perform extended response remediation actions, such as automatically generating firewall rules to block traffic from malicious IP addresses, blocking phishing emails, initiating quarantines, and taking other measures to isolate compromised endpoints and halt the spread of attacks. FortiXDR also includes a free-to-use REST-based API, empowering organizations to develop custom integrations and implement additional automations as necessary.

FortiXDR integrates with several tools, including Fortinet Security Fabric, to correlate data to better detect and respond to attacks. For example, by integrating with Google Cloud's SCC, FortiXDR can ingest critical data that is used to defend the enterprise.

SCC strengthens FortiXDR's ability to identify and respond to potential cyberthreats and shares valuable threat intelligence, including indicators of compromise, affected devices, and file identifiers (hashes). FortiXDR analyzes Google Cloud SCC's vast pool of security event data to pinpoint potential attacks and conduct threat hunting to look for additional IOCs across the connected ecosystem.



BACK TO CONTENTS

Fortinet's FortiXDR provides an integrated, evasion-resistant XDR solution built to protect an organization's endpoints from compromise and lateral movement. Using automated response capabilities, lightweight agents, support for legacy operating systems, and strong integration capabilities, FortiXDR on Google Cloud offers a single platform that protects endpoints, servers, and virtual machines, both on premises and in the cloud, from advanced threats.

Fortinet partners with Google Cloud to better find and detect malicious activity and stop it. Google Cloud SCC shares security event information with FortiXDR, which then works within the Fortinet Security Fabric to detect attacks and automate response. This integration reduces the mean time to detect and respond to potential attacks. It also helps security teams increase efficiency and effectiveness, even as the IT environment grows more complex.

Building its solutions in partnership with Google Cloud means that Fortinet can bring massive scale to its solutions while providing broader visibility, faster analysis, and more effective response to its customers. Fortinet secures its customers' endpoints without the need for multiple or duplicate data lakes, reducing total cost of ownership while maintaining a high standard of security. Integration with Google Cloud provides another source of data that FortiXDR can use to quickly diagnose and stop attacks before they irreparably damage customer data, an organization's IT infrastructure, or its brand.

Fortinet on Google Cloud

LEARN MORE

FORTINET®

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.