Enterprise Strategy Group™ by TechTarget

TECHNICAL VALIDATION

Google Cloud Security Ecosystem

Leveraging the Google Platform to Accelerate the Delivery of Differentiated Security Offerings

By Tony Palmer, Practice Director and Principal Analyst, Validation Services
Enterprise Strategy Group

August 2023

Contents

Introduction

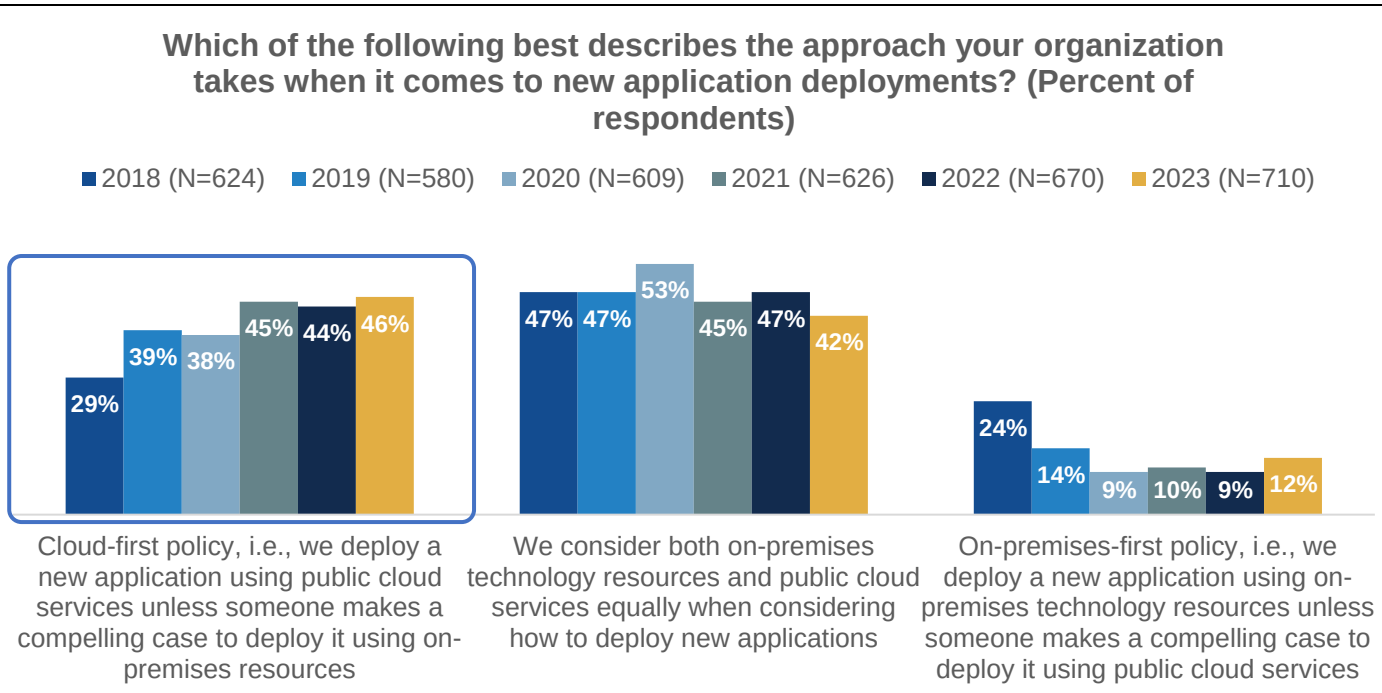
This Technical Validation from TechTarget's Enterprise Strategy Group documents our evaluation of the Google Cloud Security Ecosystem. Our analysis focused on how the Google Cloud enables cybersecurity independent software vendors (ISVs) to provide differentiated security offerings and capabilities, accelerate time to market, and help their customers secure their cloud applications.

Background

Momentum for digital transformation is accelerating, and organizations are under increasing pressure to improve productivity and drive innovation to serve their customers and are leveraging cloud services to meet that demand. In fact, 86% run production workloads on public cloud infrastructure/platforms,[1] and organizations are increasingly adopting a cloud-first policy for new applications.[2]

Cloud services enable teams to modernize their application development processes for greater operational efficiency, which helps them meet their digital transformation objectives, including becoming more operationally efficient, providing a better customer experience, using technology that enables collaboration, and improving product development.[3]

Figure 1. Cloud-first Policy for New Applications on the Rise



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.
[2] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.
[3] Ibid.

Organizations recognize the growing complexity across their IT environments and the ongoing cybersecurity skills gap is not making things any easier. In fact, 42% of respondents told Enterprise Strategy Group that cloud computing security was one of the most difficult roles for them to fill.[4] They are looking for ways to efficiently manage risk to support the demands of their businesses with the move to the cloud.

This has serious implications for cybersecurity solution vendors. Organizations with mission- and business-critical workloads in the cloud need to be confident that they can control and secure their environment, and trust in their technology partners is key. ISVs need access to sophisticated tools to enhance their development efforts across the development lifecycle. ISVs should be looking for a partner that can provide capabilities and expertise that add value. A partner that offers not just infrastructure, but go-to-market support, network analytics, visibility, integration opportunities, and complementary security capabilities will let them focus on their core mission rather than tooling and support infrastructure.

The Google Cloud Security Ecosystem

Google Cloud is designed, built, and operated with security as a primary design principle to help protect its customers against threats in their environments. Google layers on security controls to enable organizations to meet their own policy, regulatory, and business objectives. Customers can leverage elements of Google's compliance framework in their own compliance programs.

Google Cloud secures more than three billion users globally. To accomplish that, Google's cloud infrastructure can't rely on any single technology to make it secure. Google's 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. This means that only specifically authorized services can run and only specifically authorized users and processes can access them.
- Data is automatically encrypted at rest and in transit and 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.
- Google's network and infrastructure have multiple layers of protection that 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 round-the-clock operations teams to detect and respond to threats to the infrastructure from both internal and external threat actors.

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

[4] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.

Google operates from the precept that clients are always in control of their data. Google is committed to transparency in data handling. Google's privacy commitments and data processing addendum clearly state that Google does not use cloud customer data for advertising, any AI model, or product improvement. Google adheres to their clients' data storage, processing, and management preferences, so organizations control what happens to their data. In addition, all Google customers benefit from the privacy protections and fine-grained security controls built into Google Cloud by default.

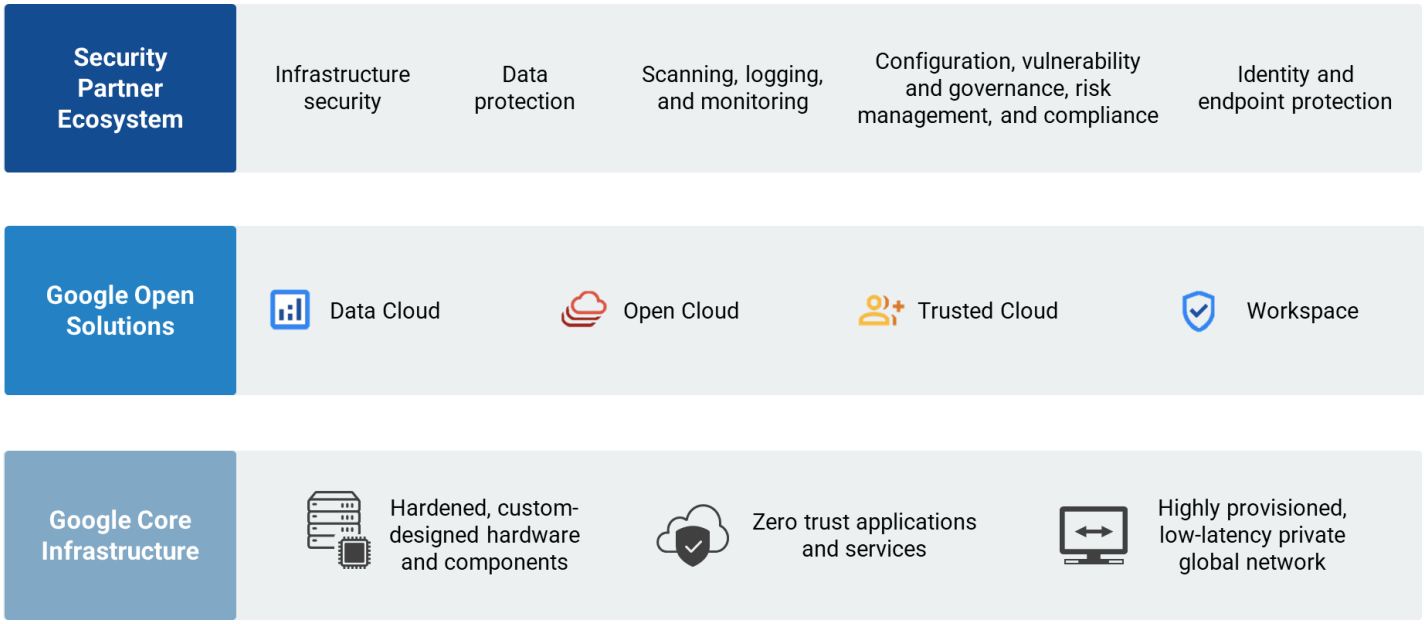
Google's products regularly undergo independent third-party audits with over two million control instances audited annually. Google maintains certifications, attestations of compliance, or audit reports against standards and regulations enforced across the globe. Google Cloud supports customer risk management and regulatory compliance needs with dedicated teams, offering compliance validation, support for due diligence, and security assessments, with an ongoing commitment to continuous assurance.

Google Cloud hardware infrastructure is custom designed by Google to precisely meet stringent requirements, including security. Google's servers are designed for the sole purpose of providing Google services. 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—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.

Google was an early proponent, designer, and practitioner of zero trust computing. Google developed foundational concepts that underpin zero trust architectures with its Beyond Corp and Beyond Prod 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, accessing only the machines specifically authorized by the correct code, is accessing just the data they are authorized to, in the correct context. Beyond Prod uses these same core principles to enable partners and Google Cloud customers to protect their operations in the same way, focusing on their own assets and resources and the entities and groups accessing them.

Layered over this foundation of trust are the tools and technologies that Google Cloud provides its partners— that 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.

Figure 2. Google Cloud Security Ecosystem Overview



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (BI), 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.

Google's **Open 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 Open 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.
- Open 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.

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

- The **Google Cybersecurity Action Team (GCAT)** is Google's security advisory team, with the singular mission of supporting 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 such as 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 is deployed and accessed by Google Cloud customers.
- 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.
- **Support for DevSecOps** includes secure software supply chain (S3C).

Google Workspace

Google Workspace has its own ecosystem of cybersecurity partners to extend its native security capabilities. This provides an opportunity for security ISVs to reach Google Workspace enterprise customers. 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.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group examined three cybersecurity ISVs, focusing on how the Google Cloud enables them to provide differentiated security offerings and capabilities, accelerate time to market, and help their customers secure their cloud applications in three different use cases:

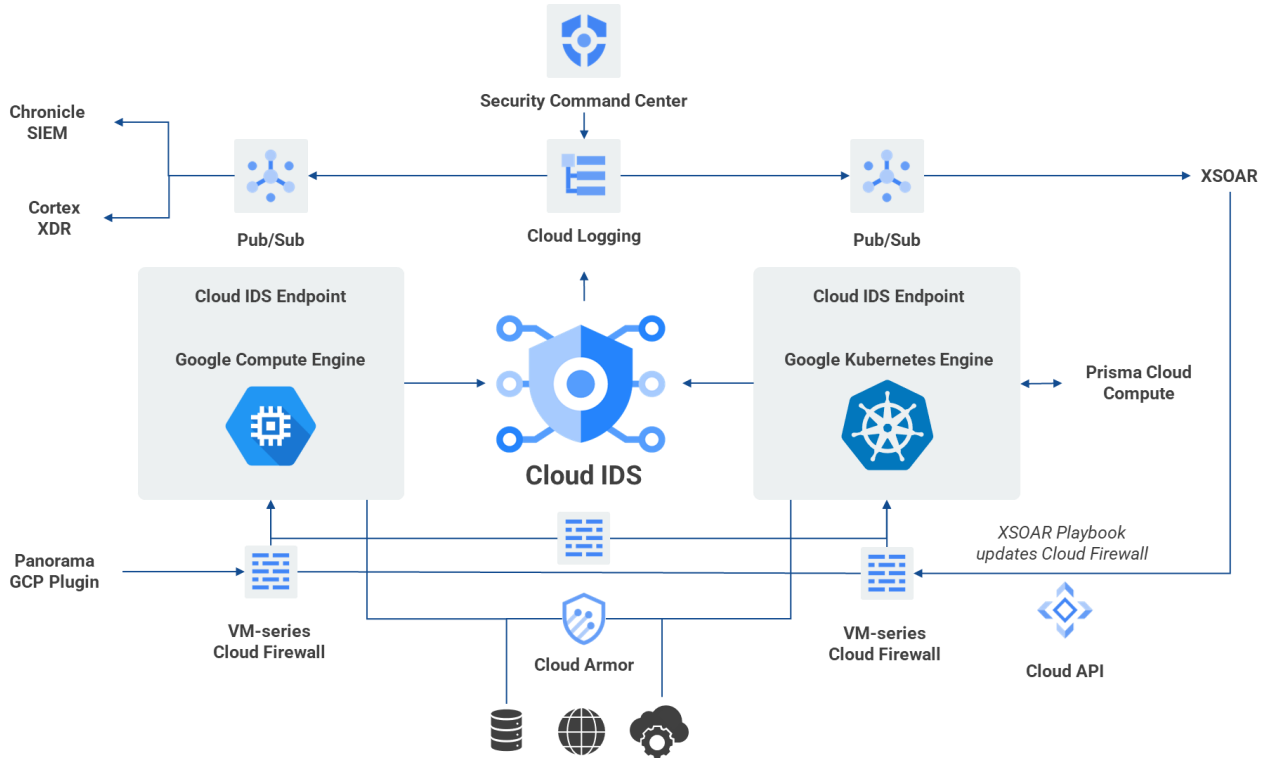
1. **Original Equipment Manufacturer (OEM):** Leveraging Google core technologies via an OEM agreement with a partner to provide a differentiated cybersecurity offering to joint customers. In this report, we look at Cloud Intrusion Detection System (IDS).
2. **Digital Transformation:** Leveraging the power of Google Cloud to accelerate digital transformation of a cybersecurity offering from non-digital native to cloud native.
3. **Secure Workspace:** Leveraging Google Cloud components to deliver differentiated secure file access, storage, and governance solutions.

Palo Alto Networks – OEM

Palo Alto Networks has been bringing security and network solutions to the market for almost two decades, with the goal of enabling organizations to remain agile and accelerate transformations while also mitigating risk, driving operational efficiencies, and enabling digital innovation.

Since 2018, Google Cloud and Palo Alto Networks have partnered to protect customers' applications and data as they utilize cloud-based infrastructure and platforms to modernize their businesses. The close relationship of the two organizations has enabled a multi-threaded view of how to integrate solutions and infrastructure, aimed at consolidating tools and improving security outcomes for customers. This has manifested in numerous solution architectures, which help customers seamlessly deploy and operate infrastructure with reduced friction across hybrid cloud and multi-cloud IT domains.

Figure 3. Cloud IDS Reference Architecture for Palo Alto Networks on Google Cloud



Source: Google and Enterprise Strategy Group, a division of TechTarget, Inc.

Palo Alto Networks has leveraged the foundational technologies of Google Cloud infrastructure and the first-party tools underpinning Data Cloud and Open Cloud to build these solutions. Google Cloud is partnering with Palo Alto to leverage its expertise to augment and enhance Google Trusted Cloud with Cloud IDS. Cloud IDS is an intrusion detection system built with Palo Alto Networks' threat detection technologies and delivered as a native cloud service managed, scaled, and operated by Google.

As enterprises migrate applications and workloads to—and in—the cloud, security teams are challenged by the complexity of replicating their on-premises network security stack in the cloud. With Cloud IDS enabled, cloud security teams can get immediate value from the managed service with granular application-level visibility of traffic within a Virtual Private Cloud (VPC)—between subnets, specific workload instances, or container pods—wherever inspection is required to secure applications and address compliance or regulatory requirements. The combination of the deep security expertise of Palo Alto Networks and the simple, secure, and scalable infrastructure of Google Cloud provides a unique offering.

The value of Cloud IDS is extended by leveraging the unique detection capabilities of the service and automating enforcement across the network or host/endpoint. As illustrated in the Cloud IDS reference architecture (see Figure 3), this leverages the capabilities of Cortex XSOAR to orchestrate response actions from the VM-Series Firewall for inline protection and Cortex XDR at the host level. This integration is coupled with native Google solutions like Security Command Center and Chronicle to gather a broad view of security automation across a customer environment.

Why This Matters

Enterprise Strategy Group research shows that organizations have faced a wide range of attacks on their cloud-native applications, making it clear that they need to take steps to reduce their security risk. 88% of organizations reported having been attacked across a wide range of incidents, including malware moving laterally across workloads, targeted penetration attacks, and exposed or lost data from an object store.[5]

Google Cloud partnered with Palo Alto Networks to develop and deliver Cloud IDS to provide cloud-native threat detection that detects network-based threats, such as malware, spyware, and command-and-control attacks with both north-south and east-west traffic visibility. Customers benefit from a cloud-native, managed experience that combines high performance and high-fidelity network-based threat data for investigation and correlation with the simple, secure, and scalable infrastructure of Google Cloud.

Detecting threats in traffic between workloads within the trust boundary of a VPC has been a significant challenge for cloud network security teams. With Cloud IDS, Google Cloud customers can deploy on-demand application visibility and threat detection between workloads or containers in any Google Cloud VPC to support their compliance goals and protect applications.

Palo Alto Networks leveraged the foundational capabilities of Google Cloud's infrastructure and Google Cloud's first-party tools to create and deliver differentiated products and offerings to their customers and in turn, Google is leveraging Palo Alto Networks' expertise in an OEM relationship to deliver differentiation and enhance the value of Google Trusted Cloud.

Exabeam - Digital Transformation

Exabeam created cloud-scale security information and event management (SIEM) for advancing security operations. Exabeam's products and solutions are designed to reduce business risk and elevate the performance of security operation teams. Enterprise Strategy Group has previously validated how the combination of cloud-scale security log management, behavioral analytics, and automated investigation experience can give security operations an advantage over adversaries, including insider threats, nation-states, and other cybercriminals. By understanding the normal behavior of users and devices—even as normal keeps changing—security operations teams have a holistic view of incidents for faster investigations and response.

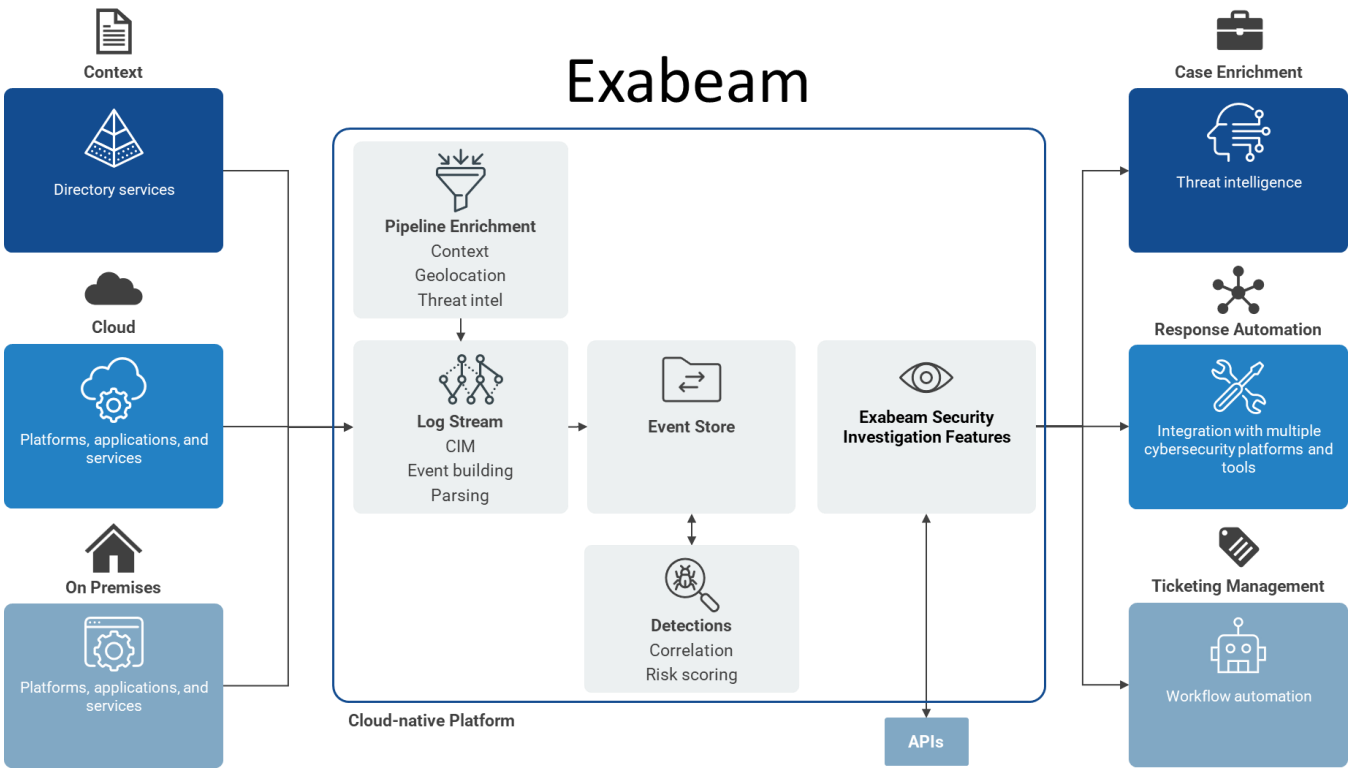
Their cloud-native platform ingests unlimited amounts of data from anywhere. Behavioral analytics can run on any data lake and leverage existing investments with more than 600 integrations and is well-suited to address compromised credentials, one of today's most utilized and elusive threat vectors. We found that Exabeam helps security teams focus on meaningful work by automating the entire threat detection, investigation, and response (TDIR) workflow, eliminating repetitive manual tasks. Automatic reconstruction of incident timelines accelerates and streamlines security operations resulting in faster response times and more thorough investigations.

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

Exabeam Advanced Analytics uses machine learning with more than 1,800 rules and over 750 behavioral models to automatically baseline the normal behavior of users and devices with histograms to detect, prioritize, and respond to anomalies based on risk. Automated incident response and case management enable teams to respond to security incidents rapidly and with less effort.

Exabeam's journey to digital transformation is rooted in its partnership with Google. Now fully cloud-native, Exabeam leverages Google Cloud tools and technologies to deliver the Exabeam Security Operations Platform at scale. The Exabeam Security Operations Platform uses a cloud-native data lake architecture to securely ingest, parse, and store security data from any location. Exabeam customers benefit from comprehensive log collection combined with powerful search capabilities that allow analysts to accelerate threat investigation across petabytes of data.

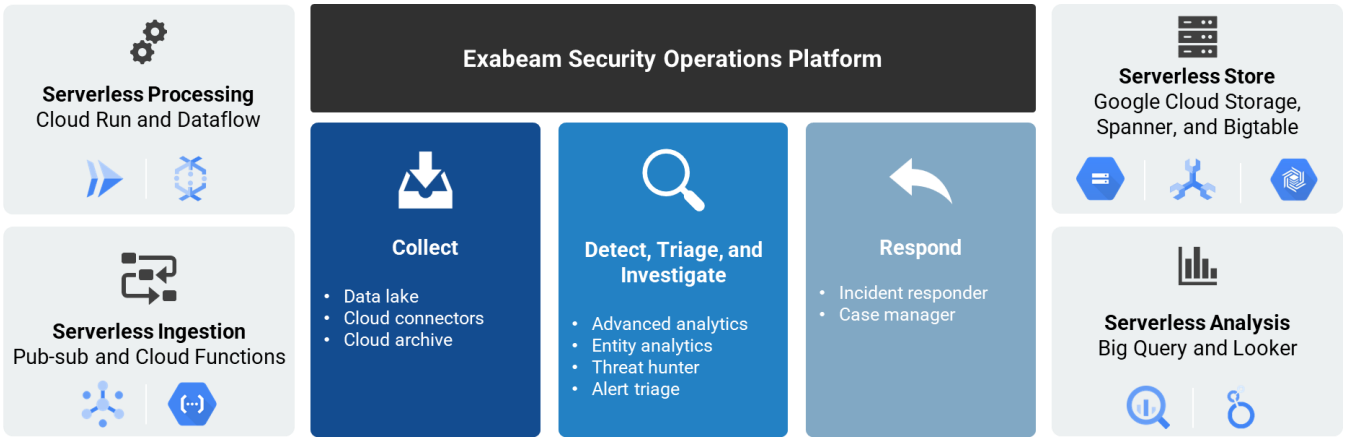
Figure 4. The Exabeam SecOps Platform



Source: Exabeam and Enterprise Strategy Group, a division of TechTarget, Inc.

Over the past two years, Exabeam has deepened its partnership with Google Cloud. In 2021, they announced their availability on the Google Cloud Marketplace to ease the adoption of their SIEM technology. Last year they announced how they are using the Google Cloud Stack which includes BigQuery, Data Flow, Looker, and other services to architect their new portfolio of cloud-scale products. As a result of the integration with Exabeam, Google Cloud enhanced the security they provide to Google Workspace and Gmail customers.

Figure 5. Google Stack Impact



Source: Google and Enterprise Strategy Group, a division of TechTarget, Inc.

Google Cloud has helped Exabeam drive positive business outcomes to security operations customers in numerous ways:

- Exabeam certifies that it can process more than one million events per second (EPS) per tenant, but it has seen customers with volumes of over 2.5 million EPS with no performance issues.
- On Google Cloud, Exabeam was able to accelerate the entire software delivery life cycle significantly, with an average of 10 to 15 updates and releases per month, triple what it was able to accomplish on-premises, improving the timeliness and accuracy of detection and response.
- Exabeam has improved customer support and responsiveness. The average age of support tickets has decreased by 65% with Google Cloud.
- Compliance certifications have been accelerated from their previous standard of once a year for all components. With Google Cloud, Exabeam is able to complete certifications faster. In addition to ISO 27001, Exabeam recently achieved ISO 27017 and ISO 27018 much faster than was possible before by leveraging Google's summary of controls. Where ISO 27001 focuses on an organization's management of information security risk, ISO 27017 and ISO 27018 are tailored specifically to cloud operations and privacy.[6]

[6] Source: Exabeam InfoSec Trends Blog, *Exabeam Achieves ISO 27017 and ISO 27018 Certifications*, November 2022.

Why This Matters

Companies continue to embrace the cloud to create and deploy business applications. According to Enterprise Strategy Group research, 46% of organizations surveyed indicated that they have a cloud-first policy for deploying new applications.[7] This has led to a change in how organizations *build* applications that Exabeam has experienced first-hand.

Google Cloud provided Exabeam with a secure, highly scalable platform on which to develop and deploy its cloud-native SecOps offering, reaping numerous business benefits from the partnership. An Exabeam executive told Enterprise Strategy Group: "Google … makes it so much easier for us to deal with our own challenges without having to worry about the back end."

Running in Google Cloud means that Exabeam can leverage Google Cloud's infrastructure and first-party tools to create and deliver differentiated products and offerings to their customers at scale and with performance that was impossible with their on-premises infrastructure.

Egnyte - Secure Workspace

Egnyte offers an all-in-one platform designed to simplify access, management, and control of content on any device, from anywhere. Egnyte designed its platform with fully integrated content security, governance, and collaboration. Egnyte protects its customers from multiple threats and risks, including accidental data deletion, and data exfiltration. Egnyte's platform offers a single, centralized content repository for privacy management for structured and unstructured data. Egnyte's Advanced Privacy and Compliance solution fully automates answering specific access requests like CCPA, GDPR, HIPAA, FCRA, and eDiscovery.

Figure 6. Egnyte's Content Intelligence Engine

Source: Egnyte and Enterprise Strategy Group, a division of TechTarget, Inc.

[7] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

Egnyte's proprietary content intelligence engine enables organizations to detect and prevent zero-day ransomware attacks, proactively locate and protect sensitive data, simplify compliance and audit responses, and perform centralized content discovery.

In 2021, Egnyte completed its migration to Google Cloud Platform. Egnyte chose Google Cloud for multiple reasons, including the reach of the network, with its own transoceanic fiber with points of presence in all markets where Egnyte currently does business as well as markets where they intend to expand in the future.

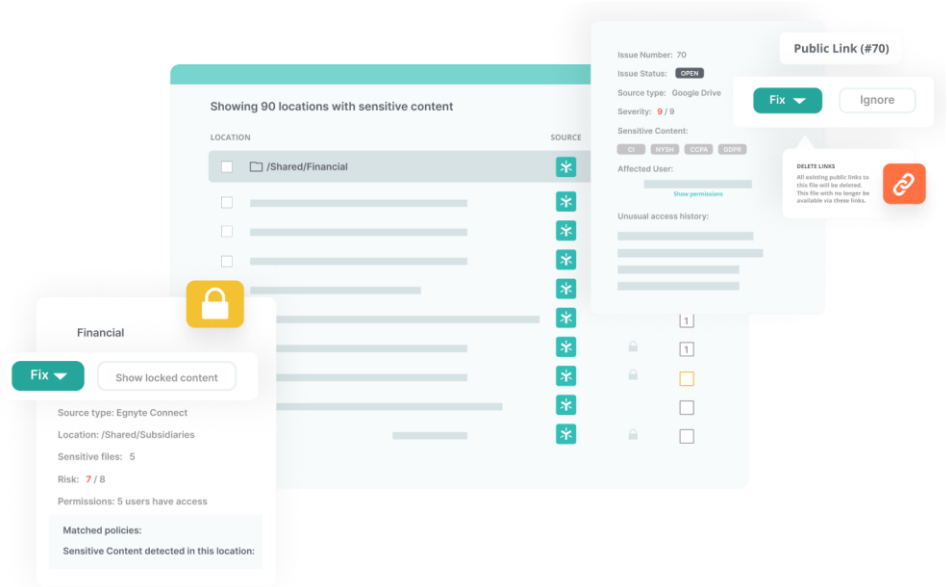
Egnyte completed the migration gradually and without disrupting services at any point. The close collaboration with the Google Cloud team contributed greatly to their success. The Google Cloud team anticipated some of the challenges Egnyte faced and helped resolve them quickly. Egnyte CIO Frank Sicilia described their experience this way, "Using Google Cloud means that we no longer rely on aging infrastructure, which is a very limiting factor when you're developing and engineering a platform as complex as Egnyte. Our entire platform is now always operating on the latest storage, processing, network, and services available on Google Cloud."

Egnyte embeds multiple Google Cloud services on its infrastructure, including Cloud SQL, Cloud Bigtable, BigQuery, Dataflow, Pub/Sub, and Memorystore for Redis. This means they no longer need to build services from scratch, nor do they have to purchase, install, and build them into the product and company workflow. In short, Google Cloud services have significantly simplified Egnyte's processes and now support their flagship products.

Egnyte partnered with Google Cloud to provide secure enclave services for its clients. Secure enclaves are controlled collaboration environments for sensitive content that are designed to be simple to use and manage (see Figure 7).

Egnyte secure enclaves control access and sharing using centralized policy controls and analytics to detect and prevent unauthorized access and anomalous insider behaviors. Organizations can exercise policy-based proactive risk management with the ability to customize retention, archival, deletion, content sharing, data residency, and compliance. Egnyte is ISO 27001, CMMC 2.0/NIST SP 800-171, and GxP compliant.

Figure 7. Egnyte Secure Enclave



Source: Egnyte

Egnyte's Google Drive integration allows organizations to identify and protect sensitive and regulated data including personally identifiable information (PII), like Social Security Numbers and dates of birth, financial records (credit card numbers, for example), and protected health information (PHI) such as patient IDs.

Why This Matters

File sharing and collaboration solutions can improve productivity, and users have become accustomed to obtaining easy access from any device and being able to easily share with internal and external users. However, organizations need to be able to control end-user access to sensitive or regulated content and their ability to share such data.

Egnyte's integration provides access to the most current information anytime, from anywhere. Secure enclaves were designed to increase productivity and efficiency by improving security and control over sensitive and regulated data, making the business smarter and more efficient.

Running on Google Cloud means that Egnyte can offer even higher reliability and faster scalability to their clients whenever they need a platform to protect and manage critical content on any cloud or any app, anywhere in the world.

Conclusion

Cloud services are an integral part of organizations' efforts to increase productivity and drive innovation to serve their customers and organizations are increasingly adopting a cloud-first policy for new applications.[8] Cloud services enable ISVs to modernize their application development processes to meet their digital transformation objectives.[9] Finding and retaining skilled cloud security professionals is a significant challenge, which presents a market opportunity for cybersecurity ISVs who develop and deliver solutions to help customers efficiently manage risk and protect their businesses with the move to the cloud.

Cybersecurity vendors need a better way to scale with modern development cycles to address security issues and stay ahead of threats. They also need to be able to monitor cloud workloads to detect security issues and respond quickly to threats to protect their customers and their data.

Google's cloud infrastructure stack builds security through progressive layers designed to deliver true defense in depth, which is how Google Cloud secures more than three billion users globally. Enterprise Strategy Group validated that Google Cloud aligns with the needs of security ISVs and helps them deliver better, more capable offerings, faster. The ISVs we interviewed confirmed that Google Cloud's economies of scale, software-defined infrastructure, simplicity, shared responsibility, automation, and global reach help them accelerate time to market and optimize the delivery of new products, enhancements, and updates.

Enterprise Strategy Group validated that:

- Google Cloud enabled Palo Alto Networks to provide differentiated security offerings to their mutual customers faster, easier, and cheaper using Google's foundational technologies and services. Google is leveraging Palo Alto Networks' expertise in an OEM relationship to deliver differentiation and enhance the value of Google Trusted Cloud with Cloud IDS.
- Google Cloud's core infrastructure and first-party tools enabled Exabeam to accelerate its digital transformation to a fully cloud-native solution while providing agile, scalable, and differentiated security offerings to its customers without disruption at levels of scale and performance that were previously impossible. An Exabeam executive said it this way, "We're changing the very nature of what our product is and how it works because of Google Cloud, and that's what's extremely cool."
- Google Cloud enabled Egnyte to deliver differentiated secure file access and sharing to its customers, improving security and control over sensitive and regulated data while accelerating time to market, increasing performance and reliability, and reducing costs.

Google Cloud offers broad and deep infrastructure and security support for ISVs developing solutions to secure their customers' applications across the globe. Organizations that fully leverage everything that Google Cloud has to offer will find themselves able to bring massive scale to their solutions while providing broader visibility, faster analysis, and more effective response to their clients, without adding complexity.

[8] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.
[9] Ibid.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group 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.

contact@esg-global.com
www.esg-global.com