ESG

Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Economic Validation

# Analyzing the Economic Benefits of Google Chronicle Security Analytics Platform

By Jack Poller, Senior Analyst; and Aviv Kaufmann, Senior Validation Analyst

August 2020

## Executive Summary

Never before has it been so critical for security teams to effectively secure the infrastructure for an increasingly remote workforce while they themselves may have limited physical access to on-premises resources. Those organizations that can deploy their security analytics and operations in the cloud are in a better position to continue to provide a secure infrastructure to the business.

ESG confirmed the savings that can be realized by a security organization leveraging Google Chronicle to collect and analyze any and all security telemetry data. ESG confirmed that Google's pricing model combined with Google's economies of scale provide significant cost savings for organizations while increasing their probability of finding advanced persistent threats and improving the fidelity of forensic investigations. ESG's modeled scenario predicted that a large enterprise organization can expect to spend anywhere from 3.9 to 6 times less for Google Chronicle than alternative cloud-based or on-premises security analytics platforms to analyze security telemetry data at scale. The TCO advantage may be much greater as Google Chronicle uses a single global price and costs do not change based on location.

Chronicle ESG

**3.9x – 6x Savings**

by deploying Google Chronicle versus alternative cloud-based or on-premises security analytics.

(based on ESG's 3-year TCO analysis for a modeled large enterprise)

Lower Cost of Security Analytics

Improved Security

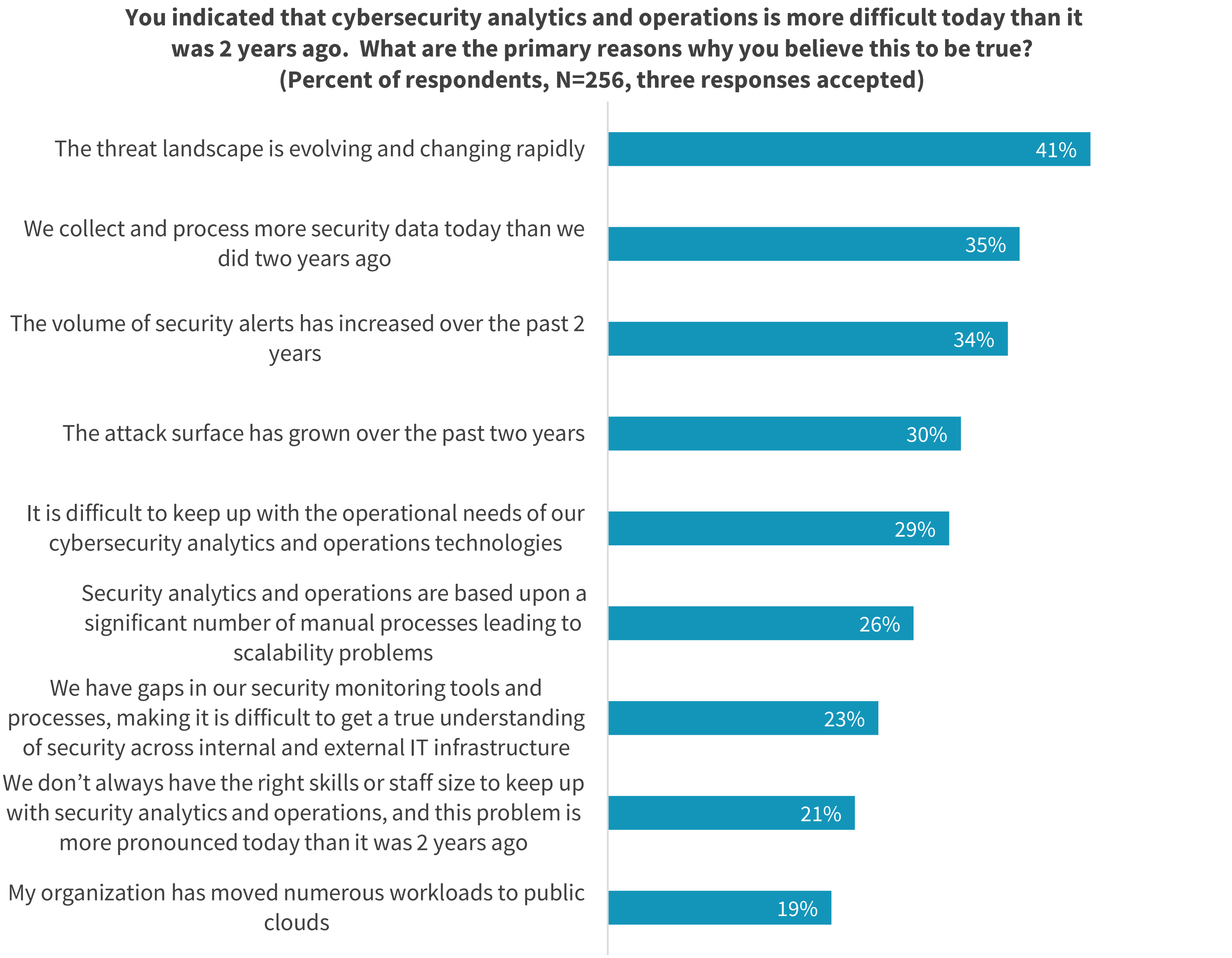
## Introduction

This ESG Economic Validation focused on the cost savings organizations can expect from deploying Google Chronicle to obtain continuous analysis of security telemetry. ESG created a modeled scenario that factored in costs of software, on-premises or cloud infrastructure, support, and maintenance over a 3-year period for enterprise deployments.

### Challenges

According to ESG research, nearly two-thirds (63%) of organizations believe security analytics and operations is more difficult today than it was two years ago, the result of both adversary and IT changes. Specifically, organizations are challenged by the evolving threat landscape, the requirement to collect and process more security data, and a growing attack surface. In addition, organizations find it difficult to keep up with the operational needs of their cybersecurity analytics and operations technologies while manual processes lead to scalability problems.[1]

**Figure 1. Primary Drivers of Increased Cybersecurity Analytics and Operations Difficulties**



*Source: Enterprise Strategy Group*

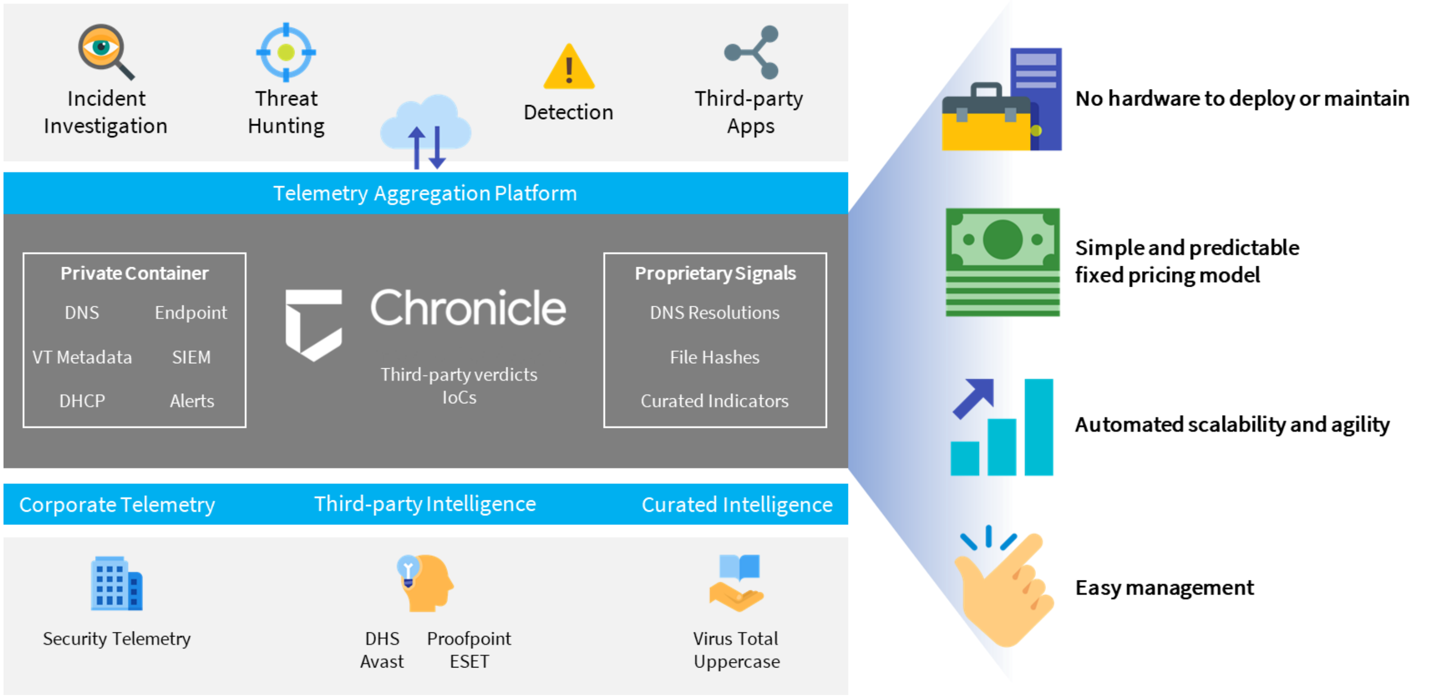
[1] Source: ESG Master Survey Results: *Cloud-scale Security Analytics Survey*, December 2019. All ESG research references and charts in this economic validation report have been taken from this master survey results set.

More than three-quarters (76%) of organizations say they collect more security data today than two years ago, and more than half (52%) retain security data for longer periods of time. One-quarter (25%) typically retain security data for more than 12 months. Thus, scaling the security analytics and operations infrastructure represents another pain point.

### The Solution: Google Chronicle

Google Chronicle is a security analytics platform built on core Google infrastructure, providing infinitely elastic storage of security telemetry data. With a predictable fixed price model based on the number of employees, organizations can store and analyze all security data, increasing fidelity. Chronicle simplifies the complex effort of managing and analyzing the massive volumes of security telemetry generated by modern enterprises. The automated analysis engine correlates intelligence from internal and third-party public sources to quickly and automatically extract signals and detect threats.

Figure 2. Google Chronicle Security Analytics Platform



*Source: Enterprise Strategy Group*

## ESG Economic Validation

ESG completed a modeled pricing comparison of Google Chronicle in medium and large enterprise environments. Focus was placed on the economic savings organizations can expect when leveraging Chronicle's pricing model and Google Cloud Platform economies of scale when compared with typical cloud or on-premises security analytics platforms.

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. The quantitative findings were used as the basis for a simple economic model comparing the expected costs of on-premises and cloud-based security analytics platforms.

### Google Chronicle Economic Overview

ESG's economic analysis revealed that Google Chronicle provided customers with significant savings by leveraging the resources and economies of scale of Google Cloud Platform and offering them a new pricing model. Whereas traditional security analytics platforms use a data volume-based pricing model, and costs increase in direct relation to the ever-growing volume of security telemetry, Google Chronicle uses employee-based pricing—the cost of the service is dependent primarily on the number of employees in the organization. Decoupling costs from data volumes increases budget stability and predictability and encourages the collection and analysis of all telemetry over longer timeframes, ensuring a greater probability of identifying long-lived threats from temporally distant indicators of attack (IOA) and indicators of compromise (IOC).

## ESG Analysis

ESG leveraged information collected through vendor-provided material, publicly available configuration guides and pricing, and industry knowledge of economics and technologies to create a three-year TCO/ROI model that compares the costs and benefits of Google Chronicle with two cloud-based and one on-premises security analytics platforms. The model compared the costs that would be expected when deploying each solution in an enterprise environment with a goal of quantifying the expected cost savings that are made possible through Google Chronicle's pricing model and Google's economies of scale.

ESG modeled the deployment and operation of a security analytics platform for two different sized organizations:

- Medium enterprise—15,000 employees, generating 1.5 TB of security telemetry data per day
- Large enterprise—125,000 employees, generating 12.5 TB of security telemetry data per day

ESG modeled employee growth using the average employee growth rate of Fortune 1000 companies, and security analytics data growth rate using information from ESG research surveys of CISOs, cybersecurity managers, and cybersecurity practitioners.

ESG research surveys indicate that a majority of medium and large enterprises retain security telemetry data for 12 months or more. Thus, the economic model accounts for 12 months of telemetry data retention.

### Why This Matters

Security budgets can't keep pace with the increasing volume of sophisticated threats and the growing attack surface area, and organizations continue to give CISOs and security teams the mandate to "do more with less."

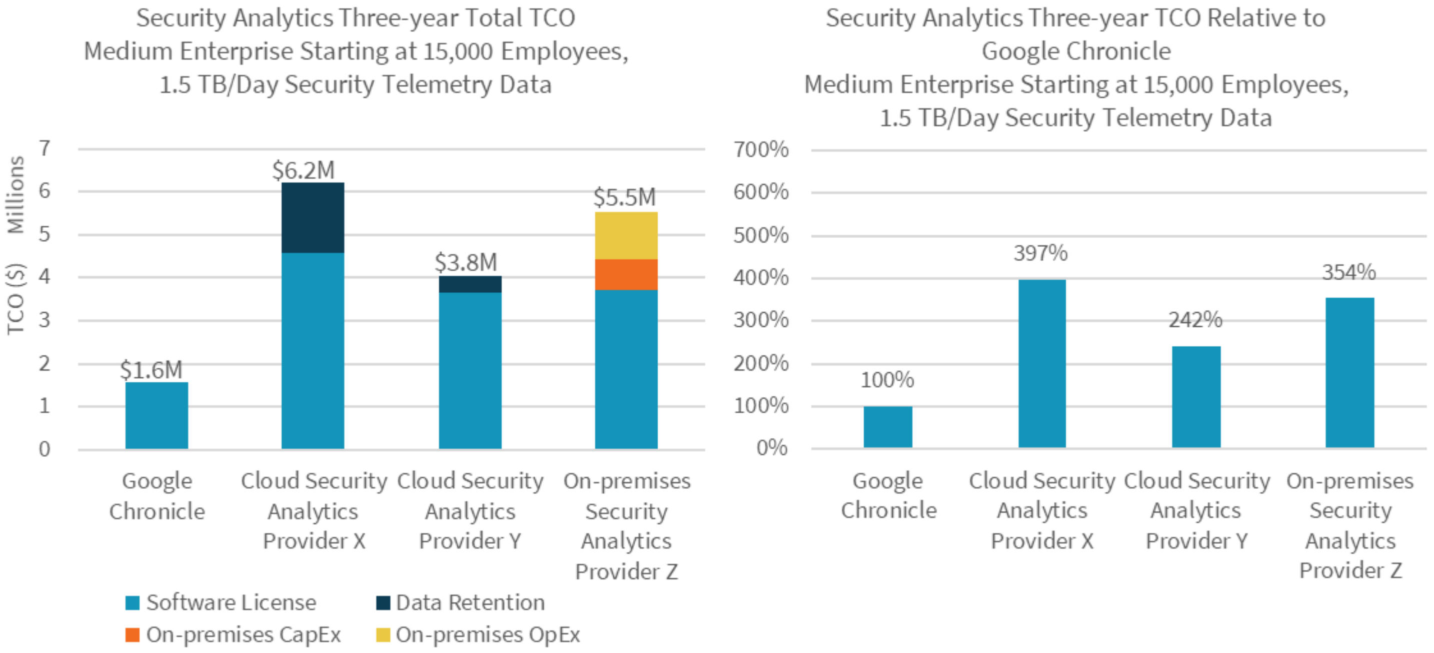
Google Chronicle provides unlimited scalability while eliminating on-premises infrastructure and operations overhead. Employee-based pricing decouples costs from data volume and velocity, ensuring organizations can predict their costs and encouraging the collection, storage, and analysis of any and all security telemetry—collecting more data over longer timeframes provides a greater probability of identifying long-lived threats.

The model calculated and reported the expected costs that would be incurred for an on-premises deployment of a security analytics platform, including the cost of hardware acquisition, power/cooling/floor space, support/maintenance, and administration over a three year period. For cloud-based security analytics platforms, the model calculated and reported costs incurred for software licenses and data retention using the lowest cost geographical region.

### ESG Modeled Scenario: Medium Enterprise

ESG's economic model calculated the expected costs over three years for a typical medium-sized organization with 15,000 employees generating 1.5 TB/day of security analytics data. The model showed that an organization deploying Google Chronicle would expect to spend $1,565,000 over three years (see Figure 3 and Table 1). The two cloud platforms would cost between 2.4 and 4 times more, and the on-premises platform would cost 3.5 times more.

## Figure 3. Expected Three-year TCO to Deploy a Security Analytics Platform in a Medium Enterprise



*Source: Enterprise Strategy Group*

## Table 1: Expected Three-year TCO to Deploy a Security Analytics Platform in a Medium Enterprise

| | Google Chronicle | Cloud Security Analytics Provider X | Cloud Security Analytics Provider Y | On-premises Security Analytics Provider Z |
|---|---:|---:|---:|---:|
| **On-premises CapEx** | $0 | $0 | $0 | $704,761 |
| **On-premises OpEx** | $0 | $0 | $0 | $1,105,951 |
| **Software License** | $1,564,768 | $4,584,929 | $3,661,729 | $3,723,750 |
| **12-month Data Retention** | $0 | $1,632,120 | $374,548 | (Included in CapEx) |
| **3-year Total** | $1,564,768 | $6,217,049 | $3,787,877 | $5,534,462 |
| **Total as % of Google** | **100%** | **397%** | **242%** | **354%** |

*Source: Enterprise Strategy Group*

The yearly expenditures for each solution are shown in Figure 4 and Table 2. The Google Chronicle pricing model is based on the number of employees in the organization, resulting in predictable and stable yearly expenditures. With 12 months of data retention built in, organizations deploying Chronicle don’t have to budget extra for data retention and storage. The entire three-year expenditure of $1.6M is OpEx.

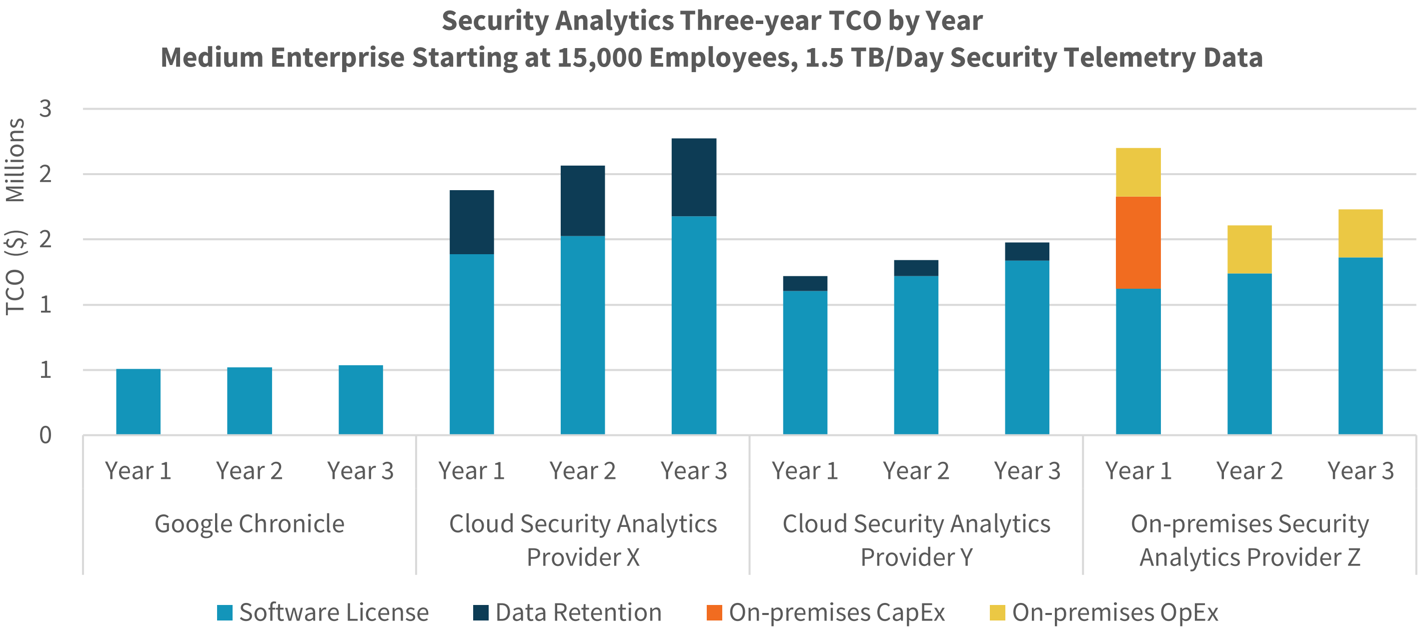
TCO for cloud security analytics provider X is based on both the amount of data processed and the amount of data retained in excess of the included retention period. The expected TCO for provider X is OpEx of $6.2M. While provider X can leverage cloud economies of scale, licensing fees are more than 2.9 times higher than Google Chronicle. And provider X includes only 90 days of data retention, requiring organizations to budget for additional storage fees. Data retention for provider X is greater than the entire TCO for Google Chronicle.

TCO for cloud security analytics provider Y is based on both the amount of data processed and retained. ESG made a conservative estimate of fees for data retained in excess of the included retention period using the cloud service provider’s object storage pricing. ESG expects actual data retention fees to be more than the estimate. All expenditures for provider Y can be classified as OpEx and totaled $3.8M over three years.

TCO for on-premises security analytics provider Z includes a license fee based on the amount of data analyzed. To store, index, and analyze the data requires on-premises storage and compute servers, and the requisite networking infrastructure. ESG's model included a solid-state drive-based storage system of sufficient size to retain 12 months of data. The number and size of compute servers was based on standard guidance from provider Z.

Provider Z TCO includes CapEx of $705,000 in year 1, and no additional CapEx in subsequent years. Infrastructure OpEx includes 1 system administrator to manage the storage, compute, and networking cluster, and power, cooling, floorspace, maintenance, and support for the storage and compute cluster at $369,000 per year. Despite the year one CapEx outlay, the three-year TCO was $5.5M, more than $682,000 less than cloud security analytics provider X.

### Figure 4. Expected Yearly TCO to Deploy a Security Analytics Platform in a Medium Enterprise



*Source: Enterprise Strategy Group*

### Table 2. Expected Yearly TCO to Deploy a Security Analytics Platform in a Medium Enterprise

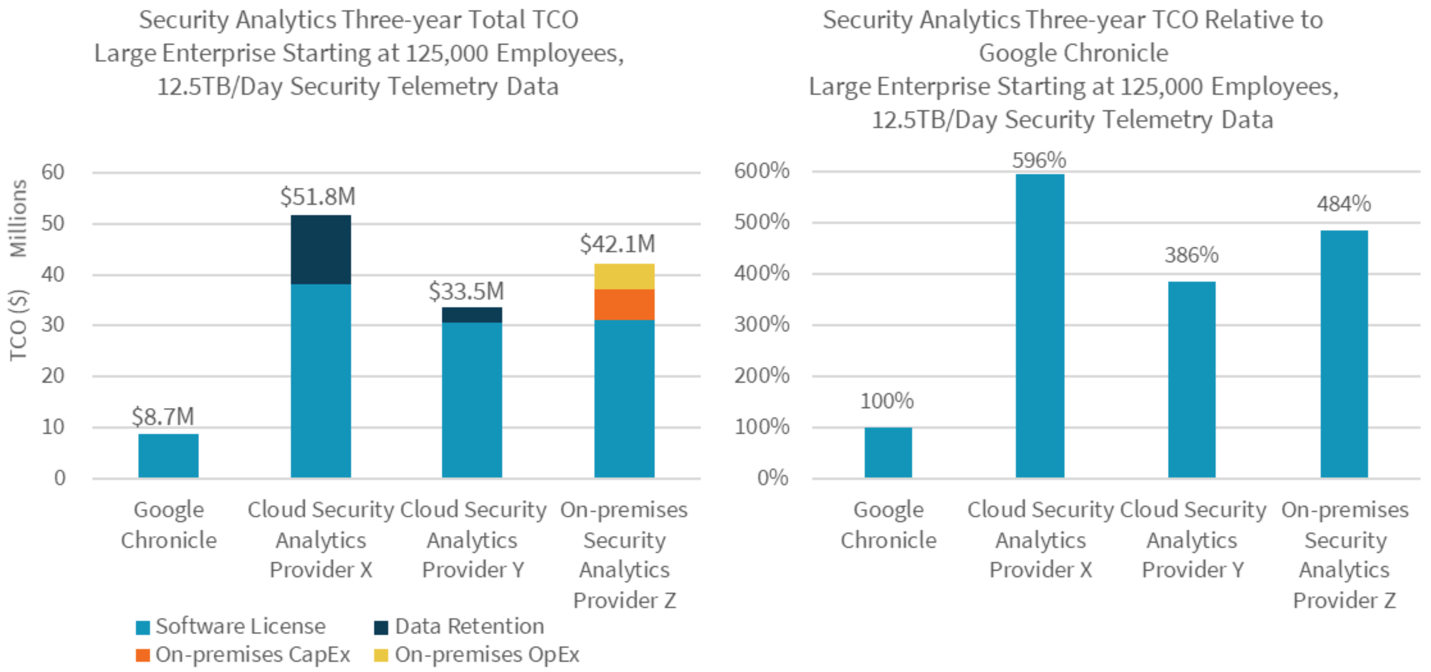
| | Google Chronicle | | | Cloud Security Analytics Provider X | | | Cloud Security Analytics Provider Y | | | On-premises Security Analytics Provider Z | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Year 1 | Year 2 | Year 3 | Year 1 | Year 2 | Year 3 | Year 1 | Year 2 | Year 3 | Year 1 | Year 2 | Year 3 |
| **On-premises CapEx** | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $704,761 | $0 | $0 |
| **On-premises OpEx** | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $368,650 | $368,650 | $368,650 |
| **Software License** | $506,250 | $521,438 | $537,081 | $1,385,175 | $1,523,693 | $1,676,062 | $1,106,262 | $1,216,889 | $1,338,578 | $1,125,000 | $1,237,500 | $1,361,250 |
| **12-month Data Retention** | $0 | $0 | $0 | $493,088 | $542,396 | $596,636 | $113,333 | $124,646 | $136,570 | (Included in CapEx) | (Included in CapEx) | (Included in CapEx) |
| **Yearly Total** | $506,250 | $521,438 | $537,081 | $1,878,263 | $2,066,089 | $2,272,698 | $1,219,595 | $1,217,334 | $1,350,948 | $2,198,412 | $1,606,150 | $1,729,900 |
| **3-year Total** | **$1,564,768** | | | **$6,217,049** | | | **$3,787,877** | | | **$5,534,462** | | |

*Source: Enterprise Strategy Group*

## ESG Modeled Scenario: Large Enterprise

ESG's economic model calculated the expected costs over three years for a large enterprise with 125,000 employees generating 12.5 TB/day of security analytics data. The model showed that an organization deploying Google Chronicle would expect to spend $8,693,000 over three years (see Figure 5 and Table 3). Because the alternatives to Chronicle are priced by data volume, the difference for large enterprises is much greater than for medium organizations: The two cloud platforms would cost between 3.9 and 6 times more, and the on-premises platform would cost 4.8 times more.

### Figure 5. Expected Three-year TCO to Deploy Security Analytics Platform in a Large Enterprise



*Source: Enterprise Strategy Group*

### Table 3: Expected Three-year TCO to Deploy a Security Analytics Platform in a Large Enterprise

| | Google Chronicle | Cloud Security Analytics Provider X | Cloud Security Analytics Provider Y | On-premises Security Analytics Provider Z |
|---|---|---|---|---|
| **On-premises CapEx** | $0 | $0 | $0 | $6,089,475 |
| **On-premises OpEx** | $0 | $0 | $0 | $4,992,262 |
| **Software License** | $8,693,156 | $38,207,744 | $30,514,406 | $31,031,250 |
| **12-month Data Retention** | $0 | $13,600,997 | $3,005,286 | (Included in CapEx) |
| **3-year Total** | $8,693,156 | $51,808,741 | $33,519,691 | $42,112,987 |
| **Total as % of Google** | **100%** | **596%** | **386%** | **484%** |

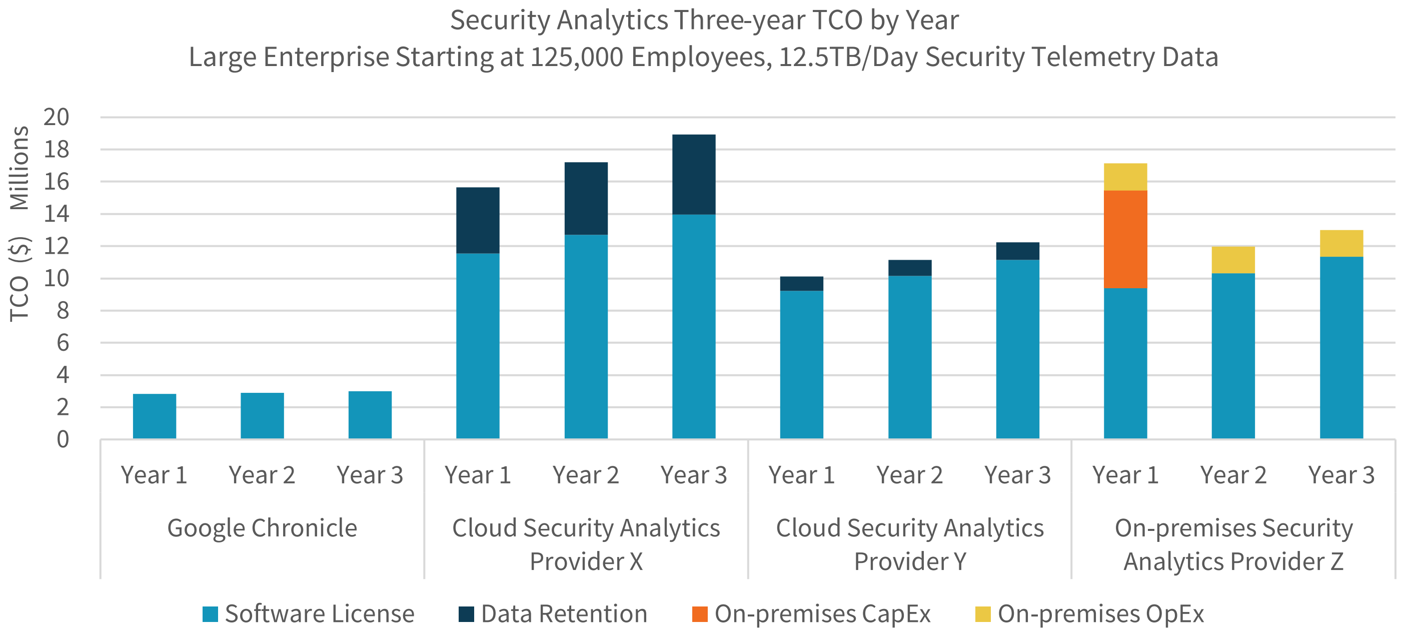
*Source: Enterprise Strategy Group*

The yearly expenditures for each solution are shown in Figure 6. As with a medium-sized organization, the data retention expenditures for provider X were 1.6 times greater than the total expenditures for Google Chronicle and represent more than one quarter of provider X TCO.

The software license for provider Y is 3.5 times the Google Chronicle TCO. ESG used a conservative estimate for data retention expenditures. While data retention is approximately 9% of provider Y TCO, the expenditure is more than one-third of the total expenditures for Google Chronicle.

On-premises security analytics provider Z expenditures included first year CapEx of $6,089,000 for storage, compute, and networking infrastructure, and infrastructure OpEx of $1,664,000 per year for one system administrator, power, cooling, floor space, support, and maintenance. The infrastructure expenditures for three years are $11,081,000, 1.3 times the total expenditures for Google Chronicle.

**Figure 6. Expected Yearly TCO to Deploy Security Analytics Platform in a Large Enterprise**



*Source: Enterprise Strategy Group*

## The Bigger Truth

Collecting and analyzing more data over longer timeframes increases the probability of finding stealthy, slow-moving, long-lived threats and attacks. According to ESG research, 84% of organizations said they would see benefit from collecting, processing, and analyzing more data. Thus, organizations are trending toward larger volumes of security data, with more than three quarters (76%) collecting more telemetry today than two years ago, and more than half (52%) retaining security data for longer periods of time. One quarter (25%) of organizations retain security data for more than 12 months.

Yet 85% of organizations say they collect, process, and analyze the same data using several independent security analytics tools; 80% are dependent upon numerous disconnected analytics engines and point tools; and 80% spend a significant amount of time on data management and fine-tuning the security analytics infrastructure.

The pricing model for traditional security analytics platforms is based on the volume and velocity of security data, and, for cloud-based platforms, the geographic region. Clearly this makes predicting costs difficult and discourages the collection of additional telemetry, degrading the fidelity of the analysis.

Google Chronicle employs a new pricing model based on the number of employees in the organization. This all-you-can eat data analysis engine provides a predictable cost that encourages rather than limits the collection of all security telemetry data, increasing fidelity and helping organizations to identify advanced persistent threats (APTs). Chronicle includes 12-month data retention, aiding searches for APTs and forensic investigations.

ESG's modeled TCO analysis shows how an organization that deploys Google Chronicle can expect significant savings in their security analytics and operations by leveraging Google's economies of scale and pricing model. Over three years, medium enterprises can expect to spend 2.4 to 4 times less on Google Chronicle than other cloud-based platforms and 3.5

times less than an on-premises deployment. Bigger organizations can expect greater differences, with a typical large enterprise spending 3.8 to 6 times more on alternate cloud solutions, and 4.8 times more for an on-premises deployment. Alternate cloud solutions may be even more expensive because the solution pricing is dependent on location.

Google Chronicle is not competing with an organization's existing security tools or looking to change the security operations. Instead, Chronicle aims to operationalize all security controls by encouraging the collection and analysis of all security telemetry over long timeframes, increasing the probability of finding and preventing stealthy attacks and improving the fidelity of forensic investigations. If you're looking to streamline your security operations and analytics while "doing more with less," ESG recommends that you contact Google to see if it's the right security analytics platform for your team.

ESG

**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.