SOCURA

See the Bigger Picture

with Socura and Google Cloud Chronicle

There is no need to compromise. Store and analyse all security data in one place to investigate and detect threats at Google speed and scale.

Chronicle

> “The world in which we work has changed and now, so must we. This year we have seen unprecedented digital transformation and we want to ensure that organisations can continue to evolve by enabling a secure environment 24/7.”

MARC CHANG – CEO & FOUNDER

SECURITY ANALYTICS:

Where are we now

The evolving threat landscape, the requirement to collect and process more security data, and a growing attack surface, means that many organisations find it difficult to keep up with the operational needs of their cyber security.

76%

More than three-quarters of organisations say they collect more security data today than two years ago.

63%

Nearly two-thirds of organisations believe security analytics and operations is more difficult today than it was two years ago.

76%

Over three-quarters of organisations typically retain security data for less than 12 months.

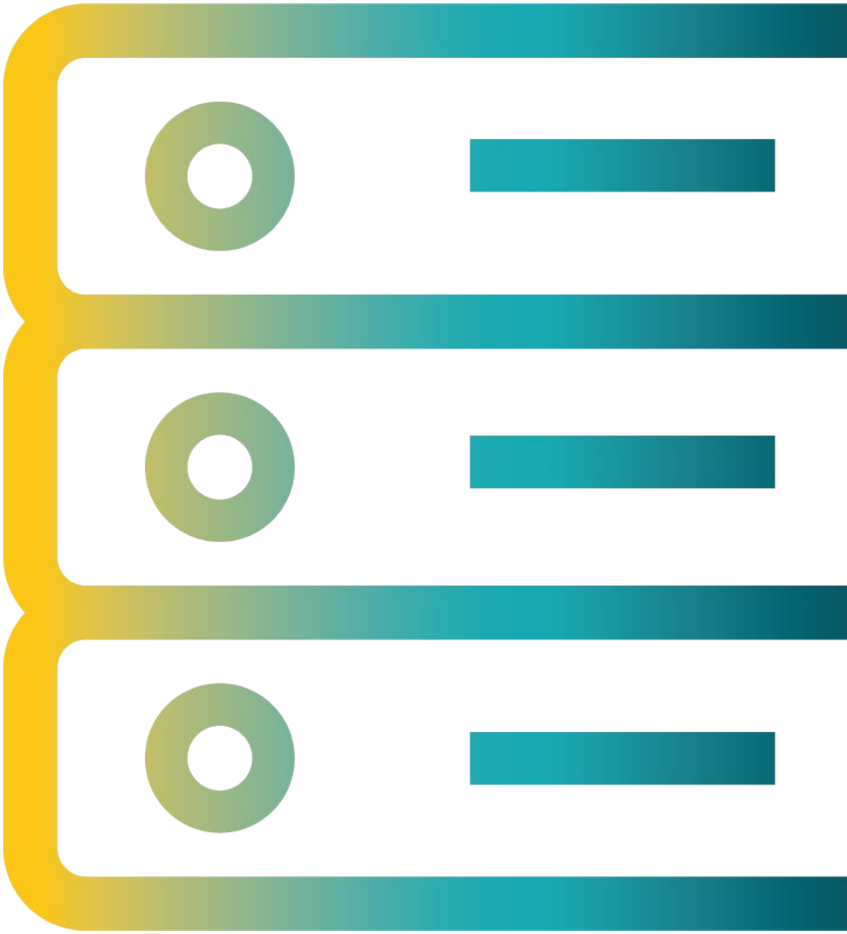
SOCURA INSIGHT

Telemetry must be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.

The Volume Challenge

Data volumes are an order of magnitude higher than they were just a few years ago due to growing infrastructure, more applications, and more security tools. Beyond storage costs, today's security data volumes require a significant infrastructure investment to enable scalable and performant analysis.

Traditional security analytics pricing models are primarily based on data volume, or number of monitored devices, incentivising you to limit the collection and analysis of information.



The Visibility Challenge

As infrastructure evolves from on-premises to IaaS/PaaS/SaaS platforms, coverage and visibility have also emerged as critical barriers to security operations. Some cloud providers focus primarily on delivering security monitoring for their own stack.

Such siloed coverage limits visibility into modern attacks that commonly span on-premises and hybrid cloud infrastructure.

With Socura, there are no compromises

We've partnered with Google Cloud Chronicle to allow us to ingest all the security data that your systems generate, resulting in complete visibility across all data sources. This data is retained for 12 months (minimum), whilst remaining hot and searchable in milliseconds, meaning that we can also instantly and retroactively match newly discovered indicators of compromise against your entire historical telemetry dataset.

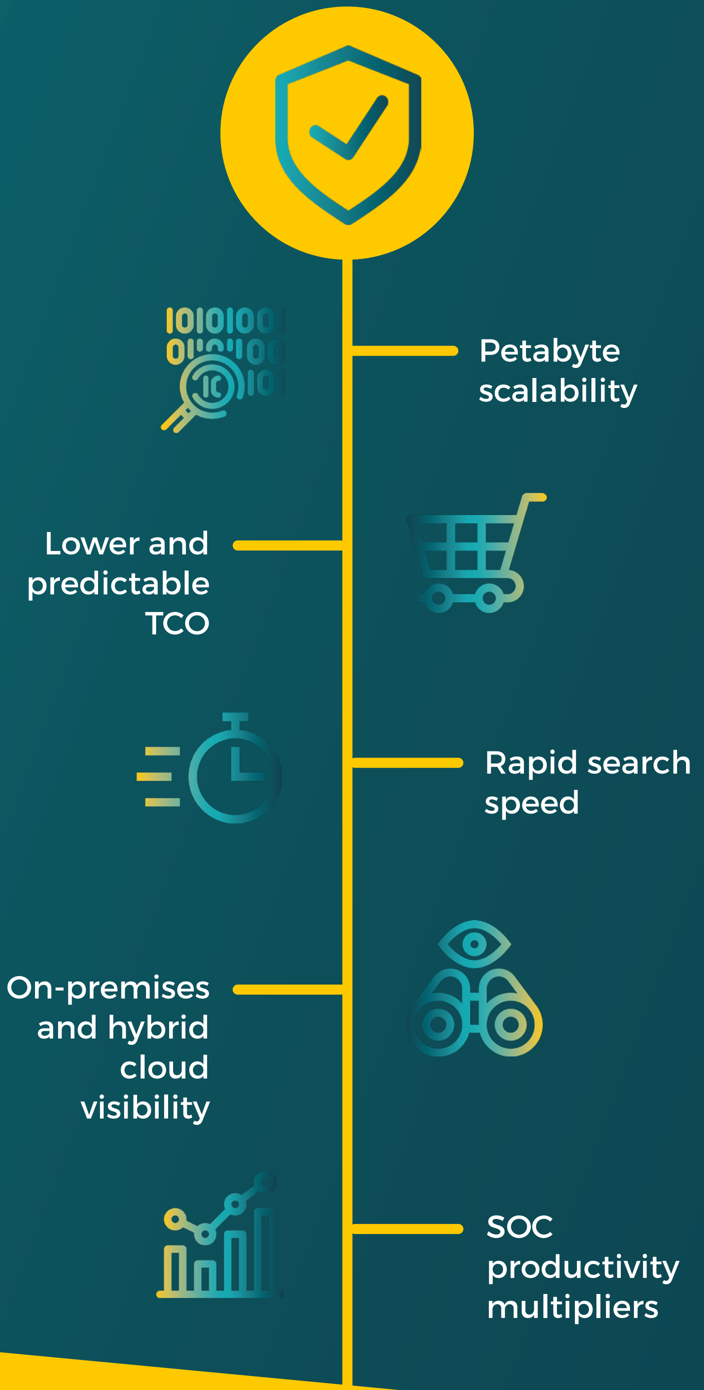
Holding more data for longer, enables us to see the bigger picture with no blind spots.

Chronicle

Modern security analytics requirements

It’s time to take a fresh look at what Is possible and how it can be achieved using the latest tools and approaches on offer. It’s time to refactor for this new world. It’s time to re-evaluate the threat, and how best to defend against it.

Chronicle, the Security Analytics element of Socura’s MDR service, is provided by Google. The elastic scale and speed of search that they are renowned for can be brought to bear on the problem of hunting for malicious activity amongst vast amounts of data.



Petabyte scalability

Lower and predictable TCO

Rapid search speed

On-premises and hybrid cloud visibility

SOC productivity multipliers

SOCURA