

# Security analytics platform overview



## Security analytics challenges

Security operations spanning detection, investigation, and response face a common set of challenges around cost (TCO), scale, performance, visibility, and analyst productivity. 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. Without this, key security metrics such as "time to investigate" or "time to remediate" suffer. Additionally, prevailing security analytics or SIEM pricing models are primarily based on data volume or number of monitored devices and thereby create a disincentive to capture and analyze all security-relevant information.

As enterprise infrastructure evolves from captive on-premise 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-premise

and hybrid cloud infrastructure. But perhaps the single biggest challenge that security teams face is a shortage of talent. Proprietary analytical frameworks and complex search syntaxes imposed by legacy security analytics providers significantly increase the dependency on highly experienced and expensive Tier 2 or 3 analysts, even for triage of commonplace attacks like phishing. Not surprisingly, many organizations have turned to managed security services to augment the shortage of in-house security staff. For the most part, this has simply shifted the same set of key challenges to a third party without a real gain in analyst efficiency or productivity.

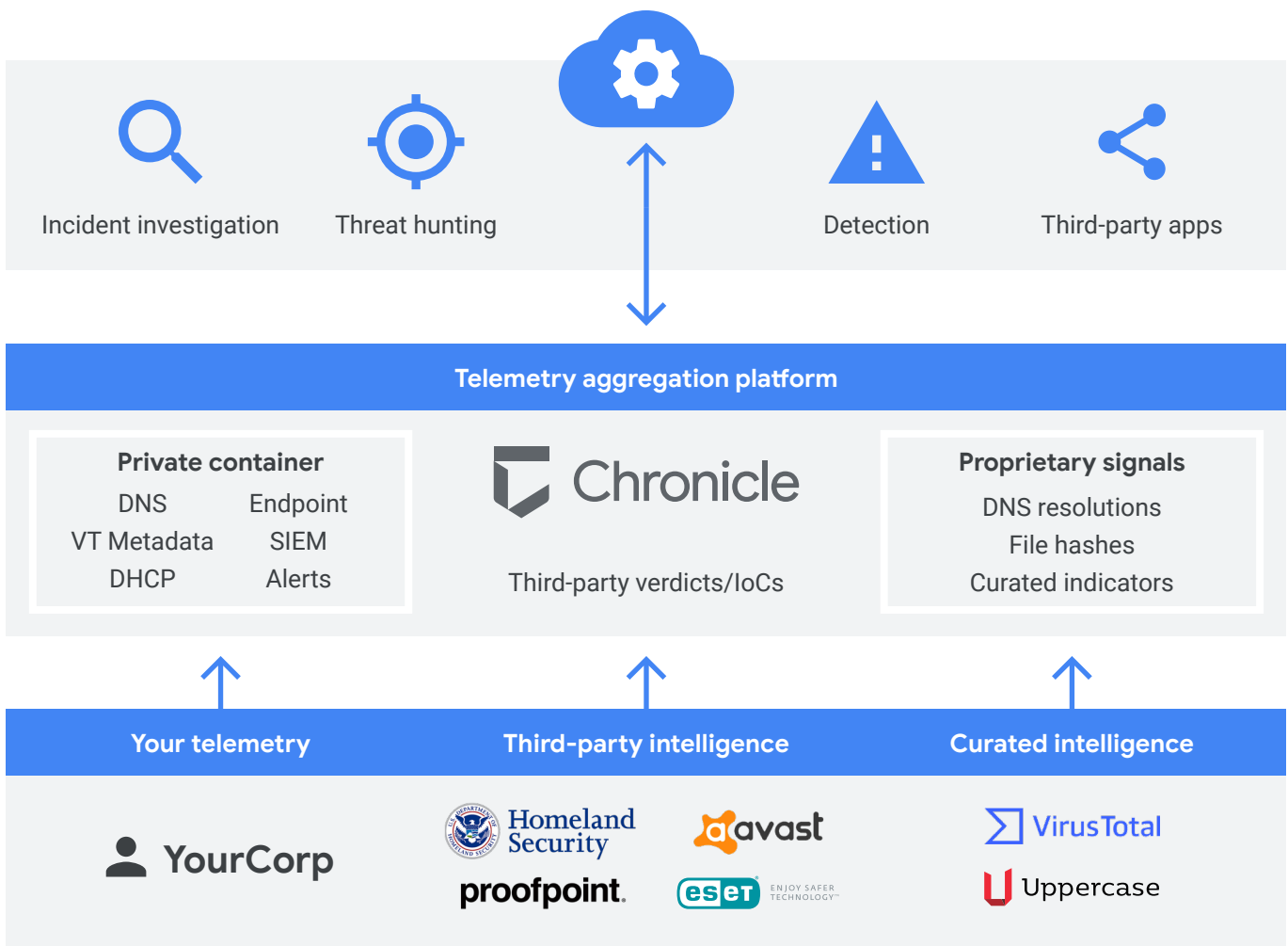
### Modern security analytics requirements

- Lower and predictable TCO
- Petabyte scalability
- Google search speed
- On-premise and hybrid cloud visibility
- SOC productivity multipliers



## Chronicle overview

Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate. Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.



## Data collection

Chronicle can ingest numerous security telemetry types through a variety of methods including:

### Forwarder

A lightweight software component, deployed in the customer's network, that supports syslog, packet capture, and existing log management / SIEM data repositories

### Ingestion APIs

APIs that enable logs to be sent directly to the Chronicle platform, eliminating the need for additional hardware or software in customer environments

### Third-party integrations

Integration with third-party cloud APIs to facilitate ingestion of logs, including sources like Office 365 and Azure AD

## Data analysis

The analytical capabilities of Chronicle are delivered to security professionals as a simple, browser-based application. Many of these capabilities are also accessible programmatically via Read APIs. At its core, the purpose of Chronicle is to give analysts a way, when they see a potential threat, to determine what it is, what it's doing, whether it matters, and how best to respond.



## What is the threat?

Here's an example: If a threat feed just informed Chronicle about a new APT network domain, Chronicle will instantly surface every hostname that accessed that domain going back a full year, regardless of the data volume. Similarly, Chronicle continuously enriches the incoming event stream by correlating IPs to hostnames so that analysts have full information, instantly – without the need to write complex queries.

## What is it doing?

Modern threats lie at the intersection of targeted assets, users, and threat campaign infrastructure (domains, URLs hosted on specific external IP addresses, and malicious files deployed from there). In Chronicle, curated views for assets, users, and IoC types operate on a Unified Data Model and enable analysts to quickly and intuitively investigate what a threat is doing.

## Does it matter?

Security telemetry alone rarely provides the full picture needed to hunt, investigate, or detect threats. Each curated view in Chronicle provides relevant context and insights to aid the investigation or hunt. This context is critical to giving analysts the ability to prioritize real threats and dismiss false positives.

## How to respond?

Large organizations with mature SOCs have documented playbooks for investigation and remediation of threats. SOAR or Orchestration technologies that automate these playbooks are now growing in adoption. Chronicle's Read APIs expose its analytical capabilities and enable enterprises (as well as managed security service providers) to integrate Chronicle findings into downstream security playbook technologies such as ticketing systems or SOC reporting tools.

---

## Security and compliance

As a specialized, private layer built over core Google infrastructure, Chronicle inherits compute and storage capabilities as well as the security design and capabilities of that infrastructure (Chronicle's "Core Infrastructure"). The underlying design of our Core Infrastructure is described in more detail in a [Google whitepaper](#).

Google Cloud



## Summary of capabilities and benefits

Feature	Description	Benefits
Continuous enrichment	<ul style="list-style-type: none"> <li>Automated IP to host correlation</li> <li>Automated, continuous, retroactive IoC enrichment</li> </ul>	<ul style="list-style-type: none"> <li>Faster time to investigate</li> <li>Greater analyst productivity</li> </ul>
Context and insights (threat / IoC, vulnerability, asset, user, file/process)	<ul style="list-style-type: none"> <li>Embedded threat intelligence sources (Proofpoint, DHS AIS, OSInt, Avast, ESET)</li> <li>Customer-provided threat intelligence sources</li> <li>Asset, vulnerability, and user context</li> <li>Derived insights</li> </ul>	<ul style="list-style-type: none"> <li>Faster time to investigate</li> <li>Greater analyst productivity</li> </ul>
Read APIs	<ul style="list-style-type: none"> <li>High performance APIs that expose functionality to downstream enterprise and MSSP SOC playbook stages and tools (ticketing, orchestration, dashboarding)</li> </ul>	<ul style="list-style-type: none"> <li>Automation of SOC playbooks</li> <li>Integration with MSSP portals</li> <li>Faster time to remediation</li> </ul>
Ingest APIs and Unified Data Model	<ul style="list-style-type: none"> <li>High throughput APIs that enable sending data directly to the Chronicle data pipeline without the need for a forwarder</li> </ul>	<ul style="list-style-type: none"> <li>Faster time to value</li> <li>Zero deployment footprint</li> </ul>
Raw Log Scan	<ul style="list-style-type: none"> <li>Access to all unparsed fields</li> <li>Search any raw security telemetry</li> </ul>	<ul style="list-style-type: none"> <li>Faster onboarding of all security telemetry</li> </ul>
Security & compliance	<ul style="list-style-type: none"> <li>Adherence to Google Cloud common controls</li> <li>SOC 2 and SOC 3</li> <li>ISO/IEC 27001</li> <li>HIPAA BAA</li> </ul>	<ul style="list-style-type: none"> <li>Documented, stringent controls to protect your data at every layer</li> <li>Key attestations and certifications</li> </ul>