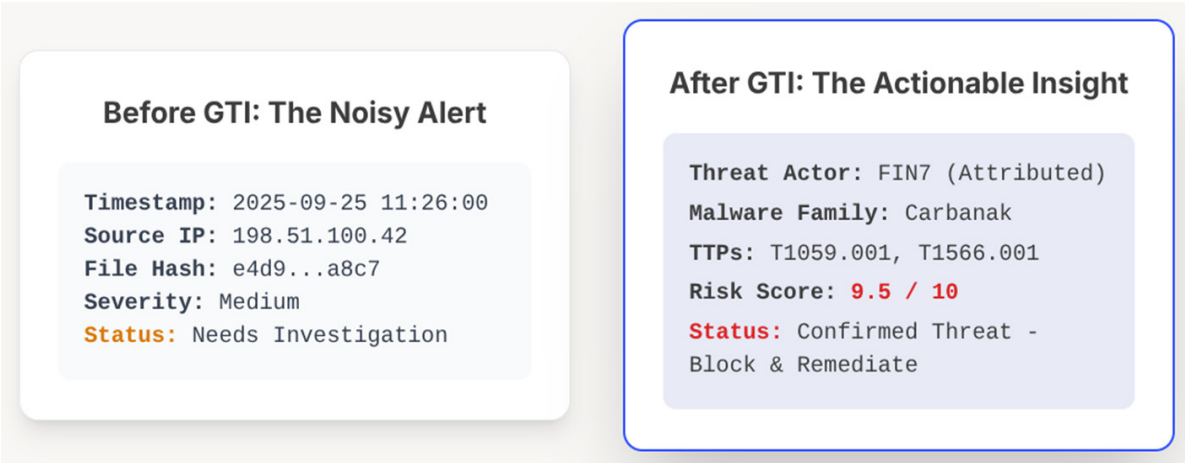
Enrich Your Security Platform. Differentiate Your Business

Stop just reporting problems. Start delivering answers.

In a world of noise offer clarity

In a crowded security market, differentiation is everything. Your customers are no longer just buying tools; they're investing in answers. The critical gap between a low-context alert and an actionable, high-confidence insight is one of the biggest challenges for modern security teams—and it's one of the biggest opportunities to add tangible value.

By embedding world-class intelligence, you can enhance your offering and the value it creates for your customers. Instead of just showing what happened, you can provide rich context, showing your customers why it matters and what to do next.



Enrich alerts with unparalleled visibility

Google Threat Intelligence cuts through the noise. We provide a single, unified solution that combines the unparalleled, real-time visibility of Google, the frontline expertise of Mandiant, and the world's largest threat repository from VirusTotal.

This isn't just another feed enriching your alerts with. It's a comprehensive intelligence offering that combines frontline, curated, open-source, and crowdsourced data to give you a complete picture of the threat landscape.

- **Frontline Expertise:** Go beyond IOCs with actor-centric intelligence, tactics, techniques, and procedures (TTPs), and reporting from 400,000+ hours of Mandiant incident investigations.
- **Unmatched Visibility:** Leverage insights from protecting 1.5 billion Gmail users and 4 billion devices with Google Safe Browsing.
- **Massive Scale:** Instantly query a database of 50B+ files and 1.5B+ sandbox reports to identify known-bad artifacts.
- **Human curated intelligence:** Hundreds of global threat experts in 30 countries speaking +30 languages provide high quality contextualized intelligence including threat actor motivations, TTPs, and likely targets.
- **AI as a Force Multiplier:** Our entire model is infused with Gemini AI to provide AI-assisted malware analysis, risk profiling, and digested threat summaries, turning complex data into clear, actionable insights.

Empower Your Products, Empower Your Customers

The Google Threat Intel OEM program allows you to embed our intelligence directly into your security products. You don't just resell our data; you make it a core, value-added feature of your own platform.

By integrating Google Threat Intel, you can transform your product from a simple alert generator into a sophisticated decision engine.

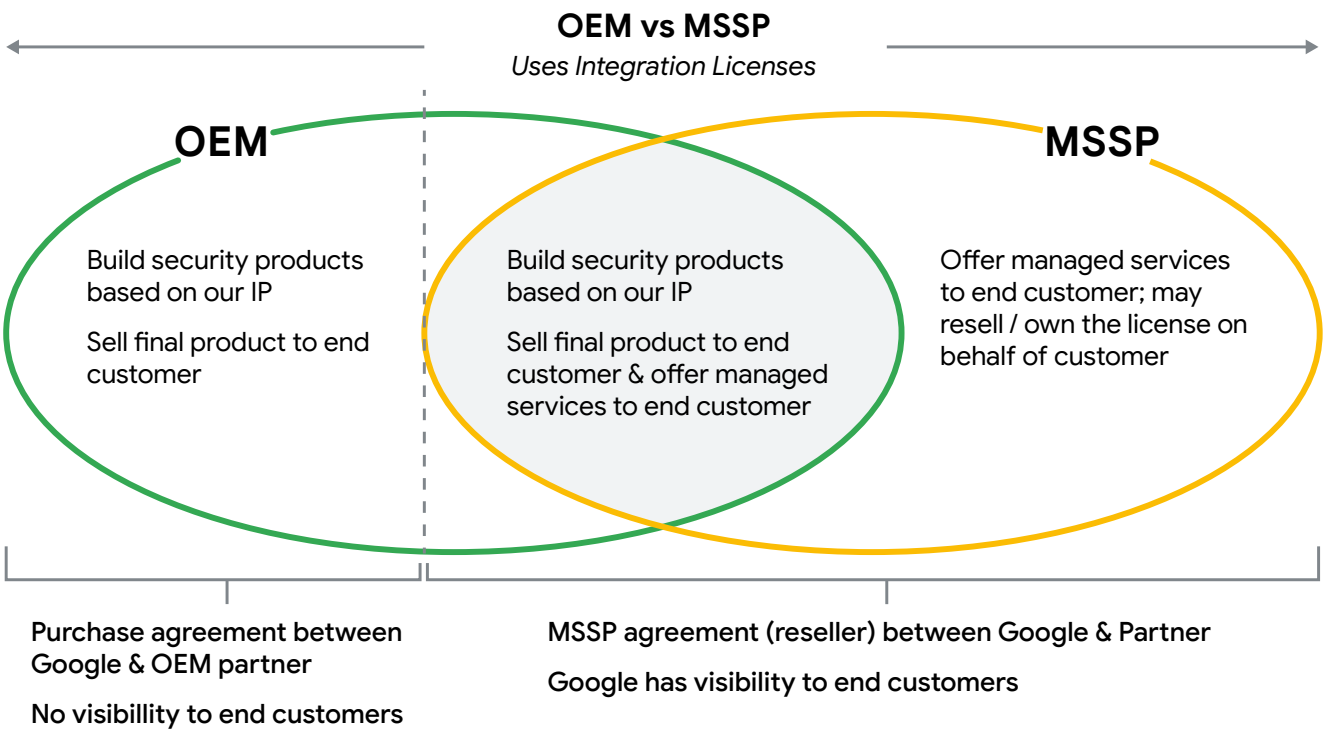
Enable your customers to:

- **Instantly Contextualize Alerts:** Automatically enrich alerts from your platform with Google's deep context. Turn a low-fidelity IP or file hash into a high-confidence verdict, complete with threat actor attribution, TTPs, and risk scoring. This drastically reduces triage time and analyst burnout.
- **Detect and Investigate from Day 1:** Integrate our curated detection rules (YARA, SIGMA, IDS) and high-fidelity feeds to proactively block threats before they execute, not just after.
- **Accelerate Investigation with AI:** Offer your customers the power of Gemini AI within your UI. Provide AI-assisted malware analysis and natural language summaries of threats, helping your users investigate and respond faster, regardless of their in-house talent.
- **Privately Scan Suspicious Artifacts:** Allow your users to privately submit files and URLs for analysis against the full power of Google Threat Intel, without sharing those submissions with the public community.
- **Manage Customer Exposure:** Move beyond reaction by offering services that continuously find and manage your customers' exposed assets and vulnerabilities that are actively being exploited.

A Partnership Model Built for Vendors

Our OEM program is built specifically for integration, allowing you to build new products, enhance existing ones, and create new revenue streams.

Your Business Benefit	Why It Matters
Differentiate Your Product	Stand out in a crowded market by enriching your alerts with unparalleled breadth and depth of visibility into threats with timely intelligence.
Increase Monetization	Create new, premium product tiers or add-on modules based on advanced intelligence, vulnerability, and AI features.
Win More Deals	Penetrate new target markets and win more competitive deals by solving a primary customer problem: alert fatigue and operational overhead.
Improve Customer Security	Drastically improve the security efficacy of your product, leading to higher customer satisfaction and retention.



Getting Started: OEM Core & Advanced

We offer two clear integration paths to fit your needs:

1. **OEM Core:** The perfect starting point to add powerful enrichment. This tier is most similar to what was included in **VirusTotal** data and includes:
    - Web Searching & IOC Lookups
    - Threat Reputation & Attribution
    - Threat Investigation & Tracking
    - Private Scanning
    - Out-of-the-Box Detection Rules
2. **OEM Advanced:** The complete solution for maximum differentiation. This includes **everything in Core** plus the full power of **Mandiant and Google curated data** and includes:
    - Vulnerability Intelligence
    - Gemini in Threat Intelligence
    - Advanced Threat Profiles
    - Ability to Share Insights with End Customers
    - *Continuous Threat & Exposure Management (CTEM) (Add-on)*

Become a Partner Today

Contact our OEM team to learn how you can build with Google Threat Intelligence

SecurityOEM@google.com