Google Cloud
Security

DATASHEET

Google Threat Intelligence

Highlights

- Threat intelligence directly from the frontlines
- Backed by insights from 1,100+ incident investigations annually
- Curated by 500+ global threat experts
- 350+ Threat actors tracked
- AI infused threat intelligence to improve security and reduce toil
- Protecting 4 billion devices online
- The world's largest threat observatory

Let's face it: being a security professional feels like a never-ending fire drill. Threat feeds flood your inbox, alerts scream for attention, and that nagging voice whispers, "Are you sure you're seeing the whole picture?" Prioritizing threats becomes a guessing game, while time—your most precious resource—slips through your fingers. You want to be more proactive but struggle to free yourself from the day-to-day reactionary process.

Google Threat Intelligence changes the threat intelligence game, bringing together insights from Mandiant frontline experts, the VirusTotal intel ecosystem and Google threat insights into a single offering giving you unmatched visibility and context on the threats that matter most to your organization.

Google Threat Intelligence leverages a very diverse collection of threat intel sources that are both broad reaching and deep. This diverse set of threat intelligence sources provides unmatched visibility into the threat landscape which should give you confidence that you are not missing threats and have the ability to take action quickly on the threats most relevant to you. No matter the size or security maturity of your organization you can rely on our expertise to provide the highest level of assistance—whether you need simple training or an embedded analyst we have you covered.

Know who’s targeting you with unmatched visibility

Google Threat Intelligence has unmatched visibility into threats enabling us to deliver detailed and timely threat intelligence to security teams around the world. With a diverse set of intelligence sources, Google is able to provide unmatched breadth and depth to this visibility.

Diverse intel sources provide unmatched breadth and depth

Google Threat Intelligence draws from stable of powerful sources, ensuring you have the most comprehensive and timely information:

- **Human-curated intelligence:** Our team of 500+ global threat analysts meticulously research, verify, and analyze information, providing high-quality, contextualized intelligence. Understand threat actor motivations, tactics, techniques, and procedures (TTPs), and identify likely targets.
- **Frontline intelligence:** Leveraging insights from 1,100+ incident investigations annually, Mandiant experts provide a detailed, contextual view of real-world threats. Stay ahead of the curve with up-to-the-minute information on adversary TTPs and the latest tools they leverage.

- **Crowdsourced intelligence:** VirusTotal, the world's largest crowdsourced intelligence platform, offers real-time visibility into emerging trends and indicators of compromise (IOCs). Tap into the collective knowledge of millions of users to proactively hunt for breaches and identify new threats.
- **Google threat insights:** Google monitors attacks and protects 4B devices and 1.5B mailboxes across the world. The more threats you see the better prepared you can be.
- **Open-source intelligence:** We continuously gather and analyze publicly available information, such as blogs, security forums, news articles, vendor reports, and social media. This cost-effective source provides a broad perspective on malware, vulnerabilities, and hacking trends.

The diversity of these sources, both broad and deep, allow us to connect the dots between a threat actor, a new phishing technique to distribute malware, and the payload characteristics of the malware. Putting all this together empowers you to see the full picture of your threat landscape, from emerging trends to specific attacks targeting your organization.

Turning insights into action

Google Threat Intelligence goes beyond a simple threat feed, providing actionable insights that empower your team to respond effectively. Our machine learning models prioritize threat analysis by surfacing the most relevant threats, helping you focus on what matters most and quickly assess potential impact. Gemini provides generative AI-powered assistance, distilling complex threat intelligence into easy-to-understand summaries so you can quickly grasp how adversaries might be targeting your organization and the broader threat landscape.

Respond to new and novel threats in minutes, not weeks by blanketing your event data with threat intel associations to reduce gaps. Fill in your blind spots and identify potential threat activity in your environment, maximizing containment and minimizing the potential impact. Dramatically reduce response times by leveraging the massive VirusTotal partner ecosystem. Seamlessly integrate threat intelligence directly into your existing security tools and workflows, either through native integrations or APIs, turning insights into automated actions, reducing manual effort and accelerating response times.

Looking for additional human touch? Access Mandiant experts directly within the Google Threat Intelligence console to get quick answers, validate findings, and receive tailored guidance to strengthen your security posture.

Partner with Google for threat intelligence excellence

No matter where you are in your threat intelligence journey, Google is here to help. Our team of experts can provide cyber threat Intel training, threat landscape assessments, and even dedicated analysts embedded within your team. Leverage our industry-leading expertise to accelerate your journey towards proactive, intelligence-led security.

Actionable threat intelligence at Google scale

Take Mandiant Threat Intelligence further with Google Threat Intelligence Gain deeper visibility into the threat landscape by leveraging Google's insights from over 4 billion devices and 1.5 billion email boxes. With access to threats targeting this extensive network, we can offer more comprehensive threat intelligence to you. Streamline workflows with Gemini, detecting threats faster and automating processes for simplified protection. Google Threat Intelligence enables you to leverage Mandiant's expertise while tapping into Google's vast resources for greater efficiency and insight.

Key features

Feature	Benefit
Gemini in threat intelligence	AI-driven workflows to help you find, understand, and share knowledge faster. Gemini helps simplify many time consuming analysis so you can be more proactive against threats targeting you.
Threat intel workbench	Get all threat intelligence tools, data, and pivoting capabilities are integrated within a single, trusted workbench—streamlining investigations and saving valuable time.
Unified verdict	Google Threat Intelligence pulls together inputs from Google's vast threat insights, Mandiant's frontline and human curated threat intelligence, and VirusTotal's massive threat collection to provide you with a single answer on whether an indicator or suspicious object is something you should prioritize or if it is benign, giving you confidence to take action quickly.
Private collections	Private collections offer a continuously updated, curated view of active threat campaigns and actors—replacing outdated static data sources.
Threat monitoring	Continuously track relevant threat activity and campaigns, accessing tactical and strategic intelligence for targeted mitigation and informed risk reduction. Extract real-world TTPs gleaned from malware analysis to stay ahead of evolving attacks and understand attacker methods.
Threat Campaigns	Prioritize your time by focusing on the most active threats targeting organizations like yours. Understand the tactics, techniques and procedures currently being used in active threat campaigns to be more proactive against the threats.
Threat Profiles	Personalize your experience to the most relevant threat intelligence. Quickly understand your threat landscape and what has changed. In a single dashboard, see an up-to-date view of who's targeting you, active campaigns, malware, and relevant vulnerabilities. Receive daily or weekly notifications on changes to your threat landscape to prepare the organization and stay ahead of the threats.