Trellix Private Global Threat Intelligence

Utilize Trellix Private Global Threat Intelligence for maximum protection of critical assets

For organizations with privacy requirements due to compliance or sensitive security requirements, Trellix offers the Trellix® Private Global Threat Intelligence (pGTI) packaged cloud solution for closed or hybrid networks. Our packaged approach provides you with up-to-date reputational services for use at the boundary and/or endpoints across your enterprise. Additionally, Trellix consolidates third-party threat feeds into a single service, delivering maximum protection for your critical assets.

The best environment to enhance threat intelligence is often one that combines both enterprise resources and a version of public or private cloud. Our private cloud and single-tenant-dedicated environment offers you the ability to securely tap into threat intelligence solutions and share critical information across your enterprise. Trellix has both on-premises and off-premises cloud offerings so that your organization can deploy global or regional cloud services.

Trellix Private GTI Use Cases

- **Closed Networks:** Trellix File/IP/URL reputations are available for our products, protecting your endpoints and perimeter.

- **Custom Reputations:** Private GTI Cloud stores up to 10 million of your reputations that supersede GTI Public Cloud reputations.

- **Analyst Research:** Your analysts have access to billions of File/Certificate/IP/URL reputations through a web-based and command-line interface.

- **Telemetry Data:** You have complete access to your pGTI query logs for advanced analytics to discover advanced threats.

- **Trellix pGTI Ecosystem:** Integrated in many of Trellix technologies such as endpoint, network, web, SIEM and sandbox.

- **Quick React/Short-Term Deployment:** pGTI 'in-a-box' can be installed for temporary network deployments, training sessions, and smaller offices.

RESTful Interface

The RESTful interface enhances the capabilities of pGTI. It not only allows the integration of third-party protection tools, it also integrates with custom analyst tools.

A root certificate authority is provided and allows for a server certificate and key to be generated to protect REST calls to pGTI. An API Key system has been created to allow or deny access to pGTI. Please note that these functions are controlled by Trellix Professional Services employees.

Query capabilities include File/Certificate/IP/URL reputation, custom reputation, reputation metadata, and historical file reputation. Queries can be in singular or bulk format. Insert capabilities include File/Certificate/IP/URL reputation and custom reputation.

How Trellix pGTI Cloud Helps Your Business

Reduce costs and maximize coverage

Trellix pGTI cloud protects and services large enterprise environments. We maximize coverage by providing availability to all devices capable of connecting to the Trellix public cloud. We reduce IT costs by providing a single source for reputational services without manual intervention. We also deploy faster than traditional distribution for connected products.

Scalability and performance

Our private cloud offering is based on the Trellix global point-of-presence (PoP) technology that serves billions of queries a day. The architecture provides organizations with scalability for enterprise demands. Trellix pGTI cloud protects and services heavy or unpredictable traffic with solid and proven performance capabilities.
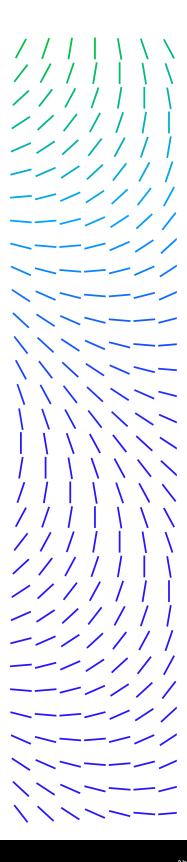
Security and custom reputations

When you need enhanced security and ultimate control for business-critical applications and data, incorporate the Trellix pGTI. It lets you add your own reputations into the cloud for tailored coverage and additional protections for known signatures.

Integration and Managing Reputations

Enterprise integration needs to be simple and powerful. Our RESTful interface provides integration with third-party tools and applications. This interface is tightly controlled with certificates and API key security to secure communications and transactions. Support for metadata tagging enriches the reputations stored in pGTI to assist analysts in their research.

Trellix pGTI provides threat reputation (File/Certificate/IP/URL) on a near real-time basis and allows clients to manage their own threat repository to inform boundary and endpoint protection.

Customers have the flexibility to override reputations in their local pGTI.

Trellix Private GTI is built on the latest GTI Public Cloud architecture that is installed around the world. This architecture handles approximately 65 billion queries per day, which is on par with Facebook and Twitter.

It can be scaled up to handle the largest enterprise deployments as well as small- to medium-sized offices.

Don't wait for the next attack to happen. Prevent it.

At Trellix, we give our customers the most comprehensive picture possible. Our cybersecurity experts track threat actors as well as campaigns, techniques, and tools the attackers use so we can better equip you to prevent future attacks and enhance your situational awareness giving you a more actionable view of threat exposures.

Want to learn more? Visit our Threat Intelligence page. And to learn more about Trellix's other products and services, visit trellix.com.