REVERSINGLABS

DATA SHEET

TitaniumCore Malware Analysis Solution

World's Fastest, Most Comprehensive Static Analysis for Threat Intelligence

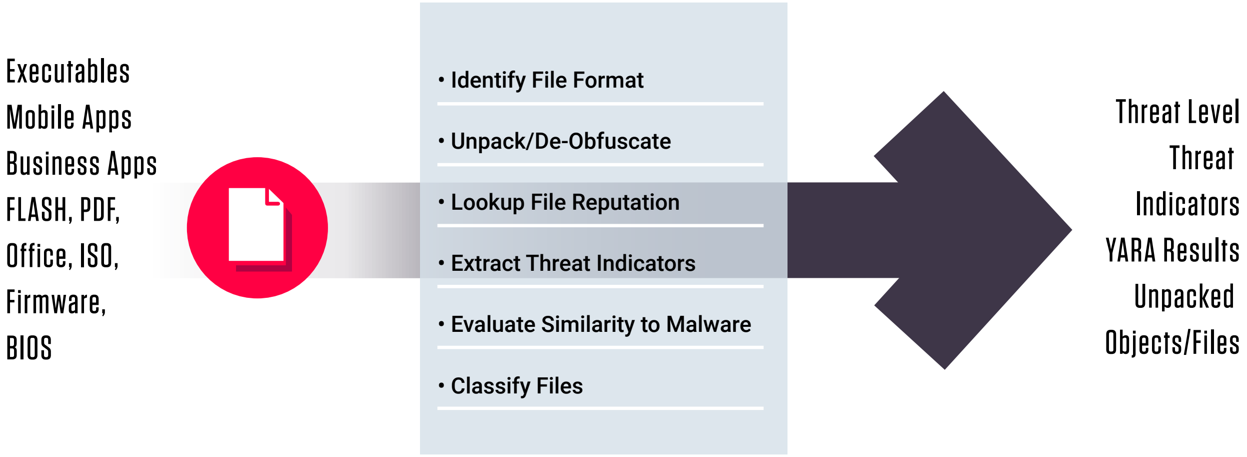
Key Benefits

- **Automated Static Analysis:** recursively unpacks, de-obfuscates, extracts internal indicators and assigns threat levels in milliseconds.
- **Unpacks over 360 File Formats:** including PE, ELF, MachO, Dex, .NET, Java, JS, documents, firmware, and business apps.
- **SDK for Integration:** includes API for file submission and access to unpacked files, extensive file metadata and threat calculations.
- **Customized Classification and Identification:** YARA rules supplied by ReversingLabs or written by the customer can help classify files and identify file formats.
- **Complements Sandbox and other Technologies:** performs lightning fast unpacking and analysis to pre-process files to make further analysis with tools such as sandboxes more productive and efficient.
- **Advanced Analysis Option:** optional integration with ReversingLabs' industry leading file reputation database and RHA analysis to identify functional similarity to known malware.

TitaniumCore uses highly scalable automated static analysis to recursively unpack and extract internal indicators to calculate threat levels of files to support real-time and/or high-volume applications. Under static analysis files are not required to be executed, this enables a detailed analysis to be performed in milliseconds versus minutes in the case of dynamic analysis. In addition, ReversingLabs' static analysis enables broad coverage, performing analysis on an extensive list of file types. TitaniumCore consists of software and an SDK for ntegration into advanced automated workflows, products and services.

High-Speed Analysis for a New Generation of Advanced Threats

TitaniumCore performs advanced file analysis at millisecond speeds with a powerful engine for applications of any scale from a few samples to millions of samples daily. The rules engine calculates threat levels based on rules provided by ReversingLabs and YARA rules supplied by the customer. Extracted files can automatically be routed to additional analysis tools (e.g., de-compilers, debuggers, sandboxes) or an analyst for further analysis based on threat levels and type to make the most efficient use of security assets. No other product (e.g., sandboxes or scanners) exposes the breadth and depth of threat indicators extracted by TitaniumCore.



Flexibility in Type of Metadata Collected by TitaniumCore

TitaniumCore allows the user to define which types of metadata will be collected. The metadata provides critical information not often available from other tools for determining the intent and capabilities of the sample.

- **Strings**: all strings present in any supported file format. Strings from executable file formats, such as PE or ELF.
- **Certificates**: all digital certificates that are recognized by the engine. This includes but is not limited to: Java, Authenticode, iOS™, Android™ and Windows Phone™ certificates.
- **Application**: all application file types including but not limited to PE, ELF, Mach-O, DEX, and Flash. Metadata that is extracted commonly covers class, function, and variable names with relevant data about file segments and resources.
- **Mobile**: all mobile applications and mobile application packages. Currently supported mobile platforms are: iOS™, Android™, and Windows Phone™.
- **Document**: document types such as PDF, RTF, CHM, and Microsoft Office.
- **Behavior**: static data about application behavior. Data presented within this metadata object shows all possibilities that can occur during application execution but not limited to the current application execution run.
- **Protection**: any kind of DRM or cryptographic content attached to any supported file type.
- **Security**: any kind of security-related information. In the list of exploits, you can see if the engine has detected any CVEs attached to a supported file type.
- **Media**: additional metadata present in multimedia formats. The most common example of such metadata would be EXIF information that shows relevant forensic data about a multimedia item.
- **Web**: web applications such as browser plugins. Currently supported browsers include but are not limited to Mozilla FireFox ™, Google Chrome™, Opera™, and Safari™.

Advanced File Analysis Option

The TitaniumCore Enterprise Platform extends the base TitaniumCore Solution with additional powerful capabilities to support more comprehensive analysis for enterprise applications, by adding:

- **ReversingLabs Hashing Algorithm (RHA) to calculate functional similarity to known malware.**
- **TitaniumCloud File Reputation Service integration to identify known goodware and malware.**

TitaniumCore Features

TitaniumCore Engine Automated Static Analysis

- Unique automated static analysis fully dissects internal contents of files without execution.
- Every sample processed to extract all objects and uncover threat indicators.
- 3600 file formats identified from PE/Windows, ELF/Linux, Mac OS, iOS, Android, firmware, FLASH, and documents.
- Over 360 file formats unpacked and analyzed including archives, installers, packers & compressors.

Results and Reports

- The platform produces detailed XML reports for consumption by backend systems and databases for further analysis.

TitaniumCore Enterprise Platform – Advanced Capabilities

- RHA functional similarity analysis.
- TitaniumCloud File Reputation Integration.

Detection Customization

- YARA-based rules matched on all decompressed content.
- Third party modules supported.

Integration Requirements

- Linux and Windows 64-bit platforms.
- Multi-threaded architecture fully utilizes underlying host processing to maximize file processing capacity.
- CLI and API (C, C++, Python, .NET) for integrating with automated workflows or OEM products.

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com