Bitdefender

DATASHEET

Advanced Threat Control SDK

Traditional anti-malware solutions can combat simple malware like trojans, but when it comes to advanced threats like code injections, file-less attacks or zero-day exploits, security service providers need a different approach. That is why Bitdefender built the ATC SDK.

The ATC SDK employs advanced heuristics and AI-powered behavioral analysis to detect malicious processes. It operates on a zero-trust principle, monitoring all active processes and tagging every potentially malicious action. Despite this, it maintains low false positives, and a marginal impact on performance.

At-A-Glance

The ATC SDK is a proactive, dynamic detection technology that monitors all processes on a Windows endpoint and tags suspicious activities. It is especially effective against file-less attacks, zero-day exploits, LotL attacks and other advanced threats.

Features

- **Proactive Detection:** The ATC SDK is effective against complex threats. It detects advanced attacks early, preventing costly breaches.
- **Industry-Leading Protection:** Bitdefender's anti-malware technology maintains 99,9% detection rates across industry tests, with minimal false positives.
- **Zero-Trust Approach:** The ATC SDK monitors all processes on a Windows machine. It also operates on the user, and kernel level, to detect malicious processes with escalated privilege.
- **AI-Powered Detection:** The ATC SDK employs several machine learning algorithms trained to identify any kind of malicious behavior.

Benefits

- **Low system impact:** The ATC SDK is optimized to use very few resources and monitor processes without affecting performance.
- **Quick Remediation:** The ATC SDK is designed to facilitate remediation and cleanup on detection.
- **Last Layer of Defense:** With its aggressive detection and behavior-based profiling, the ATC SDK is a must-have safety net when all other protection layers fail.
- **Dedicated Support:** The ATC SDK comes with code samples, comprehensive documentation, and dedicated support from an experienced team.

How The Bitdefender Sandbox Prefilter Works

The ATC SDK constantly monitors all processes on the protected endpoint. Each action taken by a process is given a score, based on how potentially malicious it is. Whenever the total score of a process exceeds a threshold set by the integrator, an alert is created.

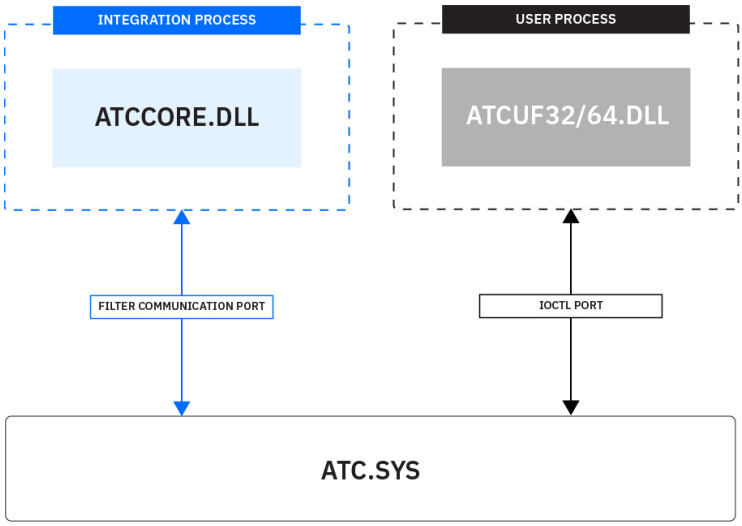
This can be used for further processing by an existing endpoint protection product, and integrators can set different remediation options, like killing the process, undoing the potentially malicious actions, or ignoring the alert.

The ATC SDK has three main components:

- ATC - A kernel-level filter which registers callbacks for notifications provided by Windows and injects ATC code into the monitored processes.
- ATCUF - A user-level component injected into running processes.
- ATCCORE - A user-level library allowing integrators to send commands to the kernel-level ATC component and receive notifications from it.

Bitdefender

DATASHEET



FREE Evaluation

Evaluating the Bitdefender ATC SDK is free of charge and includes technical support.

Contact us

For more information regarding the ATC SDK please reach us at **https://www.bitdefender.com/oem/contact-us.html**

26072024-Bitdefender-OEM-ATC_SDK-datasheet-creat7899-en_EN