Trellix

DATA SHEET

Trellix® Scan Engine

Get effective malware protection for embedded systems

Trellix Protection for Embedded Systems

- Includes the Trellix Scan Engine, .DAT files, and SDK
- Scans 32-bit and 64-bit program executables, Microsoft Office files, Adobe PDF and Flash files, Oracle Java, boot sectors, and other file formats
- Sees through the encryption used in compressed, archived, packed, and protected files
- Advanced heuristic analysis evaluates code behavior
- Generic detection identifies and cleans many viral variants
- Rigorous .DAT file testing minimizes false alarms
- Allowlisting of known clean files enhances scanning performance

The primary function of any anti-malware product is to find and remove viruses, worms, and other types of threats. The key measure of a product's anti-malware effectiveness is how well it isolates a threat and prevents it from spreading. It sounds easy, but it's a complex endeavor. The nature of threats has changed significantly in recent years, and is much more sophisticated and distributed.

Alongside traditional virus threats, there are now email worms, internet worms, distributed denial-of-service (DDoS) attacks, backdoor and remote access Trojans, spyware, rootkits, and advanced persistent threats. Many of these threats combine multiple attack vectors to maximize their chances of spreading quickly through global corporate networks.

It's not uncommon to see threats that blend multiple attack techniques, including mass mailing, infection via network shares, autoruns, exploits, or rootkits. Some try to terminate existing security controls, while others install Trojans, rootkits, or keyloggers to steal and exfiltrate credentials and data.

These advanced persistent threats have had a particularly marked effect, combining the use of system exploits—formerly associated with hacking activities—with the stealth capabilities of rootkits and backdoors. An increasing number of advanced persistent threats are designed to cash in on vulnerabilities in operating systems and applications. Threats that once required hours or days to propagate from one region to another are now exploited globally in minutes or less.

No matter how the exploits against our systems and data evolve, the challenge for our security controls remains the same—to find and remove the threat. The advanced scanning technology in the Trellix Scan Engine is the foundation of our response to the threats of yesterday, today, and tomorrow.

Supported Platforms

- Microsoft Windows (on Intel x86 and x64): Windows 7, 8.x, 10, and 11; Server 2008
- Microsoft Windows (only on Intel x64): Windows Server 2012, 2016, 2019, 2022, and 2025
- Microsoft Windows (on ARM64): Windows 10 and 11
- Linux 32-bit distributions shipping with version 2.6, 3.x, 4.x, or 5.x production kernels, with libstdc++.so.5.0.5 installed
- Linux 64-bit distributions shipping with version 2.6, 3.x, 4.x, 5.x, or 6.1 production kernels, with libstdc++.so.6 installed
- Linux ARM64 distributions shipping with version 3.13+, 4.x, or 5.x production kernels, with libstdc++.so.6 installed
- Sun Solaris (on SPARC): Versions 9, 10, and 11 with the latest Solaris OS recommended cluster installed
- Sun Solaris (x86): Version 10 and 11 with the latest Solaris OS recommended cluster installed
- FreeBSD (on Intel x86 and x64): FreeBSD 9.x–11.x with legacy compatibility library libc.so.3 installed
- FreeBSD (on Intel x64): FreeBSD 12.x, 13.2 with legacy compatibility library libc.so.3 installed
- IBM AIX (on RS6000): Versions 6.1, 7.1, and 7.2
- IBM AIX (IBM Power Systems): 7.3
- MacOS 10.13 High Sierra, MacOS 10.14 Mojave, MacOS 10.15 Catalina, MacOS 11.0 BigSur, MacOS 12.0 Monterey, MacOS 13.0 Ventura, MacOS 14.0 Sonoma, and MacOS 15.0 Sequoia
- HP-UX (on PA-RISC): Versions 11i v3

Trellix Scan Engine: Core Technology

The Trellix Scan Engine contains the functionality necessary to inspect 32-bit and 64-bit program executables, Microsoft Office files, Adobe PDF and Flash, Oracle Java, boot sectors, and other file formats that could conceal or be exploited by a piece of malicious code. Additionally, our scan engine is capable of inspecting encrypted, compressed, archived, packed, and protected files.

That's why it's essential to keep the engine updated. Each time a new operating system appears or a new type of file format becomes susceptible to infection, Trellix immediately adds support for it—always keeping the scan engine up to date and ready to protect your data.

Virus definitions

Understanding how to inspect different file structures is only part of the solution. It's just as important to know what to look for. Virus definition files, also known as .DAT files, store specific characteristics that identify a particular virus, worm, or Trojan. The .DAT files are released daily, with interim emergency releases for threats rated medium or higher by the Trellix Advanced Research Center.

Protection for Trellix customers

The scan engine and virus definition files operate in tandem to deliver effective protection for our customers. This core technology is wrapped into different product solutions, as appropriate for each platform and operating system. The same scan engine is integrated into all Trellix self-managed, antivirus solutions, including Trellix Endpoint Security, and it also forms the foundation of the Trellix Total Protection suites.

The Trellix AntiMalware Engine Software Development Kit (SDK)

Using the Trellix AntiMalware Engine SDK, application developers and managed service providers can integrate advanced scanning technology directly into their own solutions, enhancing what they offer to their customers. With the increase in outsourcing, customers have come to expect that effective protection from today's malicious code is automatically included in such services. Our AntiMalware Engine SDK, with its easy-to-implement, C-based application programming interface (API), makes it easy for Trellix embedded partners to deliver the protection their customers demand.

System Requirements

- At least 1024 MB of free hard disk space
- At least an additional 1024 MB of free hard disk space reserved for temporary files
- At least 1024 MB of RAM (2048 MB recommended minimum)
- At least 2048 MB of RAM for updating operations

Comprehensive scanning for today's and tomorrow's threats
The Trellix Scan Engine delivers comprehensive detection for all of today's threats—not only those found in the field, but also those that might become widespread at some point in the future. New threats appear all the time, and many of today's viruses, worms, and other threats travel at internet speed—they strike fast and move quickly. So a scan engine's ability to flag new, unknown pieces of malware is more important than ever.

Heuristic detection
Our advanced heuristic analysis lets us look through the code in a file to determine if the actions it takes are typical of a virus. The more virus-like code that's found, the more likely the file is to be infected. To reduce the risk of false alarms—identifying a virus when there isn't one—we combine positive heuristics with negative heuristics to search for those things that are distinctly non-virus-like.

Broad-based detection and cleaning
Generic detection involves using a single virus definition to detect and clean many variants of the same virus family. Of course, all threats must be detected, but it is much less efficient to build individual signatures for each one as they appear. Piecemeal detection isn't just less efficient—it also means that a new variant has the opportunity to spread before the scanner is able to detect it. The use of generics has also helped in managing the size of the .DAT files as the number of threats grows at a geometric rate.

The Trellix generic detection capability, developed over several years, has brought enormous benefits to Trellix customers by protecting them from threats such as ransomware, spyware, fake antivirus, Conficker, Sality, Virut, Zeus, and many others.

Ensuring confidence through accuracy
False alarms—mistakenly flagging a clean file as being infected—cost money and undermine confidence in a company's antivirus defenses. That's why it is essential to minimize the risk of false alarms. Every day, our .DAT files undergo rigorous quality-assurance testing on a test server containing multiple terabytes of real-world applications, minimizing the risk of costly false alarms.

Allowlisting technology
Our scan engine uses allowlisting technology for known clean Microsoft Windows operating system and popular software application files. This provides a significant performance benefit for both on-access and

on-demand scanning when these files are accessed. We continue to update the allowlist with qualifying information in line with new releases of popular software files.

Maintaining business continuity

Trellix scanners make full use of the engine's important ability to clean infected files. If a scanner simply flags an infection, the system administrator must replace the file—either from an original master disk, an installation DVD (in the case of .EXE files), or from a backup (for documents and spreadsheets)—if a backup even exists. If the scanner is able to clean the infected file, business continuity is maintained, downtime is minimized, and costs are reduced.

To learn more about Trellix, visit trellix.com.