Independent Tests of Cybersecurity Software

Operational Technology (OT) Certification Test 2026

Trellix Endpoint Security

TEST PERIOD: JANUARY 2026
LAST REVISION: 16TH FEBRUARY 2026

WWW.AV-COMPARATIVES.ORG

Introduction

Every year, AV-Comparatives conducts focused certification tests to which vendors can apply in order to validate specific security capabilities under clearly defined and realistic threat conditions. This certification focuses on the protection of Operational Technology (OT) environments against execution-based attacks under fully offline, post-breach conditions.

The convergence of Information Technology (IT) and Operational Technology (OT) has brought increased efficiency and connectivity to industries such as manufacturing, energy production, transportation, oil and gas, water management, and healthcare. At the same time, this convergence has expanded the attack surface of critical infrastructure systems, where security failures can lead to significant operational disruption, safety risks, or loss of availability. Unlike traditional IT systems, OT systems are often designed to operate continuously over long periods, may rely on legacy platforms, and are frequently deployed in environments with restricted or no internet connectivity.

Many security mechanisms commonly used in IT environments rely on continuous connectivity, cloud-based intelligence, or frequent signature updates. These assumptions often do not hold true in OT deployments, where systems are intentionally air-gapped or operate in fully offline environments for safety, reliability, or compliance reasons. As a result, security solutions that depend on external services may be ineffective or unsuitable in such contexts.

To address these constraints, OT-specific security strategies increasingly emphasize strict control over code execution. One of the most critical attack vectors in offline or air-gapped environments is the execution of untrusted binary code. Such execution may be initiated through direct user interaction, memory-based techniques such as code injection, DLL sideloading, or by using modified or impersonated binaries delivered via removable media. Preventing the execution of untrusted code is therefore a fundamental requirement for protecting OT systems after an attacker has obtained local access.

The AV-Comparatives Operational Technology Certification Test evaluates whether security products can prevent execution-based attacks under these conditions. All test scenarios assume a post-breach situation in which an attacker already has local access to the system, for example through insider threats, physical compromise, or removable media, and attempts to execute malicious code using techniques designed to evade traditional detection mechanisms. The focus of the certification is on protecting system integrity and operational continuity in fully offline environments.

Multiple security products were evaluated as part of the AV-Comparatives Operational Technology Certification Test using identical infrastructure and a uniform methodology. Certification reports are published only for products that meet the certification requirements. Tested vendors receive detailed technical feedback on the executed test cases and observed product behaviour to support further product improvement.

This report documents the certification results for **Trellix** only, based on the results achieved by the tested product in the Operational Technology Certification Test.

OT and Zero-Trust Certification Tracks

AV-Comparatives offers two closely related but distinct certification tracks for execution-based protection: the **Operational Technology (OT)** Certification and the **Zero-Trust (ZT)** Certification. While both certifications are based on a similar core methodology and evaluate the prevention of untrusted code execution under post-breach conditions, they are designed to reflect different operational realities and deployment assumptions.

The OT Certification is designed specifically for industrial and critical infrastructure environments where systems are fully offline or air-gapped. In this certification track, products are tested on **Windows 10** systems operating in a **completely offline environment**, without any cloud connectivity or access to external intelligence services. This reflects common OT deployment scenarios, where internet connectivity is unavailable or intentionally disabled for safety, reliability, or compliance reasons.

The Zero-Trust (ZT) Certification, by contrast, is intended for enterprise environments where continuous connectivity is available and expected. In this certification track, products are tested on **Windows 11** systems with **active cloud connectivity**. This allows the evaluation of zero-trust enforcement models that rely on centralized policy management, cloud-assisted intelligence, or continuous trust validation.

Although the underlying test methodology is conceptually similar in both certification tracks, focusing on execution-based attacks and post-breach scenarios, the environmental assumptions differ significantly. A product that depends on cloud connectivity to make trust decisions may perform well in a connected zero-trust environment but cannot be assumed to provide the same level of protection in an air-gapped OT deployment.

For this reason, AV-Comparatives does not award OT Certification to products that require active cloud connectivity in order to enforce their protection model. In OT environments, where cloud access is typically unavailable, such products would not be able to operate as intended. This distinction ensures that the OT Certification accurately reflects real-world OT deployment constraints and provides meaningful guidance to organizations operating critical infrastructure.

Test Procedure

The goal of this certification test is to evaluate whether a security product can effectively prevent execution-based attacks in post-breach scenarios under conditions that reflect real-world Operational Technology (OT) deployments. The test focuses on the ability of a product to prevent or detect the execution of untrusted binary code when an attacker already has local access to the system.

AV-Comparatives offers two closely related certification tracks based on the same core methodology: the **Operational Technology (OT) Certification** and the **Zero-Trust (ZT) Certification**. While both certifications evaluate execution-based protection in post-breach scenarios, they differ in their environmental assumptions and technical setup in order to reflect distinct deployment realities.

For the **Operational Technology (OT) Certification**, products are tested on **Windows 10** systems operating in a **fully offline and air-gapped environment**. No internet connectivity or access to cloud-based services is available at any point during testing. This setup reflects common OT environments, where systems are intentionally isolated and must rely exclusively on local protection mechanisms. Products that require active cloud connectivity in order to enforce trust decisions are therefore not eligible for OT Certification, as such dependencies would not be viable in real-world OT deployments. For the **Zero-Trust (ZT) Certification**, products are tested on **Windows 11** systems with **active cloud connectivity**. This allows evaluation of protection models that rely on centralized policy management, continuous trust evaluation, or cloud-assisted intelligence. Although the execution-based attack techniques and test logic remain fundamentally the same, the availability of connectivity represents a materially different operational context.

This report documents the results of the **Operational Technology Certification**, and all testing described below was conducted under fully offline conditions.

All systems under test were deployed in dedicated, isolated environments and were not connected to any external networks. The test scenarios simulate a situation in which an attacker has already obtained local access to the system, for example through insider activity, physical access, or removable media. The objective is to determine whether the security product can prevent the execution of untrusted code under these constraints.

To reflect realistic OT attack conditions, the test emphasizes execution-based techniques that do not rely on network communication or external infrastructure. This includes both file-based and memory-based execution paths, such as the execution of shellcode, DLL sideloading, binary impersonation, and the use of modified or backdoored executables. The evaluation does not cover initial compromise, persistence mechanisms beyond execution, or command-and-control communication.

All malicious components and legitimate software used during testing were delivered via removable media, such as USB drives. In addition to the core attack scenarios, an application update test was performed using a legitimate offline installer delivered via removable media. This test assesses whether the product can distinguish malicious execution attempts from valid administrative workflows, which is essential to avoid operational disruption in air-gapped OT environments. The test methodology is designed to assess execution control under post-breach conditions and is applied consistently across all products participating in the certification. Results are evaluated based on whether execution attempts are prevented or detected with an active alert, in accordance with the certification requirements.

Application Update Test

In addition to the execution-based attack scenarios, an application update test was conducted to evaluate whether the tested product can correctly distinguish between malicious execution attempts and legitimate software execution under fully offline conditions.

The test simulates a typical offline update process commonly observed in OT environments. An existing application is updated using a signed installer delivered via removable media. The update procedure includes file modifications and writes to system directories and is intended to reflect a realistic administrative workflow performed without access to cloud-based verification or external reputation services.

Correct handling of this scenario is essential in air-gapped OT environments. Blocking or corrupting legitimate update processes can result in loss of functionality or operational downtime, while allowing malicious code under the guise of an update represents a security risk. Successful certification therefore requires both effective enforcement against malicious execution and correct handling of legitimate offline updates.

Test Setup & Workflow

Each security product was evaluated on a dedicated Windows 10 workstation, configured to operate in fully offline mode. These systems were completely air-gapped and not connected to the internet at any point during testing. All attack scenarios, including the application update scenario, were performed under these offline conditions. To reflect real-world constraints in OT environments, USB drives were used to deliver all software components. This included the deployment of malicious payloads for the core attack scenarios, as well as legitimate software updates used in the application update test. This setup mirrors common infection and update vectors in isolated systems, where network-based delivery is not feasible.

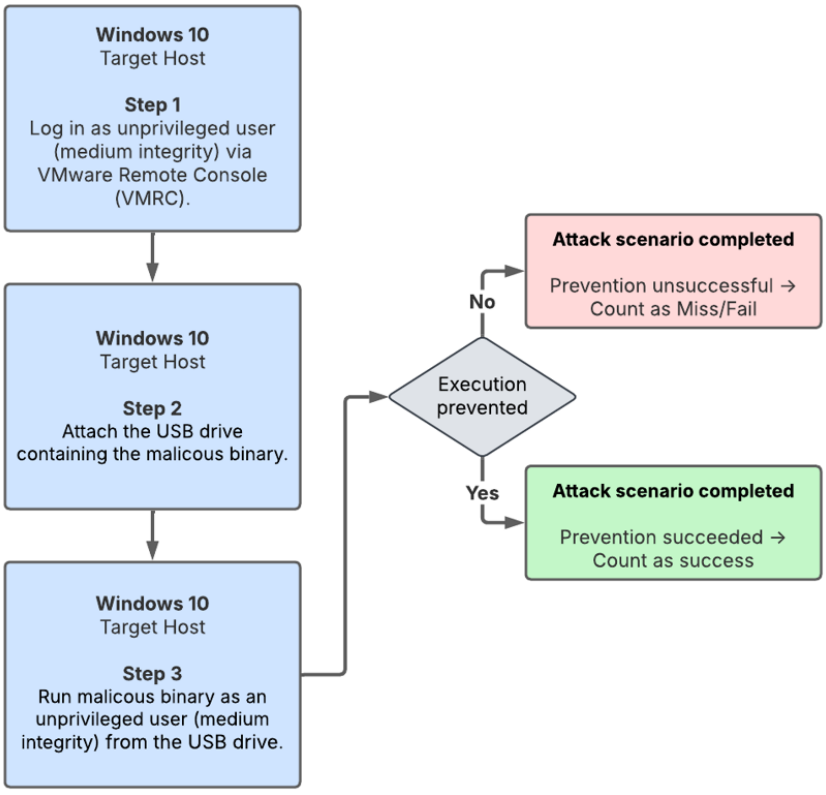


Figure 1 Test Setup & Workflow

Attack Scenarios

To evaluate the enforcement capabilities of the tested product in offline environments, AV-Comparatives designed a set of execution-based attack scenarios simulating realistic post-breach conditions. Each scenario attempts to execute untrusted code using techniques commonly observed in adversarial activity, with the goal of assessing whether the product can prevent or detect execution attempts without relying on cloud connectivity or internet-based validation.

For the Operational Technology Certification, five to eight scenarios are used each year. The exact scenarios vary between test cycles, while the high-level structure and objectives remain consistent to ensure comparability over time. In the test cycle covered by this report, five scenarios were executed.

Unless otherwise stated, all actions were performed by a **local user with medium integrity**, reflecting realistic post-compromise conditions in OT environments.

Case 1: Binary with Legitimate Metadata

This scenario evaluates whether execution is permitted when a malicious binary mimics the metadata of a legitimate application previously observed during the product's deployment phase. Selected metadata attributes from a trusted application are applied to a custom shellcode launcher to assess whether metadata-based impersonation is sufficient to bypass execution enforcement.

Relevant techniques: Replication Through Removable Media (T1091), User Execution (T1204), Masquerading: Rename System Utilities (T1036.003)

Case 2: Binary with Legitimate Metadata and an Invalid Certificate

This scenario extends the first case by combining legitimate-looking metadata with a deliberately invalid code-signing certificate. The objective is to determine whether enforcement decisions rely solely on metadata or also incorporate certificate validation, even under fully offline conditions.

Relevant techniques: Replication Through Removable Media (T1091), User Execution (T1204), Masquerading: Rename System Utilities (T1036.003), Masquerading: Invalid Code Signature (T1036.001)

Case 3: Binary with Legitimate Metadata and a Leaked Certificate

In this scenario, a custom binary mimics a previously observed legitimate application and is additionally signed using a leaked but valid code-signing certificate. This represents a more advanced impersonation technique and tests whether trust enforcement mechanisms remain effective when both metadata and certificate information appear legitimate.

Relevant techniques: Replication Through Removable Media (T1091), User Execution (T1204), Masquerading: Rename System Utilities (T1036.003), Subvert Trust Controls: Code Signing (T1553.002)

Case 4: DLL Sideloading

This scenario evaluates whether execution enforcement can be bypassed through DLL sideloading. A legitimate executable already present during the deployment phase is used to load a malicious DLL containing shellcode. The objective is to assess whether execution via a trusted host process allows the malicious payload to evade protection.

Relevant techniques: Replication Through Removable Media (T1091), User Execution (T1204), Hijack Execution Flow: DLL Side-Loading (T1574.002)

Case 5: Backdoored Binary

In the final scenario, a legitimate application present during deployment is modified to include and execute shellcode while retaining its original metadata. This test evaluates whether prior trust in a known binary persists after unauthorized modification.

Relevant techniques: Replication Through Removable Media (T1091), User Execution (T1204), Compromise Host Software Binary (T1554)

Application Update Test

In addition to the malicious execution scenarios above, an application update test was conducted to evaluate whether the tested product can correctly distinguish between malicious activity and legitimate software execution under fully offline conditions.

The scenario simulates a typical offline update process in an OT environment. An existing application is updated using a signed installer delivered via removable media. The update includes file modifications and writes to system directories and is performed by a local user with medium integrity. Correct handling of this scenario is essential to avoid operational disruption, while still enforcing execution control against malicious code.

Scope

The scope of this certification test is limited to evaluating the ability of the tested product to prevent or detect execution-based attacks in fully offline Operational Technology (OT) environments under post-breach conditions.

The evaluation focuses on scenarios in which an attacker has already obtained local access to the system and attempts to execute untrusted binary code. The objective is to assess whether the security product can prevent such execution or detect it with an active alert, either locally on the endpoint or via the product's management interface, depending on the product architecture.

The certification test covers execution techniques that are particularly relevant to air-gapped and offline OT environments, including:

- Execution of binaries impersonating legitimate applications
- Execution of binaries using invalid or misused code-signing certificates
- Execution of binaries signed with leaked or compromised certificates
- DLL sideloading via trusted executables
- Execution of modified or backdoored binaries
- Memory-based execution paths, including execution of shellcode

In addition to malicious execution attempts, the scope includes a legitimate **offline application update scenario** delivered via removable media. This test evaluates whether the product can correctly distinguish between malicious activity and a valid administrative workflow, which is essential to avoid operational disruption in production OT environments. All evaluations are performed under fully offline conditions, without access to internet connectivity, cloud-based services, or external reputation systems. Results reflect the behaviour of the tested product under these specific conditions and with the applied configuration.

Out of Scope

The following aspects are not evaluated in this certification test and are therefore out of scope:

- Initial access techniques, including phishing, exploitation of remote services, or other pre-compromise infection vectors
- Network-based attacks, lateral movement over a network, or command-and-control communication
- Cloud-assisted detection mechanisms, online reputation services, or internet-based telemetry
- Threat hunting, forensic investigation, or analyst-driven activities within management consoles
- Evaluation of persistence mechanisms beyond what is required to execute the defined test scenarios
- Assessment of the overall security posture or hardening of the operating system outside the tested product
- Availability, performance, or usability testing beyond the handling of execution attempts and the offline update scenario

The certification does not aim to assess complete attack chains or full enterprise detection and response capabilities. It is deliberately focused on execution control in offline, post-breach OT environments, in accordance with the defined certification scope.

Tested Product and Used Settings

In this certification test, performed in January 2026, the following up-to-date and publicly available product was used: **Trellix Endpoint Security 10.7**

In OT environments, security products are commonly configured on a case-by-case basis to reflect the specific infrastructure and operational requirements. For this test, the product was configured in a hardened, security-focused configuration appropriate for an OT environment.

Trellix[1]**:** In Adaptive Threat Protection, "Rule Assignment" was set to "Security". "ML Protect Scanning" set to "High". "Enable offline scanning" activated. In "Action Enforcement", the reputation thresholds were set to "Might Be Trusted", "Unknown", and "Might Be Malicious". "Monitor and remediate deleted and changed files" was enabled. The containment rule "Creating files with the .exe extension" was set to "Block".

Please note that the results reached are valid only for the tested product with its respective settings. With other settings, the certification requirements might not be reached.

[1] The “ENS” version of **Trellix** in this test uses the erstwhile **McAfee** engine (now owned by Trellix), opposed to the “HX” version which uses the FireEye engine (McAfee Enterprise and FireEye were merged into Trellix in 2022).

AV-Comparatives Operational Technology Certification

To be approved by AV-Comparatives for **Operational Technology** Protection, a product must meet **all** of the following requirements under the conditions defined for the OT Certification track.

Environmental Requirements

- The product must be capable of operating and enforcing its protection mechanisms in a fully offline, air-gapped environment.
- All certification testing for OT Protection is conducted on Windows 10 systems with no internet connectivity and no access to cloud-based services at any point during testing.
- Products that require active cloud connectivity, external reputation services, or continuous online policy evaluation in order to make trust or enforcement decisions are not eligible for OT Certification. They must apply for Zero-Trust (ZT) Certification.

These requirements reflect real-world OT deployment constraints, where systems are commonly isolated for safety, reliability, or compliance reasons.

Configuration and Testing Conditions

- Each product is tested once, using the specific version and configuration provided by the vendor prior to the start of testing. Vendors can only apply once per year for this certification.
- Vendors are responsible for selecting and validating the configuration they submit for certification.
- No reconfiguration, tuning, or policy changes are permitted after testing has begun.
- No retesting is performed for the purpose of achieving certification, regardless of test outcome.

This approach ensures fairness, consistency, and comparability across all products and reflects real-world deployment conditions, where protection must be effective at the time of use and not rely on post-hoc adjustments.

Technical Certification Criteria

To achieve OT Protection Certification, a product must:

1. **Successfully prevent all defined execution-based attack scenarios executed under the certification conditions.**
   The product must successfully prevent all malicious execution attempts executed under post-breach, fully offline conditions.
2. **Demonstrate consistent enforcement**
   Prevention must occur at the time of execution, by blocking the execution. Silent failures or post-execution detections without an active alert are not considered sufficient.
3. **Correctly handle a legitimate offline application update**
   In addition to malicious scenarios, the product must correctly handle a legitimate offline application update delivered via removable media. The update must complete successfully without breaking the updated application or causing operational disruption under the tested configuration.
4. **Operate within the tested configuration**
   Certification results are valid only for the specific product version and configuration tested. Protection outcomes may differ with alternative configurations. Vendors and users are responsible for ensuring that equivalent or stronger configurations are applied in production environments.

Pass / Fail Determination

- A product is **certified** if it meets all environmental requirements and satisfies the technical certification criteria defined above.
- If a product fails to meet the minimum execution-based protection threshold or disrupts the legitimate offline update scenario, the certification requirements are **not met**.
- Only products that meet the certification requirements are eligible for a public certification report.

Relationship to Zero-Trust (ZT) Certification

AV-Comparatives also offers a **Zero-Trust (ZT) Certification**, which evaluates similar execution-based attack scenarios but under **connected environments** using **Windows 11** systems with active cloud connectivity. While the core test methodology is conceptually similar, the operational assumptions differ.

A product that qualifies for ZT Certification does **not automatically qualify** for OT Certification. The OT Certification is awarded only to products that demonstrate effective protection **without reliance on cloud connectivity**, in accordance with the constraints of air-gapped OT environments.

The certification methodology is reviewed and updated periodically to reflect evolving threat techniques while maintaining consistent evaluation principles.

Test Cases, Results and Certification Verdict

To be approved by AV-Comparatives for Operational Technology (OT) protection, a product must have successfully prevented all the malicious test scenarios without blocking the legitimate update scenario.

Only products which were submitted for the Operational Technology Test, and which passed the test, are published.

Successfully prevented all execution-based offline post-breach attack scenarios. In the application update scenario, the product handled the legitimate offline update correctly under the tested configuration.	✔

Based on these results, **Trellix Endpoint Security** is awarded the AV-Comparatives Operational Technology Protection Certification.

The following scenarios were tested:

Untrusted scenarios	Binary with Legitimate Metadata	**PASS – Execution Prevented**
	Binary with Legitimate Metadata and an Invalid Certificate	**PASS – Execution Prevented**
	Binary with Legitimate Metadata and a Leaked Certificate	**PASS – Execution Prevented**
	DLL Sideloading	**PASS – Execution Prevented**
	Backdoored Binary	**PASS – Execution Prevented**
Trusted scenario	Offline Application Update (legitimate update delivered via USB)	**PASS – Handled Correctly**

Key

- **PASS** (untrusted scenarios): The product successfully blocked the execution of an untrusted or malicious component at execution time.
- **PASS** (trusted scenario): The product correctly allowed or handled a legitimate action (e.g. offline update) without incorrectly blocking it.
- **FAIL**: The product either allowed an untrusted execution attempt or incorrectly blocked a legitimate action.

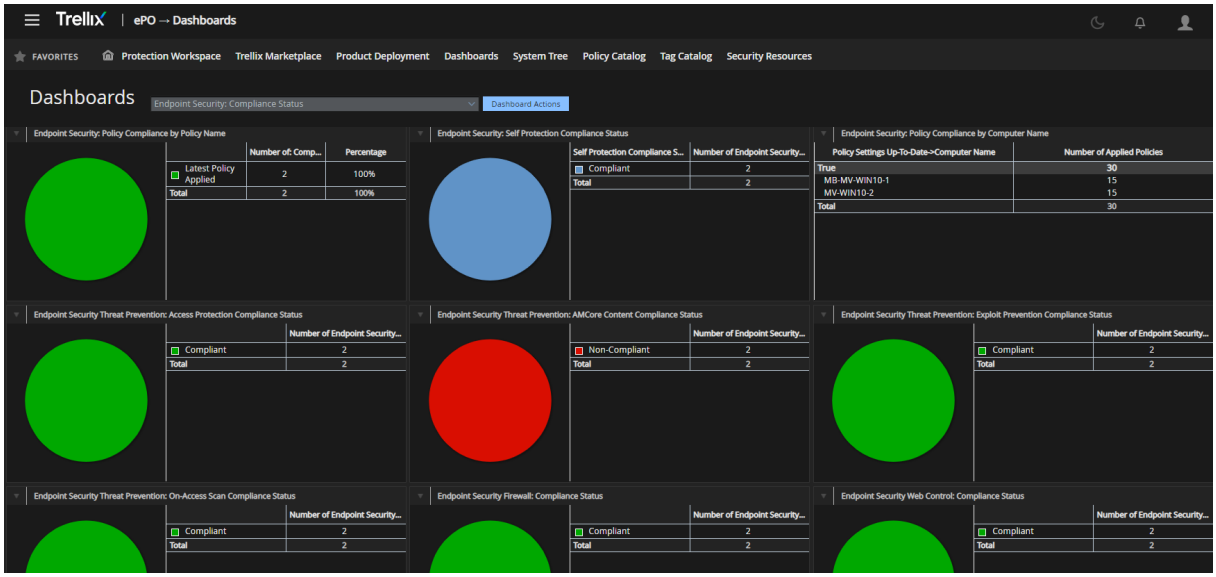
Notes and Comments:

Trellix Endpoint Security successfully prevented all execution-based offline post-breach attack scenarios. In the application update scenario, the product handled the legitimate offline update correctly under the tested configuration.

The tested malicious scenarios were mainly blocked by Trellix's *Adaptive Threat Protection* module.

Product Overview[2]: Trellix Endpoint Security (ENS)

Trellix Endpoint Security (ENS) is a comprehensive security solution designed for enterprise networks of all sizes. The ePolicy Orchestrator management console offers flexible options, including both cloud-based and on-premises consoles, for efficient management of the endpoint protection software.



Key Features

Customizable Dashboard: The dashboard and reporting can be tailored to display relevant endpoint status information for each user.

Deployment Flexibility: The console offers a variety of deployment options, including cloud-based, on-premises hosting, and Amazon hosting.

Management Console: The ePolicy Orchestrator console is easily accessed through the primary navigation menu located at the top left of the main dashboard. It provides access to different sections and pages, such as *Dashboard*, *Reporting*, *Policy Management*, *Automation*, and *Software and Systems Administration*. Integration of additional components like DLP, Mobile Security, and Insights Threat Intelligence and EDR is also available.

[2] *Note: This product description page was provided by Trellix. It is included here for informational purposes only and does not represent an endorsement by AV-Comparatives.*

ML Protect: Through machine learning classification, threats are detected in real time, and behaviour classification continually evolves to identify future attacks. Endpoints are restored to the last known good state, preventing infections and reducing administrative burdens.

Adaptive Scanning: The system intelligently skips scanning trusted processes and gives priority to suspicious processes and applications during scanning.

Endpoint Client Deployment: Client agent packages can be created on the Product Deployment page. The installer file can be distributed via a web link, manually executed, or deployed through a systems management product. After installation, the agent downloads the necessary protection engine before full protection becomes active. The client interface displays the installed and enabled protection components.

Web Control: This feature ensures safe browsing by providing web protection and filtering for endpoints.

Hostile network attack blocking: The integrated firewall utilizes reputation scores based on GTI to safeguard endpoints against botnets, DDoS attacks, advanced persistent threats, and suspicious web connections. During system startup, the firewall only allows outbound traffic, providing protection when endpoints are not connected to the corporate network.

Antimalware protection: Trellix protects, detects, and corrects malware quickly with an antimalware engine that works across multiple devices and operating systems.

Further product details are available at: https://www.trellix.com/en-us/assets/solution-briefs/trellix-endpoint-protection-platform-solution-brief.pdf

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(February 2026)