



## Advanced Threat Protection TEST Results

20数年前から定期実施されているファイルスキャンによる検出試験とは異なり、ベンダーに対して毎回試験内容および参加の是非が聞かれる。(AV TEST社は意味のない試験から撤退か?) ある程度時間が経過しているため標的型攻撃の最新検体を得ているが、実際の攻撃手法をシミュレートしているため試験内容により自信のあるベンダーが参加する。(非参加=自信なし?) VirusTotalを利用した最新の脅威に対する防御能力の試験結果と、参加ベンダーには因果関係がある [【最近の脅威をVirusTotalで検出できるか試験した調査】](#) も参照ください。本試験は、直近2か月(公表月の1年~5か月前)に検出された標的型攻撃やランサムウェア検体を用いて実際の攻撃手法をMITRE ATT&CKに則り実施される。試験は公表月の3か月前から実施され、公表月の2か月前に完了する。その結果は参加ベンダーに対して試験結果が伝えられ、公表の是非が公表迄の間に調整される。

公表月	タイトルと記事リンク	TOP スコア	Acronis	AhnLab	Avast	AVG	Avira	BitDefender	BullGuard	Carbon Black	Check Point	Comodo	F-Secure	G DATA	Kaspersky	Malwarebytes	McAfee	Microsoft	Microworld	Norton	PC Matic	Sangpr	Seqrite	Sophos	Symantec	Total AV	Trellix	VIPRE	WithSecure	Xcitium	
2024年2月	<a href="#">More Protection Against Encryption and Data Theft</a>	30		30	30	30	24	30		30	30		30		30		30	27	27.5	30	30				30		30				
2023年12月	<a href="#">ATP Test: Defending Against Data Stealers and Ransomware</a>	30	30	30	30	30				27	30		30		30	30	30	30		30	30		30		30				30		
2023年10月	<a href="#">27 Protection Solutions Pitted against Data Stealers and Ransomware</a>	35	35	35	35	35	32	35			35		35		35	35	35	35			35		35		35				35	35	
2023年7月	<a href="#">Advanced Threat Protection against the latest Data Stealers and Ransomw</a>	35	35	35				35		31	35		35		35	35	35	35	35	35	35		35		35				31.5		35
2023年5月	<a href="#">Fending off Ransomware even Against State-of-the-art Attack Techniques</a>	30		27				30						30	30		30	30	29	27.5	30								25.5		
2023年1月	<a href="#">Do Security Solutions stop Current Ransomware under Windows 11?</a>	30	30	24.5				29		30	30			27.5	30			30	28.5	29	30				30		30	27		30	
2022年3月	<a href="#">29 Protection Solutions against Data Stealers and Ransomware under Win</a>	45		45	45	45		45	40	45		45	45	45		45	45	45	45	45	45	45		45	45	40		45			
2021年12月	<a href="#">9 Security Packages for Consumer Users in an Advanced Threat Protectio</a>	34						31.5	28					34		34		34								28		34			



AV-TESTによる本試験は、AMTSO社によるAVエンジン試験評価標準化を用い、各社のマルウェア対策ソリューションの試験に関連し、テスターおよびベンダーに期待されるテストプロトコルおよびエンジン挙動が詳細に規定されており、これに準拠した形で実施されています。具体的には、実際に行われた脅威をMITRE ATT&CK®に準拠し攻撃をシミュレートした形で実施されます。

### See also



AV Engine detections by VirusTotal from the latest security columns (新マルウェア起動防御率)  
[https://pcmatic.jp/pro/security/Detection\\_realscore.pdf](https://pcmatic.jp/pro/security/Detection_realscore.pdf)