2025 Cyber-Incidents in Numbers

Period Covered by Report January 01st - December 31st, 2025

Date of the report: March 06th, 2026

SITS

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

In Focus –

2025 Cyber Threat Analysis in Europe – Trends, Structural Shifts and Projections

The 2025 telemetry identifies a fractured security landscape across Europe, defined by extreme variances in attack volume and vector composition. At the forefront of this activity is Ukraine, which remains the primary focal point of high-volume cyber activity in the region. Recording the highest singular incident count (916), its threat profile is monolithic: 95% of all recorded events are DDoS attacks, indicating a sustained, high-intensity campaign aimed purely at infrastructure saturation. A similar statistical footprint is observed in Israel (753 incidents), where the combination of massive DDoS volumes and a high number of unspecified intrusions creates a highly volatile threat environment that remains distinct from the European average.

In stark contrast to these singular focus zones, Western European nations—led by Germany (763), France (548), and the United Kingdom (407)—face a far more diversified "multi-vector" threat. Unlike the conflict zones, these nations are not subject to a single dominant attack type but must manage a complex mix of hostile activity. Germany, for instance, records a near-even split between disruptive DDoS attacks (466) and extortive Ransomware incidents (226). This data suggests that security operations centres (SOCs) in major Western economies face the highest operational complexity, as they are required to simultaneously defend against volumetric network saturation and sophisticated encryption payloads.

This complexity fades again on the EU's eastern flank, where the data reveals a statistically uniform attack composition in Poland and Lithuania. Despite lower total volumes than their Western counterparts, their attack composition is the most uniform in the dataset. Lithuania records a 97% DDoS share, while Poland sees 94% of its incidents as DDoS attacks. The near-total absence of ransomware in these figures highlights a targeted shift in adversary tactics on the eastern border, focusing almost exclusively on service degradation rather than financial extortion.

Country	Ransomware	DDoS	Unspecified	All Attacks
Ukraine	2	877	37	916
Germany	226	466	71	763
Israel	9	519	225	753
Italy	123	371	81	575
France	133	375	40	548
United Kingdom	192	157	58	407
Poland	14	356	7	377
Spain	112	243	13	368
Belgium	35	260	6	301
Lithuania	2	180	3	185
Denmark	13	122	1	136
Finland	5	116	2	123
Switzerland	47	59	15	121
Turkey	9	101	7	117
Netherlands	26	65	7	98
Czechia	15	41	6	62

Sweden	32	24	3	59
Cyprus	6	43	1	50
Romania	7	37	5	49
Austria	29	11	7	47
Norway	12	30	2	44
Russia	3	15	20	38
Portugal	13	12	1	26
Luxembourg	6	15	1	22

Table 1: Presents a tabulated summary of cyber-attacks for the top 24 European countries attacked in 2025, categorised by type: Ransomware, DDoS, Unspecified, and the total number of attacks for each country.

2025 Cyber Risk Density: Attacks per Million Inhabitants

While absolute incident numbers naturally emphasise populous nations, a normalised analysis based on population size reveals a fundamentally different risk landscape. Adjusting for demographic data highlights that smaller, strategically positioned nations often face a higher intensity of cyber aggression than larger economic powers.

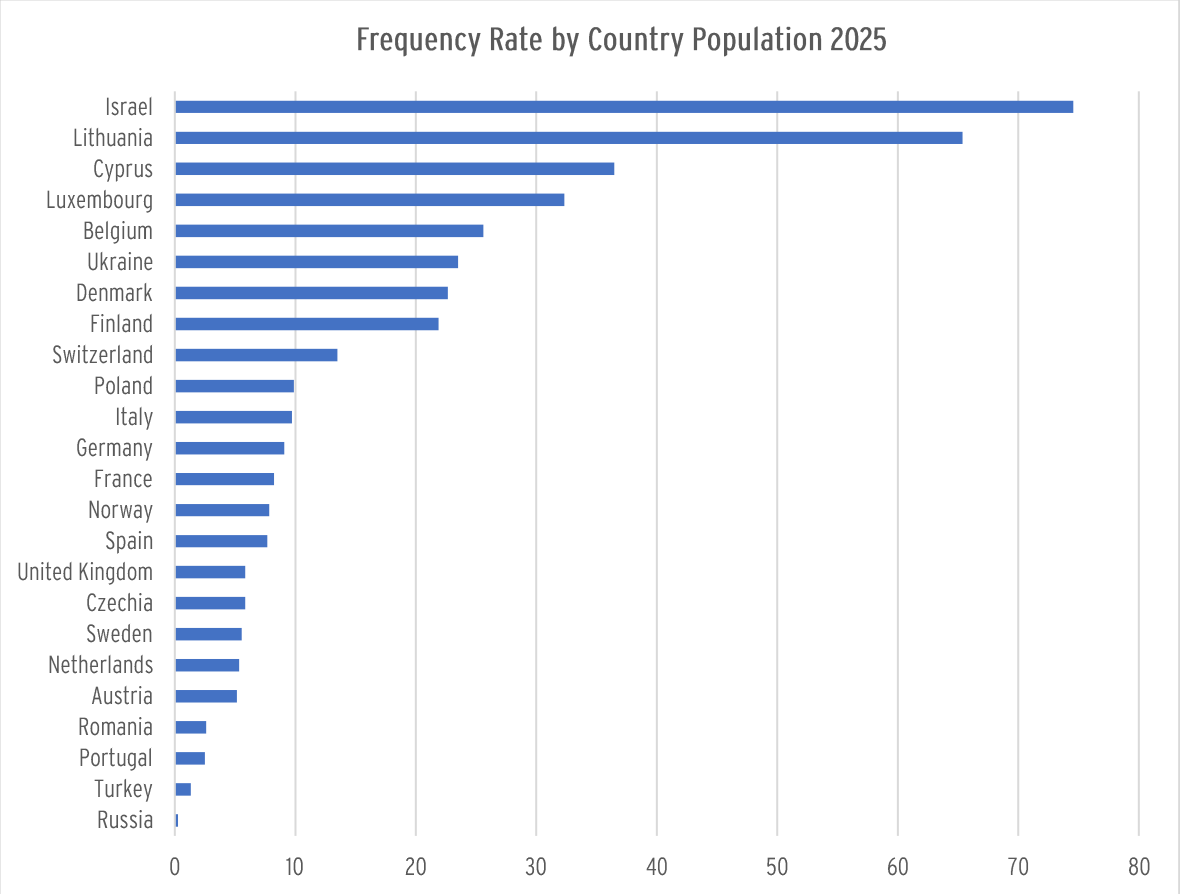

Figure 1: Displays the distribution of cyberattacks across the top 24 attacked European and strategically relevant neighbouring countries in 2025, measured per million inhabitants. This metric normalises the incident volume against population size to identify regions with the highest relative threat intensity.

- **High-Density Environments:** Israel records the highest density in the index with 74.55 attacks per million inhabitants. This metric is significantly higher than the European average, indicating a concentrated hybrid threat environment. Lithuania ranks second with 65.37 attacks per million. This high statistical density suggests that the Baltic region experiences a disproportionate level of incident activity relative to its population size, which correlates strongly with geopolitical exposure.

- **Highly Digitized Economies:** The normalized data highlights elevated risk metrics in smaller economies with advanced digital infrastructures. Cyprus (36.48), Luxembourg (32.33), and Belgium (25.60) rank in the upper quartile of the index. This distribution indicates that high internet penetration rates, combined with a smaller demographic baseline, allow threat actors to achieve a higher statistical impact per capita.

- **Populous Nations:** Major European economies, including Germany (9.08), France (8.22), and the United Kingdom (5.85), position in the middle to lower tiers of this index. Although these nations record the highest total volume of incidents, their large populations mathematically distribute the relative density of the attacks. This confirms that while the absolute threat volume in Western Europe is high, the per capita probability of targeted incidents is statistically lower than in regions situated on the geopolitical periphery.

Three-Year Vector Analysis (2023-2025)

The longitudinal data covering the period from 2023 to 2025 highlights a structural change in the operational volume of cyber threats. While both primary attack vectors exhibit an upward trajectory, their rates of acceleration differ, indicating a variation in adversary tactics as well as advancements in threat detection methodologies.

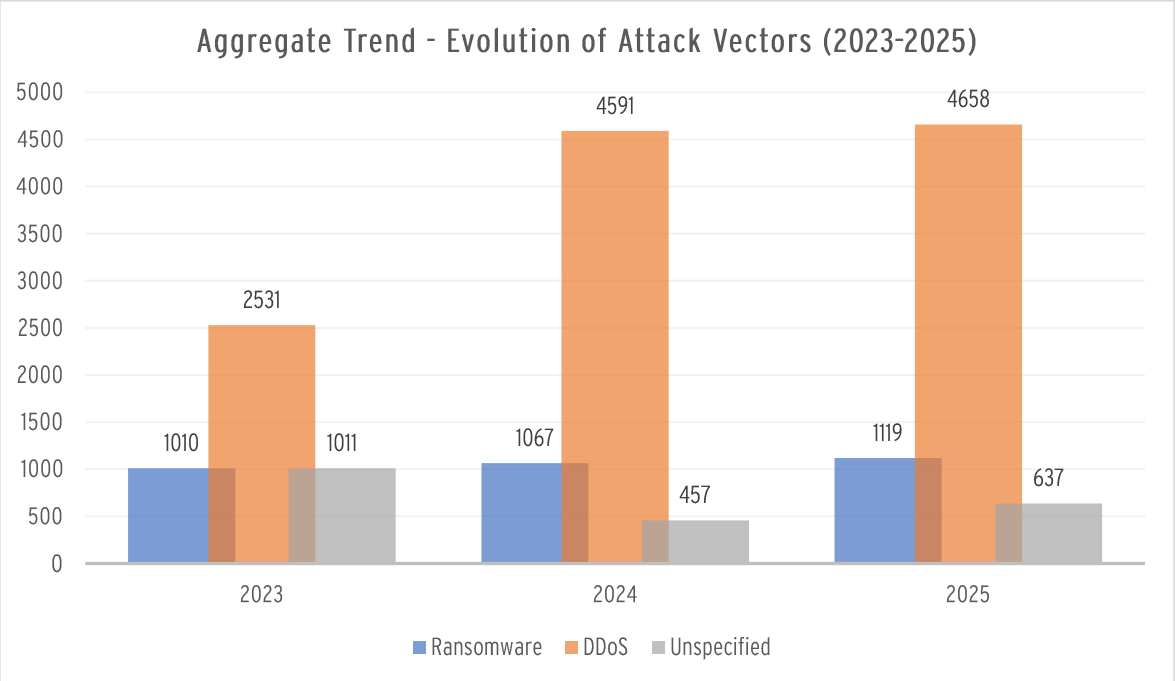

Figure 2: Illustrates the aggregate volume of recorded incidents for Ransomware and DDoS attacks from 2023 to 2025. The chart highlights a distinct divergence in growth patterns, comparing the volatility of disruptive attacks (DDoS) against the linear progression of extortion attempts (Ransomware).

Distributed Denial of Service (DDoS) incidents constitute the dominant vector by volume. A significant increase occurs between 2023 and 2024, where incident numbers rise from 2,531 to 4,591. This statistical shift is attributable to both an intensification of conflict-driven activity and an expanded monitoring scope introduced in 2024, which improved visibility into hacktivist operations. In 2025, this volume stabilises at an elevated baseline of 4,658 incidents rather than receding. This confirms that high-volume availability attacks aiming to degrade service infrastructure remain a persistent feature of the current security landscape.

In contrast to the volatility of DDoS, ransomware activity demonstrates a consistent, linear expansion. Incident counts rise steadily from 1,010 in 2023 to 1,119 in 2025, indicating a resilient and economically sustainable threat ecosystem. It should be noted, however, that availability attacks are inherently easier to detect and quantify, whereas ransomware incidents are frequently resolved confidentially and therefore remain underreported. Consequently, the dominance of DDoS in volume terms does not equate to proportional economic impact.

The discrepancy between the rapid surge in DDoS and the steady progression of Ransomware indicates a dual-threat environment. Organisations face a sustained level of mass-volume disruptive events while simultaneously contending with the persistent risk of targeted data extortion.

Year-over-Year Volatility: 2024 vs. 2025

The comparative analysis of incident volumes between 2024 and 2025 reveals a pronounced geographical shift in threat actor focus. Rather than a uniform increase across the continent, the data indicate a volatile redistribution of offensive resources.

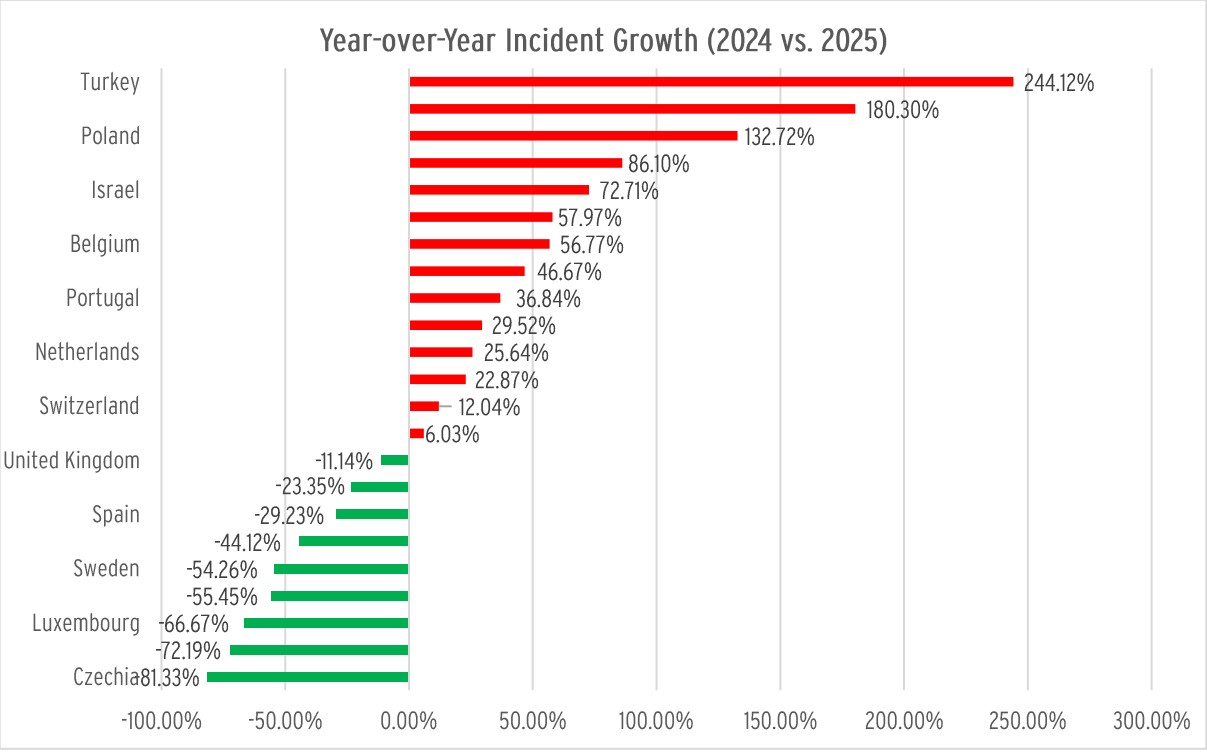

Figure 3: Illustrates the year-over-year percentage change in incident volume from 2024 to 2025. The chart highlights the significant volatility in the threat landscape, categorising nations into those experiencing a surge in activity (right) versus those recording a statistical decline (left).

- **Targeted Escalation on the Periphery:** The most significant growth is observed on the geopolitical periphery. Turkey records a pronounced surge of 244.1%, identifying it as the fastest-growing target within the dataset. This trend is mirrored on NATO's eastern flank, where Lithuania (+180.3%) and Poland (+132.7%) experience triple-digit percentage increases. This distribution confirms that the operational focus for high-intensity cyber campaigns has shifted towards the borders of conflict zones. Concurrently, major economies face renewed pressure, with Germany recording an 86.1% increase and Israel observing a 72.7% rise, reinforcing their status as primary, high-priority targets.

- **Statistical Recessions in Central and Northern Europe:** Conversely, significant portions of Central and Northern Europe record a sharp statistical decline. Czechia (-81.3%), Austria (-72.2%), and Sweden (-54.3%) show a marked reduction in recorded incidents compared to 2024. This contraction indicates a tactical redeployment of adversary infrastructure rather than a definitive cessation of hostility. As attackers concentrate capabilities on high-friction zones such as the Baltic states and the Middle East, the operational pressure on secondary targets temporarily recedes.

This polarisation—substantial growth in eastern and southern regions versus statistical recession in central and northern areas—characterises the 2025 landscape not as one of general expansion, but of targeted operational escalation.

The Wealth Paradox - GDP and Geopolitical Influences on the 2025 Attack Landscape

The analysis of the 2025 threat landscape indicates a distinct correlation between a nation's economic output and its predominant threat profile. Plotting Gross Domestic Product (GDP) per capita against the proportion of ransomware incidents reveals a clear bifurcation in adversary motives, distinguishing between financially driven cybercrime and politically motivated disruption.

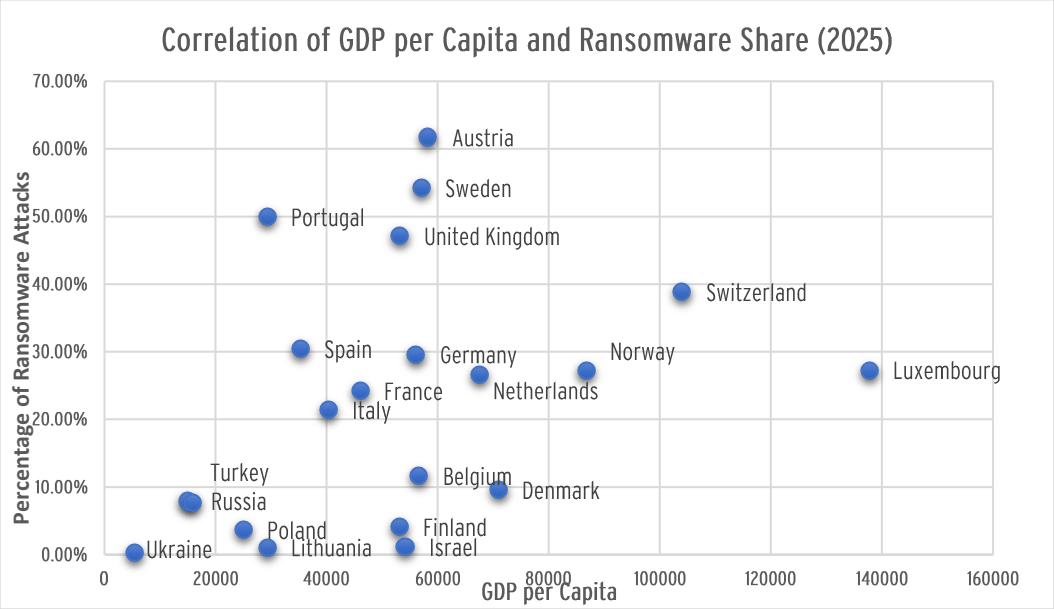

*Figure 4: Depicts a scatter plot correlating the Gross Domestic Product (GDP) per capita with the share of ransomware incidents across selected nations in 2025. Each data point represents a country, illustrating the divergence between financially driven cybercrime targets and regions affected by geopolitical destabilisation. *Note: Microstates and countries with statistically insignificant incident volumes were excluded to ensure data validity.*

- **Financially Motivated Targeting:** Austria (61.7%), Sweden (54.2%), and the UK (47.2%) record substantial incident volumes in this category. In these stable economies, threat actors prioritise high-value corporate targets to maximise financial returns, confirming that the primary adversary in these regions remains the extortionist.

- **Conflict-Driven Disruption:** Conversely, the data highlights a distinct cluster of nations where the ransomware share is negligible, irrespective of economic development. Ukraine (0.22%) and Israel (1.20%) represent significant statistical outliers. Although Israel possesses a high GDP comparable to Western European nations, its ransomware proportion is near zero. This distribution indicates that the sheer volume of politically motivated availability attacks (DDoS and wipers) statistically obscures financially driven cybercrime. In these regions, the operational objective is infrastructure disruption rather than extortion.

- **The Geopolitical Periphery:** A similar pattern is observed in Poland (3.71%), Lithuania (1.08%), and Finland (4.07%). Despite their integration into the broader European economy, proximity to active conflict zones significantly influences their threat profiles. The low ransomware share indicates that these nations absorb a high frequency of availability attacks linked to regional tensions, reflecting hybrid operational tactics rather than opportunistic criminal campaigns.

The 2025 data indicates differing attack patterns across regions. Financially motivated ransomware activity is more prevalent in high-GDP economies, whereas availability-focused attacks account for a larger share of incidents in geopolitically exposed regions. While Western European countries record higher proportions of extortion-related cases, countries in closer proximity to active conflict environments show a sustained concentration of disruptive activity where financial gain appears to play a lesser role.

Projections: The 2026 Cyber Threat Landscape

Based on the empirical data and operational shifts observed throughout 2024 and 2025, several trajectories can be anticipated for the upcoming year. The threat landscape in 2026 will likely be shaped by the convergence of geopolitical strategies, regulatory shifts, and adversarial automation.

1. **The Weaponisation of Regulatory Frameworks**
   With the strict enforcement of European cybersecurity directives (such as NIS2 and DORA), ransomware syndicates will increasingly weaponise compliance obligations. Extortion tactics are projected to evolve beyond mere data encryption and public shaming. Threat actors will leverage the threat of regulatory exposure—using the prospect of severe non-compliance fines as additional leverage to force ransom payments from compromised organisations.

2. **Increasing Overlap Between Politically and Financially Motivated Activity**
   The operational data from the geopolitical periphery indicates a blurring line between state-sponsored advanced persistent threats (APTs) and financially motivated cybercrime. In 2026, state actors are projected to increasingly utilise established cybercriminal syndicates as proxies. This strategy provides nation-states with plausible deniability while maintaining high-intensity disruptive pressure on target nations, particularly along the eastern and southern European flanks.

3. **Automated and Scaled Extortion Campaigns**
   The steady, linear progression of ransomware observed over the past three years demonstrates a highly resilient criminal ecosystem. The integration of generative artificial intelligence into attack chains—ranging from reconnaissance to payload deployment—will significantly lower the technical barrier to entry. Consequently, 2026 will likely see a surge in high-volume, automated extortion campaigns targeting the broader supply chain and small-to-medium enterprises (SMEs), rather than focusing exclusively on top-tier corporate targets.

4. **Evasion through Supply Chain Compromise**
   As evidenced by the "Wealth Paradox", highly developed economies such as the DACH region, the UK, and the Nordics remain prime extortion targets despite their robust defensive postures. As direct intrusion into hardened enterprise environments becomes increasingly resource-intensive, adversaries will pivot towards third-party vulnerabilities. Attacks on managed service providers (MSPs) and critical software supply chains enable indirect access to high-value networks through less mature secondary vendors.

Methodology and Data Scope

This report is based on aggregated telemetry data, verified incident disclosures, open-source intelligence (OSINT), and partner reporting channels monitored by AV-TEST throughout 2023–2025.

A "cyber incident" within the scope of this analysis refers to a verified malicious cyber event resulting in measurable service disruption, confirmed system compromise, or extortion activity. Scanning activity, unverified claims, and unsuccessful intrusion attempts were excluded.

Incidents were classified into three primary categories:

- **Ransomware** – confirmed encryption and/or extortion-based campaigns
- **DDoS** – volumetric or application-layer attacks resulting in service degradation
- **Unspecified** – verified malicious activity where the primary vector could not be conclusively determined

Where multiple techniques were observed, classification was based on the dominant operational objective.

Population data used for per-capita density calculations is derived from official national statistics for 2025. GDP per capita data reflects internationally recognised economic datasets for 2025 estimates.

Comparative year-over-year analysis accounts for expanded telemetry coverage introduced in 2024. While part of the observed increase reflects improved monitoring scope, sustained incident levels in 2025 indicate a structural continuation of elevated threat activity.

It should be noted that availability attacks are inherently more visible and statistically quantifiable than covert extortion or data exfiltration operations, which may be underreported due to confidential settlements or non-disclosure agreements.

Collected and Curated by
Erik Heyland, Head of Testing Labs, AV-TEST Institute
Jens Lichtenstein, Testing Engineer, AV-TEST Institute

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

About **AV-TEST**

AV-TEST is part of SITS Deutschland GmbH, it is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience.

The AV-TEST laboratories include 300 client and server systems, where more than 2,500 terabytes of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

For more information please visit our website at https://www.av-test.org .

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org