Endpoint Protection Market in Russia, Kazakhstan, and Uzbekistan: Slow Growth, Significant Potential

N4A Analytics has completed its annual update of the ongoing study of the endpoint protection market in Russia, Kazakhstan, and Uzbekistan. The research covers both basic security functionality—such as antivirus and other core features of endpoint protection platforms (EPP)—as well as advanced capabilities, including SOC services. All types of endpoints are considered: stationary and mobile workstations, servers, network edge devices (CPE), and Internet of Things (IoT) devices.

As of the end of 2025, total market consumption reached 72 billion rubles, with growth of 9% compared to 2024 in constant prices. In 2026, the market is expected to grow by 5% in constant prices, reaching 75 billion rubles. The compound annual growth rate (CAGR) for 2021–2026 is projected at 7%, with a clear tendency toward deceleration.

The slowdown is driven not only by a challenging macroeconomic environment. More fundamentally, the issue lies in the fact that the achievable potential of existing product and service offerings has already been largely exhausted, and the emergence of new market niches requires fundamentally new products and services.

The main limitation of the current offering is its polarization. The market is represented by two extremes: basic EPP configurations on one side, and full-featured systems integrated into corporate and/or commercial SOCs on the other. In strict accordance with Pareto's principle, basic configurations cover more than 80% of protected endpoints, while advanced solutions account for only around 20%. At the same time, neither configuration is optimal for defending against APT attacks, which currently represent the greatest threat.

Experts interviewed during the study unanimously noted that the speed of cyberattacks has increased dramatically—from several days to less than one hour. At the same time, the severity of consequences has also increased: in most cases, attacks are aimed at the complete destruction of corporate applications and data, including backups. The primary attack vector is endpoints. The intensity of APT attacks has also grown, with endpoints—primarily automated workstations (AWPs)—serving as the main entry point.

Basic endpoint protection configurations are simple and convenient to use, do not require qualified cybersecurity personnel, and are cost-effective. However, they are unable to detect most APT attacks, let alone prevent them. Full-featured SOC-based systems capable of doing so are not only extremely expensive but, due to low levels of automation and organizational challenges, often fail to cope with the rapidly increasing speed of attacks.

"On both sides—vendors reaching the limits of growth and organizations facing constraints in detecting and containing APT attacks—there is a growing need for next-generation solutions with broad automated orchestration of detection and response based on LLMs and AI agents, integrated with SIEM/SOAR and MDM/EDR," noted Andrey Novikov, an information security expert.

Technically and organizationally, this is an extremely complex challenge that clearly requires broad cooperation to solve, as well as a transition to more advanced business models that take into account the economic effect of using cybersecurity tools.

The need for new business models for vendors of a wide range of mass-market software used to protect endpoints is also driven by the emergence of new opportunities in internal corporate development associated with so-called vibe coding—that is, the use of LLMs and AI agents for

software development. When properly organized, vibe coding can significantly reduce development costs and ensure high-quality outcomes.

Endpoint protection is a set of processes. Any software for process automation requires deep customization and relatively complex, costly implementation. From this perspective, cybersecurity process automation software is no different from ERP and BI systems. If and when the cost of in-house development becomes lower than the cost of customizing and implementing off-the-shelf solutions, the latter will "die" as a commercial product category. This applies both to software and to hardware-software systems (HSS). In such a scenario, only fully packaged services and service-level agreements (SLAs) will be sold, and it will no longer matter to the customer what is "under the hood" or which software is used to achieve the SLA—the focus will shift entirely to results (SLA parameters), not the means of achieving them.

It should also be noted that endpoint protection requires involvement not only of specialized tools and services, but also indirectly nearly all types of cybersecurity solutions. Therefore, the need for such fundamental changes in the cybersecurity landscape extends beyond the endpoint protection market itself and affects the entire information security market.