Positive Technologies

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 4,000 organizations worldwide use technologies and services developed by our company.

Positive Technologies is the first and only cybersecurity company in Russia publicly available on the Moscow Exchange (MOEX: POSI), with 205,000 shareholders and counting.

Our new class of solutions—metaproducts—focuses on the results-oriented approach to cybersecurity. Positive Technologies first metaproduct, MaxPatrol O2, automatically detects and prevents attacks before non-tolerable damage is done to the company. MaxPatrol O2 can replace the entire team of a security monitoring center, and it only takes one person to manage it. This protection system requires minimum knowledge and effort from a specialist.

To demonstrate that the results-oriented approach to information security truly works, we conduct cyberexercises (on our own infrastructure as well as others') and publicly test our products. Our solutions are based on 20 years of research experience and expertise of several hundred information security experts.

We have seven Russian offices located in Moscow, St. Petersburg, Nizhny Novgorod, Samara, Novosibirsk, Akademgorodok, and Tomsk, and one office in Kazakhstan. The team has over 1,800 employees, including world-class experts specializing in the protection of SCADA and ERP systems, banks and telecommunications, as well as mobile and web applications.

Positive Technologies is highly rated by international analytical agencies: the company is a three-time recipient of the Visionary status in the Gartner Magic Quadrant for Web Application Firewalls (WAF).

We have provided cybersecurity for the following events:

2013 Summer Universiade in Kazan

2014 Sochi Olympic Games

2018 FIFA World Cup

2018 Russian presidential elections

2019 Winter Universiade in Krasnoyarsk

2020 Russian constitutional referendum

2021 Russia's State Duma elections

Positive Technologies is known globally as a visionary and a leader in the field of ethical security research. Each year our experts identify hundreds of zero-day vulnerabilities in IT systems of various classes and types, including products by Cisco, Citrix, IBM, Intel, Microsoft, and VMware. For detecting dangerous vulnerabilities, our experts have been added to the halls of fame of such companies as Adobe, Apple, AT&T, GitLab, Google, IBM, Mastercard, Microsoft, PayPal, VK, and Yandex. All detected vulnerabilities are reported to software vendors as part of the responsible disclosure policy and are not published until the vendors release the required updates.

We readily share what we know about information security with others:

- For 12 years we have been holding our own research and practical forum Positive Hack Days. One of the largest information security events in Russia and the CIS, it is attended by thousands of people who care about cybersecurity: IT and infosec experts, business and government representatives, security researchers and white hats, pupils and students. Over Positive Hack Days, hundreds of talks and workshops are held, covering the most interesting topics in information security, while competitions add excitement to analysis of protection of industrial control systems, banking and mobile services, and web apps. In 2023 the forum was held for the first time in the format of an open cybersecurity festival and brought together infosec experts, technology developers, as well as residents and guests of Moscow.
- We actively develop educational programs for leading universities and help prepare students to get a head start in their careers: Positive Education materials written by our company's experts are used at over 65 universities.

- We hold the world's largest cyberbattle, Standoff, which brings together the best Russian and foreign experts in both offensive and defensive cybersecurity. The cyberrange contains full-fidelity replicas of the production chains, business scenarios, and technology landscape typical of different industries. Experts analyze the odds of non-tolerable events being triggered and ways to prevent them.

Positive Technologies products, solutions, and services

For over 20 years, we have developed a visionary approach to creating solutions. Positive Technologies metaproducts are changing the industry and significantly increasing the security of companies, and, by extension, industries and nations. This makes results-oriented cybersecurity available to any organization in the world.

We develop our solutions based on longstanding experience and the unique knowledge of our research center, one of the largest in the world. This center brings together white hats who analyze the security of various systems, and cybersecurity experts who investigate real incidents and know which techniques hackers use to attack. Positive Technologies products comply with Russian and international security standards.

The company's product portfolio includes over a dozen high-end products that enable business to:

- Stop attacks in automatic mode with the help of just one person.
- Monitor security and quickly detect vulnerabilities in infrastructure.
- Detect security incidents in infrastructures of any scale, including industrial systems.
- Detect attacks in internal and external traffic.
- Protect web applications from APT attacks.
- Detect vulnerabilities and errors in applications, as well as support secure development processes.
- Detect and counter targeted and mass attacks involving modern malware.
- Respond to cyberthreats both at endpoints and inside the infrastructure, leveraging events and context from multiple information security systems to verify an attack.

Based on our products, we have developed several solutions to leverage Positive Technologies experience in protecting businesses of all types and implement national and international security standards.

We also offer cybersecurity services and consulting, including continuous security assessment of business, response to and investigation of challenging information security incidents, and security monitoring of corporate information systems.