5 REASONS TO USE INFOWATCH APPERCUT

No special skills required
The results of app code (or its fragment) analysis are returned as a report with error correction recommendations. Neither specific knowledge, nor programming skills are needed to obtain or interpret the analysis results.

Compliance with international standards and business specifics
InfoWatch Appercut takes into account PCI DSS and HIPAA requirements, CERT and OWASP best practices, as well as SDLC recommendations and those from platform vendors, such as SAP, Oracle and Microsoft. Users can add custom templates to the database of irregular software constructions in order to cope with the specifics of corporate business processes.

Ease of scalability and 20+ programming languages supported
An InfoWatch Appercut license allows for any number of applications to be checked as often as needed, with the most common business app development languages being supported, including, ABAP4 and web programming languages.

Business process continuity
There is no need to stop business-critical applications, unlike in case of a labor-intensive and long manual code check or external audit.

Perfectly suitable for any stage of software development lifecycle
If integrated, InfoWatch Appercut can be executed from a command line interface to run a source code analysis at any stage of the software development lifecycle, from programming to acceptance.

INFOWATCH APPERCUT

SOURCE CODE QUALITY CONTROL FOR BUSINESS APPLICATIONS

INFOWATCH

INFOWATCH

Бизнес-центр «Верейская плаза»

121357, Москва,ул. Верейская, д.29, стр.134

www.infowatch.ru
iw-global@infowatch.com

SOURCE CODE QUALITY CONTROL FOR BUSINESS APPLICATIONS

AP InfoWatch Appercut — automatically checks business app source code for compliance with custom development requirements.

90%
companies fine-tune their business applications* either with their FTE programmers or outsourced teams.

75%
new attacks occur at the business application layer*, but the market offers solutions to address insecure code threats.

10x
code error correction is **10 times less expensive at the software development stage** than when accepting a finished product.

INFOWATCH APPERCUT TO CHECK INSIDERS AND MAKE SAFE FROM STRANGERS

InfoWatch Appercut is designed for an accepting party or end customers and does not require any professional code programming or audit skills.

The compliance check of the entire application code, its updates and application modules only takes a few seconds with an automatically generated description of irregularities and recommendations on how to eliminate them.

InfoWatch Appercut features faster and more effective analysis than manual code checks and dramatically cuts bills raised by third-party auditors.
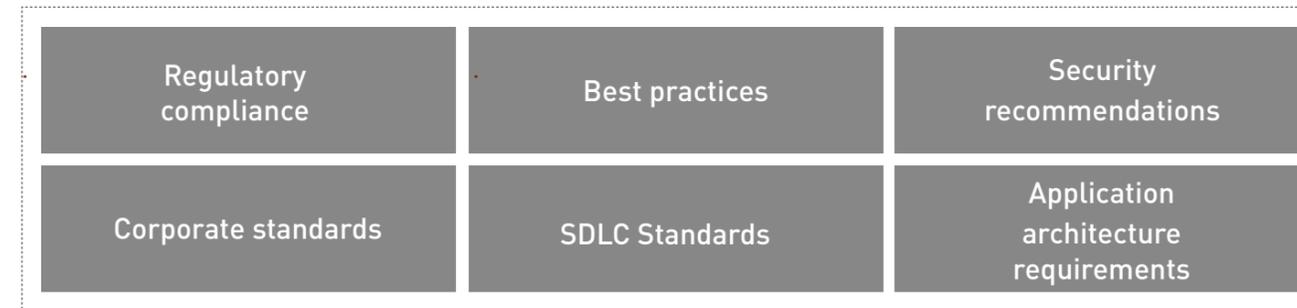
* Gartner Research

CASE STUDY

In a securities transaction app, a programmer left a backdoor that unnoticeably took a certain number of shares from client accounts and returned them back after several stock exchange transactions.

The resulting profits of RUB 5.7M were credited to the fraudster's account, with a total of 110,000 shares being sold. Damage to the employer's reputation was not assessed and the fraud scheme was revealed only a year later, with the malicious programmer being convicted and sentenced to five years in prison.

AP INFOWATCH APPERCUT

is specially designed to control the compliance with the entire range of effective and secure programming requirements and is flexible and customizable to both the specifics of a particular business application and unique nature of each company's business processes

Regulatory compliance	Best practices	Security recommendations
Corporate standards	SDLC Standards	Application architecture requirements

⬇

Source code → **AP INFOWATCH APPERCUT**

Fix task ← **InfoWatch Appercut Knowledge base** ← **Compliance report**

APPERCUT TECHNOLOGIES

Leveraging static application security testing (SAST), InfoWatch Appercut checks the quality of code as early as at the programming stage when error correction is easier and cheaper. Its lexer, semantic and data flow types of analysis quickly detect all insecure constructions at the very moment they are saved in a software design, with the number of false positives remaining at an acceptable level. Moreover, data flow analysis technology improves search quality via the accurate identification of real threats.

INTEGRATION WITH WEB APPLICATION FIREWALL AND ANTI-DDOS FOR WEB INFRASTRUCTURE PROTECTION

AK INFOWATCH ATTACK KILLER
continuously, actively, and automatically protects web infrastructure from external attacks.

The synergy of four technologies (SAST, DAST, WAF and Anti-DDoS) delivers high-quality security unattainable by similar technologies if used separately.

CCS InfoWatch Attack Killer Custom Code Scanner (CCS)
detects application vulnerabilities, using source code analysis by InfoWatch Appercut

WAF InfoWatch Attack Killer WEB Application Firewall (WAF)
prevents hacker attacks on web applications and detects web infrastructure vulnerabilities, leveraging Wallarm technology

DDOS InfoWatch Attack Killer AntiDDoS
guarantees DDoS attack prevention leveraging Qrator Labs technology

InfoWatch Attack Killer, an integrated solution for web infrastructure protection from external attacks, employs source code static analysis technologies, while its Appercut-based CCS is integrated with WAF, thus providing the technology synergy to automate the secure web application development and accelerate the release of updates by up to 10 times. InfoWatch Attack Killer ensures continuous and active protection of business-critical web assets.