Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Press release

EU Cyber Resilience Act raises the bar for physical security technology providers

Genetec outlines five questions security leaders should ask their provider when evaluating product security, transparency, and lifecycle support

LONDON, 9 September, 2026 —Genetec Inc. (“Genetec”), the global leader in enterprise physical security software, today released guidance to help physical security leaders assess how technology providers design, maintain, and support connected products as the EU Cyber Resilience Act (CRA) raises cybersecurity expectations across the product lifecycle.

The CRA establishes cybersecurity requirements for products with digital elements sold in the European Union. It places greater emphasis on secure product development, vulnerability management, cybersecurity transparency, and ongoing product support throughout the product lifecycle. While the legislation primarily applies to manufacturers, the regulation will also affect the organisations that distribute, install, procure, and operate connected devices.

"The Cyber Resilience Act reinforces many of the secure-by-design and lifecycle management principles that Genetec has been advocating for years," said Mathieu Chevalier, Principal Security Architect at Genetec Inc. "By raising expectations for product security and transparency, the CRA regulations give buyers a clear basis for evaluating technology providers and the long-term cyber resilience of their products."

With the CRA's vulnerability-reporting obligations coming into force on 11 September, organisations will increasingly rely on technology providers to meet new cybersecurity and vulnerability-handling requirements. To help evaluate vendor readiness, Genetec encourages organisations to ask prospective technology providers five key questions:

How long will the product receive security updates and support?
The CRA reinforces the importance of maintaining product security throughout its lifecycle. Security leaders should understand how long the provider will deliver

updates, how it will address vulnerabilities, and what support it will offer when products reach end-of-life. The CRA regulations require manufacturers to provide security updates and vulnerability handling for at least five years, making long-term support an important consideration when evaluating products.

Was cybersecurity built into the product from the beginning?

The principles of Secured by Design and Secure by Default are central to the CRA. Ask the provider to explain how it incorporates cybersecurity into product design, development, testing, and the product's ongoing lifecycle.

How does the provider identify, disclose, and address vulnerabilities?

No software is immune to vulnerabilities. How a provider responds is a strong indicator of its commitment to cybersecurity. Look for an established vulnerability management program that includes regular security testing, a coordinated vulnerability disclosure policy, risk-based remediation without undue delay, secure delivery of security updates, and clear advisories about fixed vulnerabilities

Is the provider transparent about its own cybersecurity practices?

Cybersecurity is a shared responsibility. Responsible providers explain how they develop, test, and maintain their products and give customers and integrators clear guidance for secure deployment. Ask how the provider regularly tests and reviews product security, communicates vulnerabilities and security updates, and provides system-hardening guidance.

How will the provider support your long-term cyber resilience?

Product cybersecurity does not end at installation. Working with trusted technology partners is critical. Organisations should evaluate how the provider determines and communicates the product's support period, handles vulnerabilities, delivers security updates, supports secure operation, and manages the product's end of life. They should also ask what evidence the provider can supply to demonstrate that the product meets applicable cybersecurity requirements throughout its lifecycle.

"Organisations best positioned to manage future cyber threats treat cybersecurity as an ongoing partnership, not a one-time procurement decision," concluded Chevalier. "The CRA

helps reinforce that approach by setting common expectations for transparency, disciplined vulnerability management, and long-term product support, benefiting manufacturers, integrators and the organisations that depend on connected physical security systems."

For more than 25 years, Genetec has applied cyber secure development practices to its physical security technology. It builds solutions based on open architecture and designs them with cybersecurity at the core, incorporating encryption, identity and access management, continuous monitoring, vulnerability management, and guidance that helps customers maintain resilient systems over time.

For more information about cybersecurity best practices for physical security systems, visit https://www.genetec.com/trust-cybersecurity.

--ends--

About Genetec

Genetec Inc. is a global technology company that has been transforming the physical security industry for over 25 years. The company's portfolio of solutions enables enterprises, governments, and communities around the world to secure people and assets while improving operational efficiency and respecting individual privacy.

Genetec delivers the world's leading products for video management, access control, and ALPR, all built on a unified, open architecture and designed with cybersecurity at their core. The company's portfolio also includes intrusion detection, intercom, and digital evidence management solutions.

Headquartered in Montreal, Canada, Genetec serves its 42,500+ customers via an extensive network of accredited channel partners and consultants in over 159 countries.

For more information about Genetec, visit: https://www.genetec.com

Press Contacts:

United Kingdom
Anna Short
Phoenix Communications
genetec@phoenix-comms.co.uk
+44 (0) 774 791 7235