Global Headquarters

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

T: +1 514.332.4000

Media Alert

Genetec alerts organizations to risks of legacy access control systems in light of rising cyberattacks

Company shares best practices for protecting access control systems from cyberattacks.

MONTRÉAL, November 16, 2022— With the ever-increasing rise in cybercrime, Genetec Inc. ("Genetec"), a leading technology provider of unified security, public safety, operations, and business intelligence solutions, is cautioning organizations of all sizes to be vigilant about the cybersecurity risk posed by legacy access control systems.

"Many organizations are operating with access control systems that date back 10 years or more. While these older systems still allow employees to badge in and out, there's a very high likelihood that these systems employ technologies that are extremely vulnerable to modern cyber threats," says Christian Morin, Vice President of Product Engineering and Chief Security Officer at Genetec Inc.

Vulnerabilities in legacy access control systems can introduce cybersecurity weaknesses that may put an entire organization at risk. Cybercriminals can exploit weaknesses in access control system credentials, controllers, servers, readers, or workstations connected to the network. Once a cybercriminal has breached access control system credentials, they can then move on to an organization's network and can gain control of other building systems, view or steal confidential information from internal records, or launch attacks designed to take key systems offline.

Companies that are affected pay a heavy price; the average cost of a data breach rose from USD 4.24 million in 2021 to USD 4.35 million in 2022. Hence, it's never been more important for organizations to be educated on the risks associated with legacy systems and the advantages that new cybersecure access solutions can offer.

Cybersecurity best practices for access control systems

To improve the cybersecurity of access control systems, Genetec recommends the following steps:

- Upgrade the system. Older systems were not built to address today's threats. When evaluating a new access control system or upgrading an existing system, make sure that cybersecurity is a key component of the vendor selection criteria
- Use advanced secure credentials and the latest communications protocols to secure data transmission since older credentials are easy to clone using readily available tools
- Educate employees and partners about cybersecurity best practices and ensure they are prompted to change passwords often
- Regularly check for firmware and software updates and install once available
- Use a centralized identity access management system to ensure virtual and physical authentication and authorization of employees for better control and more effective maintenance of your systems
- Create a dedicated network for access control systems so that there is clear segregation of networks based on their purpose
- Choose a security provider who can demonstrate compliance with established security certifications
- Ensure that the access control system uses proven data encryption standards as well as multi-factor authentication
- Work with a partner that has strong supply chain risk management, a dedicated team to monitor cyber threats, and ensures software is updated frequently and patched as needed

Access control technology has undergone a huge transformation in recent years. Customers are gradually freeing themselves from proprietary solutions and demanding more flexible, open solutions. Forward-thinking technology manufacturers have now introduced a new breed of more cyber secure solutions that offer benefits beyond locking and unlocking doors.

A unified access control system that uses the latest cybersecurity standards to secure communication, servers, and data such as Genetec Security Center Synergis™ can not only protect an organization's assets and people but help them improve their business operations and decision making. By choosing an open architecture IP-based access control system,

organizations have the flexibility to upgrade to the latest supported technology at any time, move at their own pace, and work within their available budget.

For more information, please download the Genetec white paper: *"Cybersecurity risks of legacy access control systems"*

--ends--

About Genetec

Genetec Inc. is a global technology company that has been transforming the physical security industry for over 25 years. Today, the company develops solutions designed to improve security, intelligence, and operations for enterprises, governments, and the communities in which we live. Its flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Founded in 1997, and headquartered in Montreal, Canada, Genetec serves its customers via an extensive network of certified channel partners and consultants in over 159 countries.

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

© Genetec Inc., 2022. Genetec, Synergis, and the Genetec logo are trademarks of Genetec Inc. and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective product.

Press Contacts:

North America
Véronique Froment
HighRez
Veronique@highrezpr.com
Tel: +1 603.537.9248