Genetec shares its top physical security trends predictions for 2021

Key trends include innovative applications of security technology, focus on privacy, growing cybersecurity concerns, hybrid cloud adoption, and increasing scrutiny into vendors

SYDNEY, AUSTRALIA/MONTRÉAL, January 13, 2021—Genetec Inc. (“Genetec”), a leading technology provider of unified security, public safety, operations, and business intelligence solutions, today shared its top five predictions for the physical security industry in 2021. Innovative security solutions will help businesses thrive post pandemic While the world remains optimistic for 2021, organisations will need to remain creative about how they use, update, and redeploy their security systems across their facilities. This will allow them to start thinking more broadly about the role of physical security and what it can do beyond traditional applications to deliver more value. We have already seen proof of this resilience and resourcefulness over the last few months with many organisations quickly adapting to the new needs and challenges posed by COVID-19, using their physical security technology as a strategic tool in the fight against the pandemic. In many ways, the extraordinary difficulties brought on by the current situation have put an increased focus on the role and importance of the physical security industry. And once the pandemic is finally in the rear-view mirror, we believe organisations will continue to look at their physical security technology and related data as both strategic and enterprise-shaping. Businesses will focus on privacy protection In an effort to keep people safe during the COVID-19 pandemic, many organisations rushed to implement ‘fever detection’ devices and other new sensors without necessarily having the time to consider privacy implications. Public privacy concerns related to COVID-19 contact tracing and other social challenges will continue to grow. These sensitivities will require the physical security industry to address privacy head-on and find appropriate solutions. Rather than hindering the development of new technologies, privacy will prove to be a driving force in the pursuit of responsible and innovative design, encouraging forward-thinking, ethical developers to embrace Privacy by Design methodologies. This involves proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices from the first line of code to the third-party vendors selected for partnership and integration. And, in the physical security industry, building a software solution from the ground up with privacy in mind means that organisations won’t have to choose between protecting individual privacy and ensuring their physical security. Privacy should always be the default option rather than the other way round, and security technology developers who take it seriously will gain distinct advantages, notably their customers’ trust. Cybersecurity risks will continue to rise While cybersecurity has been an issue for some time, it will unfortunately continue to be a vital concern in 2021. From schools and hospitals to private businesses and governments, there’s been a rise in cyber-attacks over the last year. In Q3 of 2020 alone, Trend Micro reported that there were almost 4 million email threats and over 1 million hits on malicious URLs related to COVID-19. Much of this can be linked to the overnight shift to remote work, which left companies scrambling to keep business running while also trying to secure corporate assets. This shift highlighted the fact that the traditional IT perimeter no longer exists. Businesses, organisations, and governments will need to take decisive steps to strengthen their cyber posture, or risk undermining the safety of their intellectual property, sensitive data, and personal information. Choosing trusted vendors and deploying physical security solutions that come with layers of cyber defense is critical. Security teams understand that built-in encryption, multi-factor authentication, and password management are the first lines of defense. Beyond that, taking advantage of other features such as cybersecurity risk scoring, system vulnerability alerts, and automated reminders for firmware and hardware updates are significant advantages in this heightened risk environment. Greater focus on trust in the supply chain Physical security technology has become an integral part of an organisation’s IT strategy and is, thankfully, now under the same level of scrutiny as other elements of an organisation’s technology stack. Some governments are already discouraging the use of certain products from security manufacturers, citing trust and security vulnerabilities. End users, especially in the enterprise space, are taking more time to scrutinise the manufacturers, suppliers, and distributors with whom they choose to work. This includes asking vendors more pointed questions about how they manage emerging threats, how forthcoming they are about product vulnerabilities and their partner ecosystem, and what their data and privacy policies are. For a physical security solution provider to be considered a reputable, reliable partner to their customers, they are going to have to meet more stringent requirements as part of the procurement process. Demand for hybrid cloud solutions will continue to grow According to Forrester’s recent report, Predictions 2021: Cloud Computing Powers Pandemic Recovery, global public cloud infrastructure will grow 35% to a market value of $120 billion over the next year. As online usage and remote work spiked during the pandemic, a global shift towards digital transformation, already underway, greatly accelerated. In order to thrive, physical security professionals will need to follow the lead of IT departments. In the coming year, physical security leaders should let go of the either/or division between cloud and on-premises security systems and embrace a hybrid deployment model in their physical security infrastructure. This will allow them to implement specific systems or applications in the cloud while keeping existing on-premises systems. With a hybrid cloud approach, security directors will become more agile in making decisions about how they can enhance scalability, redundancy, and availability to suit their organisation’s evolving needs. They will also be able to quickly migrate to newer technologies, minimise hardware footprint, boost cybersecurity, and reduce costs. Cloud offerings need to become an essential option to quickly adapt to changes and ensure business continuity. --ends-- About Genetec Genetec Inc. is an innovative technology company with a broad solutions portfolio that

encompasses security, intelligence, and operations. The company's flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ANPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security, and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montreal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 80 countries. For more information about Genetec, visit: www.genetec.com

Press Contacts:

Sue Ralston Einsteinz Communications Ph: +61 02 8905 0995 sue@einsteinz.com.au

Contacts

Karen Terranova

mailto: admin@einsteinz.com.au
Sue Ralston
0466 964 786
mailto: sue@einsteinz.com.au
Pru Quinlan
+61 2 8905 0995
mailto: pru@einsteinz.com.au
Antoinette Georgopoulos
02 8905 0995
mailto: antoinette@einsteinz.com.au