



## Taktgeber der Sicherheitsbranche

**Beim Genetec Press Summit'26 treffen Marktprognosen, Innovations-Roadmap und reale Anwendungen auf internationale Fachpresse**

**Zwischen Marktprognosen, Technologie-Roadmap und realer Anwendung**

Die strategischen Leitlinien wurden in Montreal unmittelbar erlebbar. Im Februar 2026 lud Genetec internationale Fachjournalisten zum Press Summit'26 nach Montreal (Kanada) ein – darunter auch Euro Security als Fachmedium für Sicherheits- und Technologiethemen in der EMEA-Region.

Während des Events stand dabei nicht nur die Produktperspektive im Fokus, sondern die strategische Gesamtschau: Wie entwickelt sich der globale Markt für physische Sicherheit? Welche Prognosen prägen 2026? Und welche Rolle spielen KI, hybride Architekturen und Cybersecurity in der technologischen Roadmap? So erhielten die Fachjournalisten aus erster Hand Einblicke in Marktanalysen, Innovationsstrategien und konkrete Lösungen. Der Summit machte deutlich, dass sich die Branche an einem strukturellen Wendepunkt befindet – weg von isolierten Einzeltechnologien, hin zu integrierten, offenen und verantwortungsvoll entwickelten Plattformmodellen. Besonders relevant war der Praxisbezug. Bei Besuchen im Luxus-Einkaufszentrum Royalmount in Montreal sowie bei ABB konnte die Redaktion die Implementierung der Technologien in realen Betriebsumgebungen nachvollziehen. So wurde sichtbar, wie strategische Konzepte in operative Sicherheitsarchitektur übersetzt werden – von intelligenter Suche bis zur raumorientierten Systemlogik. Der Press Summit'26 war damit nicht nur eine Branchenveranstaltung, sondern eine redaktionelle Standortbestimmung: Montreal wurde zum Schauplatz einer Sicherheitsindustrie, die technologische Innovation mit langfristiger Partnerschaft, Offenheit und Verantwortung verbindet.

Die zentrale Botschaft: Die physische Sicherheit steht nicht vor einer punktuellen Innovation, sondern vor einer strukturellen Verschiebung. Technologie wird strategischer, Entscheidungen langfristiger – und Vertrauen messbar.

#### **Künstliche Intelligenz: Priorität mit Fragezeichen**

Besonders auffällig ist die dynamische Entwicklung rund um KI. Andrew verweist darauf, dass das Thema innerhalb nur eines Jahres deutlich an Bedeutung gewonnen hat: Es ist vom fünften Platz im vergangenen Jahr auf Platz zwei gestiegen und hat damit die Videoüberwachung als Priorität verdrängt “.

Diese Verschiebung ist bemerkenswert, weil Videoüberwachung traditionell als Kerntechnologie gilt. Dass KI sie in der Priorisierung überholt, signalisiert eine strategische Neuorientierung. Doch Andrew relativiert die Euphorie bewusst. Immer wieder sei im Rahmen der Studie eine entscheidende Frage aufgekommen:



# Zukunft der physischen Sicherheit 2026

**Vertrauen, verantwortungsvolle KI und offene Plattformen als strategische Wegweiser einer Branche im Umbruch**

Als Andrew Elvish, Vice President, Global Marketing von Genetec, den aktuellen Branchenreport vorstellt, wählt er keinen dramatischen Ton, sondern eine präzise Einordnung: Der Genetec State of the Industry Report 2026 hat sehr klare Einblicke geliefert, wohin sich die Branche bewegt. Hinter dieser nüchternen Feststellung steht eine umfassende Datengrundlage: Mehr als 7.300 Befragte aus Integrator-Channel, Beratungsumfeld und globaler Endanwenderbasis.

Welches Ergebnis wollen Sicherheitsverantwortliche mit KI erzielen?

Damit ordnet er die Diskussion fachlich ein: KI ist kein Selbstzweck. Sie ist ein Mittel zur Zielerreichung. Seine Metapher verdeutlicht das: Es ist ein Hammer – die Frage ist, was gebaut werden soll.

Für Entscheider bedeutet das: Nicht die Einführung von KI entscheidet über Erfolg, sondern die klare Definition operativer Mehrwerte – etwa die Beschleunigung von Ermittlungen, die Reduzierung von Fehlalarmen oder die Verbesserung von Entscheidungsprozessen.

## **Verantwortungsvolle KI als betriebliche Notwendigkeit**

Die hohe Priorisierung von KI geht mit erheblichen Vorbehalten einher. Mehr als 70 Prozent der Befragten sehen offene Fragen, die vor einer vollständigen Integration beantwortet werden müssen. Andrew nennt exemplarisch zentrale Punkte: Wie wurden die Trainingsdatensätze entwickelt? Wem gehören die Trainingsdaten? und Welche Schutzmechanismen wurden implementiert?

Diese Fragen sind nicht abstrakt. Sie betreffen Haftungsrisiken, regulatorische Anforderungen und die langfristige Nutzbarkeit von Systemen. Andrew formuliert die Sorge pointiert: Niemand möchte in eine Situation geraten, in der die KI nicht mehr nutzbar ist, weil der Trainingsdatensatz rechtlich oder technisch nicht valide ist.

Besonders in sicherheitskritischen Anwendungen müssen KI-Entscheidungen nachvollziehbar bleiben. KI-Entscheidungen müssen erklärbar und prüfbar sein, um regulatorischen und rechtlichen Anforderungen standzuhalten („AI decisions... must be explainable and auditable to satisfy compliance and legal scrutiny“). Damit wird Responsible AI nicht zur Option, sondern zur Voraussetzung für Marktfähigkeit.

## **Neue Bedrohungsdimensionen durch KI**

Parallel zur Integration von KI verändern

sich auch die Bedrohungsszenarien. Andrew stellt klar, dass klassische Angriffsmuster – etwa SQL-Injection – nicht mehr alleinige Referenz sind. Im Gegensatz zu klassischen SQL-Injection-Angriffen geht es heute mit KI eher darum, dass Menschen durch geschickte Formulierungen oder Täuschungen die KI manipulieren.

Damit verschiebt sich die Angriffsfläche: Prompt-Injection, manipulierte Inhalte oder semantische Täuschung können operative Entscheidungen beeinflussen. Hinzu kommt eine strukturelle Eigenschaft generativer Modelle, die Andrew mit einem Zitat seines CEO einordnet: Sie hat ein impressionistisches, kein detailliertes Verständnis von Dingen.

Für die physische Sicherheit ist das ein entscheidender Unterschied. Zutrittsentscheidungen oder Alarmprozesse dulden keine Annäherungen, sondern verlangen Präzision. KI muss daher kontrolliert, überwacht und architektonisch abgesichert implementiert werden.

## **Vertrauen als zentrales Entscheidungskriterium**

Der vielleicht eindrucksvollste Befund der Studie betrifft nicht Technologie, sondern Partnerschaft. 73 Prozent der Befragten priorisieren Vertrauen und Verlässlichkeit hinsichtlich der langfristigen Beständigkeit des Anbieters als wichtigstes Auswahlkriterium.

Andrew betont, dass dieser Wert deutlich vor klassischen Faktoren wie Preis, Performance oder Skalierbarkeit liegt. Für die Branche ist das ein klares Signal: Sicherheitsinfrastrukturen sind langfristige Investitionen. Anbieter müssen Stabilität, Kontinuität und Verlässlichkeit demonstrieren – nicht nur Innovationskraft.

## **Offene Plattformen als strategische Grundlage**

In diesem Kontext positioniert Andrew Offenheit als philosophisches Fundament („philosophical bedrock“) des Unternehmens. Geschlossene Systeme bewertet er

kritisch: Geschlossene Systeme sind fragil, riskant und setzen Endanwender unnötig dem Risiko der technologischen Überalterung aus.

Die fachliche Einordnung ist klar: Proprietäre Ökosysteme erhöhen Lock-in-Risiken und begrenzen Wahlfreiheit. Offene Plattformen hingegen ermöglichen Integratoren und Endanwendern, Best-of-Breed-Komponenten zu kombinieren und langfristig flexibel zu bleiben.

Sein Verweis auf das Gefangenendilemma („Prisoner's Dilemma“) unterstreicht diese Argumentation strategisch: Kooperation schafft langfristig den größten Mehrwert – sowohl für einzelne Akteure als auch für das Gesamtsystem.

## **Hybridarchitekturen als pragmatische Antwort**

Auch in der Cloud-Debatte plädiert Andrew für Differenzierung. Statt eines Entweder-oder betont er, dass es einen Mittelweg gibt.

Viele Organisationen wollen Innovation und Updatefähigkeit, gleichzeitig aber Resilienz und Kontrolle. Seine bildhafte Beschreibung bringt die Ambivalenz auf den Punkt: Sie wollen ihren Kuchen behalten und gleichzeitig essen.

Hybridmodelle verbinden lokale Stabilität mit cloudbasierter Innovationsgeschwindigkeit. Für regulierte Märkte – insbesondere in Europa – wird diese Balance zunehmend zur strategischen Notwendigkeit.

## **Operative Effizienz durch intelligente Suche**

Die technologische Weiterentwicklung zeigt sich besonders deutlich in der intelligenten Suche innerhalb der Plattform. Andrew beschreibt den Unterschied in der Ermittlungsarbeit eindrücklich: Ermittlungen konnten viele Stunden oder sogar Tage dauern – heute reduziert sich das auf Minuten.

Natürliche Sprachsuche, Trajektorienanalyse und KI-gestützte Zusammenfassungen verkürzen Prozesse signifikant. Damit wird



KI nicht abstrakt, sondern messbar wirksam.

### Vom Gerätebaum zum Raumverständnis

Ein weiterer Innovationsschritt betrifft die strukturelle Darstellung von Sicherheitsumgebungen. Man kann besser verstehen, was in einem Raum geschieht („You can understand better what happens in the room“), erklärt Andrew im Zusammenhang mit neuen Raumtopologien. Räume werden als funktionale Einheiten betrachtet, in denen Kameras, Sensoren und Zutrittskontrollen logisch zusammenwirken. Diese semantische Strukturierung verbessert Kontextanalysen und Entscheidungsprozesse.

### Strategische Verschiebung: Risikominimierung und Wettbewerbsvorteil

Andrew bringt die Gesamtentwicklung prägnant auf den Punkt: Technologie hat sich von reiner Risikominimierung zu einem strategischen Vorteil entwickelt.

Sicherheit ist damit nicht mehr isoliertes Schutzinstrument, sondern integraler Bestandteil organisatorischer Wertschöpfung. IT und physische Sicherheit wachsen zusammen, Silos lösen sich auf, Kooperation wird zum Erfolgsfaktor.

### Drei zentrale Anstrengungen für die Zukunft

Aus Andrews Analyse lassen sich drei prioritäre Handlungsfelder ableiten:

- Erstens die Entwicklung verantwortungsvoller, audittierbarer KI mit klaren Trainingsdatengrundlagen und Schutzmechanismen.
- Zweitens der konsequente Ausbau offener, hybrider Plattformarchitekturen zur Sicherstellung von Wahlfreiheit und Resilienz.
- Drittens die tiefgreifende Integration von Cybersecurity und Compliance als strukturelle Bestandteile jeder Lösung.

### Schlussbetrachtung: Strategische Klarheit und rhetorische Präzision

Was Andrews Vortrag auszeichnet, ist die Verbindung aus Marktdaten, technischer Detailkenntnis und strategischer Argumentation. Seine Zitate sind keine Schlagworte, sondern Ankerpunkte einer konsistenten

Logik. Er kombiniert analytische Evidenz mit verständlichen Bildern, ohne in Vereinfachungen zu verfallen. Die Metapher vom Hammer oder der Verweis auf das Gefangenendilemma sind keine rhetorischen Spielereien, sondern strukturierende Elemente seiner Argumentation.

Seine Fachkenntnis zeigt sich darin, dass er Innovation nicht isoliert betrachtet, sondern in regulatorische, wirtschaftliche und operative Kontexte einbettet. Gerade in einer Branche, die zwischen Innovationsdruck und Sicherheitsverantwortung steht, wirkt diese nüchterne, strategische Klarheit wie ein Stabilitätsfaktor. Die Zukunft der physischen Sicherheit wird damit nicht allein durch Technologie be-

stimmt – sondern durch die Fähigkeit, sie verantwortungsvoll, offen und langfristig tragfähig einzusetzen. **DCM**

### Anmerkung der Redaktion

Der vorliegende Beitrag mit Andrew ist Teil einer fünfteiligen Fachartikelreihe, die Euro Security in den kommenden Ausgaben veröffentlicht. Ziel dieser Serie ist es, die zentralen Ergebnisse des State of the Industry Report 2026 sowie die strategischen, technologischen und marktbezogenen Entwicklungen der physischen Sicherheitsbranche differenziert zu beleuchten.

## DER REPORT

**Der State of the Industry Report 2026 von Genetec basiert auf mehr als 7.300 Befragten aus Integrator-Channel und globaler Endanwenderbasis und zeigt eine deutliche strategische Verschiebung in der physischen Sicherheitsbranche.**

Zentrale Erkenntnis: Künstliche Intelligenz ist innerhalb eines Jahres von Platz fünf auf Platz zwei der Investitionsprioritäten aufgestiegen und hat damit die Videoüberwachung überholt. Gleichzeitig wird deutlich, dass es nicht um KI als Selbstzweck geht, sondern um konkrete Ergebnisse im Sicherheitsworkflow.

Responsible AI und Transparenz stehen im Mittelpunkt. Über 70 Prozent der Befragten sehen vor einer vollständigen Implementierung Klärungsbedarf – etwa hinsichtlich Trainingsdaten, Eigentumsrechten, Schutzmechanismen und Auditierbarkeit.

Ein weiterer zentraler Befund betrifft die Anbieterwahl: 73 Prozent der Endanwender priorisieren Vertrauen und langfristige Stabilität des Herstellers. Partnerschaft und Verlässlichkeit rücken damit stärker in den Fokus als kurzfristige Innovationsversprechen.

Strategisch setzt Genetec auf Offenheit und Kooperation innerhalb eines breiten Technologie-Ökosystems. Offene Plattformarchitekturen sollen Lock-in-Risiken vermeiden und maximale Wahl-

freiheit ermöglichen. Gleichzeitig bleibt Cybersecurity ein Kernbestandteil jeder Sicherheitsarchitektur. KI erweitert die Angriffsflächen, etwa durch Prompt-Injection oder manipulative Inhalte. Systeme müssen daher gegen neue Bedrohungsvektoren abgesichert und KI-Komponenten kontrolliert integriert werden.

Technologisch steht 2026 im Zeichen operativer Effizienz. Intelligente Suche, Logo- und Objekterkennung, Trajektorienanalyse, KI-gestützte Zusammenfassungen und raumorientierte Sicherheitslogik verkürzen Ermittlungen von Stunden oder Tagen auf Minuten.

Der Report zeigt insgesamt eine Branche im Wandel: von isolierter Risikominimierung hin zu strategisch integrierter Sicherheit, von geschlossenen Systemen zu offenen Plattformen, von Technologiebegeisterung zu verantwortungsbewusster Implementierung.

Für 2026 zeichnet sich damit ein klarer Trend ab: Sicherheit wird nicht nur intelligenter – sondern partnerschaftlicher, transparenter und langfristig ausgerichtet.