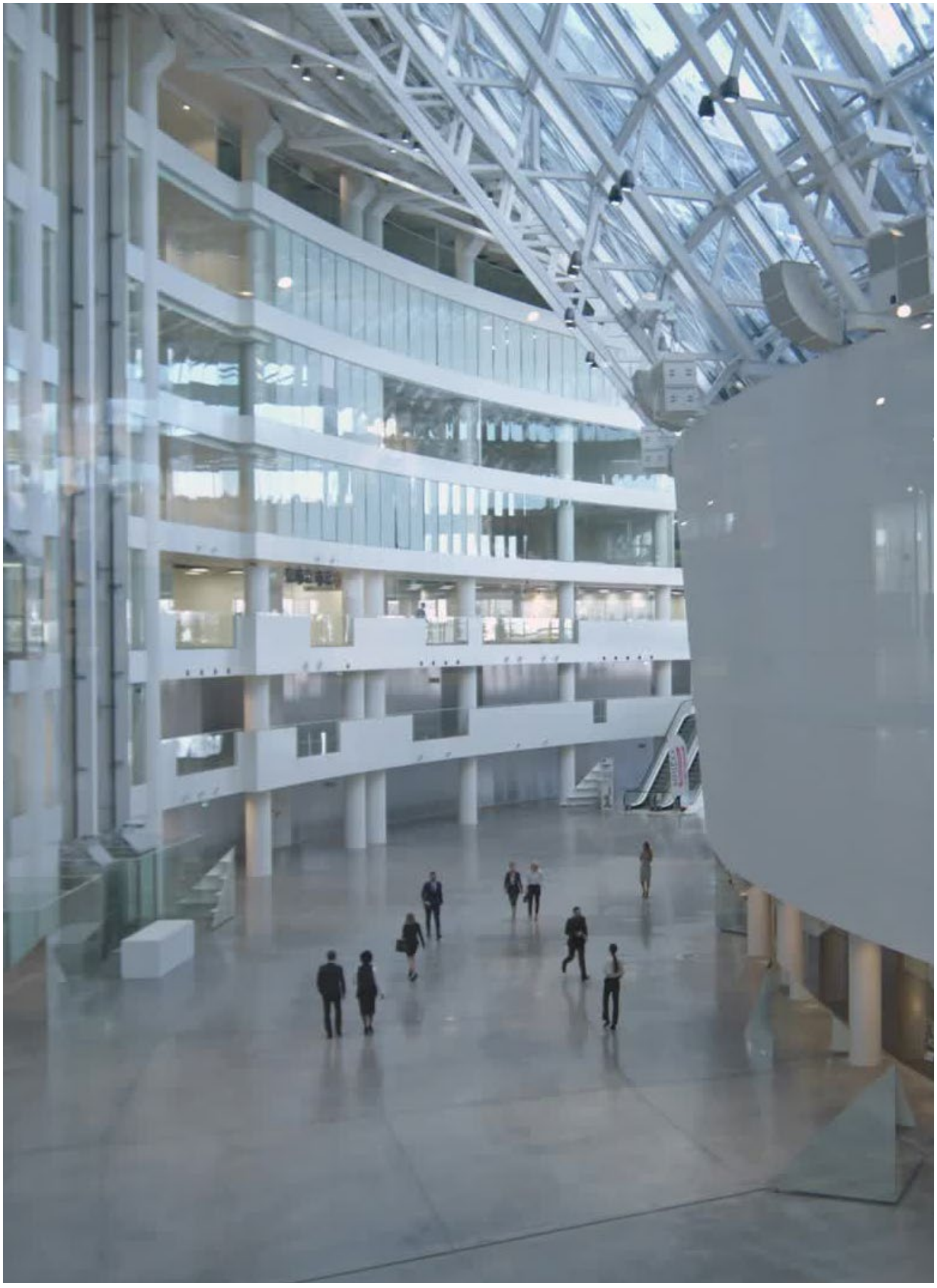
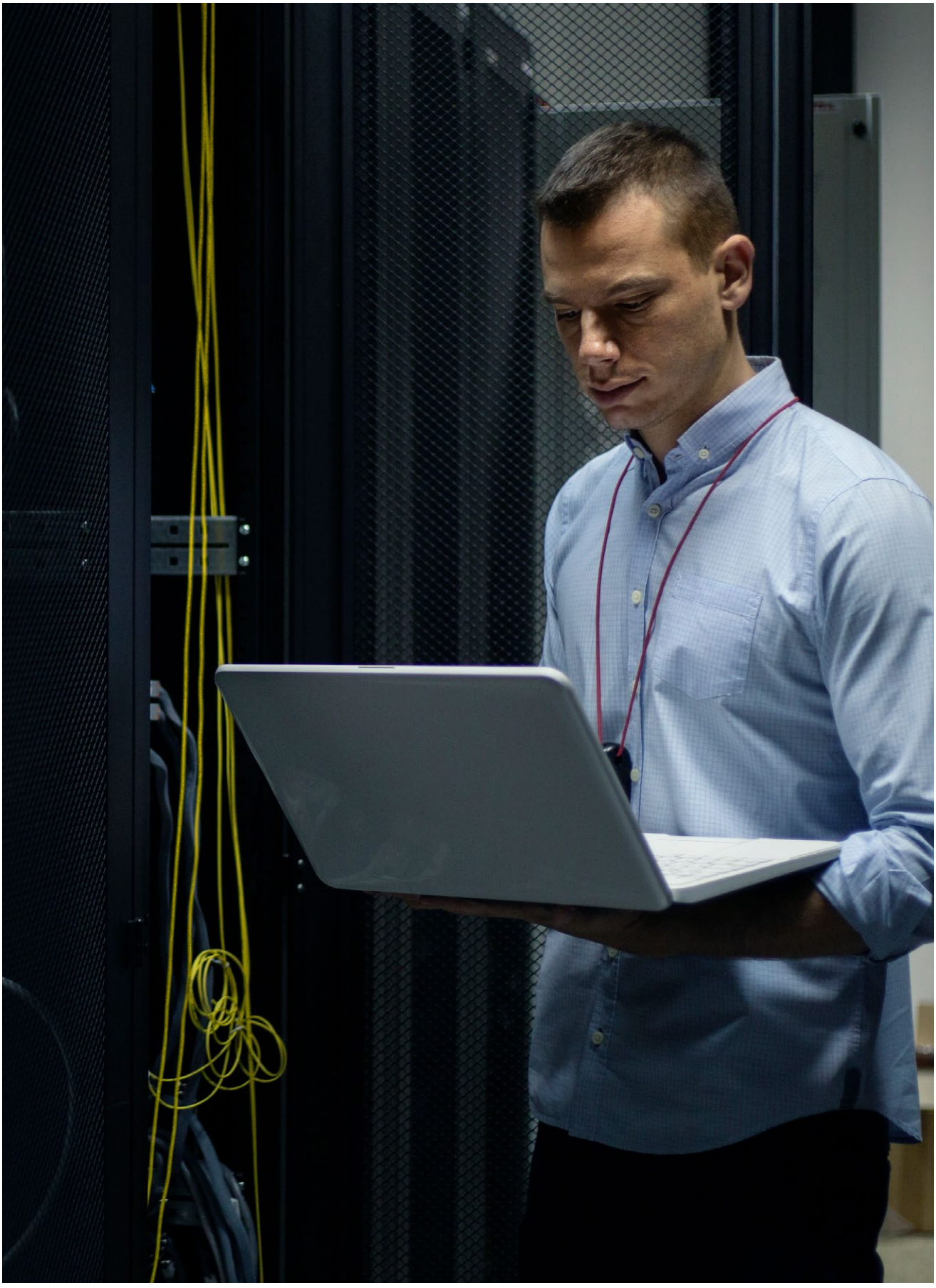
Whitepaper

Verlängerung der Lebensdauer physischer Sicherheit durch Vereinheitlichung

Genetec™



Inhalt



Kurzfassung

Viele Unternehmen arbeiten mit proprietären Lösungen, die ihren wachsenden Sicherheitsanforderungen nicht mehr genügen. Bei dem Versuch, neuen, aufkommenden Sicherheitsbedrohungen, einer wachsenden Infrastruktur und dem zunehmenden Druck zur Dezentralisierung gerecht zu werden, können diese Lösungen zu einer echten Belastung werden.

Wenn Unternehmen ihr bestehendes physisches Sicherheitssystem modernisieren möchten, müssen sie sich überlegen, was die beste Grundlage für ihre neue Sicherheitsinfrastruktur ist. Es gibt zwei Möglichkeiten:

- Systemintegration
- Vereinheitlichung

1

Der Prozess der Modernisierung

Die Entscheidung zur Modernisierung des physischen Sicherheitssystems ist der erste Schritt in einem mehrstufigen Prozess, mit dem die Sicherheit und die Geschäftsabläufe eines Unternehmens erheblich verbessert werden können. Der Prozess der Modernisierung kann in vier Phasen unterteilt werden: Erweiterung, Verbindung, Automatisierung und Erkenntnisse.

Phase 1: Erweiterung

In der ersten Phase wird die Sensorabdeckung durch eine eigenständige Sicherheitsanwendung erhöht. Nachdem sich ein Unternehmen zur Modernisierung entschieden hat, beginnt es mit der Aufrüstung seiner Infrastruktur und der Verbesserung der Sicherheit. Dazu wird die Reichweite des aktuellen Systems durch zusätzliche Hardware, einschließlich hochauflösender Kameras und biometrischer Lesegeräte, erweitert.

Phase 2: Verbindung

Sobald ein Unternehmen seine Ziele hinsichtlich einer besseren Sensorabdeckung erreicht hat, sucht es nach Möglichkeiten, die Sicherheit anhand von Daten aus anderen Systemen zu erhöhen. In dieser Phase vernetzen Unternehmen verschiedene Systeme miteinander und verbinden beispielsweise Videoüberwachungs- und Zutrittskontrollsysteme, um die Geschwindigkeit der Zugangsprüfung und -untersuchung zu erhöhen. Ebenso können Videoüberwachung und Kommunikation verknüpft werden, um die Notfallmaßnahmen in öffentlichen Bereichen zu verbessern.

Phase 3: Automatisierung

Die zunehmende Anzahl und Vielfalt von Sensoren und das anschließende Streaming all dieser Daten über eine zentrale Plattform haben zur Folge, dass eine bestimmte Anwendung des Sicherheitssystems mit Daten überflutet wird, die oft keine Priorisierung aufweisen. Das Sicherheitspersonal ist in der Folge überfordert, weil es nicht ohne Weiteres erkennen kann, welche Daten wichtig und handlungsrelevant sind. In dieser Phase muss das Unternehmen die täglichen Routineaufgaben automatisieren, damit sich die Mitarbeiter auf die wesentlichen Tätigkeiten konzentrieren können.

93 % der Unternehmen, die auf eine zentrale Plattform umgestiegen sind, verzeichneten eine Reduzierung der Kompatibilitäts-probleme in ihrem Sicherheitssystem.

Phase 4: Erkenntnisse

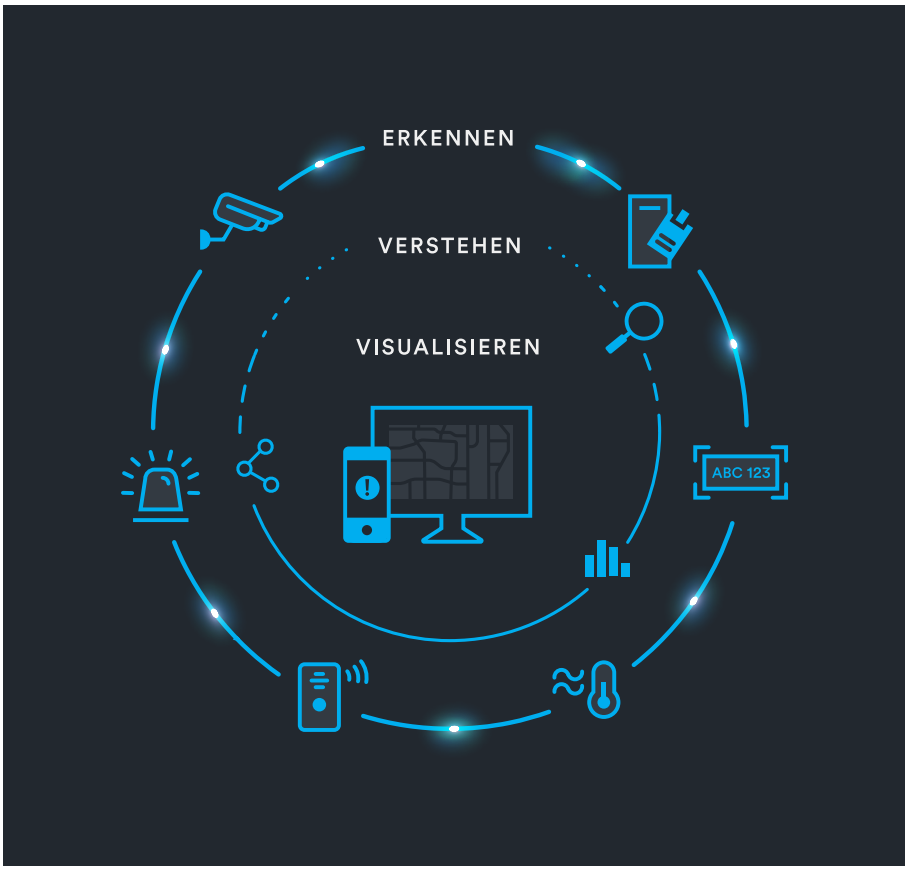
Angesichts all dieser Daten, die im physischen Sicherheitssystem erfasst werden, kann ein Unternehmen nun überlegen, wie es anhand dieser Daten Erkenntnisse über seine Abläufe und Prozesse gewinnen kann. In dieser Phase der Modernisierung geht es nicht mehr nur um Sicherheit, sondern auch um die Verbesserung der Business Intelligence und von Geschäftsabläufen. Ziel ist es, die in Sicherheitssystemen gesammelten Daten als potenziellen Wettbewerbsvorteil zu nutzen.

Für die meisten Unternehmen endet der Prozess der Modernisierung zwischen der 2. und 3. Phase: Nachdem sie die Sensorabdeckung mit ihrem neuen System erhöht und einige ihrer bestehenden Sensoren teilweise integriert haben, sind die Systemadministratoren mit der Verwaltung dieses komplexen und fehleranfälligen Technologiestapels überfordert. Wenn Unternehmen jedoch eine langfristige Vision verfolgen und diese Gelegenheit zur Modernisierung nutzen, um eine zentrale Plattform zu implementieren und größere Probleme im Zusammenhang mit Skalierbarkeit und mangelnder betrieblicher Effizienz zu lösen, können sie die letzte Phase erreichen und damit beginnen, Daten zur Steuerung von Geschäftsabläufen einzusetzen.

Der wesentliche Grund dafür, dass der Prozess für so viele Unternehmen zwischen der zweiten und dritten Phase endet, liegt im Aufbau ihres physischen Sicherheitssystems. Bei der Modernisierung verfolgen Unternehmen häufig den Ansatz der Systemintegration anstatt der Vereinheitlichung. Durch Systemintegration können Unternehmen zwar unmittelbare Probleme sowie einige kurzfristige Sicherheitsprobleme lösen. Dabei handelt es sich aber um keine langfristige Vision. Da die Wartung einer nach diesem Ansatz erstellten Lösung sehr aufwändig ist, verlieren sich Unternehmen in einem ständigen Zyklus von Veröffentlichung, Fehlerbehebung, Validierung und Upgrade. Sie sind nicht in der Lage, die Business Intelligence zu verbessern, weil ihre Kernkomponenten ständig in verschiedenen Veröffentlichungszyklen aktualisiert werden müssen und sie Zeit und Geld für die Wartung aufwenden müssen.

In einer kürzlich von Genetec durchgeführten Studie zu den Auswirkungen einer Vereinheitlichung gaben 93 % der Unternehmen, die auf eine zentrale Plattform umgestiegen sind, eine Reduzierung der Kompatibilitätsprobleme in ihrem Sicherheitssystem an. Vereinheitlichung ermöglicht den Datenfluss über alle Sicherheits- und Betriebsaktivitäten hinweg und versetzt Unternehmen dadurch in die Lage, die einzigartigen Herausforderungen in jeder Phase des Prozesses zu bewältigen. Die Implementierung einer zentralen Softwareplattform, die eine zentrale Schnittstelle für die Verwaltung der wesentlichen Sicherheitssysteme wie Zutrittskontrolle, Sprechanlage, Einbruchüberwachung und Videogeräte bietet, ist unerlässlich. Da sich das Innovationstempo in der Branche jedoch beschleunigt, müssen Unternehmen in der Lage sein, externe Sensoren und Daten einzubinden und gleichzeitig ein kohärentes, intuitives Benutzererlebnis zu gewährleisten, um langfristig nachhaltig zu sein.

Vereinheitlichung schützt Unternehmen nicht nur kurzfristig vor potenziellen Störungen, sondern unterstützt sie auch bei der Geschäftserweiterung, indem langfristiges Wachstum und Entwicklung gefördert werden. Da eine offene, zentrale Plattform den Fluss und die Verwaltung von Daten im Rahmen sämtlicher Aktivitäten erleichtert, können Unternehmen auf herkömmliche reaktive Maßnahmen der physischen Sicherheit verzichten und sich auf die Verbesserung ihrer Geschäftsabläufe konzentrieren.



Bei den meisten integrierten Lösungen müssen Anwender mehrere Systeme verwenden, da keines die erforderlichen Funktionen in einer einzigen Benutzer-oberfläche bietet.

2

Systemintegration

Systemintegration ist aufgrund des technologischen Fortschritts und der zunehmenden Zusammenarbeit zwischen den Herstellern zu einem beliebten Ersatz für herkömmliche Schnittstellen geworden. In der Sicherheitsbranche werden meist Standardprotokolle und Software Development Kits (SDK) verwendet, um verschiedene Computersysteme und Softwareanwendungen physisch oder funktional miteinander zu verbinden.

Standardprotokolle sind leistungsfähig und gelten im Allgemeinen als effektiver als ein SDK. Sie unterstützen unterschiedliche Betriebssysteme und ermöglichen Benutzern die Verwaltung ihrer Anwendungen in Echtzeit. Standardprotokolle sind für die Integration von Edge-Geräten wie IP-Kameras oder Türsteuerungen beliebt, werden aber am häufigsten zwischen zwei Softwareanwendungen verwendet. Im Gegensatz zur Verwendung eines SDK ist die Integration von zwei Systemen über ein Standardprotokoll jedoch zeitaufwändig und erfordert möglicherweise eine gemeinsame Datenbank für die Systeme.

Ein SDK, auch als Anwendungsprogrammierschnittstelle (API) bezeichnet, besteht aus einem DLL-Paket, das von Softwareherstellern erstellt und vertrieben wird und anderen Herstellern die Integration in ihre Systeme ermöglicht. SDKs vereinfachen die Integration, indem sie komplexe Mechanismen vor anderen Softwareentwicklern verbergen, darunter Authentifizierung, Videodekodierung und komplexe Standardprotokolle.

2.1 Vorteile der Systemintegration

Unabhängig von der Art der Integration geben integrierte Systeme Benutzern die Werkzeuge an die Hand, die sie für effizienteres Arbeiten benötigen. So kann eine integrierte Zutrittskontroll- und Videomanagementlösung auf der Benutzeroberfläche für die Zutrittskontrolle beispielsweise Live- oder Wiedergabevideos anzeigen, die mit einem Zutrittskontrollereignis verbunden sind.

Ein weiterer Vorteil der Systemintegration ist, dass Unternehmen bei ihrem Sicherheitssystem nicht mehr auf einen einzigen Hersteller angewiesen sind. Die Nutzung integrierter Lösungen ermöglicht es ihnen, mit mehreren unabhängigen Anbietern zu arbeiten, von denen jeder über ein eigenes Netzwerk von Technologiepartnern verfügt. Das senkt die Kosten, denn wenn ein Unternehmen beispielsweise mit seinem aktuellen Videomanagementsystem (VMS) nicht zufrieden ist, kann es zu einem anderen Hersteller wechseln, ohne von vorne beginnen zu müssen, solange das neue VMS mit den anderen Komponenten des Sicherheitssystems kompatibel ist.

2.2 Nachteile der Systemintegration

Durch Systemintegration kann zwar eine tiefere Produktintegration erreicht werden, doch hat dieser Ansatz auch einige Schwächen.

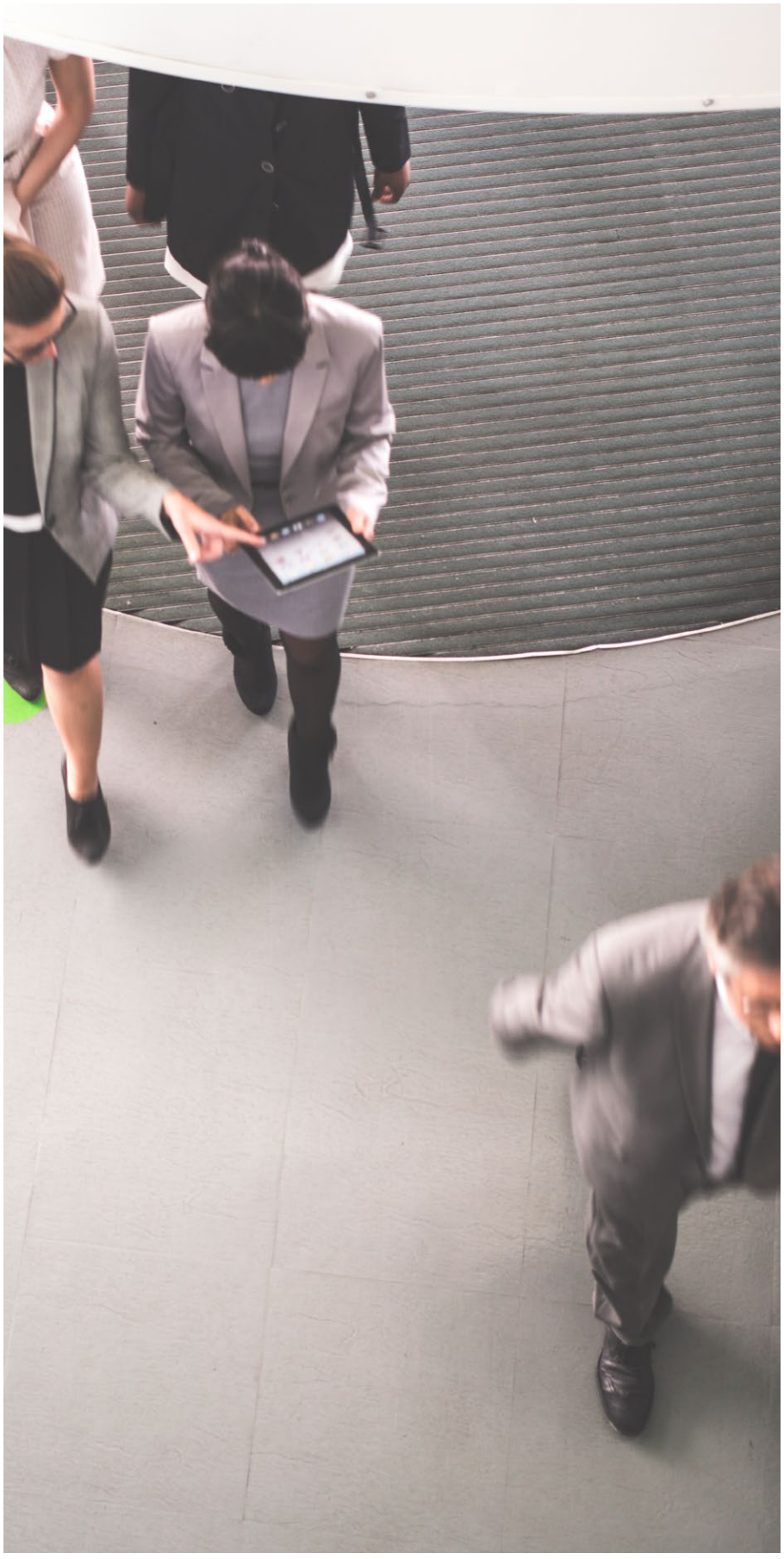
Bei den meisten Integrationslösungen müssen Anwender dennoch mehrere Systeme verwenden, da keines die erforderlichen Funktionen in einer einzigen Benutzeroberfläche bietet. Selbst wenn fortschrittliche Funktionen zum Zeitpunkt der Installation unterstützt werden, können neue Funktionen, die von anderen Anbietern eingeführt wurden, nicht im Primärsystem genutzt werden. Dies hindert Unternehmen daran, ihre Prozesse schrittweise zu modernisieren und neue Bedrohungen zu bewältigen.

Das bedeutet, dass ein Anwender in manchen Fällen zwischen Systemen hin- und herwechseln muss. So kann es z. B. sein, dass ein Anwender im VMS eine Schwenk-Neige-Zoom-Funktion (PTZ) führen muss, weil diese Funktion im Zutrittskontrollsystem (ACS) des Unternehmens nur eingeschränkt möglich ist. Zu den weiteren Einschränkungen von ACS, die Anwender dazu zwingen könnten, zwischen verschiedenen Systemen zu wechseln, zählen die fehlende Unterstützung von Kamerasequenzen, Schwierigkeiten beim Durchsuchen von Videoaufzeichnungen und das Fehlen von Funktionen zur Bewegungssuche.

Künftige Wartungs- und Konfigurationsaufgaben sind weitere Nachteile, die bei einem integrierten System zu berücksichtigen sind. Da der Administrator zwei oder drei unabhängige Systeme konfigurieren und synchronisieren muss, dauert die Wartung länger. Ein integriertes System ist auch deshalb so ineffizient, weil viele der erforderlichen Konfigurationen redundant sind, d. h. Administratoren müssen dieselben Aufgaben auf mehreren Systemen durchführen. Dies ist z. B. der Fall, wenn Sicherheitsmanager für Benutzer in mehreren Systemen Konten erstellen und Berechtigungen festlegen müssen oder wenn Sicherheitsmitarbeiter jede neue Kamera für mehrere Systeme konfigurieren müssen.

Für Unternehmen kann es auch schwierig sein, Upgrades durchzuführen und Support für ihre integrierten Systeme zu erhalten. Da Hersteller ihre Software ständig ändern, um neue Funktionen zu unterstützen, können sich diese Änderungen auf die Funktionsweise bestehender Integrationen auswirken und sogar dazu führen, dass integrierte Systeme nicht mehr kompatibel sind, insbesondere wenn das SDK oder die API des Herstellers geändert wird. In der Folge können sich Upgrades verzögern oder ein Unternehmen kann gezwungen sein, in die erneute Integration der betroffenen Systeme zu investieren.

Außerdem kann es kompliziert sein, Support für eine integrierte Lösung zu erhalten. Da eine integrierte Lösung aus verschiedenen Systemen von unterschiedlichen Anbietern besteht, kann die Behebung von Problemen längere Zeit in Anspruch nehmen. Die Hersteller und oft auch der Systemintegrator müssen zunächst das Problem untersuchen und herausfinden, welches System das problematische Verhalten aufweist. Dann müssen sie das Problem beheben, was je nach der Beziehung zwischen den Herstellern zu weiteren Verzögerungen führen kann.



3

PSIM-Lösungen

Wie bereits erwähnt, kommen die meisten Unternehmen, die sich zu einer Modernisierung ihrer physischen Sicherheitssysteme entschließen, aufgrund der zunehmenden Komplexität und der steigenden Wartungskosten nicht über die zweite Phase hinaus.

PSIM-Lösungen (Physical Security Information Management) können Unternehmen helfen, die dritte Phase ihres Modernisierungsprozesses zu erreichen. Ein PSIM ist ein Softwareprodukt, das mehrere verschiedene Systeme beaufsichtigen kann. Seine Funktion besteht in erster Linie darin, Informationen aus verschiedenen Systemen zu verwalten und diese Daten in einer zentralen Benutzeroberfläche anzuzeigen.

Ein PSIM verfügt i. d. R. nicht über eine integrierte Zutrittskontroll-, Einbruchüberwachungs- oder Videoüberwachungslösung. Stattdessen wird es normalerweise auf der Grundlage mehrerer bereits vorhandener Sicherheitssysteme speziell für ein Unternehmen entwickelt und integriert diese über proprietäre SDKs und APIs. Diese Art von Software ist zwar teuer in der Installation, aber flexibel, da sie mit einer Vielzahl von Sicherheitsprodukten integriert werden kann.

Diese Lösung trägt auch dazu bei, dass Anwender alle in das System eingehenden Daten auf skalierbare Weise verwalten können. Durch die Installation eines PSIM kann ein Unternehmen Arbeitsabläufe entwerfen, um Reaktionen der Anwender zu steuern, und automatisierte Prozesse erstellen, die kein menschliches Eingreifen erfordern.

3.1 Nachteile von PSIM-Lösungen

Unternehmen, die den Einsatz eines PSIM in Erwägung ziehen, sollten sich über mögliche Kompatibilitätsprobleme sowie über die langfristigen Kosten für den Support einer Reihe stark angepasster Produkte im Klaren sein.

Da ein PSIM auf demselben Ansatz wie herkömmliche Integrationen beruht, kann es zu Kompatibilitätsproblemen kommen, wenn eines der Teilsysteme gewartet oder aktualisiert werden muss. Außerdem muss jedes im PSIM integrierte System separat konfiguriert werden. Die Folge ist ein hohes Maß an Redundanz und doppeltem Aufwand. Bei Verwendung eines PSIM müsste ein Unternehmen beispielsweise Benutzer im PSIM und zusätzlich in jedem der zugrundeliegenden Systeme für Zutrittskontrolle, Video, Sprachkommunikation und Einbruchüberwachung konfigurieren. PSIM-Lösungen sind außerdem statisch, was es sehr schwierig macht, Prozesse und Arbeitsabläufe zu verbessern, wenn die Lösung erst einmal implementiert ist.

4

Vereinheitlichung: die offene, zentrale Plattform

Eine offene, zentrale Plattform ist eine umfassende Softwarelösung, mit der Unternehmen ihre unmittelbaren und langfristigen Sicherheitsanforderungen erfüllen können. Sie bietet nahtlose Konnektivität zwischen mehreren Systemen, einschließlich Videoüberwachung, Zutrittskontrolle, Intercom- und Einbruchmeldungssysteme, und stellt damit alle Funktionen, die Sicherheitsmitarbeiter benötigen, in einer zentralen, vereinheitlichten Software-Suite bereit.

4.1 Alle Fakten auf den Tisch

Vereinheitlichung ist außerdem kosteneffektiv. In der Genetec Studie zu den Auswirkungen einer Vereinheitlichung gaben 77 % der Befragten an, dass sie durch Vereinheitlichung den Platzbedarf ihrer Infrastruktur reduzieren konnten, 78 % konnten die Wartungskosten senken und 89 % konnten die Wartungszeit reduzieren.

Eine offene, zentrale Plattform ist kostengünstiger in der Anschaffung und Wartung als individuell integrierte Lösungen und schützt zudem durch Interoperabilität die Sicherheitsinvestitionen eines Unternehmens. Durch die sofort verfügbare Interoperabilität zielt diese Lösung auf den Massenmarkt ab und bietet integrierte Unterstützung für handelsübliche Sicherheitsprodukte, ohne dass für jede Installation Anpassungen erforderlich sind. Zu diesen handelsüblichen Produkten zählen IP-Kameras, DVRs, Türsteuerungen, Alarmsysteme, Sprechanlagen, Ausweisdrucker, Active Directory für die Authentifizierung und Kartenmanagement.

Da eine offene, zentrale Plattform handelsübliche Produkte unterstützt, sind auch Hardwareinvestitionen geschützt. Wenn ein Unternehmen mit der vereinheitlichten Softwarelösung nicht zufrieden ist, kann es die Softwarekomponenten austauschen, ohne erneut in spezielle Appliances investieren zu müssen.

Auch wenn bei der Bereitstellung einer offenen, zentralen Plattform keine Anpassungen erforderlich sind, ermöglicht die Plattform dennoch die Integration von Drittanbieteranwendungen und Anpassungen über ein SDK oder eine API. Da eine zentrale Plattform auf Aktivitäten wie Überwachung und Berichterstellung basiert und nicht für eine einzige Technologie konzipiert ist, unterstützt die Schnittstelle nahtlos neue Integrationen. Mit dieser Art von Tools können Unternehmen bestehende Integrationen nutzen und auch selbst individuelle Integrationen entwickeln und pflegen, anstatt sich auf den Hersteller der zentralen Plattform verlassen zu müssen.

Bei einer vereinheitlichten Lösung müssen Benutzer nur eine einzige Software-Suite erlernen, konfigurieren, aktualisieren und sichern.

4.2 Die vereinheitlichte Serverinfrastruktur

Bei einer wirklich vereinheitlichten Plattform wird die Ressourcennutzung durch die gemeinsame Verwendung von Servern und Datenbanken optimiert:

- Authentifizierung und Berechtigungen
- Lizenzen
- Konfigurationseinstellungen
- Alarmmeldungen und Ereignisse
- Überwachungs- und Aktivitätsprotokoll
- Videoaufzeichnung
- Zugriffsprotokolle
- Zeitpläne

Die Bereitstellung einer vereinheitlichten Serverinfrastruktur bedeutet, dass Benutzer nur eine einzige Software-Suite erlernen, konfigurieren, aktualisieren und sichern müssen. Daher ist es einfacher, eine offene, zentrale Plattform zu installieren und zu verwalten, als ein integriertes System. Auch der Zugriff ist einfacher, da Administratoren das System über eine zentrale Anwendung verwalten können, unabhängig von der Anzahl der Server oder Technologien. Über diese Verbindung können sie dann auf alle vom System angebotenen Services zugreifen, da die Daten an einem zentralen Ort gespeichert sind.

Eine Vereinheitlichung vom Server bis zur Schnittstelle bietet Unternehmen entscheidende Vorteile, unter anderem:

- mehr Effizienz durch die Verwendung einer zentralen Schnittstelle
- mehr situationsbezogene Erkenntnisse durch automatische systemübergreifende Ereigniskorrelation
- geringere Kosten durch gemeinsame Konfiguration und Wartung

4.3 Die Benutzererfahrung

Eine offene, zentrale Plattform bietet außerdem eine zentrale Benutzeroberfläche für mehrere Sicherheitsanwendungen. Dies erleichtert den nahtlosen Wechsel von einer Anwendung zur anderen. Anwender können so einfach und effizient von einer Sicherheitsaufgabe zur nächsten wechseln, was Zeit und Aufwand spart und die Sicherheit erhöht. Bei der Genetec Umfrage unter Kunden, die zentrale Plattformen eingerichtet haben,

- gaben 63 % an, dass sie wesentliche Verbesserungen bei der Ereigniserkennung feststellen konnten
- gaben 59 % an, dass sie wesentliche Verbesserungen bei den Reaktionszeiten feststellen konnten

- verzeichneten 70 % eine wesentliche Beschleunigung der Sammlung von Beweisen und anderer relevanter Informationen

Durch die einheitliche Benutzeroberfläche verringert sich auch der Zeitaufwand für die Schulung neuer Anwender in den einzelnen Systemen der Sicherheitsinfrastruktur. Laut der von Genetec durchgeführten Studie zu den Auswirkungen einer Vereinheitlichung verzeichneten 86 % der Teilnehmer eine Reduzierung des Zeitaufwands für die Schulung neuer Anwender. Außerdem meldeten 88 % eine Reduzierung von Bedienfehlern.

Alle Systeme, die auf einer offenen, zentralen Plattform aufbauen, verfügen auch über gemeinsame Kernfunktionen. Das bedeutet, dass die Arbeitsabläufe für Alarmverwaltung, Ereignisse zu Maßnahme, Berichterstellung, Untersuchung und Vorfälle gleich sind, unabhängig davon, ob es sich um Videoüberwachung, Zutrittskontrolle oder Sprachkommunikation handelt. Dadurch wird die Gesamtzahl der Arbeitsabläufe, die Anwender erlernen und verwenden müssen, erheblich reduziert.

4.3.1 Ereigniskorrelation

Da Ereignisse und Alarme von einer zentralen Serverinfrastruktur verwaltet werden, bietet ein vereinheitlichtes System von vornherein Ereigniskorrelation. Durch die Korrelation von Zutritts- und Videoereignissen ermöglicht eine zentrale Plattform Anwendern beispielsweise eine schnelle Überprüfung der Identität eines Karteninhabers bei einem Zutrittsereignis, um die Authentizität seiner Berechtigungsnachweise zu bestätigen. Durch die Ereigniskorrelation kann auch die Reaktionszeit erheblich verkürzt werden, indem Fehlalarme herausgefiltert werden.

4.3.2 Wartungsfreundlichkeit und unkomplizierter Support

Ein vereinheitlichtes System ist einfacher zu aktualisieren und zu warten als eine integrierte Lösung, da es über eine zentrale Softwareplattform verfügt. Anstatt ein Upgrade mehrerer Systeme vorzunehmen, muss ein Integrator nur die Plattform aktualisieren, was Zeit spart und die Wartung vereinfacht, sollte Support vom Hersteller benötigt werden. Außerdem werden die Ausfallzeiten des Systems bei Upgrades minimiert. In der von Genetec durchgeführten Studie zu den Auswirkungen einer Vereinheitlichung gaben 83 % der Teilnehmer an, dass sie den Zeitaufwand für einzelne technische Probleme reduzieren konnten, und 53 % erklärten, dass die Vereinheitlichung wesentliche Auswirkungen auf die Wartung hatte.

4.3.3 Die Bedeutung von Integration

Im Gegensatz zu Systemen mit offener Architektur verwenden offene, zentrale Plattformsysteme in der Sicherheitsbranche keine Industriestandards für die Integration von Hardware verschiedener Hersteller. Für diese Art der Integration wird zunächst eine generische Integrationsschicht erstellt, welche die gängigsten Funktionen bereitstellt, und dann für jedes spezifische Produkt, mit dem das System integriert wird, ein Treiber entwickelt.

Bei diesen Systemen sind die Hersteller offener, zentraler Plattformen für die Entwicklung, Prüfung und Wartung der Integration mit jedem Gerät verantwortlich, das von ihrem Produkt unterstützt wird. Offene, zentrale Plattformsysteme unterstützen i. d. R. eine Vielzahl von Herstellern, die ähnliche Funktionen und standardisierte Produkte anbieten. Diese Strategie eignet sich gut für spezielle Appliances, da sie feste, genau definierte Funktionen aufweisen. Bei diesen Systemen haben Unternehmen auch die Möglichkeit, den Software- oder Hardwareanbieter zu wechseln, ohne die gesamte vorhandene Sicherheitstechnik ersetzen zu müssen.

5

Auswahl einer Lösung

Vor Beginn des Modernisierungsprozesses müssen Unternehmen eine geeignete Grundlage für ihr neues physisches Sicherheitssystem wählen. Auch wenn die meisten Unternehmen in Systemintegration investieren, ist Vereinheitlichung die bessere Option. Eine Vereinheitlichung ermöglicht nicht nur den Einsatz der effizientesten, flexibelsten und kostengünstigsten Anwendungen, sondern gibt Unternehmen auch das nötige Vertrauen, um den mehrstufigen Prozess hin zu verbesserten Geschäftsabläufen und nachhaltigem, langfristigem Wachstum in Angriff zu nehmen.


25
56
51.79%
8 / 23

Genetec Inc. ist ein innovatives Technologieunternehmen mit einem breit aufgestellten Lösungsangebot, das die Bereiche Sicherheit, Informationen und Operations abdeckt. Das Hauptprodukt des Unternehmens, Genetec™ Security Center, ist eine Plattform für die physische Sicherheit, die IP-basierte Videoüberwachung, Zutrittskontrolle, Nummernschilderkennung (Automatic License Plate Recognition, ALPR), Kommunikation und Analyse vereinheitlicht. Genetec entwickelt auch cloudbasierte Lösungen und Services, welche die Sicherheit erhöhen und dazu beitragen, dass Regierungen, Unternehmen, Verkehrsbetriebe sowie Städte und Gemeinden, in denen wir leben, neue Erkenntnisse über ihre Betriebsabläufe erhalten. Das Unternehmen mit Sitz in Montréal, Kanada, wurde 1997 gegründet. Genetec betreut Kunden weltweit mit einem umfangreichen Netzwerk aus Wiederverkäufern, Systemintegratoren, zertifizierten Vertriebspartnern und Beratern in über 159 Ländern.

Videoüberwachung: Verbessern Sie die Situationseinschätzung und die Sicherheit in Ihrer Stadt dank der Möglichkeit, Kameras für verschiedene Behörden und Organisationen freizugeben. So erhalten Sie ein gemeinsames Bild der Situation und verkürzen die Reaktionszeit bei Vorfällen.

Zutrittskontrolle: Mit einer integrierten IP-fähigen Plattform können Sie die Sicherheit Ihrer Organisation erhöhen, effektiv auf Bedrohungen reagieren sowie schneller klare Entscheidungen treffen – ganz gleich, ob Sie ein neues Zutrittskontrollsystem installieren oder eine bestehende Installation aktualisieren.

Automatische Nummernschilderkennung: Automatisieren Sie die Erkennung gesuchter Fahrzeuge, setzen Sie Parkvorschriften effizienter durch und beschleunigen Sie Untersuchungen zum Schutz der Öffentlichkeit, indem Sie Nummernschilddaten an ausgewählte Behörden und Partnerorganisationen weitergeben, ohne Abstriche beim Eigentums- und Datenschutz.

Operationelle Entscheidungsunterstützung: Gestalten Sie den Umgang mit Vorfällen sowie die Entscheidungsfindung effizienter – mit fortschrittlichen Workflows, die Sicherheitsverantwortliche durch das System führen - von der Warnmeldung über richtlinienbasierte Vorgehensweisen bis hin zum Export detaillierter Fallzusammenstellungen.

Investigative Fallverwaltung: Mit einer Plattform, auf der Sie digitale Beweise zentral ablegen und sicher mit Ermittlern, externen Stellen und der Öffentlichkeit zusammenarbeiten können, lässt sich die Fallverwaltungvereinfachen und Untersuchungen beschleunigen.

Cloud-Services: Erweitern Sie die Funktionen Ihres lokalen Sicherheitssystems und senken Sie die IT-Kosten – dank äußerst skalierbarer On-Demand-Cloud-Services, mit denen Ihre Stadt die sich rasch verändernden Sicherheitsanforderungen problemlos bewältigen und effizienter arbeiten kann.

Genetec Inc.
genetec.com/standorte
info@genetec.com
@genetec

STAND:25-MÄRZ-21