Genetec-Portfolio für Banken und Finanzwesen

Vereinheitlichte Lösungen, die mit Ihnen wachsen

Die Finanzindustrie hat seit jeher mit Silos zu kämpfen – im Personalwesen, in der Technologie und in betrieblichen Prozessen. Als Akteur im Finanzbereich müssen Sie die Anforderungen einer immer komplexeren Bedrohungslage und die zunehmend anspruchsvollen Kundenbedürfnisse erfüllen. Dazu benötigen Sie ein zentralisiertes Sicherheitssystem der Enterprise-Klasse, das nicht nur Mitarbeiter, Vermögenswerte und Daten schützt, sondern sich auch im Hinblick auf zukünftiges Wachstum mit Ihnen weiterentwickelt. Doch wie können Sie die Silos abbauen, um Ihre physische und Cybersicherheitsumgebung zu sichern, Kundendaten zu schützen und die betriebliche Effizienz zu steigern, damit Sie Ihren Kunden eine optimale Erfahrung bieten können?

Genetec™

Wie sich der Bankensektor weiterentwickelt

Veränderte Bedrohungslage

Angriffe auf die Cybersicherheit nehmen in quantitativer und qualitativer Hinsicht zu. Zu den bevorzugten Zielen solcher Attacken gehören Banken. Dies führt zu finanziell äußerst schmerzhaften Umsatz- und Ansehensverlusten. So haben Banken im Jahr 2017 insgesamt 16,8 Milliarden US-Dollar an Cyberkriminelle verloren. Aufgrund der immer stärkeren Vernetzung von Technologien dürfen Sicherheitssysteme nicht mehr allein auf physische Bedrohungen ausgerichtet sein. Unverschlüsselte Kommunikation, unzureichend gesicherte Kameras, Sprechanlagen oder Zutrittskontrollgeräte sind ein gefundenes Fressen für Cyberkriminelle. Wenn Sie mit der Modernisierung beginnen und neue Technologien einführen, um Ihre sensiblen Daten besser zu schützen, drohen neue Schwachstellen zu entstehen.

Ist Ihr Sicherheitssystem so ausgestattet, dass Sie eine Sicherheitsstrategie entwickeln können, die sowohl vor physischen als auch virtuellen Attacken schützt?

Funktionsübergreifende Optimierung

Sicherheits- und IT-Teams stehen unter dem Druck, bei der Umstellung auf digitales Banking tiefere Kosteneinschnitte vorzunehmen. Die Einführung eines modernen Technologiesystems kann hohe Kosten mit sich bringen und in den Prozess sind mehr Teams als früher eingebunden. Wenn Sie die Risiken mithilfe von Technologie verringern wollen, müssen Ihre Systeme abteilungsübergreifend für spürbar mehr Transparenz und Skalierbarkeit sorgen. Nur so überzeugen Sie die Entscheidungsträger im Unternehmen.

Bietet Ihr Sicherheitssystem betriebliche Einblicke, die zur unternehmensweiten Effizienzoptimierung beitragen – von der IT bis hin zum operativen Geschäft?

Digitaler Wandel und Big Data in Filialen

Bankfilialen sind dabei, ihre Services grundlegend umzustellen. Dies betrifft die unterschiedlichsten Bereiche – von Transaktionen bis hin zur Interaktion mit Kunden. Dabei dienen sie als Finanzberater für Kunden, die eine reibungslose und sichere Erfahrung erwarten. Zur Verbesserung der Kundenerfahrung müssen Sie zunächst ein entsprechendes Verständnis entwickeln. Dazu sind Sie auf Daten angewiesen. Ihr Sicherheitssystem basiert auf einem Datenlager, dem Sie nur dann aussagekräftige Informationen entnehmen können, wenn die Daten nicht auf mehrere Silos aufgeteilt sind. Zur Wahrung des Wettbewerbsvorteils müssen Sie in der Lage sein, Ihre Daten richtig zu interpretieren und auszuwerten, um Customer Insights zu präsentieren und die Abläufe in der Filiale zu verbessern.

Wie können Sie Ihre Daten sichern, abrufen und interpretieren, wenn diese in separaten Systemen gespeichert werden, die nicht für eine Zusammenarbeit ausgelegt sind?

Der Bankensektor braucht neue Denkansätze für Zusammenarbeit und Wachstum

Um Risiken zu mindern und Ihren Gewinn zu schützen, wollen Sie Ihre dezentralen Altsysteme ausmustern und durch eine ausgereiftere Sicherheitsinfrastruktur ersetzen. Sie investieren in eine größere Anzahl von Tools, die Ihnen einen Vorteil verschaffen, und richten dabei Ihren Blick auch auf die Cloud. Die Entscheidungen, die Sie heute treffen, können sich auf die zukünftigen Möglichkeiten Ihres Teams auswirken. Stellen Sie die richtigen Fragen im Hinblick auf die Zukunftssicherheit Ihrer Investition? Noch wichtiger: Denken Sie an die Grundlage Ihres Sicherheitssystems und dessen Fähigkeit, sich mit Ihnen weiterzuentwickeln?

Verfügt Ihr Team über eine zentrale Schnittstelle für Recherchen und über die Möglichkeit, Vorfälle über mehrere Filialen und Verwaltungsstandorte hinweg zu überwachen und zu validieren? Oder macht die Suche und Weitergabe von Daten, die in separaten Systemen gespeichert werden, das Weiterleiten von Nachweisen zu einem logistischen Albtraum? Können Sie neue Tools rechtzeitig einführen oder verliert Ihr IT-Team Zeit und Geld durch die Wartung und Aktualisierung paralleler Systeme? Ihr Sicherheitssystem sollte zum Abbau von Datensilos und nicht zur Entstehung neuer Silos beitragen.

Sie benötigen mehr als nur eine Toolsammlung, nämlich eine vereinheitlichte Plattform, die von vornherein auf Sicherheit und Konnektivität ausgelegt ist. Diese sollte auf einer Architektur basieren, mit der Sie entsprechend Ihrem Wachstum skalieren können, die zugänglich, leicht zu verwalten und vor allem sicher ist. Genetec kann Ihnen beim Aufbau einer vernetzten Bank helfen, die mit Ihnen wächst und Ihr Unternehmen schützt, während sich der Markt weiterentwickelt.

Ein Finanzinstitut kann unternehmensweit bis zu

1.000

Anwendungen im Einsatz haben.

Banken geben in der Regel etwa

75 %

ihrer IT-Budgets für die Instandhaltung der bestehenden Architektur aus.

Erfolgreicher Bankbetrieb ohne Hindernisse

Ein Sicherheitsverstoß, der durch ein ungesichertes Gerät oder den Zugriff auf privilegierte Daten verursacht wurde, kann Ihr Unternehmen mehrere Millionen Dollar kosten und sich direkt negativ auf Ihre Marke auswirken. Daher benötigen Sie ein Portfolio von Sicherheitslösungen, die Ihre Systeme miteinander vereinen – mit dem Ziel einer stärkeren Automatisierung und Transparenz bei betrieblichen Abläufen, sodass Sie über Unternehmens- und Filialstandorte hinweg skalieren können.

Kommunikation standortübergreifend zentralisieren

Verschaffen Sie sich von einem zentralen Ort aus umfassende Transparenz über abgelegene Filialen, ohne deren Geschäftsbetrieb zu stören. Erleichtern Sie Recherchen mithilfe einer einzigen Schnittstelle für die Videoüberwachung, Datenerfassung und Alarmverwaltung.

Daten in der Cloud abrufen und sichern

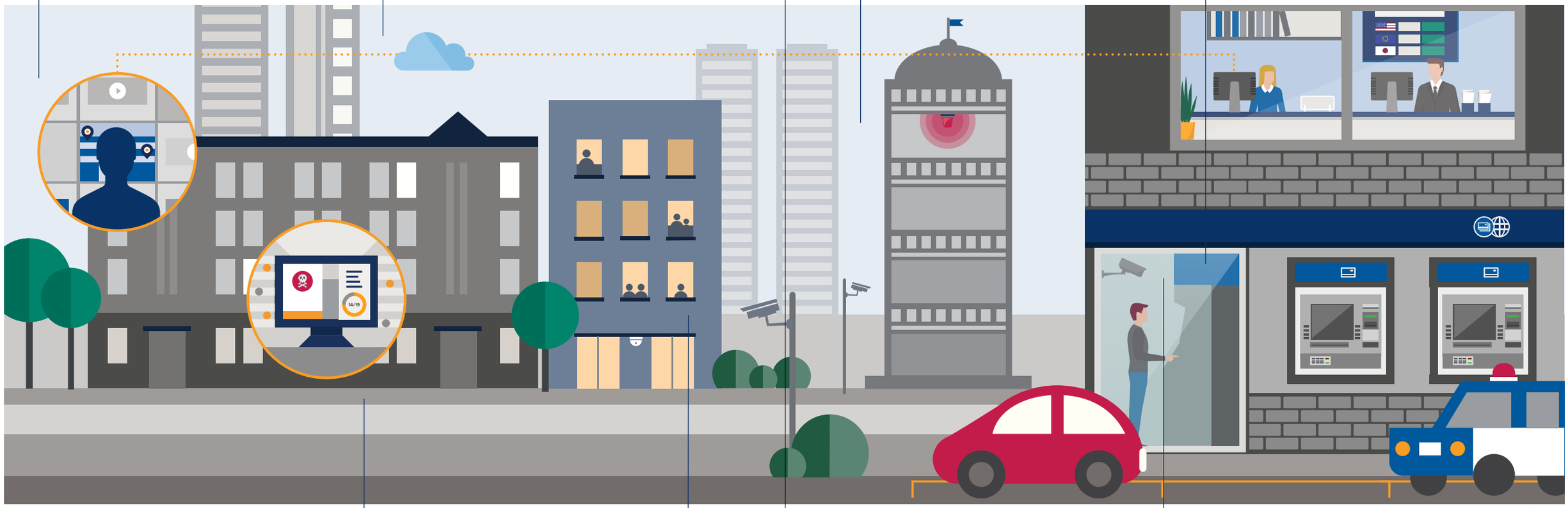
Sorgen Sie dafür, dass Ihre Sicherheit in der Cloud gewahrt und vor Hardwarefehlern und -diebstahl geschützt ist. Senken oder verringern Sie Infrastruktur- und damit verbundene Wartungskosten standortübergreifend und profitieren Sie so von einer höheren Skalierbarkeit.

Vorfälle durch Videotechnik kontextualisieren

Lassen Sie sich Einbruchalarme parallel zu Live-Videos schicken. So können Sie schnell beurteilen, ob auf einen Vorfall reagiert werden muss, und Fehlalarme zugunsten maximaler Effizienz herausfiltern. Fügen Sie dynamische SOPs hinzu, um Ihr Team in Echtzeit durch Vorfallreaktionen zu begleiten.

ATM-Transaktionen mit Videos validieren

Suchen Sie nach Kriterien für verdächtige Transaktionen und zeigen Sie sofort die entsprechenden ATM-Transaktionen parallel zum zugehörigen Video an. So können Sie beurteilen, ob eine weitere Untersuchung notwendig ist, ohne dass Sie zwischen mehreren Systemen hin- und herwechseln müssen.



Cybersicherheit mit automatisierten Dashboards demokratisieren

Verfolgen Sie Ihre Cybersicherheitsbewertung dynamisch und führen Sie präskriptive Schritte aus, um Ihr System widerstandsfähiger zu machen. Sorgen Sie mit anpassbaren Dashboards für die konsequente Anwendung von Best Practices.

IP-basierte Zutrittskontrolle

Sichern Sie zentral den Kunden- und Mitarbeiterzugriff auf Ihre Unternehmens- und Filialstandorte. Verschaffen Sie sich anhand Ihrer Daten weitere hilfreiche Informationen wie Gebäudenutzung, räumliches Bewusstsein und Belegung.

Offene Videoüberwachung auf IP-Basis

Überwachen Sie Unternehmens- und Filialstandorte mit einem IP-basierten Videosystem. Dieses stützt sich auf eine offene Plattform, die Ihnen hilft, Kunden und Mitarbeiter mit Ihrer bevorzugten Hardware zu schützen.

Mit Strafverfolgungsbehörden zusammenarbeiten

Sie können verschlüsselte Videos über eine zentrale Anwendung ganz einfach verwalten, prüfen und freigeben. Dadurch sparen Sie Kosten, die beim Kopieren von Nachweisen auf DVDs entstehen. Machen Sie Passanten unkenntlich, um die geltenden Datenschutzgesetze einzuhalten.

Das Genetec-Portfolio für Banken und Finanzwesen

Unser Portfolio ist speziell auf Finanzinstitute wie Ihres ausgerichtet, die ihre Sicherheitsrisiken verringern, Abläufe automatisieren und sensible Daten schützen möchten, die Ihre Kunden ihnen anvertrauen. Auf Basis flexibler Bereitstellungsmethoden bieten wir ein cloudfähiges Portfolio an, bei dem Sie die Wahl zwischen einem standortgebundenen, vollständig gehosteten oder hybriden Konzept haben. So können Sie Ihr Tempo und den Zeitpunkt der Umstellung selbst bestimmen.

Genetec™ Security Center.

Security Center ist die vereinheitlichte Sicherheitsplattform von Genetec, die IP-Sicherheitssysteme auf einer zentralen intuitiven Oberfläche zusammenführt, um Ihnen die Verwaltung Ihrer Bank oder Ihres Finanzinstituts zu erleichtern. Von Zutrittskontrolle, Videoüberwachung, und automatischen Nummernschilderkennung bis hin zu Einbruchserkennung und Analysen vereinfacht Security Center Ihre Abläufe. Zudem sind Sie mit dieser Sicherheitsplattform in der Lage, Ihre Investitionen zu erweitern und die neuesten Tools einzubinden, um Risiken zu mindern und Ihrer veränderten Umgebung Herr zu werden.

Security Center Omnicast.

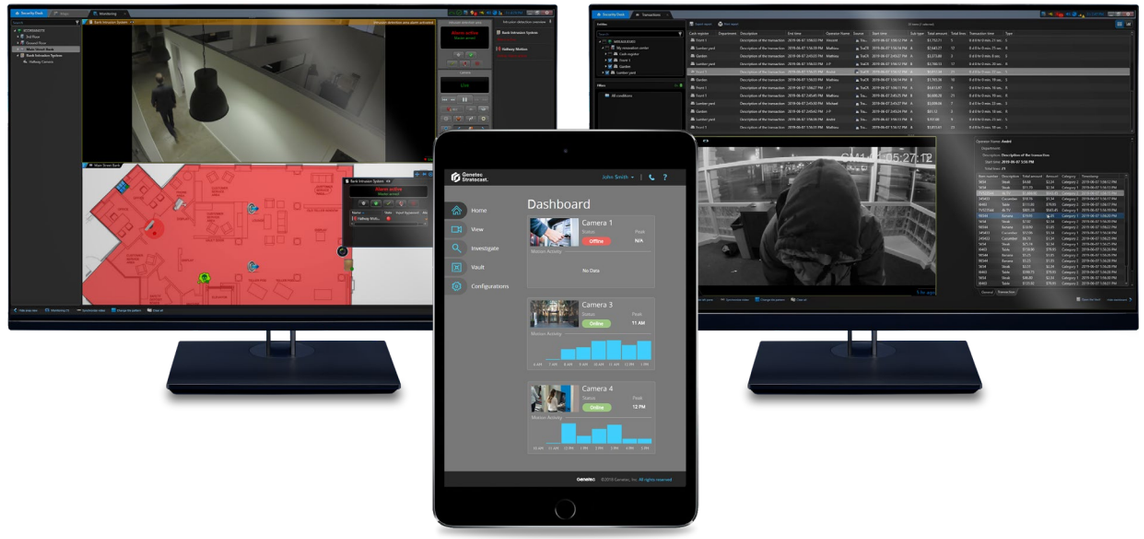
Mit dem IP-Videomanagementsystem (VMS) Security Center Omnicast™ können Banken aller Größen sicher sein, dass ihre Videos aufgezeichnet werden. Das Omnicast-System unterstützt ein breites Spektrum an branchenführenden Kameras, Encodern und CCTV-Geräten. So lässt es sich problemlos skalieren und an die wechselnden Anforderungen Ihrer Bankumgebung anpassen, ohne dass Sie an proprietäre Geräte gebunden sind.

Security Center Synergis.

Mit dem IP-Zutrittskontrollsystem (Access Control System, ACS) Security Center Synergis™ verstärken Sie die Sicherheit Ihrer Bank durch richtlinienbasierte Zutrittsregeln, ohne auf Ihr vorhandenes Netzwerk oder auf Zutrittskontrollgeräte von Dritten verzichten zu müssen. Failover und P2P-Kommunikation sind integriert, sodass Sie für einen ungehinderten Strom von Kunden, Mitarbeitern und Auftragnehmern und somit für eine nahtlose Erfahrung sorgen können.

Security Center AutoVu.

Die automatische Nummernschilderkennung (Automatic License Plate Recognition, ALPR) Security Center AutoVu™ automatisiert das Lesen und Identifizieren von Nummernschildern, sodass Sie auffällige Fahrzeuge leichter orten und zählen können.



Einbruchsüberwachung mit Security Center

Lassen Sie sich von Ihrem Einbruchmeldesystem nützliche Informationen senden und geben Sie Ihren Bedienern Entscheidungsbefugnis auf Basis eines umfassenderen Überblicks über Ihre Sicherheitsumgebung – alles über eine zentrale intuitive Oberfläche. Mit Einbruchsereignissen und -alarmen verknüpfte Videoaufnahmen helfen, die Zahl der Fehlalarme zu reduzieren, und lassen Ihr Sicherheitsteam effizienter arbeiten.

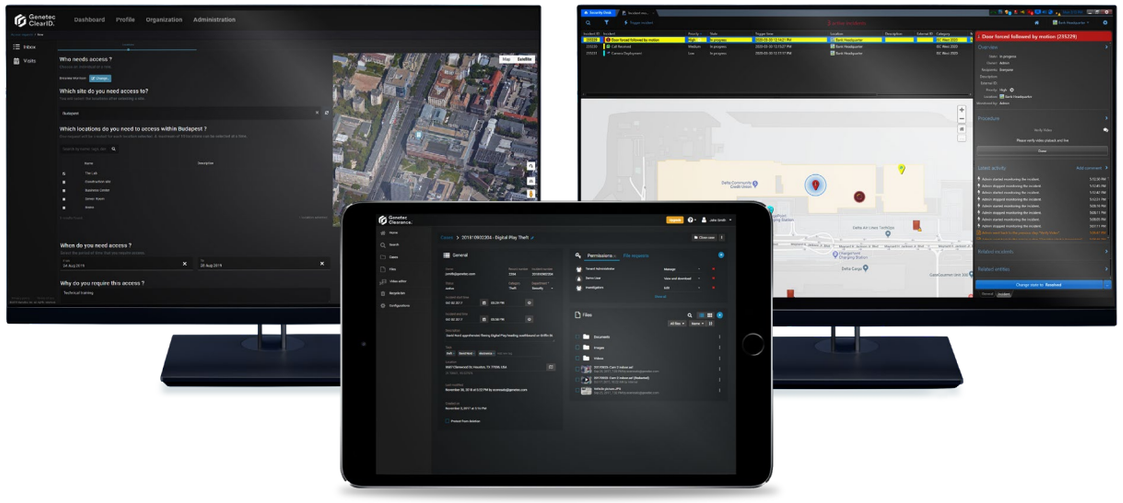
Genetec™ Stratocast.

Genetec Stratocast™ ist eine cloudbasierte Video-Surveillance-as-a-Service-Lösung, mit der Sie kleinere Filialstandorte oder Remote-ATMs zentral überwachen können. Bei dieser skalierbaren und kosteneffizienten Lösung werden keine standortgebundenen Aufzeichnungsgeräte benötigt. Durch den Einsatz von Stratocast entfallen Hardware- und Wartungskosten. Dank redundanter Server sind Sie zudem besser vor Hardwareausfällen geschützt.

Security Center Transaction Finder

Erleichtern Sie die Validierung von ATM-Transaktionen im Rahmen der Betrugsbekämpfung. Mit Transaction Finder können Sie Videos und Videoanalysen mit möglicherweise fragwürdigen ATM-Transaktionen (z. B. Skimming) in Ihren Filialen verknüpfen, sodass Ihr Team in kürzerer Zeit mehr verdächtige Transaktionen feststellen kann.

Das Genetec-Portfolio für Banken und Finanzwesen



Genetec ClearID™
ist ein Identitäts- und Zutrittsmanagementsystem, mit dem Sie Ihre Sicherheitsrichtlinien an allen Unternehmens- und Filialstandorten automatisieren können. Verwalten und automatisieren Sie die Zutrittsrechte von Besuchern, Mitarbeitern und Auftragnehmern, um jederzeit für Compliance und Sicherheit zu sorgen.

Genetec Clearance™ ist ein kooperatives digitales Nachweisverwaltungssystem zum sicheren Erfassen, Verwalten und Weitergeben von Nachweisen aus unterschiedlichen Quellen an Strafverfolgungsbehörden und Auditoren und trägt so zur schnelleren Durchführung von Untersuchungen bei.

Genetec Mission Control™
ist ein kooperatives Entscheidungsmanagement-system, mit dem Ihre Filialen nicht nur einfache Ereignis- und Alarmverwaltung betreiben, sondern auch Daten von Tausenden Sensoren und Sicherheitsgeräten erfassen und auswerten können. Filtern Sie Fehlalarme heraus, etwa bei geöffneten Türen, entdecken Sie besonders komplexe Situationen und Vorfälle und leiten Sie Ihre Sicherheitsteams so an, dass sie vorschriftsgemäß oder richtlinien-konform reagieren.

Funktionen für Banken und Finanzwesen

Unsere integrierten Kernfunktionen

Security Center Federation (standortgebunden oder als Service)
Zentralisieren Sie die Überwachung, Berichterstellung und Verwaltung Ihrer Filialen und greifen Sie zentral auf alle Systeminformationen zu.

Kartenbasierte Echtzeitüberwachung
Dynamische Echtzeitkarten dienen zur Veranschaulichung Ihrer Umgebung. Überwachen Sie Zutrittskontroll- oder Einbruchsereignisse und sehen Sie sich Live-Videos und Aufzeichnungen an.

Disaster Recovery/Failover
Konfigurieren Sie Failover-Verzeichnisse für Ihre Standorte. Stellen Sie sicher, dass Ihre Daten und Speicher im Katastrophenfall und bei Außerbetriebnahme von Servern zugänglich sind.

Mobile Apps und Web-Apps
Sorgen Sie durch Positions-Tracking, Messaging, Videostreaming und Archivfreigabe dafür, dass alle Mitarbeiter auf dem gleichen Stand sind. Sehen Sie sich Videoaufnahmen an, steuern Sie PTZ-Kameras, empfangen Sie Alarme und heben Sie Türsperren auf.

Überwachung der Systemverfügbarkeit (System Availability Monitoring, SAM)
Mit Echtzeit-Zustandsinformationen aus allen Ihren Systemen können Sie Probleme rasch untersuchen und lösen, ehe sich diese auf den Betrieb und die Sicherheit auswirken. Automatisieren Sie den Systemzustand mit detaillierten Kennzahlen, z. B. Verfügbarkeit von Kameras, Lesegeräten und Einbruchserkennung.

Zustands- und Ereignisüberwachung
Empfangen Sie Echtzeit-Benachrichtigungen und -Alarme über den Systemstatus und über Ereignisse, die mit dem Systemzustand zusammenhängen. Rufen Sie über eine eigene Engine Statistiken über den Systemzustand ab, um die Systemleistung vollständig zu optimieren.

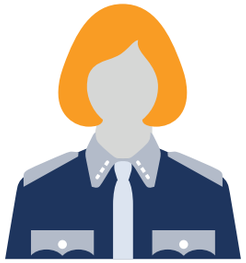
Cloudspeicher
Senken Sie die Kosten für physische Datenspeicher in kleinen Filialen und greifen Sie auf einen einfachen, sicheren und leicht zu verwaltenden Cloudspeicher zu.

Bedrohungsstufenverwaltung
Ändern Sie das Verhalten und die Vorgänge des Security Center-Systems. Als Reaktion auf Ereignisse können Mitarbeiter das Verhalten sofort ändern.

Intelligentes Schlüsselmanagement
Stellen Sie von mechanischen Metallschlüsseln auf ein elektronisches Schließsystem um, lassen Sie die Probleme beim Austausch von Schlössern hinter sich und erfüllen Sie die Prüf- und Rechenschaftspflicht.

Umfassende Datensicherheit und umfassender Datenschutz
Schützen Sie Ihre Video-, Karteninhaber- und Systemdaten durch eine sichere Kommunikation zwischen Clients, Servern, Edge-Geräten und allen betreffenden Parteien. Security Center verschlüsselt übertragene bzw. stationäre Videodaten und den Export von Nachweisen.

Wer profitiert davon?



Manager für physische Sicherheit (Unternehmen und Filiale)

Diese Person ist für die physische Sicherheit verantwortlich und sorgt für die durchgängige Bereitstellung einer Sicherheitstechnologie mit offener Architektur – ob standortgebunden, in der Cloud oder eine Kombination aus beidem. Personen in dieser Funktion profitieren von einem geringeren Upgrade- und Wartungsaufwand, indem sie ein vereinheitlichtes System mit mehreren Verteidigungslinien zur Beseitigung von Schwachstellen einführen.

IT-Manager

Zu den Aufgaben von IT-Managern gehört es, die Einhaltung von Cybersicherheitsstandards beim Betrieb des Systems kontinuierlich in Echtzeit zu aktualisieren und anzuzeigen. Durch End-to-End-Verschlüsselung und Multi-Faktor-Authentifizierung wird die ständige Einhaltung dieser Standards sichergestellt. Die Umstellung auf die Cloud ist unkompliziert und flexibel.

Leitender Betrugs-/Datenanalyst

Die Mitarbeiter des Teams können Untersuchungen schneller durchführen und deutlich produktiver arbeiten, indem sie ATM-Transaktionen durch Videoaufnahmen und -analysen validieren. So können verdächtige Aktivitäten bevorzugt untersucht werden. Weitere Vorteile ergeben sich durch die unkomplizierte Weitergabe von Nachweisen an Strafverfolgungsbehörden und Wirtschaftsprüfer, während die Daten der Kunden geschützt sind.

GSOC-Manager

GSOC-Manager überwachen Filial- und Unternehmensstandorte zentral und optimieren die Reaktion auf Alarme dank einer vereinheitlichten Übersicht über Einbruchmeldungen oder Zutrittskontrollereignisse mit zugehörigen Videoaufnahmen. Das cloudbasierte System ermöglicht eine einfache Überwachung von jedem Standort aus.

Der Abbau von Silos und die Vernetzung der Bank gehen über die physische Sicherheit hinaus. In einer zunehmend miteinander vernetzten Branche, deren Umfeld sich immer wieder ändert, benötigen Banken mehr als nur vernetzte Tools, um für ständige Datensicherheit und reibungslose Abläufe zu sorgen. Eine vereinheitlichte Sicherheitsplattform bildet die Grundlage, auf der Sie Ihre Sicherheitsüberwachung über eine intuitive Oberfläche zentralisieren können.

Durch die Zentralisierung in einem einheitlichen Sicherheitsportfolio kann Ihr Team die Cyberrisiken verringern sowie die Handhabung und Untersuchung von Vorfällen optimieren. Mit dem Genetec-Portfolio für Banken und Finanzwesen verfügen Sie über eine zentrale Schnittstelle für alle Ihre Lösungen. Somit können Sie Ihr Unternehmen skalieren, um sich gegen die Gefahren der Gegenwart zu wappnen und für die Zukunft zu planen.

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

STAND: 08.04.2020