

Das Genetec Portfolio für Energie- und Versorgungsbranche

Projekte mit vereinheitlichten Lösungen optimieren



Energie- und Versorgungsbetriebe wenden sich vom analogen, skalenbasierten und zentralisierten Modell ab und werden immer digitaler und dezentraler. Die sich stetig verändernden Anforderungen von Verbrauchern, Behörden sowie einer immer komplexeren Bedrohungslandschaft zwingen Unternehmen dazu, ihre Sicherheitsstrategie an die aktuellen Gegebenheiten anzupassen. Die Frage lautet: Wie können Sie der Entwicklung einen Schritt voraus sein und die Sicherheit Ihrer kritischen Infrastruktur optimieren, um eine sichere Arbeitsumgebung zu gewährleisten und auf zukünftige Anforderungen vorbereitet zu sein?

Die Entwicklung der Energie- und Versorgungsindustrie



Erneuerbare Energien fördern Fusionen und Übernahmen

Globale Investitionen in erneuerbare Energien sowie die Konvergenz der Öl-, Gas- und Stromversorgung sorgen für Konsolidierung der Branche durch Fusionen und Übernahmen. Laut EY Power Transaction Report dominieren dabei Transaktionen im Bereich der erneuerbaren Energie mit einem Anteil von 61 % am Transaktionsvolumen.¹ Fusionen betreffen auch Sicherheitsabteilungen.

Es stellt sich die Frage, wie die Sicherheit standardisiert und zentralisiert werden kann, wenn die bestehenden Systeme für einen solchen Schritt nie ausgelegt waren?



Änderungen von Vorschriften

Verbraucher, der Markt sowie kritische Infrastrukturen sollen durch neue Gesetze und Vorschriften für den Energiesektor besser geschützt werden. Im Zuge der Globalisierung kommt es verstärkt zur Zusammenarbeit innerhalb der Lieferketten. Allerdings wurden dadurch auch fast 60 % der Organisationen Opfer von Sicherheitsverstößen, die durch Lieferanten verursacht wurden.² Sicherheitsteams stehen vor der Aufgabe, ihre Lösungen und Verfahren an die regulatorischen, juristischen und compliance-technischen Vorgaben der neuen digitalen Ära anzupassen und zu optimieren.

Wie können Sie also sicherstellen, dass Ihre Abläufe stets konform sind und gleichzeitig noch einfacher Prüfberichte erstellen?



Die Bedrohungslandschaft wird komplexer

Das industrielle Internet der Dinge (Industrial Internet of Things, kurz IIOT) und die zunehmende Beliebtheit intelligenter Stromnetze gehen mit der Einbeziehung von Netzwerken einher, die Netze und Verbraucher mit Datenbanken verbinden. Dadurch wächst aber auch die Zahl der potenziellen Angriffspunkte für Cyberangriffe. Hackergruppen sind deutlich besser organisiert und fortgeschrittener als Einzelkämpfer. Immer häufiger finden Cyberangriffe auch absichtlich oder versehentlich über vertrauenswürdige interne bzw. externe Stakeholder statt.³

Arbeiten Ihre Systeme für physische Sicherheit und Cybersecurity zusammen, um kritische Infrastrukturen gegen aktuelle und zukünftige Bedrohungen ausreichend zu schützen?

Quellen:

1. „How demand for renewables drives M&A activity“

2. Ponemon Institute Cyber Risk Report

3. „Insiders are today's biggest security threat“

Halten Sie Schritt mit Ihrem Umfeld

Die Nachfrage nach erneuerbaren Energien ist der zentrale Markttrend, da Regierungen weltweit saubere Energieziele für die Zukunft festgelegt haben. Angesichts des regulatorischen Drucks, des verschärften Wettbewerbs und der aktuellen Marktvolatilität müssen Sie jedoch mit der dynamischen Marktentwicklung Schritt halten können. Wie können Sie also eine steigende Anzahl von Anlagen in einem dynamisch skalierenden und weit verstreuten Gebiet schützen, während Hackergruppen immer neue und komplexere Angriffe starten und sich Rahmenbedingungen durch regulatorische Vorschriften stetig ändern?

Betreiber kritischer Infrastrukturen müssen eine Sicherheitsvision haben, die sowohl aktuelle als auch künftige Anforderungen berücksichtigt. Diese Vision sollte sich nicht auf den Schutz von Personen und Sachen beschränken. Sie sollte Kernbestandteil Ihrer betrieblichen, sicherheitstechnischen und regulatorischen Strategie sein. Leitet Ihre Sicherheitsplattform die Mitarbeiter durch die Compliance-Prozesse, wenn neue Vorschriften eingeführt werden? Wissen Sie, wie viel Zeit Sie für die Erstellung und den Austausch von Sicherheitsnachweisen aus unterschiedlichen Systemen benötigen, die nicht für eine Zusammenarbeit konzipiert wurden, um die Anforderungen bei einem Audit zu erfüllen?

Die Sicherheit ist Kernelement Ihres Unternehmens. Sie sollte nicht nur Sie schützen, sondern auch die notwendige Plattform bieten, um sicherzustellen, dass Mitarbeiter und Auftragnehmer zu Ihrem Erfolg beitragen. Genetec kann Ihnen dabei helfen, indem verschiedene Sicherheitssysteme miteinander verbunden, die Compliance maximiert und gleichzeitig laufende Prozesse auf die nächste Stufe gehoben werden.

Geldstrafen können bis zu einer **Million US-Dollar** pro Tag betragen.



* Quelle: North American Electric Reliability Corporation

Aufbau vernetzter, resilienter Arbeitsorte

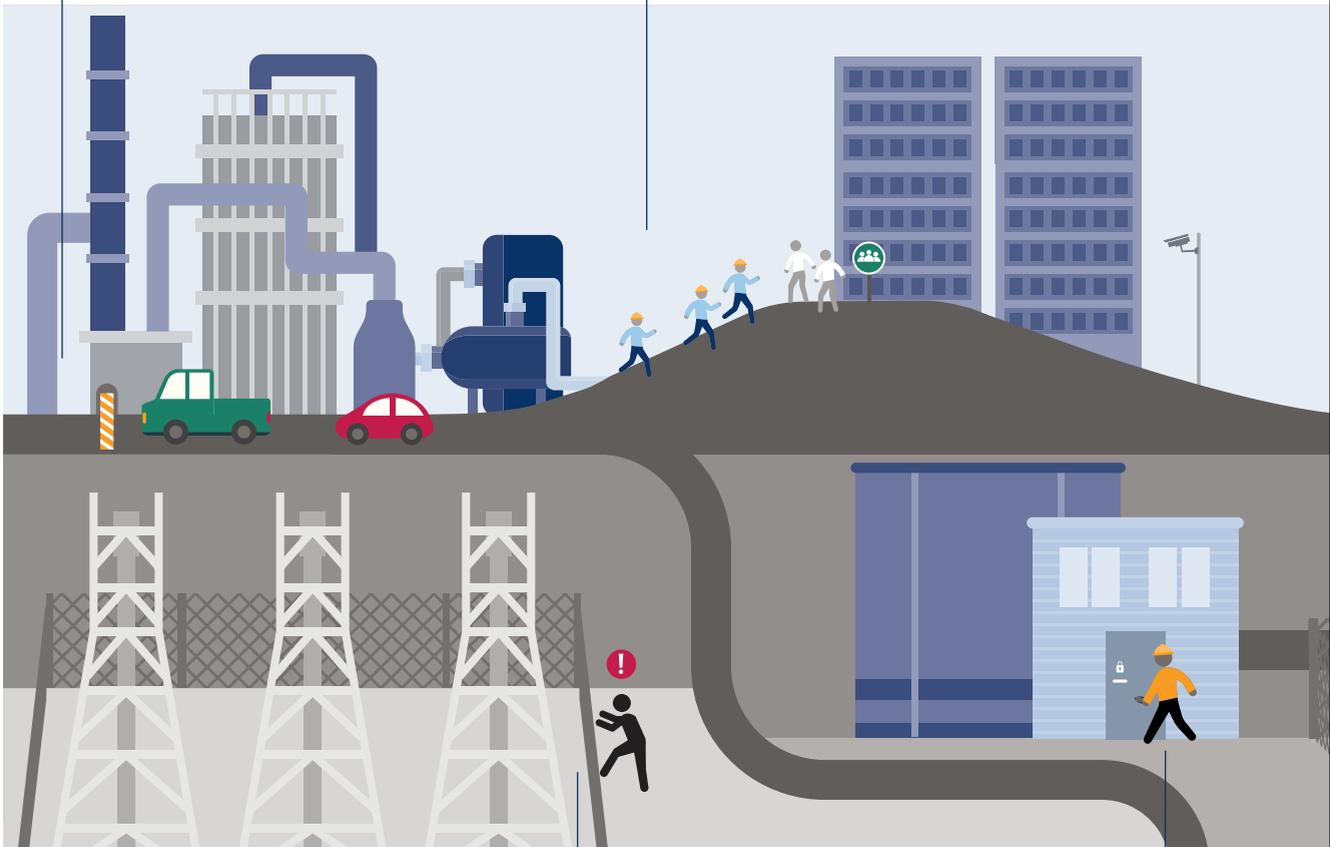
Betriebsunterbrechungen können Millionenschäden verursachen. Aus diesem Grund sollten betriebliche Prozesse möglichst reibungslos ablaufen und Compliance, Sicherheit sowie Abläufe synchron aufeinander abgestimmt sein, um eine größtmögliche Effizienz zu gewährleisten. Sie sollten auf ein Portfolio an Sicherheitslösungen zurückgreifen, das auf die Erfordernisse von kritischen Infrastrukturen zugeschnitten ist. Sie sollten den Betrieb automatisieren und umfangreiche Einblicke ermöglichen.

Erweiterung von Betriebshöfen- und Perimeterschutz

Mit der automatischen Nummernschilderkennung (Automatic License Plate Recognition, ALPR) wissen Sie immer, welche Fahrzeuge sich auf dem Betriebshof oder Standort befinden. Sie können den Fahrzeugbestand in Echtzeit einsehen und den Zutritt zu bestimmten Bereichen anhand des Nummernschilds verwalten.

Erfassung aller Personen in Echtzeit

Erfassen Sie jederzeit alle Mitarbeiter und externe Dienstleister im Routinebetrieb oder im Rahmen von Ernstfällen und Evakuierungen. Geben Sie aktuelle Berichte über Personenzahlen an die Sicherheitsteams weiter, um den Schutz aller Personen vor Ort zu gewährleisten.



Eindringlinge noch vor dem Perimeter erkennen

Mithilfe von Radarsystemen, LiDar, Zaunalarmen und Videoanalysen erkennen Sie potenzielle Eindringlinge, bevor sie das Gelände erreichen.

Bereichsspezifischer Zutritt für externe Dienstleister

Stellen Sie sicher, dass externe Dienstleister nur die Zutrittsrechte erhalten, die sie im Rahmen ihrer Funktion benötigen.

Optimierung Ihrer Beweissicherung

Automatisieren Sie die Weitergabe von digitalem Beweismaterial an interne und externe Prüfer, statt diese auf DVDs zu brennen.

Digitalisierung Ihrer Standardbetriebsverfahren (SOPs)

Digitale SOPs führen Ihre Mitarbeiter im Ernstfall durch vorab benutzerdefinierte Prozesse. Durch Exportfunktionen und die Weitergabe von Ablaufdiagrammen sowie Vorfallsberichten an Prüfer bleibt die Compliance gewährleistet.



Zugangsverwaltung mit IP-basierter Zutrittskontrolle

Die Migration von traditionellen Metallschlüsseln zu elektronischen Key-Cards sowie eine fehlertolerante IP-basierte Zutrittskontrolle ermöglichen es Ihnen, Ein- und Ausgänge von sensiblen Bereichen für Mitarbeiter, externe Dienstleister und Besucher adäquat zu sichern.

Maximale Videoabdeckung

Ein Team mit klarem Blick auf das Geschehen kann schneller auf Bedrohungen reagieren. Nutzen Sie die Vorteile cloudbasierter Videoüberwachung zum Schutz mehrerer Standorte.

Das Genetec Portfolio für Energie- und Versorgungsbranche

Starke Sicherheitsanwendungen auf einer Oberfläche darzustellen, kann ein komplexes Unterfangen sein und stößt schnell an seine Grenzen. Aus diesem Grund bieten wir ein Portfolio an vereinheitlichten Sicherheitslösungen an, das von Grund auf speziell für Betreiber kritischer Infrastrukturen entwickelt wurde. Sicherheitsteams können damit von einer zentralen Leitstelle aus alle Sicherheitsprozesse und -mechanismen optimieren und so die betriebliche Compliance sowie Effizienz gewährleisten.



Security Center ist die vereinheitlichte Sicherheitsplattform von Genetec, die unterschiedliche IP-basierte Sicherheitssysteme auf einer Plattform zusammenführt. Security Center vereinheitlicht Videoüberwachung, Zutrittskontrolle, Nummernschild- und Einbruchserkennung sowie weitere Systeme auf einer zentralen Plattform und bietet zusätzlich tausende Add-Ons für Betreiber kritischer Infrastrukturen.



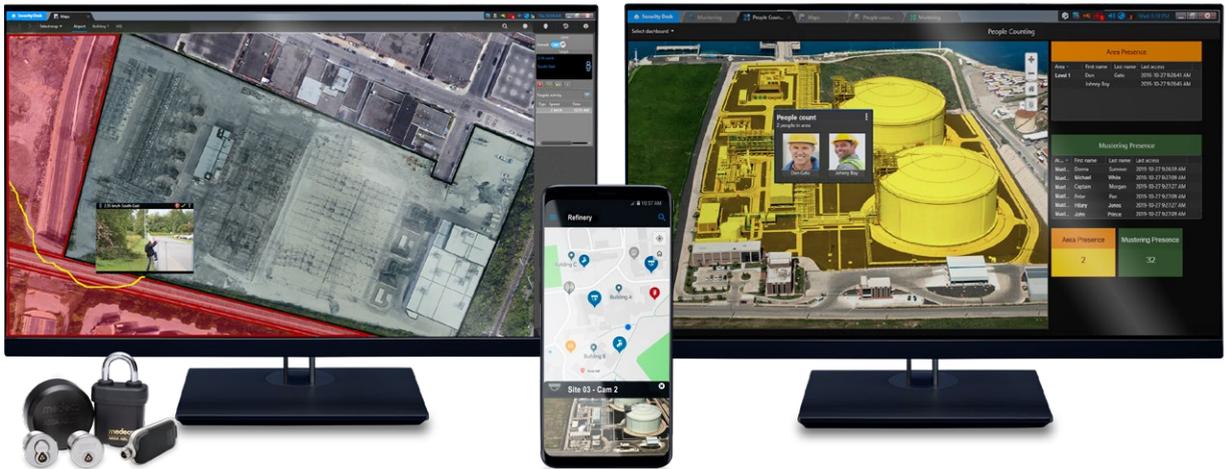
Das IP-Video managementsystem (VMS) Security Center Omnicast™ zeichnet Videomaterial auch an weit entfernten Standorten zuverlässig auf. Security Center Omnicast unterstützt ein breites Spektrum an VMS-Hardwareherstellern, damit Sie IP-Video unabhängig von Ihrer eingesetzten Hardware nutzen können.



Das IP-Zutrittskontrollsystem (Access Control System, ACS) Security Center Synergis™ gibt Ihnen volle Kontrolle über den Zugang von Personen und Fahrzeugen an Ihren Zutrittspunkten und zu gesicherten Bereichen. Während das Team ungehindert arbeitet, ist das ACS mit integriertem Failover sowie Peer-to-Peer-Kommunikation stets verfügbar.



Die automatische Nummernschilderkennung (Automatic License Plate Recognition, ALPR) Security Center AutoVu™ liest und erkennt Nummernschilder automatisch, sodass ein- und ausfahrende Transportfahrzeuge, Besucher und Mitarbeiter leichter überwacht werden können.



Einbruchversuche und zutrittsbeschränkte Bereiche

Eindringlinge werden gemeldet, bevor diese den umzäunten Bereich erreicht haben. So senken Sie gleichzeitig die Wahrscheinlichkeit falscher Alarme. Nutzen Sie die Radar- und LiDar-Zaunerkennungstechnologie, um Eindringlinge und Drohnen zu erkennen, abzuschrecken und zu bekämpfen. Sich bewegende Ziele werden intuitiv auf geografischen Karten verfolgt, sodass Ihr Team mit jederzeit zuverlässig reagieren kann.

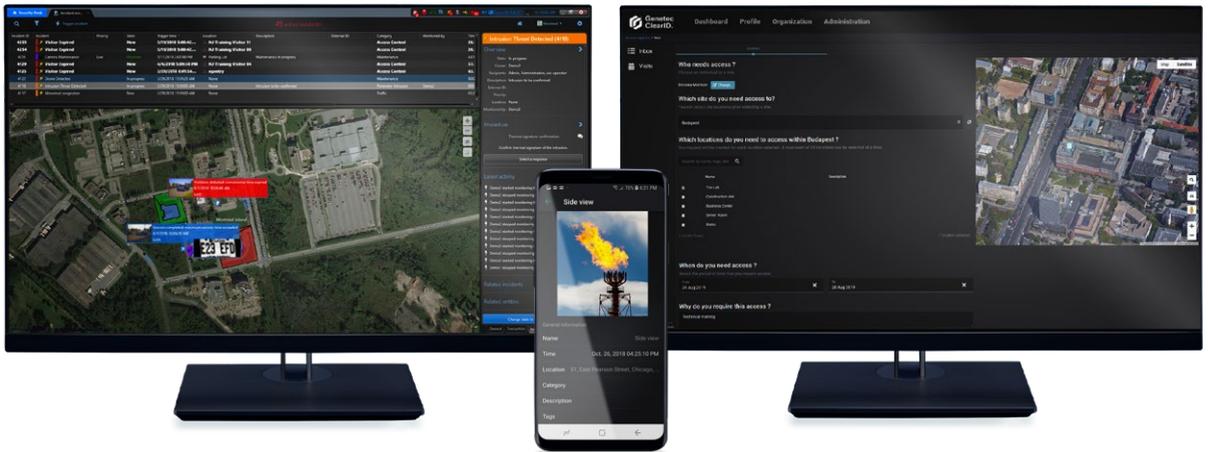
Intelligentes Schlüsselmanagement

Steigen Sie von mechanischen Schließern auf ein elektrisches Schließsystem um. Profitieren Sie von den Vorteilen der IP-basierten Zutrittskontrolle, ohne zusätzliche Kosten für einen Online-Zugangspunkt. Schwer erreichbare Bereiche ohne Personal wie Tresore, Schränke, Tore oder Zäune müssen nicht mehr extra verkabelt oder mit Strom versorgt werden. Dank umfassender Sicherheit gehören aktuelle Probleme beim Schlüsseltausch oder bei verlorenen Schlüsseln der Vergangenheit an.

Berichte über Personenzählungen und Verantwortlichkeiten

Dank der integrierten Personenzählung mit Zutrittskontrollereignissen werden Sie jederzeit darüber informiert, wo sich alle Mitarbeiter, Auftragnehmer und Besucher aufhalten. Verwandeln Sie ein mobiles Gerät während einer Notfall-evakuierung an der Sammelstelle in ein Lesegerät, damit Sie genau wissen, wer sich in der sicheren Zone befindet. Sie können Personenbewegungen anhand von Karten oder visuellen Berichten und Dashboards verfolgen und automatisch Berichte an wichtige Mitarbeiter der Organisation sowie Ersthelfer vor Ort senden.

Das Genetec Portfolio für Energie- und Versorgungsbranche



Genetec Mission Control™ ist ein kooperationsbasiertes Entscheidungsmanagementsystem, das das Sicherheitspersonal durch Sicherheitsvorfälle und betriebliche Aufgaben leitet. Mit Standardbetriebsverfahren (SOPs), die speziell für die Compliance entwickelt wurden, sorgen Sie dafür, dass Ihr Team die Vorschriften einhält.



Genetec Clearance™ ist ein digitales Beweismanagementsystem zur sicheren Erfassung, Verwaltung und Weitergabe von digitalem Beweismaterial von verschiedenen Standorten an Aufsichts- und Strafverfolgungsbehörden. Informationen von Beweismaterial zu Sicherheitsvorfällen bis hin zu Sicherheitsmaßnahmen wie Brandschutzüberwachung lassen sich schnell und sicher weitergeben.



Genetec ClearID™ ist ein Identitäts- und Zutrittsmanagementsystem, mit dem Sie Ihre Sicherheitsrichtlinien standortübergreifend automatisieren können. Die zentrale Verwaltung von Zutrittsrechten von Besuchern, Mitarbeitern und externen Dienstleistern ermöglicht die Erstellung eines umfassenden Schlüssel- und Zutrittsverwaltungsplans und gewährleistet eine durchgängige Compliance und hohe Sicherheitsstandards.

Funktionen speziell für Betreiber kritischer Infrastruktur

Unsere integrierten Kernfunktionen

Verwaltung von Bedrohungsstufen

Security Center Security Center kann Prozesse jederzeit dynamisch anpassen, um im Ernstfall sofort reagieren zu können. Bei einer Evakuierung können Sie zum Beispiel alle Türen sofort entriegeln und die Bilder pro Sekunde (Frames per Second, FPS) ihrer Videoüberwachungskameras hochsetzen.

Camera Integrity Monitor

Erstellen Sie einen Plan zur Wartung Ihrer Kameras und erkennen Sie potenzielle Manipulationen und unerwünschte Bewegungen. So stellen Sie sicher, dass Ihr Gelände und Ihre Sicherheitsbereiche ordnungsgemäß überwacht werden und Ihre Kameras vorschrittmäßig funktionieren.

Umfassende Datensicherheit und umfangreicher Datenschutz

Schützen Sie Ihre Video-, Karteninhaber- und Systemdaten durch die sichere Kommunikation zwischen Clients, Servern und Edge-Geräten. Security Center verschlüsselt Videodaten sowie den gesamten Export von Nachweisen, von der Quelle bis zum Speicherort.

Schnellsuche

Mit einer gezielten Videosuche suchen und finden Sie im Handumdrehen, wonach Sie suchen. Haben Sie einen relevanten Bereich festgelegt, werden Ihre Archive auf verdächtige Aktivitäten in dieser Szene durchsucht und relevantes Bildmaterial ermittelt, damit Sie Ihre Ermittlungen eingrenzen können.

SCADA-Integration

Über eine Verbindung zu SCADA-Daten mit Standardprotokollen wie OPC, BACnet usw. können Sie Ihre industriellen Steuerungsdaten in Security Center integrieren.

Mobile Zutrittskontrolle

Durch die Umwandlung eines Tablets in einen Zutrittskontrollleser wissen Sie immer, wo sich Ihre Mitarbeiter, Auftragnehmer und Besucher aufhalten, selbst in offenen Bereichen und Bussen.

Visuelles Tracking

Per Klick auf vorkonfigurierte grafische Overlays können Sie die benachbarte Kamera direkt über die Videokachel auswählen. Die Overlays liefern eine direkte visuelle Darstellung, sodass Sie nicht aufwendig suchen müssen, sondern Live-Überwachung und Untersuchungen effizient durchführen können.

Auswahl an Bereitstellungsoptionen

Unabhängig davon, ob Ihr System vor Ort, in der Cloud oder irgendwo dazwischen implementiert ist, profitieren Sie von einem stetigen Wertstrom, der selbst Ihre entferntesten Standorte erreicht.

Hochverfügbare Notfallwiederherstellung

Mit der Konfiguration von Failover-Verzeichnissen für alle Ihre wachsenden Standorte sorgen Sie dafür, dass Ihre Daten und Speicher unterbrechungsfrei zugänglich sind – auch im Notfall und wenn Server offline sind.

Visuell aufbereitete Berichte

Mit der Generierung leicht verständlicher Berichte mit Grafiken und Diagrammen nutzen Sie die Daten Ihres Sicherheitsnetzwerks und verschaffen sich so einen besseren Überblick über Ihre Organisation.

Datentransport

Mit der Integration Ihrer Daten in eine Datenbank Ihrer Wahl für die ausführliche Analyse und Visualisierung machen Sie Ihre Ereignisdaten von Security Center unabhängig.

Vereinheitlichtes Kommunikationsmanagement

Mit SIP-basierter Kommunikation erweitern Sie Ihre Sicherheit. Sie können ein- und ausgehende Anrufe über Sprechanlagen verwalten und über integrierte Audio- und Videoanrufe mit Kollegen zusammenarbeiten.

Wer profitiert?



Verantwortlicher für den Sicherheitsbetrieb

reduziert mit einer vereinheitlichten Sicherheitsvision die Zahl der genutzten Sicherheitsanwendungen, sodass sein Personal eine kürzere Einarbeitungszeit benötigt und im Ernstfall souverän reagieren kann.



Sicherheitsmanager

sinkt die Zahl der Vorfälle, indem er Pläne für die Sicherheit und Vorfallprävention erstellt, die mit seinen Sicherheitsverfahren koordiniert sind.



IT-Manager

profitiert von einer kontinuierlichen Bereitstellung modernster Sicherheitstechnologie - lokal, hybrid und in der Cloud. Einvereinheitlichter Sicherheitsansatz reduziert den Aufwand zur Aktualisierung und Wartung von Systemen.



Operational Compliance Manager

optimiert das Risikomanagement, die Kontrolle und die Unternehmensführung durch Workflows und Automatisierung, die das Personal anleiten, gemäß den SOPs zu reagieren. Zudem profitiert das Team vom einfachen Austausch von Beweisen mit externen Stellen.

Sich ändernde Vorschriften und immer neue Sicherheitsrisiken erschweren es Betreibern kritischer Infrastrukturen, der aktuellen Entwicklung immer einen Schritt voraus zu sein. Die Zentralisierung auf ein einheitliches Sicherheitsportfolio hilft Ihrem Team, das Sicherheitsrisiko zu senken, Ihre Sicherheitsmaßnahmen zu optimieren und die Einhaltung von Vorschriften zu verbessern.

Das Portfolio von Genetec für den Energie- und Versorgungsbranche bietet Betreibern kritischer Infrastrukturen eine Komplettlösung für vereinheitlichte Sicherheitssysteme, die die Zusammenarbeit mit Sicherheits- und betrieblichen Compliance-Teams verändern werden und einen sicheren Arbeitsplatz gewährleisten können.

Genetec Inc.
[genetec.com/standorte](https://www.genetec.com/standorte)
info@genetec.com
[@genetec](https://www.genetec.com)

© 2020 Genetec Inc. Alle Rechte vorbehalten. Genetec, Omnicast, Synergis, AutoVu, Mission Control, Genetec Clearance, ClearID und das Genetec Logo sind Marken von Genetec Inc. und können in verschiedenen Ländern eingetragen oder zur Eintragung angemeldet sein. Andere in diesem Dokument verwendete Marken sind möglicherweise Marken der Hersteller oder Anbieter der jeweiligen Produkte.

