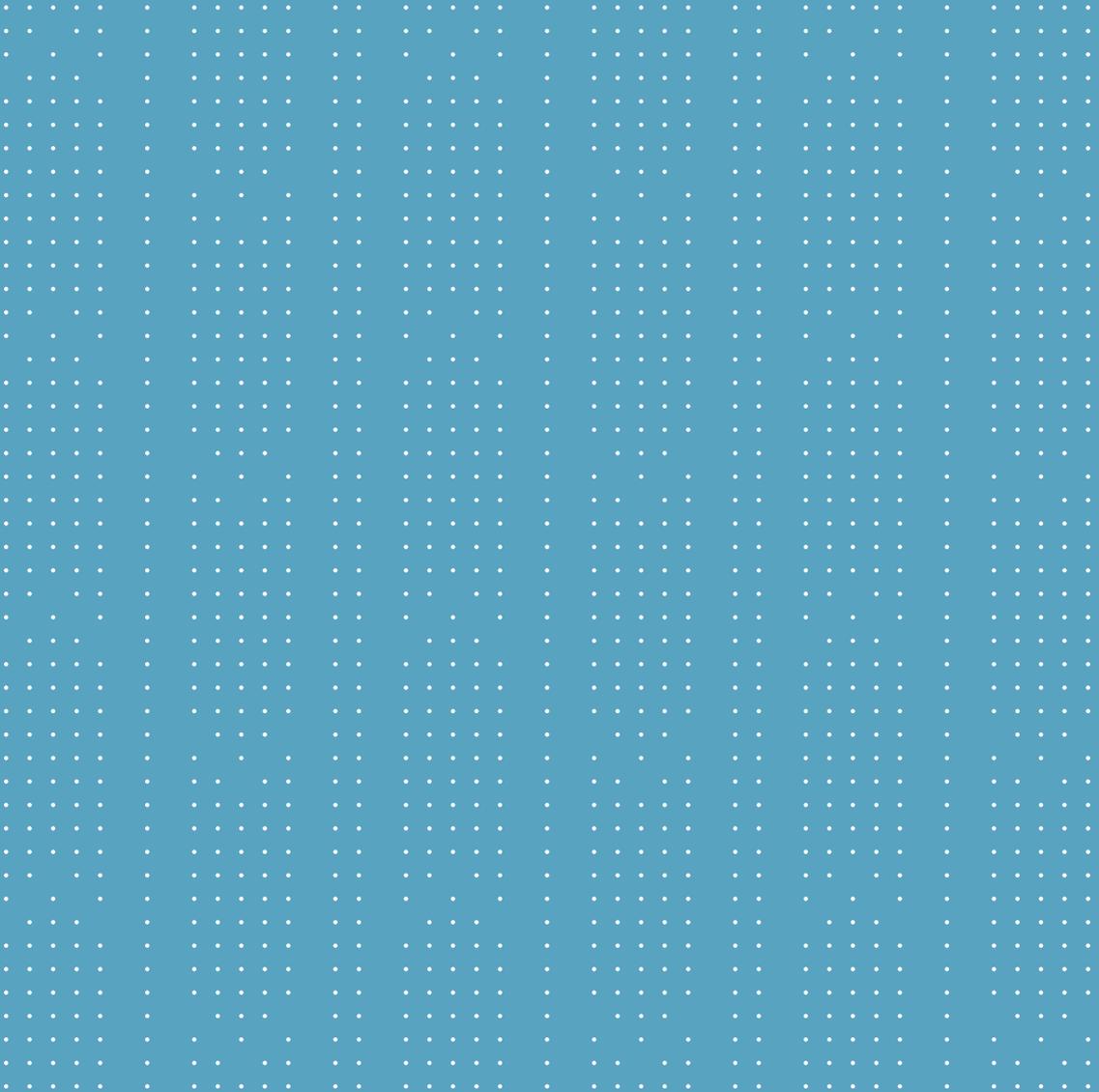




# Vereinheitlichtes physisches Identitäts- und Zutrittsmanagement





# Ein intelligenteres Zutrittsmanagement

Für Unternehmen ist es erfolgskritisch, dass Menschen sich auf dem Gelände problemlos bewegen können. Um die Sicherheit dabei stets zu gewährleisten, sollten Sie Zutrittsberechtigungen effektiv erteilen und verwalten können. Compliance-Vorgaben, neu integrierte Prozesse oder externe Vorschriften können solche Prozesse aber verlangsamen, weil sie beispielsweise Sicherheitslücken schaffen oder die Dynamik stören.

Oftmals sind es Kleinigkeiten wie verlorene Schlüsselkarten oder Zutrittsanfragen, die die wertvolle Zeit des Sicherheitspersonals in Anspruch nehmen. Aufgrund der statischen Funktionsweise typischer Zutrittskontrollsysteme, die nicht mit Unternehmensrichtlinien verknüpft sind, haben Nutzer meist keine klaren administrativen Vorgaben.

Die intelligentere Lösung heißt Genetec ClearIDTM, welche eine Self-Service-Lösung für physisches Identitäts- und Zutrittsmanagement ist. Damit lassen sich die Sicherheit erhöhen, Prozesse effizienter gestalten und gesetzliche Vorgaben einhalten. Das System lässt sich problemlos mit unserer IP-basierten Zutrittskontrolllösung Security Center Synergis vereinheitlichen, was die Implementierung deutlich vereinfacht. Als Cloud-basiertes System ist die Integration mit Synergis ein Kinderspiel. Endlose Anpassungen und die umständliche Installation von Endgeräten entfallen dadurch.

Ob Unternehmen, Universitäten oder stark reglementierte multinationalen Konzerne in der Öl-, Gas-, Bergbau- und Petrochemieindustrie - ClearID ist eine intuitiv bedienbare Lösung, welche die immer komplexere Verwaltung individueller Zutrittsrechte vereinfacht.

ClearID bietet sowohl automatisierte als auch Self-Service-Funktionen an, die Ihre firmeninternen Richtlinien einhalten und gleichzeitig eine barrierefreie, effiziente Arbeitsumgebung für alle schaffen.

# Was wir unter einer Identität verstehen.

ClearID verwaltet zentral die Zutrittsrechte aller Personen, die mit Ihrem Unternehmen zu tun haben. Was Sie wissen müssen:

## Identität

Eine Identität ist das eindeutige digitale Profil eines Mitarbeiters oder Besuchers.

Es kann permanent, für einen bestimmten Zeitraum oder kurzfristig für Mitarbeiter oder Besucher angelegt werden.

Identitäten kommen in vielen Sicherheits- und Unternehmenssystemen zum Einsatz. Dazu gehören:

- Mitarbeiterprofile in der Lohnbuchhaltung und im Personalmanagementsystem
- Windows-Konten für Microsoft Active Directory
- Ein Sales-Manager im CRM und der Lösung zur Angebotserstellung
- Ein Karteninhaber im physischen Zutrittskontrollsystem

## Lebenszyklus einer angelegten Identität

Moderne Systeme für physisches Identitäts- und Zutrittsmanagement (PIAM) verwaltet die Richtlinien, Prozesse und Identitäten eines Unternehmens, vom Anlegen von Besuchern bis hin zum Onboarding und Offboarding von Mitarbeitern.

Sobald Richtlinien festgelegt sind, überwacht ClearID die vier typischen Phasen im Lebenszyklus einer Identität:

1. Anlegen einer Identität
2. Vergabe der Zutrittsrechte
3. Anpassungen einer Identität
4. Entzug der Zutrittsrechte

## Attribute

Eine Identität besteht aus einer Reihe von Eigenschaften, auch Attribute genannt. Diese Attribute definieren die individuellen Zutrittsrechte einer Identität. Ändern sich also die Attribute einer Person, verändern sich auch ihre Zutrittsrechte.

Beispiele für Attribute sind:

- Abteilung
- Standort
- Funktion
- Name des Vorgesetzten
- Titel des Mitarbeiters
- Alter
- Ausbildung

## Wie ClearID funktioniert

ClearID befähigt Unternehmen, ihre Sicherheits- und Compliance-Richtlinien zu standardisieren und durchzusetzen. Mithilfe von Automatisierung und einem vereinfachten Zutrittsrechte-Management werden Sicherheits- und Betriebsrisiken gemindert. Dafür sorgt ein optimierter Workflow:

### Schritt 1: Erste Anfrage



Ein Mitarbeiter verbindet sich mit ClearID und bittet für einen bestimmten Zeitraum um Zugang zu einem gesicherten Bereich.

### Schritt 2: Prüfung und Genehmigung durch Vorgesetzte



Nachdem eine Zutrittsanfrage gestellt wurde, überprüft ClearID die entsprechenden Richtlinien für den Standort und genehmigt die Anfrage automatisch oder holt die Genehmigung eines befugten Vorgesetzten ein.

### Schritt 3: Änderung des Zutrittsrechts



Im Anschluss wird das Zutrittskontrollsystem aktualisiert und das Zutrittsrecht für den gewünschten Zeitraum gewährt. Bei Ablehnung wird der Zutritt verweigert und der Antragsteller erhält eine E-Mail mit einer Begründung.

# Die User-Experience der Karteninhaber verbessern

Ihre Mitarbeiter und Besucher sind täglich auf das physische Zutrittskontrollsystem angewiesen, um innerhalb des Geländes beispielsweise von öffentlichen zu gesicherte Bereiche zu gelangen. Warum sollten also nur Security- und IT-Mitarbeiter die Möglichkeit haben, Zutrittsrechte zu ändern? Möchte jemand eine Änderung beantragen, muss er in der Regel die entsprechende Abteilung aufsuchen oder sich an der Rezeption melden, was den Prozess zusätzlich verzögert.

ClearID bietet als Self-Service-Lösung für physisches Identität und Zutrittsmanagement einen neuen Workflow-basierten Ansatz für die Beantragung neuer oder die Anpassung bestehender Zutrittsrechte. Anträge können direkt an die zuständigen Bereichsleiter gestellt werden, ohne die Nutzer der Zutrittskontrollsysteme einzubeziehen.

Mitarbeitern und Besuchern haben dank ClearID nun selbst die Kontrolle über ihre Zutrittsanfragen, was die User-Experience des Karteninhabers verbessert, frustrierende Verzögerungen verringert und die Prozesse im Unternehmen in Bewegung hält.



# Mehr Sicherheit, weniger Risiken

Das Offboarding spielt eine zentrale Rolle beim Ausscheiden eines Mitarbeiters. Schließlich sollte dieser dann keinen Zugang mehr zu Ihren Einrichtungen und besonders zu gesicherten Bereichen haben. Immer wieder kommt es aber vor, dass Nutzer nicht alle entsprechenden Richtlinien kennen, um Zutrittsrechte zu beenden, oder nicht alle Workarounds und Ausnahmen kennt, die in einem Zutrittskontrollsystem individuell festgelegt wurden.

Viele Nutzer setzen beispielsweise kleine Systemoptimierungen selbst um, ohne diese zentral zu steuern. Im Laufe der Zeit häufen sich diese Fälle, wodurch Sicherheitslücken entstehen.

Mit ClearID legen Sie die standardisierten -Sicherheits- und Compliance-Richtlinien fest und das System erledigt den Rest. Die eingesetzte Workflow-Engine beruht auf Unternehmensrichtlinien, um anhand aktueller Identitätsattribute die individuelle Zutrittsrechte kontinuierlich zu aktualisieren. Bereits minimalste Änderungen an einem Attribut sorgen dafür, dass bestehende Zutrittsrechte angepasst werden. Das macht eine manuelle Bearbeitung oder Ad-hoc-Änderungen überflüssig.

Wird die Identität eines Mitarbeiter deaktiviert, werden ihm die Zutrittsrechte in allen Systemen entzogen, was ein sauberes Ausscheiden aus dem Unternehmen gewährleistet.

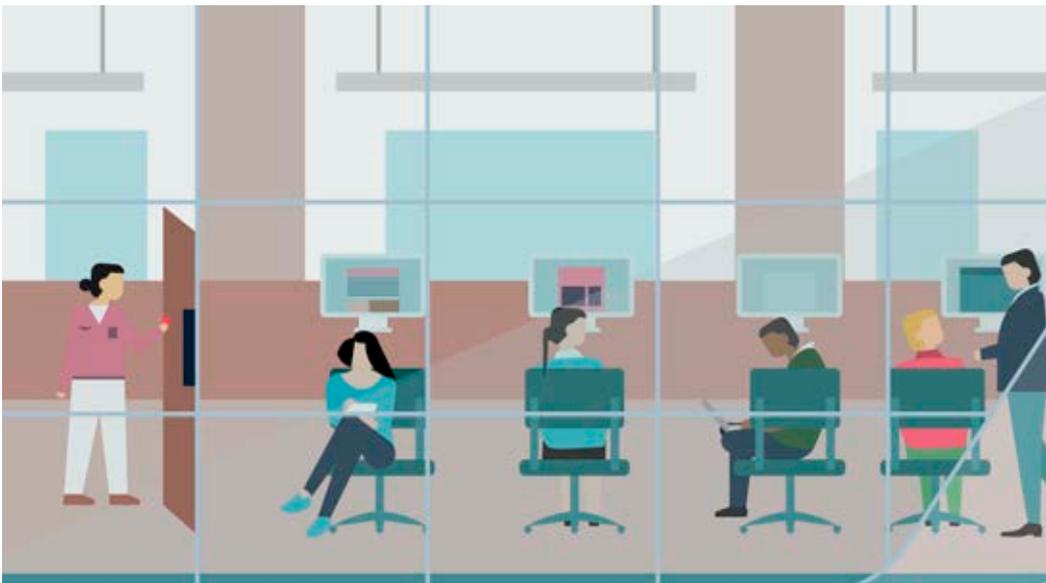
# Optimierte systematische Übersicht

Im Alltag kommt es immer wieder vor, dass Nutzer individuelle Zutrittsrechte vergeben, die nicht immer den strikten Compliance-Richtlinien entsprechen. So werden beispielsweise Zutrittsberechtigungen kurzfristig von einem Vorgesetzten für einen seiner Mitarbeiter beim Sicherheitspersonal beantragt.

In älteren Systemen werden solche Änderungen zwar umgesetzt, in der Regel aber weder die Anweisung noch eine schlüssige Begründung erfasst und hinterlegt.

ClearID speichert und archiviert jeden an eine Identität gebundenen Vorgang während ihres gesamten Lebenszyklus. Die Archivierung aller temporären oder permanenten Zutrittsanfragen sowie Genehmigungen ergeben ein vollständiges Bild, in dem jede Ausnahme und einmalige Anfrage in einem zeitlichen Kontext einsehbar ist. Damit können Unternehmen routinemäßige Zutrittsprüfungen und Audits durchführen und sicherstellen, dass alle Mitarbeiter und Besucher nur in autorisierten Bereichen Zutritt haben.

Damit werden alle die Unternehmenssicherheit betreffenden Aktionen vollständig nachvollziehbar und ermöglichen eine Compliance- und Corporate-Governance-konforme Zutrittssteuerung.

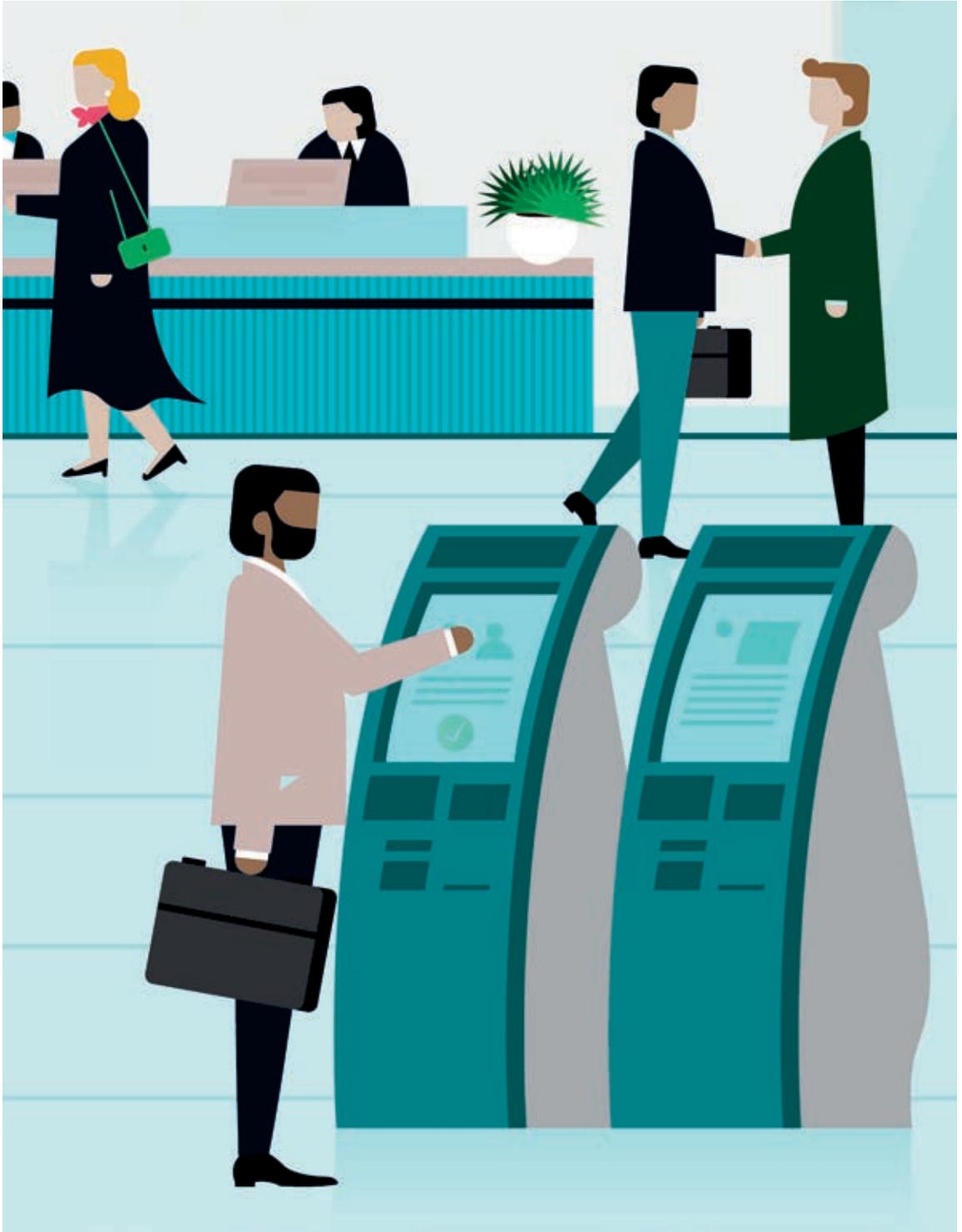


# Erhöhung der betrieblichen Effizienz

Herkömmliche Zutrittskontrollsysteme benötigen für die Vergabe von Zutrittsrechten und -genehmigungen manuelle Eingaben des Nutzers. Besonders bei größeren Unternehmen ist mit den begrenzten personellen Ressourcen aber fast unmöglich, die Zutrittsrechte jedes Mitarbeiters und Besuchers zu kennen.

Wenn vor der Rechtevergabe für bestimmte Unternehmensbereiche ein Training notwendig ist, müssen Sicherheitsverantwortliche sich in der Regel mit einem Bereichsleiter oder Vorgesetzten in Verbindung setzen, um sich die Freigabe einzuholen, bzw. ihre E-Mails manuell durchsuchen, um die entsprechende Genehmigung zu finden. Sind diese Vorgesetzten dann auch noch in einem Meeting oder im Urlaub, verzögert sich dieser manuelle Ansatz weiter. Je größer ein Unternehmen wird, desto mehr Nutzer werden bei diesem Ansatz benötigt, um die steigende Zahl an Mitarbeitern und Bereichen zu verwalten.

Unternehmen reagieren auf die zunehmende Überlastung und Überarbeitung des Teams mit der Einstellung von zusätzlichem Personal. Das lenkt aber nur von der eigentlichen Ineffizienz des manuellen Systems ab. Ein automatisiertes Zutrittsmanagement wie ClearID stellt sicher, dass alle Mitarbeiter und Besucher alle Anforderungen erfüllen, bevor ihnen Zutritt zu einem Bereich gewährt wird. Dadurch lassen sich tägliche Zutrittsanfragen, Compliance-Vorgaben und sonstige Richtlinien erheblich leichter verwalten. Sicherheitsteams arbeiten effizienter und können sich auf relevante Aufgaben konzentrieren.



# Die User-Experience von Besuchern verbessern

In Unternehmen mit hohem Kundenaufkommen gelangt das eigene Personal schnell an seine Grenzen. Sie müssen meist gleichzeitig eingehende E-Mail-Anfragen lesen, Besucher in Besucherlisten eintragen, Besucher manuell einchecken und die Mitarbeiter über die Ankunft ihrer Gäste informieren. Diese zeitaufwendigen und ineffizienten Prozesse führen zu längeren Wartezeiten, welche sich nachhaltig negativ auf die User-Experience Ihrer Kunden auswirken kann.

ClearID sorgt für ein reibungsloses Besuchermanagement. Sobald ein Meeting aufgesetzt wird, beginnt ein Prozess. Zunächst meldet sich der lokale Mitarbeiter (oder Host) über ein Webportal bei ClearID an und erstellt ein Profil für seinen Besucher, in dem er dessen Namen, Kontaktdaten sowie Zweck, Datum, Uhrzeit und Dauer des Besuchs angibt. Die Besprechungsanfrage muss anschließend vom verantwortlichen Manager genehmigt werden. Sofern alle relevanten Kriterien erfüllt sind, kann diese auch von ClearID automatisch genehmigt werden. Der Besucher erhält dann eine E-Mail-Einladung von ClearID im Namen des Unternehmens.

Es ist auch möglich, den Besuch automatisch von ClearID genehmigen zu lassen, falls dem Einladenden von einem Systemadministrator erlaubt wurde, ohne Genehmigung des Vorgesetzten Gäste einzuladen. Sowohl Besucher als auch Mitarbeiter erhalten anschließend Bestätigungs-E-Mails für den anstehenden Termin. Am Tag der Besprechung meldet sich der Besucher im Eingangsbereich mithilfe eines via E-Mail übermittelten QR-Codes oder seiner ID an einem entsprechenden Terminal an.

Nach der Anmeldung erhält der Besucher vom Terminal einen selbstklebenden Besucherausweis oder einen gültigen Berechtigungsausweis von einem Empfangsmitarbeiter. Gleichzeitig wird der Mitarbeiter über die Ankunft seiner Gäste informiert. Nach der persönlichen Begrüßung geht es umgehend in den Konferenzraum, wo das Meeting pünktlich und unkompliziert stattfinden kann.



# Ein Audit richtig vorbereiten

In Branchen, in denen Unternehmen strenge Zutrittsanforderungen erfüllen müssen, sind regelmäßige Audits unerlässlich. Steht beispielsweise ein Audit an, können sich Vorgesetzte mit den Sicherheitsverantwortlichen in Verbindung setzen und Berichte über jeden zu erhalten, der Zutritt zu gesicherten Bereichen hat. Ist der Sicherheitsverantwortliche aber im Urlaub, kann schon die Erstellung solcher Berichte schwierig und zeitaufwendig werden. Anschließend erkennt der Vorgesetzte, dass es einige unbefugte Zutritte in den entsprechenden Sperrbereichen gab. Darunter waren auch ehemalige Besucher und Mitarbeiter, die das Unternehmen bereits verlassen haben.

Sollte die Regulierungsbehörde das herausfinden, droht dem Unternehmen aufgrund der Nichteinhaltung der Vorschriften eine hohe Geldstrafe. Jetzt muss der Vorgesetzte jede Person im Bericht überprüfen und bestimmen, wer weiterhin Zutrittsrechte haben darf. Am Ende muss er eine Liste von Personen erstellen, denen der Zugang in jene Bereiche verweigert werden muss, damit der Sicherheitsverantwortliche das Zutrittskontrollsystem aktualisieren kann. Dieser manuelle Prozess ist extrem langsam, ressourcenintensiv und anfällig für menschliche Fehler, weil schnell jemand auf der Liste übersehen wird.

ClearID erlaubt es Vorgesetzten nach Anmeldung im Portal direkt zu sehen, wer Zutritt zu Räumen und Bereichen hat und alle Personen zu von der Liste zu entfernen, die dort nicht sein sollten. Diese Listen können für jeden einzelnen Bereich ausgewählt werden, der überprüft werden soll. Anschließend lassen sich die Zutrittsberechtigungen jeder Person sofort entziehen und mit einer entsprechenden Begründung versehen. Der frühere kosten- und zeitaufwändige Prozess kann nun innerhalb von Minuten erledigt werden. Damit behalten Unternehmen stets die Kontrolle und vermeiden hohe Geldstrafen.

# Sicherheit, die Vertrauen schafft

Mit ClearID können Sie Ihre Sicherheitsrichtlinien vereinheitlichen und automatisieren, Unregelmäßigkeiten reduzieren und Sicherheitslücken schließen. Die Lösung von Genetec hilft auch standortübergreifend dabei, Unternehmens- und Branchenregularien einzuhalten. Sie können Identitäten zentral verwalten und Ihre Mitarbeiter durch ein Self-Service-Modell zur Zutrittssteuerung befähigen, was die operative Effizienz steigert. ClearID sorgt dafür, dass Ihr Unternehmen für die Zukunft gewappnet ist.

## **Firmensitz**

### **Genetec Inc.**

2280 Alfred-Nobel Blvd.,

Suite 400

Montréal QC H4S 2A4

Kanada

Gebührenfrei: +1 866 684 8006

Kanada & USA:

Tel.: +1 514 332 4000

genetec.de

## **© 2019 Genetec Inc.**

Alle Rechte vorbehalten. Genetec, ClearID und ihre jeweiligen Logos sind Marken von Genetec Inc. und können in mehreren Gerichtsbarkeiten registriert oder angemeldet sein.

Andere in diesem Dokument verwendete Marken können Marken der Hersteller oder Anbieter der jeweiligen Produkte sein. *Alle Bilder dienen nur zur Veranschaulichung.*

**Genetec ClearID ist ein physisches Identitäts- und Zutrittsmanagementsystem, das die Sicherheitsrichtlinien Ihres Unternehmens in Bezug auf Zutrittsrechte standardisiert und durchsetzt und Ihr Unternehmen effizienter macht.**

