

# Genetec Portfolio für Rechenzentren

Vereinheitlichte Sicherheit zum Schutz von Gebäuden  
und für mehr betriebliche Effizienz



Die Rechenzentrumsbranche entwickelt sich rasant – mit zunehmendem Datenverkehr, Cloudwachstum und zusätzlichen KI-Workloads. Richtlinien wie NIST, DSGVO, NIS 2 und neue Vorschriften in den Regionen LATAM und APAC finden immer breitere Anwendung. Doch Compliance ist nur der Anfang. Die eigentliche Herausforderung besteht darin, die Infrastruktur ohne allzu viel Komplexität vor Cyberbedrohungen, unbefugtem Zutritt und Ausfällen zu schützen. Das gilt sowohl für eigene Rechenzentren als auch für Instanzen in einer gemeinsam genutzten Einrichtung.

Wir zeigen Ihnen, wie Sie mit der richtigen Sicherheitsstrategie alle Auflagen erfüllen, Ihre Infrastruktur schützen und Ausfallzeiten reduzieren.



## Ihre Herausforderungen

### Abwägung zwischen Kapazitäten und Bedarf

KI, Cloud und digitales Wachstum drängen zu einer raschen Skalierung von Rechenzentren. Diese wird jedoch durch Leistungsbeschränkungen, steigende Infrastrukturkosten und Platzmangel ausgebremst. Ob Sie eine globale Infrastruktur aufbauen oder innerhalb einer gemeinsam genutzten Einrichtung wachsen wollen – Kapazitätsentscheidungen wirken sich unmittelbar auf die Leistungsfähigkeit und Zuverlässigkeit aus.

### Einhaltung von Vorschriften: immer wieder neue Standards

Der Druck auf Betreiber und Mieter, wechselnde Standards einzuhalten, wächst. In Nordamerika sind NIST und SOC 2 Pflicht, Europa pocht auf die DSGVO und NIS 2. In Lateinamerika und im APAC-Raum werden eigene Vorschriften eingeführt. Verstöße können Geldstrafen oder Ausfallzeiten nach sich ziehen. Wenn das Gebäude von Dritten verwaltet wird, müssen sich Mieter zudem um die Sicherheit der Racks, das Identitätsmanagement und die Vorbereitung auf Audits kümmern.

### Menschliches Versagen und Bedrohungen durch Insider

Viele Ausfälle sind auf Fehlverhalten oder Missbrauch zurückzuführen. Schon kleine Fehler und ein unsachgemäßer Umgang mit Berechtigungsnachweisen können erhebliche Probleme verursachen. Wenn es mehrere Mieter gibt, sind klare Zutrittsrechte und Verantwortlichkeiten daher unverzichtbar. Strenge Identitätskontrollen, Überwachung und Audits reduzieren die Risiken für alle Beteiligten.

### Physische Sicherheit: Bedrohungsmanagement

Rechenzentren sind physischen Bedrohungen wie Einbrüchen, Diebstahl und Naturkatastrophen ausgesetzt. Davor müssen Betreiber die Umgebung, Infrastruktur und unterstützenden Systeme schützen. Für Cages, Racks und Zutrittsberechtigungen sind die Mieter verantwortlich. Doch ohne vereinheitlichte Systeme wird bei Auftreten einer Bedrohung das Wichtigste leicht übersehen.

### Nachhaltigkeit und Energieeffizienz

Der Energieverbrauch wird kritisch beäugt. Europa verlangt die Nutzung grüner Energie. Die USA und Lateinamerika setzen auf Anreize. Von Betreibern wird erwartet, dass sie eine effiziente Kühlung, erneuerbare Energiequellen und Überwachungsinstrumente nutzen, um Umweltziele zu erreichen. Auch für Mieter ist Nachhaltigkeit zu einem entscheidenden Faktor bei der Anbieterwahl geworden.

### Schnelle technologische Veränderungen und Upgrades

Der Wandel vollzieht sich immer schneller. Betreiber legen bei Infrastruktur-Upgrades und Automatisierung ein hohes Tempo vor. Folglich brauchen Mieter Tools, die Schritt halten können, sich über hybride Umgebungen skalieren lassen und auch in gemeinsam genutzten Einrichtungen funktionieren. Ohne diese Flexibilität werden die Systeme immer langsamer und die Risiken immer zahlreicher.

## Warum Genetec?



### Vereinheitlichte Plattform

**Genetec™ Security Center** ist eine Plattform für physische Sicherheit mit einer einzigen Schnittstelle für alle Sicherheitsanwendungen. Bei Bedarf können Sie neue Funktionen aktivieren und genau die Geräte und Add-ons auswählen, die zur Erweiterung und Weiterentwicklung Ihres Systems sinnvoll sind. Eine Plattform, auf der Ihre Daten konsolidiert und vereinheitlicht werden, bietet Ihren Nutzern nicht nur mehr Effizienz bei der Verwaltung von Sicherheitsrichtlinien und der Durchführung von Untersuchungen. Sie ermöglicht ihnen auch, sich auf die wirklich wichtigen Dinge zu konzentrieren.



### Erweiterte Funktionen

Vom Videomanagement über die Zutrittskontrolle und Nummernschilderkennung bis hin zu Videoanalysen, forensischer Suche, Protokollen für Ereignisse, die Maßnahmen erfordern, und erweiterten Cybersicherheitsfunktionen haben wir die passenden Lösungen für Ihre Anforderungen.



### Offene Architektur

**Genetec™ Security Center** geht über die grundlegenden Systeme für Zutrittskontrolle, Videomanagement, automatische Nummernschilderkennung und Kommunikationsverwaltung hinaus. Da es auf einer offenen Architektur basiert, können Sie verschiedene Zusatzfunktionen, Plug-ins und andere Lösungen nutzen – das System funktioniert stets als Einheit. Dank unseres großen Ökosystems an Partnern und Anbietern können Sie es ganz nach Bedarf erweitern und in modernste Technologien investieren.



### Service und Schulungen

Wir haben Service- und Schulungsprogramme entwickelt, damit Sie bestmöglich von Ihren Investitionen in die Sicherheit profitieren können. Dazu gehören sowohl technischer Support rund um die Uhr als auch umfangreiche Online-Ressourcen und individuelle Beratung. Darüber hinaus haben Sie die Möglichkeit, an Schulungen vor Ort oder online sowie an Zertifizierungskursen teilzunehmen.

# Wie wir Sie unterstützen können

## Keine Komplettansicht der Überwachung von Umgebung, Büros und Serverräumen

Mit dem [Omnicast™](#) Videomanagement zur Echtzeitüberwachung und schnellen Untersuchung von Vorfällen können Sie sämtliche Kamera-Streams überwachen.

## Begrenzte Daten zu Kühlung, Stromverbrauch, Luftqualität und Beleuchtung

[Security Center™](#) ermöglicht die Integration von Daten zum industriellen IoT für eine zentrale Überwachung und automatische Warnungen.

## Langsame Reaktion auf Bedrohungen für die gesamte Einrichtung

Mit [Security Center](#) können Sie vordefinierte Bedrohungsstufen auslösen und Nutzer durch SOPs für alle Systeme führen.

## Zeitaufwendige, uneinheitliche Compliance-Berichterstellung

Automatisierte Zutritts-, Video- und Ereignisprotokolle erleichtern die Einhaltung der ISO-, SOC-2- und NIST-Anforderungen.

## Keine klaren Entscheidungen auf Grundlage von Attributen für ISO-27001- und SOC-2-Audits möglich

[ClearID™](#) verwendet Sicherheitsrichtlinien zur automatischen Zuweisung von Zutrittsrechten je nach Funktion. Mitarbeiter können für sich, bestimmte Funktionen oder andere Personen temporäre Zutrittsrechte online anfordern.

## Langsame Reaktion aufgrund manueller Abstimmung zwischen Sicherheits- und Facility-Management-Teams

Durch die zentrale Überwachung von Gebäudesystemen, Einbruchsmeldungen und Sprechanlagen in [Security Center](#) wird die Abstimmung beschleunigt.

## Beeinträchtigte Systemverfügbarkeit und Datensicherheit durch System- oder Hardwareausfälle

Durch Failover-Strategien und Zustandsüberwachung der Systeme wird die Betriebskontinuität aufrechterhalten.

## Wiederholt unbemerkte Zutritts- oder Regelverstöße

Mit [Security Center](#) können verdächtige Muster erkannt und Vorfälle anhand regelbasierter Analysen an die zuständigen Stellen weitergeleitet werden.

## Probleme bei der Schlüsselverwaltung und dem Nachweis, wer sie nimmt und nutzt

Mit [Synergis](#) verwalten Sie den Zugang zu Türen, Schlüsseln und Vermögenswerten in einem System. Für zusätzliche Nachprüfbarkeit sehen Sie auch, wer auf Schränke zugreift.

## Unbefugter Zutritt zu Serverräumen und zugriffsbeschränkten Bereichen

Durch [Zutrittskontrollen](#) mit biometrischer Authentifizierung können Hochrisikobereiche gesichert und sämtliche Zutrittsversuche erfasst werden.

## Einhaltung der NIS-2-Anforderungen an die Systemresilienz und Zutrittsnachvollziehbarkeit

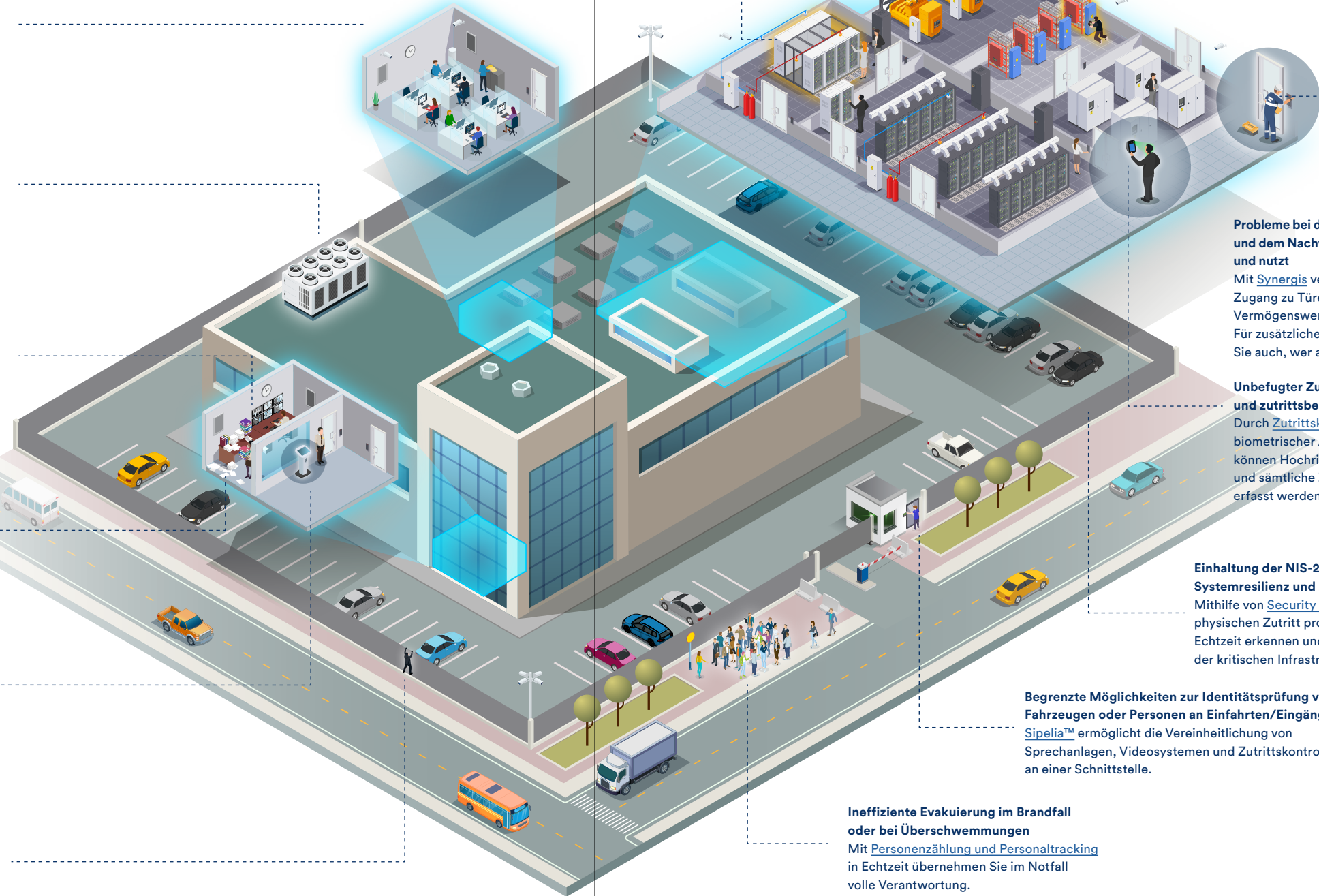
Mithilfe von [Security Center](#) können Sie den physischen Zutritt protokollieren, Vorfälle in Echtzeit erkennen und die Systemverfügbarkeit der kritischen Infrastruktur aufrechterhalten.

## Begrenzte Möglichkeiten zur Identitätsprüfung von Fahrzeugen oder Personen an Einfahrten/Eingängen

[Sipelia™](#) ermöglicht die Vereinheitlichung von Sprechanlagen, Videosystemen und Zutrittskontrollen an einer Schnittstelle.

## Ineffiziente Evakuierung im Brandfall oder bei Überschwemmungen

Mit [Personenzählung und Personaltracking](#) in Echtzeit übernehmen Sie im Notfall volle Verantwortung.



# Passende Bereitstellungsoptionen für Ihre Anforderungen



[Genetec Security Center](#) bietet Rechenzentrumsbetreibern auf einer Plattform alle Tools, um kritische Infrastruktur zu sichern, strenge Zutrittsregeln durchzusetzen und wechselnde Compliance-Anforderungen zu erfüllen. Es kann mit Omnicast für hochauflösende Video-Streams, mit Synergis für kontrollierten Zutritt zu sensiblen Bereichen, Sipelia für sichere Intercom-Durchsagen und Kommunikation sowie nativen IoT-Integrationen zur Überwachung der Temperatur, Luftfeuchtigkeit, Stromversorgung und anderer kritischer Ausstattung kombiniert werden. Sicherheitsteams können an einem zentralen Ort mehrere Standorte überwachen, nachvollziehen, wer Serverräume oder Bereiche mit Gebäudemanagementsystemen betritt, und auf verdächtige Aktivitäten schnell reagieren. Dank Unterstützung für Zero-Trust-Zutrittsmodelle, Anomalieerkennung und auditgerechte Berichterstellung fördert Security Center die Risikoeindämmung, ohne den Betrieb aufzuhalten. Sie können es lokal oder für eine zentrale Systemzustandsüberwachung mit cloudbasiertem Überblick über Security Center SaaS ausführen.



[Genetec Security Center SaaS](#) ist eine abonnementbasierte, cloudverwaltete Plattform und eignet sich ideal für Rechenzentren, die einen sicheren, skalierbaren Betrieb ohne zusätzliche Infrastrukturkosten wünschen. Es vereint Videoüberwachung, Zutrittskontrolle und automatische Reaktionen auf Vorfälle in einem System, das ganz ohne Patches oder Ausfallzeiten stets aktuell bleibt. Betreiber erhalten eine zentrale Übersicht über alle Standorte mit Echtzeit-Zustandsüberwachung und integrierter Unterstützung zur Einhaltung von Richtlinien wie SOC 2, ISO 27001 und NIST. Dank verschlüsselter Datenverarbeitung, detaillierten Prüfprotokollen und strengen Zutrittsregeln trägt Security Center SaaS zur Eindämmung von Risiken bei – und das bei vorhersehbaren Kosten und effizientem Betrieb. Darüber hinaus ist die Plattform skalierbar, sodass sie mit Ihnen wachsen kann.

