



Wichtige Überlegungen bei der Auswahl des richtigen Videomanagementsystems (VMS)

Ihre VMS-Checkliste

Nehmen Sie sich die Zeit, um Ihre Anforderungen an ein Videomanagementsystem (VMS) genau zu ermitteln, damit Sie sich für die richtige Lösung entscheiden.

Gehen Sie mit Ihrem Team die folgenden Fragen durch, um die richtige Wahl zu treffen.

Standort- und Geräteanforderungen

Mit der richtigen Grundlage von Anfang an verhelfen Sie Ihrem Unternehmen zum Erfolg und ermöglichen eine effiziente Skalierung bei Unternehmenswachstum. Für ein robustes Überwachungssystem müssen Sie die grundlegenden Standort- und Geräteanforderungen sowie alle Infrastruktur-, Compliance- und Datenanforderungen kennen. Diese Elemente bestimmen zusammen die Systemarchitektur, einschließlich Kameraspezifikationen, Umfang der Implementierung, Konnektivität und Zugänglichkeit für Benutzer.

Grundlegende Anforderungen:

- Wie viele Kameras benötigen wir?
- Sollten wir mehrere Kameramodelle für verschiedene Anwendungen oder lieber ein oder wenige Standardmodelle einsetzen?
- An wie vielen Standorten werden Kameras benötigt?
- Sollen all diese Standorte vernetzt und von einem zentralen Ort aus überwacht werden?
- Wie groß ist unsere Implementierung? Ist sie eher klein oder umfangreicher?
- Wie viele Nutzer greifen auf das System zu und verwenden es gleichzeitig?
- Sollen auch andere Sensoren (wie Zutrittskontrolle, Einbruchüberwachung, Audio/Kommunikation, IoT) mit der Implementierung verbunden werden?
- Müssen wir alle Daten von unseren Sensoren einsehen? Müssen wir Interaktionen von einer einzigartigen Schnittstelle erstellen?
- Wie werden Benutzergruppen für unser System definiert?
- Sollten wir kontinuierlich aufzeichnen oder nur zu bestimmten Zeiten? Welche Bedingungen bestimmen den Zeitpunkt der Aufzeichnung?

Architektur:

- Ist unsere vorhandene Hardware mit der neuen Technologie kompatibel?
- Ist genügend Platz für lokale Hardware vorhanden?
- Müssen wir viele verschiedene Kameratypen und -marken unterstützen?
- Wo soll unser eigenes System gehostet werden? Möchten wir eine On-Premise-, Cloud- oder Hybridlösung implementieren?
- Sollen alle Standorte von einem zentralen System verwaltet werden, oder benötigen wir mehrere unabhängige Remote-Standorte, die separat verwaltet werden?
- Benötigen wir die volle Kontrolle über die Verwaltung des Systems und aller seiner Komponenten?
- Möchten wir einen Cloudanbieter für die Verwaltung des Systems und seiner Komponenten einsetzen?
- Müssen wir die Bandbreite optimieren?
- Müssen wir bestimmte Codecs verwenden?
- Muss unser System bestimmte Dateiformate unterstützen?
- Sollen alle Videoaufzeichnungen lokal gespeichert werden oder alle bzw. ein Teil davon in der Cloud?
- Bietet das System Skalierbarkeit und Unterstützung für Wachstum und Expansion des Unternehmens?

Betriebliche Anforderungen

Das ideale VMS sollte nicht nur Vorfalleuntersuchungen beschleunigen, sondern auch Ihre alltäglichen Betriebsabläufe optimieren und sich nahtlos in Ihre täglichen Aktivitäten, Verfahren zur Vorfalleaktion und Untersuchungsprozesse integrieren lassen. Außerdem sollte Ihr System robust sein und Ihnen verwertbare Einblicke liefern, damit Sie bessere Entscheidungen treffen können. Dazu müssen Sie Ihr System hinsichtlich forensischer Aktivitäten, Echtzeitbetrieb, Systemresilienz, Automatisierung und Analysen beurteilen.

Forensische Aktivitäten

- Müssen wir Prozesse für Untersuchungen nach Vorfällen aufstellen?
- Wie kurz muss unser Ermittlungsverfahren sein?
- Müssen wir relevante Informationen an externe Beteiligte weitergeben?
- Müssen wir branchenspezifische und behördliche Vorschriften zu Audits und Untersuchungen einhalten?
- Benötigen wir leistungsstarke Software für die Wiedergabe von Videos bei Ermittlungen?
Wie viele Ermittlungen werden pro Monat durchgeführt?
- Müssen wir Langzeit-Backups für Beweise im Zusammenhang mit Ermittlungen aufbewahren?

Echtzeitbetrieb

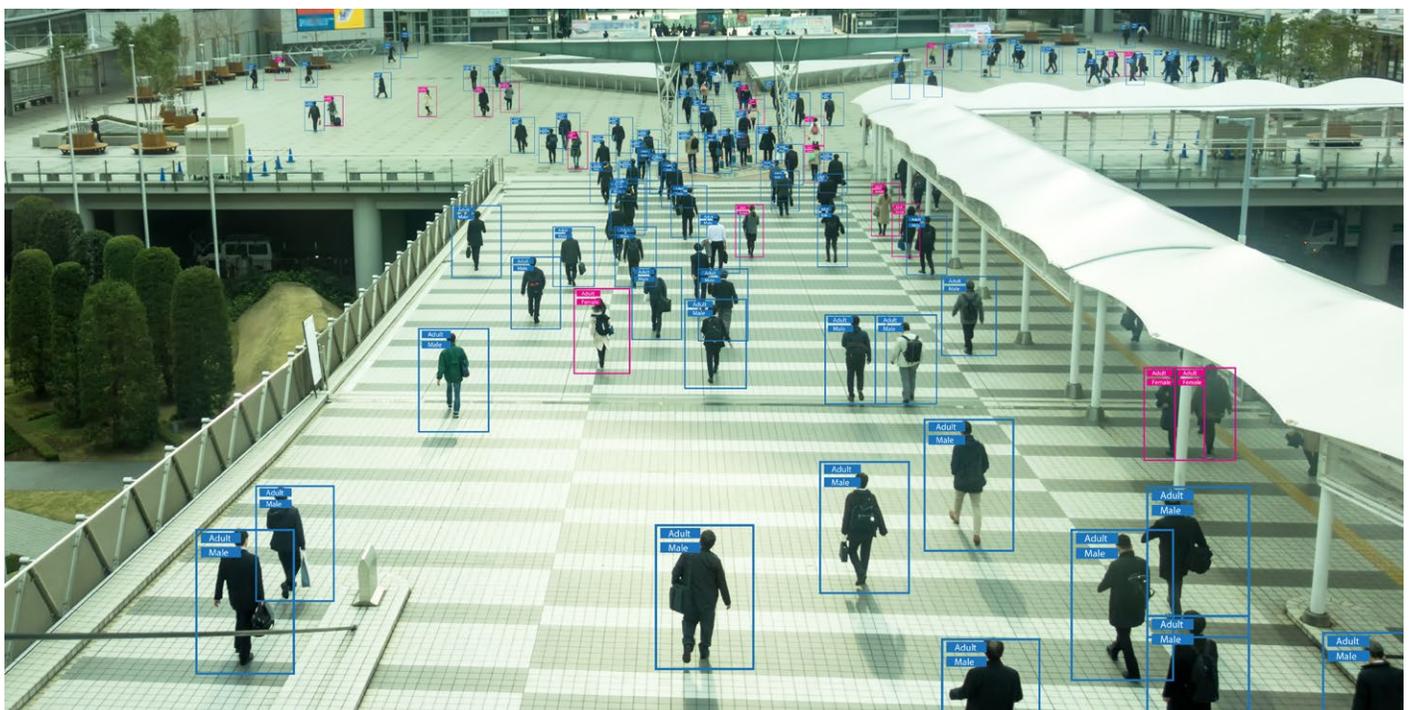
- Benötigt unsere Implementierung Live-Überwachung?
- Müssen wir Prozesse für Echtzeit-Vorfalleaktionen aufstellen?
- Wie schnell muss die Vorfalleaktion stattfinden?
- Benötigen wir einen Prozess für den Umgang mit kritischen Vorfällen?
- Benötigen wir eine nahtlose Sofortkommunikation zwischen Nutzern und Mitarbeitern, die ausschließlich im VMS und nicht über externe Tools erfolgen soll?
- Benötigen Nutzer und Mitarbeiter Zugriff auf eine Mobil-App beim Bearbeiten eines Vorfalles?
- Braucht das Team Bodycams, die mit unserem Videomanagementsystem verbunden werden müssen?
- Benötigen Nutzer Zugriff auf eine Webanwendung?
- Benötigt unsere Implementierung dynamische Karten für Vorfalleaktionen und Betrieb?
- Benötigen Nutzer Zugriff auf eine Videowand, um potenzielle Vorfälle zu überwachen?
- Benötigen wir leistungsstarke Arbeitsstationen, um die Reaktionszeit zu verbessern, besonders bei einem System mit vielen Einheiten, von denen Daten bezogen werden müssen?
- Müssen wir in der Lage sein, Alarme und operative Auslöser für bestimmte Vorfälle einzurichten?

Systemresilienz

- Wie viele Backups brauchen wir für Videoaufzeichnungen, falls es zu einem Ausfall kommt?
- Benötigen wir lokale Disaster-Recovery-Optionen (z. B. extern aufbewahrte Aufzeichnungen, mehrere lokale Kopien der Daten)?
- Benötigen wir lokales Archiver-Failover für Videoaufzeichnungen (falls der primäre Archiver ausfällt)?
- Benötigen wir einen Prozess für Directory-Failover für den Fall eines Systemausfalls?
- Benötigen wir einen Sicherungsprozess für Benutzerstatus und Konfigurationen?
- Müssen wir On-Premise-Failover-Systeme durch Cloudspeicher für Videos ergänzen?
- Müssen wir in der Lage sein, lokale Videoaufzeichnungskapazitäten durch Cloudspeicher zu erweitern (ohne weitere Investition)?

Automatisierung und Analysen

- Muss unsere Implementierung Videoanalysen umfassen? Benötigen wir Analyseserver, die das speziell unterstützen?
- Benötigen wir Bereichssicherung, um einen speziellen Bereich oder ein Gebiet durch einen größeren Bereich zu schützen? Benötigen wir Perimeterschutz?
- Müssen wir die Position oder Richtung von Objekten verfolgen?
- Müssen wir bestimmte Objekte oder Bedingungen per Video erkennen?
- Müssen wir in der Lage sein, Personen zu zählen oder Personenströme am Eingang zu erkennen?
- Möchten wir benachrichtigt werden, wenn ein Kamerabild geändert/manipuliert wurde?
- Benötigen wir anpassbare Dashboards und Berichte für Standortaktivitäten basierend auf Zusammenfassungen und Trends von Videodatenanalysen?
- Benötigen wir automatisierte Aktionen (wenn bestimmte Ereignisse oder Bedingungen erkannt werden) in den Standorten?



Cybersicherheit und Datenschutz

Bei der Suche nach einem neuen VMS dürfen Cybersicherheit und Datenschutz nicht nachrangig sein – sie haben höchste Priorität. Der Schutz sensibler Daten und die Aufrechterhaltung der Integrität Ihrer Sicherheitsinfrastruktur erfordern einen proaktiven Ansatz. Vergleichen Sie Ihre Cybersicherheitsstrategie mit branchenüblichen Best Practices, bewerten Sie Sicherheitslücken ausführlich, und prüfen Sie die Sicherheit vernetzter Geräte. Diese Schritte sind ausschlaggebend für die effektive Risikominderung.

Cybersicherheitsstrategie und Compliance

- Haben wir eine robuste Cybersicherheitsstrategie aufgestellt? Basiert sie auf den Best Practices der Branche?
- Haben wir die Cybersicherheit im Rahmen unseres Sicherheitssystems bewertet?
- Haben wir eine Schwachstellenanalyse durchgeführt, um Lücken zu identifizieren, die durch die Konvergenz von physischer Sicherheit und Cybersicherheit geschlossen werden können?
- Haben wir eine gründliche Schwachstellenanalyse aller vernetzten physischen Sicherheitsgeräte durchgeführt, um die bedenklichen Modelle und Hersteller zu identifizieren?
- Verwenden wir nur Originalprodukte und keine Fälschungen oder nicht lizenzierten Produkte?
- Gibt es neben dem technischen Aspekt noch andere Aspekte, die zur Risikominimierung beitragen?
- Enthalten die in Betracht gezogenen Lösungen die erforderlichen Zertifizierungen?
- Welche Datenschutzverordnung gilt für unsere konkrete Situation?
- Benötigen wir ein System, mit dem wir die Firmware, Passwörter oder Sicherheitszertifikate unserer Sensoren ganz einfach aktualisieren können?
- Haben wir ermittelt, welche Maßnahmen wir zur Einhaltung der örtlichen Datenschutzvorschriften ergreifen müssen (DSGVO, PIPEDA, CCPA usw.)?

Befolgen Sie in jedem Schritt Ihrer physischen Sicherheitsimplementierung Best Practices zur Cybersicherheit. Mehr dazu erfahren Sie in unserer [Checkliste zur Cybersicherheit](#).

Wenn Sie eine fundierte Entscheidung treffen, stellen Sie sicher, dass Ihr VMS Ihre betrieblichen Anforderungen nahtlos erfüllt, effektive Videoüberwachung ermöglicht, die Vorfallreaktion verbessert und zukünftiges Wachstum sowie Expansion unterstützt.

Diese fundierte Entscheidung erreichen Sie durch eine gründliche Bewertung Ihrer Anforderungen anhand der hier genannten wichtigen Überlegungen. So stellen Sie eine erfolgreiche Implementierung Ihres VMS sicher.

Sprechen wir über Ihre VMS-Anforderungen.

Besprechen Sie Ihre Anforderungen an ein Videomanagementsystem mit einem Experten.

[Unser Team unterstützt Sie gerne.](#)

Genetec ist ein Technologieunternehmen, das On-Premises- und cloudbasierte Lösungen in den Bereichen Sicherheit, Intelligence und Betriebsabläufe anbietet. Das zentrale Produkt des Unternehmens ist Genetec™ Security Center, eine Plattform für die physische Sicherheit, die Lösungen zur IP-basierten Videoüberwachung, Zutrittskontrolle, automatischen Nummernschilderkennung (Automatic License Plate Recognition, ALPR), Kommunikation und Analyse vereinheitlicht. Genetec entwickelt auch cloudbasierte Lösungen und Dienstleistungen, die die Sicherheit in den Gemeinden, in denen wir leben, verbessern.

Genetec Deutschland GmbH
genetec.com/standorte
salesdach@genetec.com
@genetec



Genetec™