Die Wahl des richtigen Sicherheitsanbieters: 3 entscheidende Faktoren

Kompatibilität

Unterstützt er Ihren vorhandenen Technologie-Stack?

Darauf sollten Sie achten:

Offene Integration

Eine Lösung, die Single Sign-On (SSO), Cloud-Plattformen und vorhandene Systeme unterstützt

Flexible Bereitstellung

Ein System, das mit On-Prem-, Cloud- oder Hybrid-Modellen funktioniert

Integrierte Interoperabilität

Eine solide API und Interoperabilitätsstandards wie ONVIF, die dafür sorgen, dass Systeme reibungslos mit anderen Tools und neuen Technologien funktionieren

Cybersicherheit und Compliance

Unterstützt er Ihren vorhandenen Technologie-Stack?

Darauf sollten Sie achten:

Datenschutz

End-to-End-Verschlüsselung, die die Datensicherheit und Privatsphäre wahrt

Einhaltung von Vorschriften

Ein Anbieter, der die DSGVO, NIS2, CCPA und andere Vorschriften einhält

Autorisierung und Authentifizierung

Ein System mit rollenbasierten Berechtigungen und Multifaktor-Authentifizierung, um unbefugten Zutritt zu verhindern

Vollständige Audit-Pfade

Eine Lösung mit vollständigen Aktivitätsprotokollen für mehr Transparenz und eine einfachere Überwachung der Compliance

Bewährte Standards für Cybersicherheit

Zertifizierungen nach SOC 2 Typ II, ISO 27001, 27017, TX-RAMP, UL 2900-2-3 und IRAP zum Schutz Ihrer Cloud-Lösungen

Zuverlässigkeit

Ist er anpassungsfähig und sorgt er für reibungslose Abläufe?

Darauf sollten Sie achten:

Garantierte Betriebszeit

Hochverfügbarkeitskonfigurationen mit garantierten SLAs für kontinuierlichen Betrieb

Disaster Recovery

Automatisierte Failover- und Disaster-Recovery-Strategien zur Aufrechterhaltung der Kontinuität

Skalierbare Performance

Ein System, das umfangreiche Implementierungen bewältigen und mit Ihrer Organisation mitwachsen kann, ohne Abstriche bei der Leistungsfähigkeit

Mit diesen Tipps stellen Sie eine gelungene Roadmap für Ihre physische Sicherheit auf.

Leitfaden herunterladen

Den Alltag schützen.

Genetec™