Libro bianco

Considerazioni e best practice per la migrazione a un sistema di controllo degli accessi basato su IP

Genetec™

Sommario

Sintesi

La migrazione da un sistema di controllo accessi (ACS) legacy esistente a un ACS basato su IP (Internet Protocol) facilita la gestione, l'espansione e la personalizzazione della propria infrastruttura di controllo degli accessi fisici.

Per avere successo, la migrazione richiede comunque una pianificazione e un'attenta valutazione. Innanzitutto, è importante che i vari obiettivi siano chiari. Quindi, prima di pianificare una migrazione, le aziende devono valutare il proprio sistema esistente, per capire quali siano i costi e il tempo necessari per completare il processo.

Infine, è importante che le organizzazioni seguano, insieme a un integratore di sistemi, i passaggi chiave per realizzare un'integrazione perfetta.

1

Le motivazioni della migrazione

La migrazione da un sistema esistente di controllo accessi (ACS) legacy, centralizzato o distribuito, a un ACS basato su IP facilita la personalizzazione del sistema in base all'evoluzione delle proprie esigenze, con conseguente aumento della sicurezza e del ritorno sull'investimento.

Un ACS aperto e flessibile basato su IP consente alle aziende di:

- sfruttare la tecnologia IP per standardizzare la propria infrastruttura di controllo degli accessi e sostituire le apparecchiature proprietarie
- semplificare l'espansione e la modifica futura dell'infrastruttura per ridurre il costo totale di proprietà (TCO)
- integrare la sicurezza, il controllo accessi e la videosorveglianza in una piattaforma unificata con un'unica interfaccia
- ottenere un maggiore ritorno sull'investimento attraverso utilizzi che vanno oltre il blocco e lo sblocco delle porte

Con una soluzione basata su IP, le organizzazioni possono inoltre sfruttare funzionalità più recenti, che non sono disponibili con i sistemi tradizionali. Per questo motivo, è importante valutare come sfruttare le nuove funzionalità ACS offerte dalle soluzioni basate su IP, tra cui:

- miglioramento della gestione e del monitoraggio multisito
- aggiunta di un numero maggiore di porte su una rete
- miglioramento della sicurezza informatica con crittografia end-to-end e autenticazione avanzata
- utilizzo della gestione globale delle tessere per passare a un’unica tessera per tutti i siti

Sono disponibili nuove tecnologie di sicurezza informatica ACS, che consentono alle organizzazioni di sfruttare il proprio sistema per migliorare la sicurezza e le operazioni, proteggendosi al contempo dagli attacchi informatici

Anche gli ACS fisici tradizionali stanno diventando sempre più costosi da mantenere. Quando i componenti ACS legacy raggiungono il fine vita, i costi associati alla manutenzione di tali sistemi o alla ricerca di pezzi di ricambio aumentano.

Inoltre, gli ACS tradizionali non sono in grado di resistere ai sempre crescenti attacchi informatici. Gli ACS legacy utilizzano una tecnologia obsoleta, che li rende vulnerabili alle minacce informatiche. Sono disponibili nuove tecnologie di sicurezza informatica ACS, che consentono alle aziende di sfruttare il proprio sistema per migliorare la sicurezza e le operazioni aziendali, proteggendosi al contempo dagli attacchi informatici.

Infine, poiché i sistemi legacy funzionano in genere con un'alimentazione separata per ciascun lettore di tessere e per ciascuna serratura, sono più costosi di un ACS basato su IP aperto e flessibile, che supporta PoE per connettere e alimentare tutti i controller, i lettori e le serrature delle porte basati su IP.

2

Gli obiettivi della migrazione

Dopo aver deciso di procedere alla migrazione da un sistema legacy precedente a un ACS aperto e flessibile basato su IP, le organizzazioni dovrebbero valutare i seguenti obiettivi durante la ricerca del fornitore.

2.1 Acquisto di un sistema di lunga durata

Quando si cerca di stabilire la durata di un ACS, sono numerosi i fattori da tenere in considerazione:

- **La soluzione è un'architettura non proprietaria e aperta?** Un'architettura ACS aperta e non proprietaria rende più facile l'espansione e la modifica futura del sistema.
- **Il solution provider dispone di un ampio ecosistema di partner?** La scelta di un fornitore che abbia dei partner tecnologici in settori quali la gestione degli asset, le risorse umane e la gestione dei visitatori garantisce più flessibilità e un maggior numero di opzioni durante la migrazione e in caso di modifiche future.
- **Il fornitore di soluzioni offre un kit di sviluppo software (SDK) in pronta consegna?** Un SDK in pronta consegna consente l'integrazione e lo scripting personalizzati e rende possibile lo sviluppo futuro di plug-in per l'ACS basato su IP.

2.2 Riutilizzo delle apparecchiature esistenti

La migrazione a un ACS basato su IP aperto e flessibile può migliorare e proteggere l'investimento a lungo termine delle aziende nell'attuale infrastruttura di sicurezza, estendendo la vita dei componenti esistenti e sfruttando nuove funzionalità e applicazioni di sistema.

La migrazione a un ACS IP può migliorare e proteggere l'investimento a lungo termine delle aziende nell'attuale infrastruttura di sicurezza, estendendo la vita dei componenti esistenti e sfruttando nuove funzionalità e applicazioni di sistema.

2.3 Lavoro in parallelo

Per ottenere una migrazione ACS senza interruzioni, il lavoro preparatorio dovrebbe essere svolto in parallelo e offline per creare la configurazione del nuovo ACS basato su IP nel software, mediante:

- mappatura del sistema
- importazione degli input e degli output (IO) dai componenti del sistema
- integrazione della logica per il controllo dei componenti

2.4 Minimizzazione dei tempi di inattività

Quando si esegue la migrazione di un sistema esistente, si deve considerare l'impatto che i tempi di inattività avranno sugli utenti del sistema. In fase di selezione è importante stabilire:

- le ore di punta durante le quali l'ACS deve essere pienamente funzionante
- se il nuovo ACS basato su IP consenta o meno la preparazione
- se il nuovo ACS basato su IP possa essere collegato alle porte esistenti in parallelo

Oltre ad analizzare le funzionalità, si dovrebbe anche esaminare il proprio flusso di lavoro nel controllo degli accessi corrente, per garantire che il fornitore sia quantomeno in grado di mantenere, se non migliorare, tale flusso di lavoro nel nuovo sistema.

2.5 Garanzia della disponibilità di tutte le funzionalità cruciali

È importante esaminare le funzionalità hardware e software attualmente utilizzate nell'ACS legacy per garantire che tali funzionalità siano disponibili anche nel nuovo sistema.
Le funzionalità che dovrebbero essere analizzate includono:

- il numero di porte che possono essere supportate
- la gestione dei titolari delle tessere
- la gestione dei diritti di accesso
- il design del badge
- le esigenze del web client
- le esigenze dell'app mobile
- la gestione dei visitatori
- i dispositivi di registrazione

Oltre ad analizzare le funzionalità, si dovrebbe anche esaminare il proprio flusso di lavoro nel controllo degli accessi corrente, per garantire che il fornitore sia quantomeno in grado di mantenere, se non migliorare, tale flusso di lavoro nel nuovo sistema.

3

Panoramica delle considerazioni

Le seguenti considerazioni hanno lo scopo di aiutare le organizzazioni a valutare il loro attuale ACS.

I risultati di queste valutazioni hanno un impatto diretto su (1) la decisione di effettuare una migrazione con sostituzione completa o parziale, (2) il costo della migrazione (3) il tempo necessario per la migrazione.

3.1 Considerazioni sull'hardware

Qualsiasi migrazione da un ACS legacy a un ACS aperto e flessibile basato su IP deve iniziare valutando il sistema corrente.

La migrazione a un ACS basato su IP viene semplificata se il sistema esistente utilizza tessere e lettori non proprietari. Se invece i lettori esistenti supportano una comunicazione proprietaria, è probabile che sia necessaria una sostituzione completa dei lettori legacy.

È anche importante stabilire se possano essere riutilizzati i controller intelligenti e i pannelli di interfaccia a valle già esistenti: se i controller sono ad architettura aperta, si potrebbero incorporare nel nuovo ACS.

3.2 Considerazioni sul software

È importante stabilire esattamente cosa deve essere portato nel nuovo sistema. È necessario prendere in considerazione i dati nativi nelle credenziali legacy, gli strumenti utilizzati per esportare tali informazioni dal database corrente e qualsiasi componente di terze parti integrato nella configurazione tramite SDK.

La migrazione ACS richiede l'esperienza di tecnici pre-vendita, specialisti tecnici, tecnici di servizio sul campo e tecnici dell'assistenza.

3.3 Considerazioni sulla rete

Quando si valuta la migrazione a una soluzione di controllo degli accessi PoE devono essere valutate anche le esigenze di rete del nuovo sistema basato su IP.

Inoltre, si devono considerare i problemi di latenza e ampiezza di banda relativi alla comunicazione tra i siti durante la migrazione dei sistemi distribuiti, con siti sia locali che remoti.

3.4 Considerazioni sul cablaggio

Il cablaggio in un ACS legacy è un'altra valutazione importante per qualsiasi migrazione, poiché potrebbe essere possibile riutilizzare parte del cablaggio esistente nel nuovo ACS basato su IP. Prima della migrazione, è importante confrontare le caratteristiche del cablaggio esistente con i requisiti delle nuove apparecchiature ACS basate su IP. Inoltre, se l'azienda vuole espandere il proprio ACS attuale durante la migrazione, è necessario prevedere un eventuale cablaggio aggiuntivo.

3.5 Considerazioni sull'alimentazione

Prima della migrazione, è necessario considerare anche il tipo di alimentazione presente nell'ACS corrente, in particolare se il sistema è a 12 V o 24 V, CC o CA e se può fornire corrente sufficiente per i nuovi componenti hardware.

3.6 Considerazioni sulla formazione

Qualsiasi migrazione di successo a un sistema basato su IP aperto e flessibile richiede una formazione completa all'utilizzo del nuovo software. Occorre quindi valutare il tipo di formazione richiesta per i vari utenti ACS, in base alle loro mansioni e alle applicazioni client che utilizzeranno con il nuovo ACS.

3.7 Assistenza durante e dopo la migrazione

Per una migrazione di successo, è importante tener conto del livello di supporto fornito dall'integratore che installa il nuovo ACS, nonché da produttori e solution provider i cui componenti integreranno il nuovo sistema. La migrazione ACS richiede l'esperienza di tecnici pre-vendita, specialisti tecnici, tecnici di servizio sul campo e tecnici dell'assistenza.

4

Le fasi del processo di migrazione

Una migrazione di successo comporta vari passaggi. Innanzitutto, il cliente collabora con un integratore di sistemi e probabilmente con i produttori e i fornitori per ottenere un preventivo e un piano di migrazione. Mentre il piano viene implementato, il supporto tecnico e i tecnici sul campo progetteranno e configureranno il nuovo sistema basato su IP.

4.1 I fatti

L'integratore di sistemi deve innanzitutto stabilire la configurazione dell'ACS corrente, inclusi dati quali l'ubicazione degli armadi elettrici e delle telecomunicazioni, il cablaggio e il tipo di alimentazione attualmente in uso. È anche importante creare un elenco completo dei componenti hardware, dei server e delle apparecchiature di rete attualmente in uso, nonché fornire dettagli sulle funzionalità software correnti che saranno necessarie.

4.2 Comprensione dei requisiti del nuovo sistema

Per sviluppare un piano di migrazione di successo, devono essere riconosciuti e confermati i seguenti requisiti del nuovo ACS aperto e flessibile basato su IP:

- Componenti hardware
- Componenti software
- Configurazione di rete
- Cablaggio
- Alimentazione

La comprensione di tali requisiti è fondamentale per progettare l'architettura del nuovo sistema.

Per stabilire quali componenti hardware, software, di alimentazione, di cablaggio e di rete possano essere riutilizzati, è essenziale avere un quadro completo dell'attuale ACS e dei requisiti per il nuovo sistema.

4.3 Sopralluogo

Il passo successivo è una visita della struttura con il cliente, l'integratore di sistemi e possibilmente i produttori, per garantire che nessuna parte del sistema esistente sia stata trascurata. Il sopralluogo può anche essere il primo passo nel processo complessivo. Lo scopo del sopralluogo è:

- creare un quadro chiaro dell'architettura esistente e del layout del sistema esistente
- stabilire dove è concentrata l'attrezzatura
- misurare le distanze tra i pannelli di controllo accessi, le fonti di alimentazione e i lettori

4.4 Definizione dei componenti riutilizzabili

Per stabilire quali componenti hardware, software, di alimentazione, di cablaggio e di rete possano essere riutilizzati, è essenziale avere un quadro completo dell'attuale ACS e dei requisiti per il nuovo sistema.

4.5 Test dei componenti esistenti

Dopo aver stabilito quali componenti del sistema esistente possano essere riutilizzati, i componenti vanno testati per garantirne la compatibilità.

4.6 Definizione dei requisiti delle nuove attrezzature

Avendo una chiara idea di ciò che può essere riutilizzato dal sistema legacy esistente e di ciò che è necessario introdurre per il nuovo sistema, l'integratore deve ora stabilire la nuova rete e i requisiti di controllo accessi.

4.7 Comprensione dei database e dei dati esistenti

Il passaggio successivo del processo di migrazione consiste nello stabilire le modalità di importazione dei dati dei titolari di tessere e delle credenziali esistenti nel nuovo ACS basato su IP. Per sfruttare i dati dei software esistenti di terze parti, gli specialisti tecnici o i tecnici sul campo dovranno esportare i dati dei titolari di tessere e delle credenziali dal sistema esistente in un formato di file utilizzabile.

4.8 Pianificazione della migrazione

Per ridurre al minimo i tempi di inattività durante la migrazione, è necessario pianificare attentamente la migrazione dell'hardware per garantire che in parallelo venga eseguita, per quanto possibile, l'installazione di software e hardware.

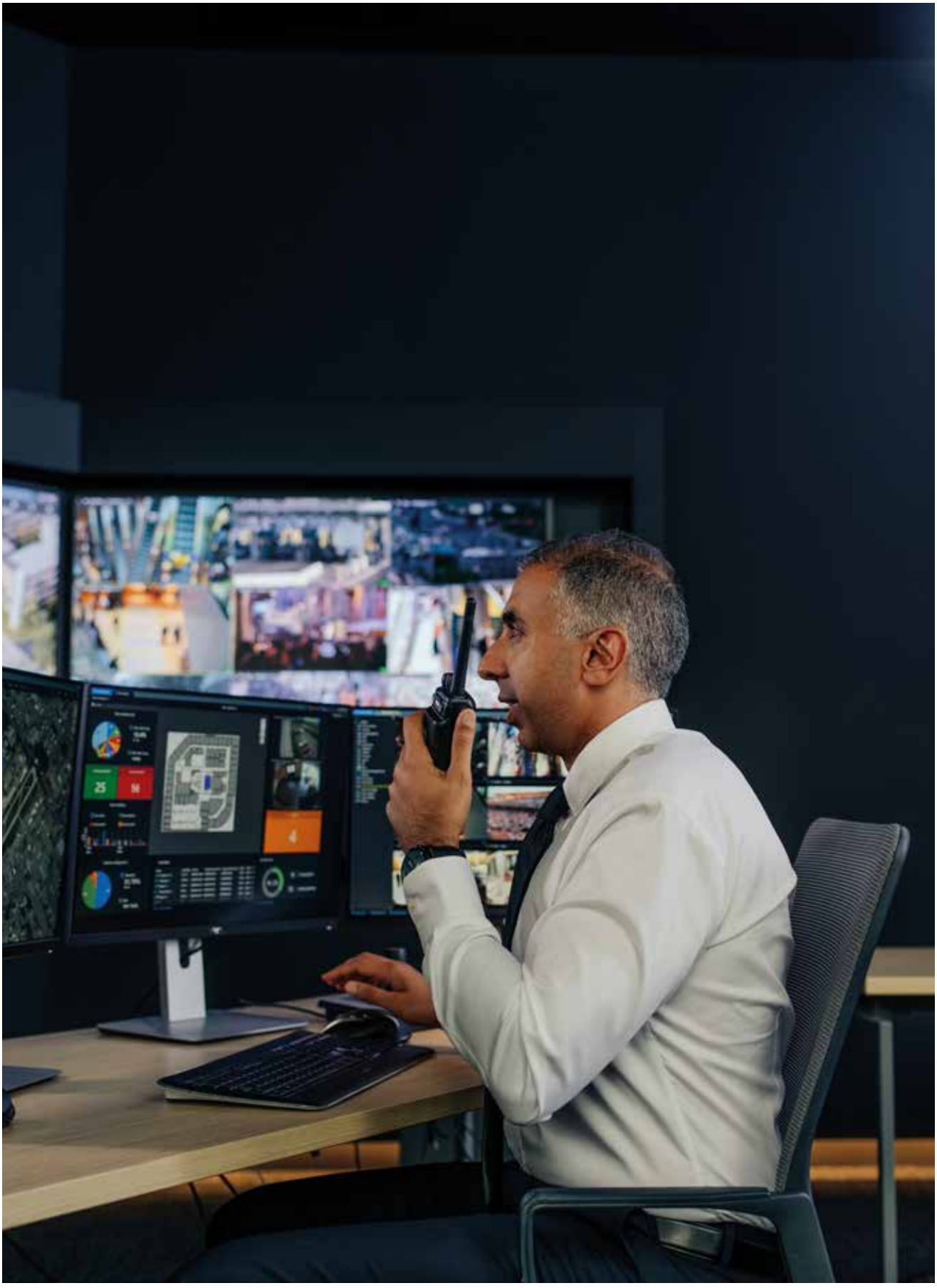
4.9 Test del nuovo sistema IP

Per garantire una migrazione senza problemi, l'integratore dovrebbe effettuare un'analisi completa del nuovo sistema IP prima di eseguire la migrazione.

4.10 Esecuzione della migrazione e test di collaudo

Seguendo il programma sviluppato nell'ambito del piano di migrazione, l'integratore dei sistemi e il cliente possono ora iniziare il passaggio dal vecchio al nuovo ACS. A questo punto, è importante avere a disposizione i produttori, in caso di problemi con uno qualsiasi dei nuovi componenti ACS.

Per garantire una migrazione senza problemi, l'integratore dovrebbe effettuare un'analisi completa del nuovo sistema IP prima di eseguire la migrazione.



5

Il nostro approccio alla migrazione

Per garantire una migrazione senza problemi, Genetec è disponibile durante l'intero processo, dalla valutazione iniziale e pianificazione della migrazione, fino al test del sistema e al supporto. Nel proprio ruolo di fornitore di soluzioni, Genetec garantisce agli integratori dei sistemi la disponibilità di tecnici pre-vendita, tecnici sul campo e tecnici del supporto tecnico.

Security Center Synergis™, il sistema di controllo accessi basato su IP di Genetec, offre ai clienti il vantaggio di lavorare con una piattaforma ad architettura aperta. Con Synergis, le aziende sono in grado di eseguire l'aggiornamento alla più recente tecnologia supportata in qualsiasi momento o persino di unificare la sicurezza e le operazioni in un'unica piattaforma. Questa piattaforma ad architettura aperta offre inoltre ai clienti molta più flessibilità per quanto riguarda le integrazioni di sistemi di terze parti. L'adattabilità di Synergis consente alle organizzazioni di far crescere il proprio sistema in base all'evoluzione delle proprie esigenze, consentendo loro di migliorare la sicurezza e di generare un maggiore ritorno sull'investimento.

Fondata nel 1997, Genetec è leader globale delle piattaforme di sicurezza unificate, con un'ampia offerta in varie specialità di sicurezza.

Videosorveglianza: Ottieni una maggiore consapevolezza situazionale e migliora la sicurezza della tua città con la possibilità di condividere le telecamere tra agenzie e organizzazioni, fornendo un quadro operativo comune e migliorando i tempi di risposta agli incidenti.

Controllo degli accessi: Aumenta la sicurezza della tua azienda, rispondi in modo efficace alle minacce e prendi decisioni più chiare e tempestive con una piattaforma unificata, IP-ready, che si tratti di implementare un nuovo sistema di controllo degli accessi o di aggiornare un sistema esistente.

Riconoscimento automatico delle targhe: Automatizza il rilevamento dei veicoli, aumenta l'efficienza dell'applicazione delle norme relative ai parcheggi e accelera le indagini relative alla sicurezza pubblica grazie alla possibilità di condividere i dati delle targhe con agenzie selezionate e aziende partner, senza problemi di proprietà e di privacy.

Supporto alle decisioni operative: Maggiore efficienza nella gestione degli incidenti e nel processo decisionale, con flussi di lavoro avanzati che guidano gli operatori nell'intero percorso: dagli avvisi, alle procedure basate sulle politiche, fino all'esportazione della compilazione dettagliata dei casi.

Gestione dei casi investigativi: Semplifica la gestione dei casi e accelera le indagini con una piattaforma che ti consente di centralizzare le prove digitali e di collaborare in modo sicuro con investigatori, agenzie esterne e pubblico.

Servizi cloud: Estendi le capacità del tuo sistema di sicurezza locale e riduci i costi IT con servizi cloud on-demand altamente scalabili, che consentono alla tua città di far fronte facilmente ai requisiti di sicurezza in rapida evoluzione e di operare con maggiore efficienza.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

AGGIORNAMENTO: 12-LUG-21