Genetec ClearID™

Geünificeerd fysiek identiteitsbeheer en toegangsbeheer

Genetec™

Een slimmere manier om toegang te beheren

Het vrij bewegen van mensen binnen een organisatie is essentieel voor het succes ervan. Hoe u toegangsrechten toewijst en beheert, helpt die stroom te beschermen. Maar na verloop van tijd kunnen nalevingsbehoeften, nieuwe processen en externe voorschriften de boel vertragen – door gaten in de beveiliging te creëren en dat alles bepalende momentum te onderbreken.

Vaak nemen kleine dingen zoals verloren kaarten en toegangsverzoeken kostbare tijd in beslag van een operator. En omdat standaard toegangscontrolesystemen statisch zijn en niet gekoppeld aan het bedrijfsbeleid, kan de operator geen duidelijk administratief pad volgen.

Genetec ClearID™ biedt een slimmere oplossing. Het is een zelfbedieningssysteem voor fysieke identiteits- en toegangsbeheer dat uw beveiligingsbeleid versterkt en uw organisatie efficiënter, meer conform en veiliger maakt. Het kan sneller en eenvoudiger worden ingezet dan andere geïntegreerde systemen, omdat het is geünificeerd met onze beveiligingssoftware voor toegangscontrole, Security Center Synergis™. En omdat ClearID een cloud gebaseerde dienst is, werkt het probleemloos met Synergis – zodat eindeloze aanpassingen en onhandige integraties van componenten tot het verleden behoren.

Van bedrijfskantoren en universiteitscampussen tot sterk gereguleerde multinationals in de olie-, gas-, mijnbouw- en petrochemische industrie, ClearID zorgt voor een vlot verloop van de dagelijkse complexiteit van het beheer van individuele toegangsrechten.

Gebaseerd op uw beleid zorgen de geautomatiseerde en selfservice capaciteiten van ClearID voor een vlottere en efficiëntere werkomgeving voor iedereen.

Identiteiten uitgelegd

ClearID beheert op centrale wijze de toegangsrechten van alle personen die contact hebben met uw organisatie. Dit is wat u moet weten:

Identiteit

Een identiteit is het unieke digitale profiel van een werknemer of bezoeker. Het kan permanent zijn voor medewerkers, semi-permanent of tijdelijk voor bezoekers. Identiteiten navigeren tussen verschillende beveiligings- en bedrijfssystemen en kunnen bestaan uit:

— een werknemer in het loonadminstratie- en HR-managementsysteem
— een Windows-gebruiker in Microsoft Active Directory
— een salesmanager in de tool voor klantenrelatiebeheer en offertes
— een kaarthouder in het fysieke toegangscontrolesysteem

Levenscyclus identiteit

Een moderne fysieke identiteits- en toegangsbeheeroplossing (PIAM, Access Management Solution) beheert op centrale wijze het beleid, de processen en de identiteiten van een organisatie, van het toelaten van bezoekers tot aan onboarding en offboarding van medewerkers.
Zodra het beleid is gedefinieerd, houdt ClearID toezicht op de levenscyclus van een identiteit in vier typische stadia:

1. Aanmaak van identiteit
2. Toegangsvoorziening
3. Verandering van identiteit
4. Toegangsbeëindiging

Kenmerken

Een identiteit bestaat uit een reeks eigenschappen die kenmerken worden genoemd. Deze kenmerken worden gebruikt om de toegangsrechten van een identiteit te bepalen. Naarmate iemands kenmerken veranderen, veranderen ook zijn toegangsrechten.

Voorbeelden zijn:
— Afdeling
— Locatie
— Rol
— Naam van de supervisor
— Functie van de werknemer
— Aantal dienstjaren
— Opleiding

Hoe ClearID werkt

ClearID stelt organisaties in staat hun beleid inzake beveiliging en naleving te standaardiseren en te verbeteren. Door het beheer van toegangsrechten te automatiseren en te vereenvoudigen, worden de veiligheids- en operationele risico's beperkt. Het is een gestroomlijnde workflow die de volgende stappen omvat:

Stap 1: initiële aanvraag

Een medewerker maakt verbinding met ClearID en vraagt voor een bepaalde duur toegang tot een beveiligde zone.

Stap 2: verificatie en goedkeuring supervisor

Wanneer een toegangsverzoek wordt gedaan, verifieert ClearID het beleid voor de locatie en keurt het automatisch goed of vraagt om goedkeuring van bevoegde supervisors.

Stap 3: wijziging toegangsrechten

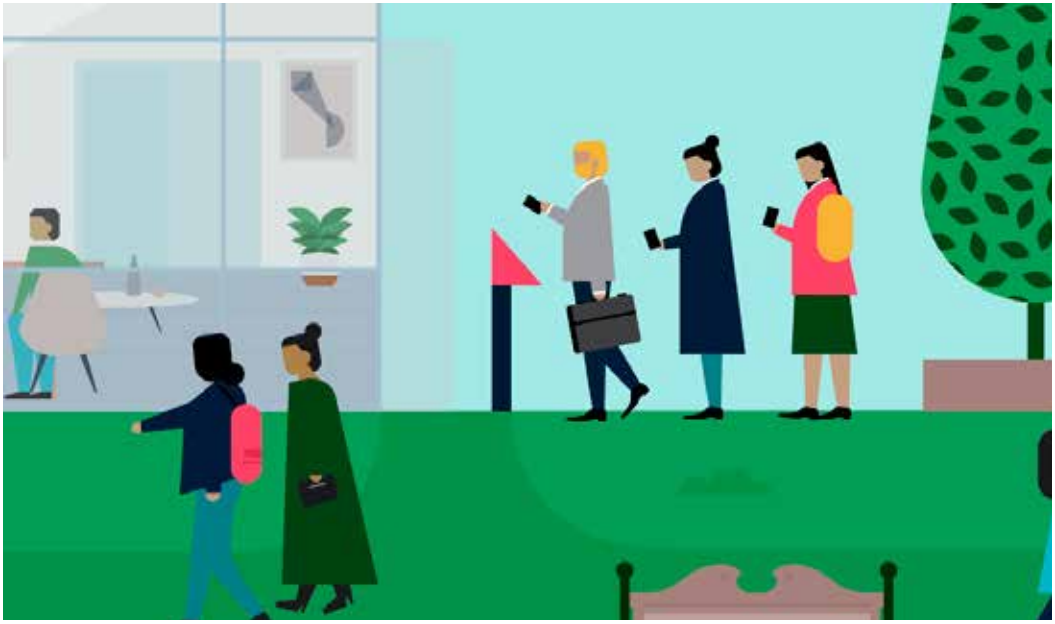
Indien goedgekeurd, wordt het toegangscontrolesysteem bijgewerkt, waardoor de juiste toegang wordt verleend voor de gevraagde periode. Bij weigering wordt de toegang geweigerd en ontvangt de aanvrager een e-mail met uitleg waarom.

Kaarthouderervaring vereenvoudigen

Uw medewerkers en bezoekers vertrouwen elke dag op het fysieke toegangscontrolesysteem om zich door uw gebouw te verplaatsen, van gemeenschappelijke ruimtes tot meer beveiligde plekken. Waarom zou u dan ook de mogelijkheid om toegangsrechten te wijzigen beperken tot beveiligingsoperators of IT-personeel? Wanneer iemand een wijziging moet aanvragen, moet hij in de meeste gevallen naar het badge bureau of de receptionist gaan, wat het proces verder vertraagt.

Als selfservice oplossing voor fysieke identiteits- en toegangsbeheer geeft ClearID iedereen een nieuwe, workflow gebaseerde benadering om nieuwe toegangsrechten aan te vragen of bestaande rechten te wijzigen. Aanvragen kunnen rechtstreeks bij gebiedsmanagers worden ingediend zonder de operatoren van toegangscontrolesystemen erbij te betrekken.

Door medewerkers en bezoekers controle te geven over hun toegangsverzoeken verbetert ClearID de ervaring van de kaarthouder, vermindert frustrerende wachttijden en zorgt voor een soepele organisatie.



Verhoogt de beveiliging, verlaagt het risico

Offboarding is een cruciaal moment in het ontslagproces van werknemers. Als een medewerker vertrekt, zou hij/zij immers geen toegang meer moeten hebben tot uw instelling en vooral tot de beveiligde ruimtes. Maar soms weet een operator misschien niet welk beleid hij/zij moet volgen om toegang te beëindigen of is hij/zij zich niet bewust van alle workarounds en uitzonderingen die in een toegangscontrolesysteem zijn geprogrammeerd.

Er worden doorgaans kleine improvisaties gemaakt door individuele operators en deze worden niet altijd centraal beheerd. Na verloop van tijd stapelen deze workarounds zich op en creëren ze hiaten in de beveiliging.

Met ClearID definieert u uw standaard beveiligings- en compliance beleid en zorgt het systeem voor de rest. De workflow motor maakt gebruik van organisatorische beleidslijnen om de individuele toegangsrechten continu te updaten op basis van de geldende identiteitskenmerken. De geringste wijziging van kenmerken wijzigt de bestaande toegangsrechten, zodat er geen handmatig ingevoerde uitzonderingen of ad hoc wijzigingen nodig zijn.

Dus wanneer uw HR-team de identiteit van een werknemer deactiveert, wordt zijn toegang in alle systemen ingetrokken, zodat u verzekerd bent van een correcte offboarding.

Verbetering van methodisch toezicht

Bij hun dagelijkse werkzaamheden maken operators soms uitzonderingen op de bedrijfsbeleidslijnen van hun organisatie. Een operator kan bijvoorbeeld een telefoontje krijgen van de supervisor van een medewerker en uitzonderlijk toegang verlenen.

In een traditioneel systeem wordt de verandering doorgevoerd, maar vaak worden de goedkeuring en de reden hiervoor nooit vastgelegd.

ClearID volgt en rapporteert elke operatie of actie gekoppeld aan een identiteit gedurende hun levenscyclus. Het schetst een volledig beeld van de tijdelijke en permanente toegangsaanvragen en goedkeuringen door de context te bieden achter uitzonderingen en eenmalige aanvragen. Dit helpt organisaties om routinematige toegangsbeoordelingen en audits uit te voeren om te bevestigen dat alle werknemers en bezoekers alleen toegang hebben tot toegestane zones.

Door de beveiliging van uw organisatie volledig traceerbaar te maken, kunt u naleving van voorschriften en corporate governance waarborgen.

Operationele efficiëntie verbeteren

Klassieke toegangscontrolesystemen vertrouwen op de operators om identificaties af te geven en toegang te verlenen. Maar hoe kan van een klein aantal personeelsleden worden verwacht dat ze de toegangsrechten van elke werknemer of bezoeker kennen?

Wanneer bewijs van opleiding nodig is voor specifieke zones, moeten operators doorgaans contact opnemen met een gebiedsmanager of supervisor voor bevestiging of om de goedkeuring te verkrijgen via hun e-mails. Deze handmatige aanpak wordt altijd uitgesteld wanneer supervisors vergaderen of op vakantie zijn. Naarmate een organisatie groeit, zijn er meer operators nodig om het groeiende aantal kaarthouders en zones te beheren.

Organisaties pakken het probleem van een overbelast of overwerkt team vaak aan door meer personeel aan te werven, maar dit maskeert alleen de onderliggende inefficiëntie van een handmatig systeem. Door het beheer van toegangsrechten te automatiseren en knelpunten weg te werken, zorgt ClearID ervoor dat medewerkers en bezoekers aan alle bedrijfsvereisten hebben voldaan alvorens toegang te verlenen tot een zone. Dat betekent dat het beheer van dagelijkse toegangsverzoeken, nalevings- en beleidsupdates aanzienlijk verbeterd is. Operators worden efficiënter en richten hun aandacht op risicovol, missiekritiek werk.

Verbeter de beleving van uw bezoekers

In een druk bedrijfskantoor kan het toelaten van bezoekers een arbeidsintensieve taak zijn voor baliemedewerkers. Activiteiten variëren van het lezen van inkomende e-mailverzoeken en het toevoegen van bezoekers aan de dagelijkse bezoekerslijst tot het handmatig inchecken van bezoekers en het bellen van hun gastheren. Deze tijdrovende en inefficiënte aanpak zorgt voor langere wachttijden voor bezoekers waardoor ze geen optimale eerste indruk krijgen.

Met ClearID wordt het bezoekersbeheer voor iedereen een vlottere ervaring. Het proces start zodra er een vergadering gepland staat. Eerst logt de lokale medewerker (of host) via een web portaal in op ClearID en maakt een profiel aan voor de bezoeker met zijn naam en contactgegevens, het doel, de datum, het tijdstip en de duur van het bezoek. De aanvraag voor de vergadering moet worden goedgekeurd door de manager van de host of ClearID kan de vergadering automatisch goedkeuren mits aan de juiste criteria wordt voldaan. De bezoeker ontvangt dan een e-mailuitnodiging van ClearID namens de organisatie van de host.

Ondertussen geeft ClearID automatisch goedkeuring voor het bezoek af, omdat de host door een systeembeheerder toestemming heeft een gast uit te nodigen zonder goedkeuring van de supervisor. De bezoeker en de host krijgen allebei bevestigingsmails voor de komende afspraak. Op de dag van de vergadering komt de bezoeker aan bij de frontlobby en scant zijn e-mail QR-code of ID bij een kiosk.

Na aanmelding wordt een zelfklevende bezoekersbadge afgedrukt bij de kiosk of wordt een actief pasje verstrekt door de receptionist – en de host wordt op de hoogte gebracht van zijn aankomst. De host kan de bezoeker vervolgens verwelkomen en naar de vergaderruimte begeleiden, waar ze op tijd en zonder complicaties aan de slag gaan.

Voorbereiden op een audit

In een sector waar organisaties moeten voldoen aan strenge toegangsvereisten, zijn regelmatige audits essentieel. Een supervisor wordt bijvoorbeeld op de hoogte gebracht van een komende audit en neemt contact op met de beveiligingsmanager, zodat hij een rapport kan krijgen over wie toegang heeft tot beperkte zones. Maar de beveiligingsmanager is op vakantie, wat betekent dat het uitvoeren van het rapport ingewikkeld en tijdrovend wordt. Zodra het definitief is overgedragen, merkt de supervisor hoeveel onbevoegden toegang hebben gehad tot deze beperkte zones. Deze omvatten oud-bezoekers en medewerkers die de organisatie hebben verlaten.

Als het regelgevend orgaan daarachter zou komen, krijgt de organisatie een forse boete voor het overtreden van voorschriften. Nu moet de supervisor elke persoon op het rapport nakijken en aangeven wie toegang moet blijven hebben. Zodra dit is afgerond, moet hij een rapport verzenden van mensen die verwijderd moeten worden, zodat de beveiligingsmanager het toegangscontrolesysteem kan bijwerken. Dit handmatige proces is pijnlijk traag, hulpbronafhankelijk en laat plaats aan menselijke fouten omdat iemand op de lijst gemakkelijk over het hoofd kan worden gezien.

Met ClearID kan de supervisor inloggen op het portaal om snel te zien wie toegang heeft tot afdelingen en zones. Hij kan zo de rechten van onbevoegde personen intrekken. Hij kan eenvoudigweg de locatie kiezen die hij wil controleren en dan de toegang van een persoon tot die afdeling onmiddellijk intrekken – met de optie om een reden op te geven. Wat vroeger een duur handmatig proces was, kan nu in enkele minuten uitgevoerd worden – de controle wordt teruggelegd in de handen van de supervisor en de organisatie voorkomt zo duizenden euro's aan boetes.

Beveiliging voor een soepele bedrijfsvoering

Met ClearID kunt u uw beveiligingsbeleid standaardiseren en automatiseren, inconsistenties verminderen en hiaten in de beveiliging verwijderen. Tijdens het proces helpt het u de naleving van organisatorische of sectorale voorschriften in al uw vestigingen te bereiken en te handhaven. Operationeel bereikt u nieuwe efficiëntieniveaus door de identiteiten centraal te beheren en door medewerkers te empoweren via een selfservice-model voor toegangscontrole. ClearID zorgt voor een vlotte organisatie en betrouwbaarheid.

Hoofdkantoor
Genetec Inc.
2280 Alfred-Nobel Blvd.,
Suite 400
Montréal QC H4S 2A4
Canada
Gratis nummer: +1 866 684 8006
Canada & VS:
Tel.: +1 514 332 4000
genetec.com

Genetec ClearID is een selfservice-systeem voor fysieke identiteits- en toegangsbeheer dat uw beveiligingsbeleid normaliseert en versterkt om toegang toe te staan en uw organisatie efficiënter te maken.

genetec.com/clearid