brivo

TOPP SÄKERHETSTRENDER

2022

Hybridarbete driver på molnbaserad åtkomstkontroll

INTRO

Historiskt sett har säkerheten varit inriktad på vakter, staket och andra åtgärder för att hålla skurkarna borta. Men i dagens samhälle är åtkomstkontroll mycket mer än så. Idag är åtkomstkontroll möjliggöraren för digitaliseringen av samhället och utökandet av Proptech-ekosystem. Organisationer räknar med att tekniken tillför värde via data – för att ge affärsinsikter, generera nya intäktsströmmar, skapa effektivitet, förstå användarbeteende, dokumentera trender, mer effektivt allokera humankapital och så vidare. Molnbaserade åtkomstsystem, särskilt när de är integrerade med andra säkerhets- och Proptech-system och funktioner, ger en rik till stor del outnyttjad datakälla.

Resultaten i denna undersökning antyder bara en bråkdel av potentialen för datainsamling, analys och intäktsgenerering i molnbaserade system. Till exempel, hälften av de tillfrågade organisationerna investerar i hybrida arbetsplatser, vilket bekräftar att framtiden verkligen har förmågan att stödja hybridarbetsmiljöer. Ändå ökar vissa organisationer antalet kvadratmeter, och den vanligaste integrationen av åtkomstkontroll är besökshantering. Den intelligensen kan hjälpa organisationer att fatta bättre affärsbeslut, som involverar områden som affärsresor, hyresförhandlingar och kapitalinvesteringar i teknik. Detta är några möjliga tillämpningar av data. Vi uppmuntrar dig att aktivt använda denna rapport som ett verktyg för att prioritera och fatta beslut om alla aspekter av fysisk säkerhet i de byggnader du ansvarar för eller innehar.

Organisationer investerar i hybrida arbetsplatser, vilket bekräftar att framtiden verkligen har förmågan att stödja hybrida arbetsmiljöer

Viktiga Punkter

1. Hybridarbete är här för att stanna
2. Data är drivkraften bakom förändring
3. Integrationer är viktiga
4. Mobil åtkomst och autentiseringsuppgifter växer
5. Molnet är nyckeln till säkerhetscentralisering och möjliggör den nya arbetsdynamiken

TOPP SÄKERHETSTRENDER 2022

Hybridarbete är här för att stanna, och åtkomstkontroll driver säkerhets- och icke säkerhetsaspekter av hybridarbetsmodellen, enligt en undersökning gjord av Brivo om säkerhetsläget 2022. Nästan 60 % av de drygt 550 respondenterna använder för närvarande en hybrid arbetsmodell, och nästan två tredjedelar rapporterar att åtkomstkontroll är extremt eller mycket viktigt för den modellen. Vidare säger 65 % av de tillfrågade att åtkomstkontroll och dess integration med andra teknologier har varit mycket viktiga eller extremt viktiga för att möjliggöra en hybrid arbetsplats sedan 2020.

Molnmigrering ligger bakom trenden mot att åtkomstkontroll blir en hörnsten i en hybrid arbetsmiljö. Fyrtio procent av de tillfrågade har centraliserat sina system i molnet, upp från 35 % i 2021 survey. Ytterligare 31 % är delvis centraliserade, medan 28 % är decentraliserade. Även de som inte använder molnbaserade säkerhetssystem idag förstår fördelarna: 57 % av de tillfrågade säger att molnbaserad åtkomstkontroll skulle förbättra deras säkerhet.

Brivo genomförde undersökningen mellan den 6 och 28 januari 2022, i samarbete med ASIS International, och fick 557 svar från säkerhets- och anläggningsproffs inom två dussin industrisektorer. Cirka 50 % av respondenterna kom från Europa, Mellanöstern och Asien, med den största enskilda uppsättningen svar från Nordamerika med andra halvan av de tillfrågade. 61% procent av de tillfrågade hanterar säkerhet för flera anläggningar på företagsnivå.

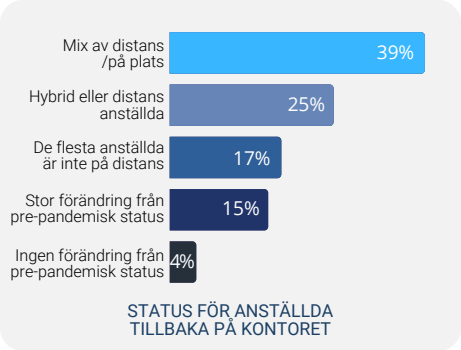
65 %

säger att integration med åtkomstkontroll med annan teknik har varit viktigt för att möjliggöra hybridarbete

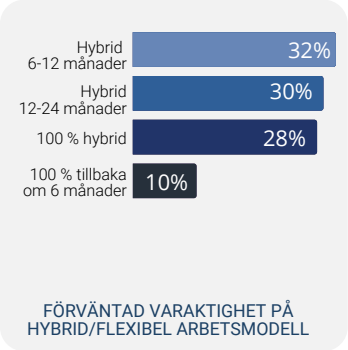
Hybridarbete är här för att stanna, och åtkomstkontroll driver säkerhets- och icke-säkerhetsaspekter av hybridarbetsmodellen

HYBRIDARBETSKRAFTEN ÄR HÄR FÖR ATT STANNA

När pandemin går in på sitt tredje år har de flesta organisationer utvecklats till en hybridarbetsmiljö - 58 % av de tillfrågade driver för närvarande en hybridarbetskraft, och endast 10 % förväntar sig att återgå till pre-pandemisk arbetsstatus inom de närmaste sex månaderna.



STATUS FÖR ANSTÄLLDA TILLBAKA PÅ KONTORET

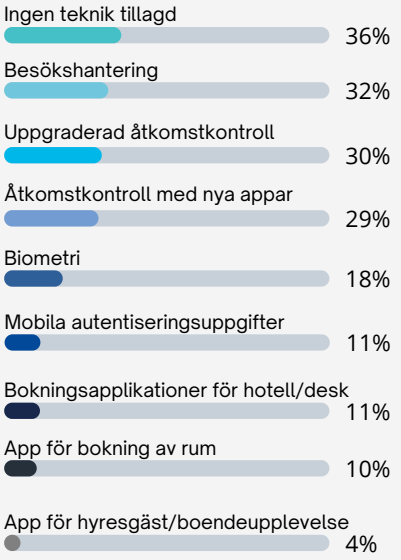


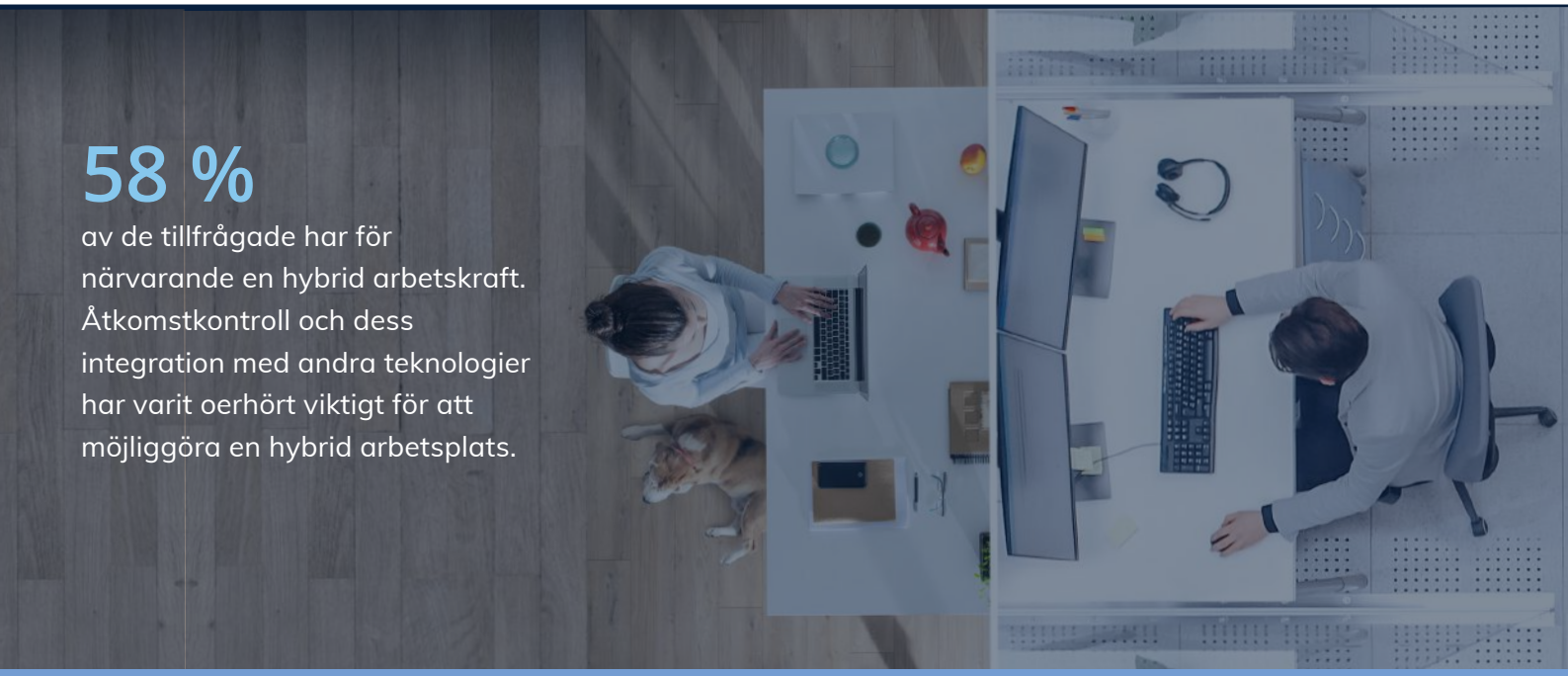
FÖRVÄNTAD VARAKTIGHET PÅ HYBRID/FLEXIBEL ARBETSMODELL

Faktum är att under de senaste 6 till 12 månaderna har nästan hälften av organisationerna lagt till teknik för att stödja en hybrid arbetsplats, och som nämnts tidigare säger nästan två tredjedelar att åtkomstkontroll och dess integration med andra teknologier har varit extremt eller mycket viktigt för att möjliggöra en hybrid arbetsplats. De vanligaste tilläggen och uppgraderingarna inkluderar besökshanteringssystem (32 %), uppgraderad åtkomstkontroll (30 %), åtkomstkontroll integrerad med nya applikationer (29 %) och biometri (18 %). Flera icke-säkerhetsfunktioner visas också: applikationer för hotell-/skrivbordsbokning (11 %), applikationer för rumsreservation (10 %) och appar för hyresgäst/boendeupplevelse (4 %). Dessa icke-säkerhetsfunktioner understryker fenomenet med åtkomstkontroll och andra Proptech-applikationer som allt oftare delar samma plattform.

VIKTIGHETEN AV ÅTKOMSTKONTROLL OCH ANNAN TEKNIK FÖR ATT MÖJLIGA EN HYBRID ARBETSPLATS

VERKTYG OCH TEKNIK SOM INFÖRTS FÖR ATT HANTERA FYSISKA PLATSER





58 %

av de tillfrågade har för närvarande en hybrid arbetskraft. Åtkomstkontroll och dess integration med andra teknologier har varit oerhört viktigt för att möjliggöra en hybrid arbetsplats.

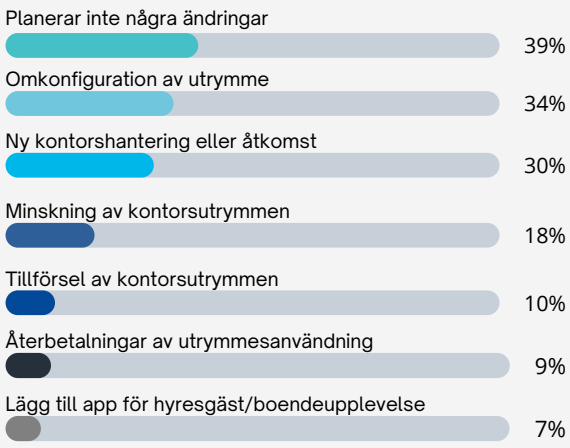
Den stora frågan för alla är vad kontorsägare och hyresgäster planerar att göra med sitt utrymme? Många spekulerade i att pandemin skulle vara slutet på kontoret och att alla kommer att arbeta på distans. Alla företag kan inte arbeta helt på distans och många arbetare har formulerat fördelarna med att arbeta på kontoret för att få mer samarbetstid med kollegor och en bättre relation med chefer och personal.

Att anpassa trygghet och säkerhet till den hybrida arbetsmiljön kräver mer än bara teknik, respondenterna identifierade andra förändringar som deras organisation är redo att göra under de kommande 6 till 12 månaderna. Medan 39 % inte förutser några andra förändringar och 30 % skulle luta sig mot tekniska lösningar, säger mer än en tredjedel att de kommer att konfigurera om sin arbetsplats. Anmärkningsvärt är att medan 18 % förväntar sig att minska kontorsytor, förväntar sig ytterligare 10 % att lägga till utrymme, vilket är goda nyheter för en osäker kommersiell fastighetsmarknad och strider mot förutsägelser om omfattande minskning av ytor.

Hybridarbetskraften erbjuder sina egna särskilda utmaningar. Respondenterna pekar vanligtvis på ökad fysisk och cyberrisker (49 %), delning av autentiseringsuppgifter, "tailgating" eller olämplig åtkomst (49 %) och inkonsekventa och oförutsägbara scheman och åtkomsthändelser (41 %) som viktiga problemområden. Många av de ytterligare svaren angav oro relaterade till isolerade situationer, såsom psykiska problem och bristande tillsyn.

STÖRSTA SÄKERHETSBEKYMMER MED DEN HYBRIDA ARBETSPLATSMODELLEN

1. 50% — Ökade fysiska risker och cyberrisker
2. 49% — Begränsad arbetaråtkomst eller legitimation delning
3. 41% — Inkonsekvent scheman och åtkomsthändelser
4. 17% — Stöld



Att anpassa säkerhet och trygghet till den hybrida arbetsmiljön innebär mer än bara teknik identifierade respondenterna andra förändringar som deras organisation är redo att göra i de kommande 6 till 12 månaderna

DATA VISAR VÄGEN

Företagen börjar inse fördelarna med att samla in säkerhetsrelaterade data. Dessa data kan användas för att förbättra säkerheten, bättre förstå utrymmesutnyttjandet och minska kostnaderna. Men det är fortfarande sant att en stor mängd av de miljarder datapunkter som skapas varje dag, t.ex. onormala aktiviteter, videoströmmar och bilder, inte samlas in, lagras eller bara delvis analyseras i traditionella säkerhetssystem.

Företagen fortsätter att kämpa med hur de bäst ska generera, utnyttja och använda säkerhetsdata. Denna kamp framträder tydligt i respondenternas val av det främsta målet för fysisk säkerhet för 2022. Det främsta målet: att använda data om fysisk säkerhet som genereras från händelser, video och intrångsdetektering för att fatta välgrundade affärsbeslut. Faktum är att organisationer nämner olika bekymmer kring säkerhetsrelaterad data: brist på handlingsbar insikt från data (33 %), underlåtenhet att generera tillräckligt med data (23 %) och inkompatibla datakällor (16 %). Men nära 35 % säger att de inte står inför några utmaningar att använda eller skaffa relevant data.

När det gäller vilka fördelar lämplig data skulle ge deras företag, säger de många svarande (38 %) att analyser skulle förbättra deras fysiska säkerhetspolicyer och rutiner. Mindre siffror tror att analys skulle ge värde för andra avdelningar, såsom process, leveranskedja och HR (16 %), hjälp personalen undersöker misstänkta beteendemönster (15 %) eller stödjer policyefterlevnad (14 %).

Utöver användning och inhämtning av säkerhetsdata önskar respondenterna flera andra fysiska säkerhetsmål för 2022. Mest framträdande är att 22 % planerar att integrera säkerhetssystem med andra tvärfunktionella områden inom organisationen (t.ex. HR-programvara, applikationer för fastighetsförvaltning, Proptech etc.), och 21 % vill bättre förstå hur man använder eller utnyttjar befintlig teknik.

Fördelarna med att använda säkerhetsrelaterad data är att den kan användas för att förbättra säkerheten, bättre förstå utrymmesutnyttjandet och minska kostnaderna

Datatillgång och dataanvändning är ett framträdande tema i årets undersökning. Många organisationer prioriterar datainsamling, analys och tillit för att fatta bättre informerade beslut och sätta upp mål för sina organisationer.

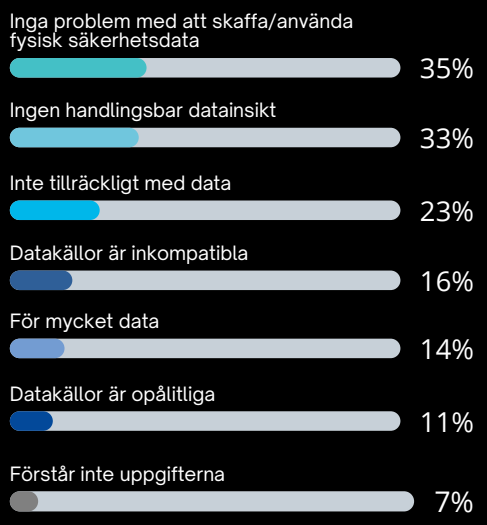
MÅL FÖR FYSISK SÄKERHETSDATA FÖR 2022

1. 25% Använd fysisk säkerhetsdata att fatta välgrundade affärsbeslut (händelser, video och intrångsdetektering)
2. 22% Säkerhetssystemen bör integreras med HR-programvara, programvara för fastighetsförvaltning, PropTech osv.
3. 21% Bli mer kunnig om hur man använder eller använder redan tillgänglig teknik
4. 11% Etablera ett säkerhetsoperationscenter eller ett virtuellt säkerhetsoperationscenter
5. 7% Automatisera vaktfunktioner (t.ex. med hjälp av drönare, robotar, besökssystem, videoövervakning, etc.)
6. 6% Förvandla kontoret till en hybridmiljö

FÖRDELAR MED FYSISKA ANVÄNDNING AV SÄKERHETSDATA FÖR DITT FÖRETAG

1. 38% Förbättra fysiska säkerhetspolicyer/procedur er baserade på analyser
2. 16% Tillför värde för andra avdelningar, såsom Process, Supply Chain, HR, osv.
3. 15% Undersök misstänkta beteendemönster
4. 14% Stöd efterlevnad av policy
5. 10% Förstå åtkomsttrender och utrymmesutnyttjande
6. 7% Prioritera onormal aktivitet för uppföljning

ATTITYDER MOT ÅTKOMSTKONTROLL OCH SÄKERHETSDATA



Fenomenet hybridarbete har inte minskat behovet av fysisk säkerhet och åtkomstkontroll

Åtkomstkontroll är ännu viktigare nu när vi skapar mer flytande, öppna och hybrida miljöer

HINDER FÖR ANVÄNDNING AV NY FYSISK SÄKERHETSTEKNIK?

Säkerhetsframsteg står inför långvariga framtida hinder. De vanligaste hindren för att implementera förbättrad fysisk säkerhet inkluderar brist på budget (34 %), brist på anpassning mellan säkerhetsavdelningar och andra avdelningar (24 %) och bristande förståelse för närvarande tillgängliga lösningar (16 %). Detta har inte förändrats mycket jämfört med våra tidigare årliga undersökningar.

Ett intressant fynd från de tillfrågade 2022 var att väldigt få svarande (7 %) säger att de har lite behov av fysisk säkerhet eftersom de flesta arbetare är avlägsna. På samma sätt visar bristen på ROI och bristen på sponsring av ledande befattningshavare (7 %) att även om det finns budgethinder och hinder mellan avdelningarna, förstår chefer behovet av ny säkerhetsteknik och har en tydlig syn på den avkastning de kan förvänta sig av sin investering i säkerhetsteknik.

Dessa datapunkter visar att fenomenet hybridarbete inte har minskat behovet av fysisk säkerhet och åtkomstkontroll. Faktum är att passerkontroll är ännu viktigare nu när vi skapar mer flytande, öppna och hybrida miljöer.

HINDER FÖR ANVÄNDNING AV NY FYSISK SÄKERHETSTEKNOLOGI

KOPPLINGAR OCH INTEGRATIONER FORTSÄTTER ATT FRÄMJA ADOPTION

Integrationer är kopplingar som samverkar mellan system och applikationer som helhet som delar information och data. Att integrera andra system och appar från tredje part förstärker funktionaliteten och funktionerna för alla plattformar.

Interoperabilitet med andra tekniker kan automatisera och förbättra kapaciteten hos en lösning som skapar affärseffektivitet och bättre användarupplevelser. I den digitala transformations-eran kan centraliserad data över det nästan oändliga teknikekosystemet hjälpa företag att fatta smarta, välinformerade beslut.

Respondenterna menade att det största hindret för införande är interoperabilitet med befintliga system. På frågan om interoperabilitet och integrationer, inklusive vilka system som är viktigast att integrera med fysisk åtkomstkontroll och säkerhetssystem, spreds svaren ganska jämnt bland de 10 erbjudna svaren, ledda av videoövervakning (22 %) och lösningar för identitets- och åtkomsthantering (21 %). Arbetsplatsledning/hybridarbetsapplikationer (13 %) och applikationer för besökshantering (11 %) registrerade de två näst högsta svarsfrekvenserna.

Största hindret för införande är interoperabilitet med befintliga system

MOBIL ÅTKOMST ÄR EN VÄXANDE AFFÄRSMÖJLIGHET

Mobila lösningar tillåter användare att öppna dörrar, grindar och andra entrésystem med en smartphone. Detta gör navigering i utrymmen på kontor, gym, garage, fabriker, skolor och andra platser bekvämare. Pandemin har påskyndat introduktionen av mobila autentiseringsuppgifter genom att öka efterfrågan på ett fjärrstyrt, kontaktlöst sätt att registrera nya människor i åtkomstsystemet. Dessutom, till skillnad från fysiska kort eller fjärrkontroller, är smartphones säkrare, lättare att hantera, och mer kostnadseffektivt för företag.

Mobil åtkomstkontroll—som kombinerar bekvämligheten och säkerheten hos smartphones med kostnadsbesparingarna för att eliminera nyckelkort—har vuxit fram som en konsekvens av kunders önskan om beröringsfria lösningar under covid-pandemin. Arton procent av de tillfrågade har redan anammat den tekniken och ytterligare 42 % överväger det. Mobila autentiseringsuppgifter har dock ännu inte integrerats brett i hela företaget.

60 %

av respondenterna använder eller överväger mobila autentiseringsuppgifter

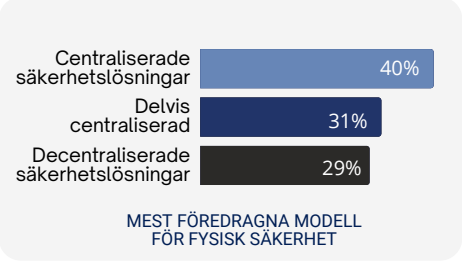
DE MEST VÄRDEFULLA FUNKTIONERNA OCH INTEGRERINGARNA I LÖSNINGAR FÖR FYSISK ÅTKOMSTKONTROLL

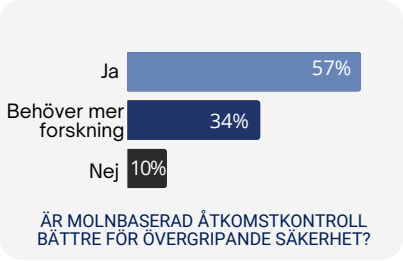
MOLNET ÄR NYCKELN TILL SÄKERHETSCENTRALISERING

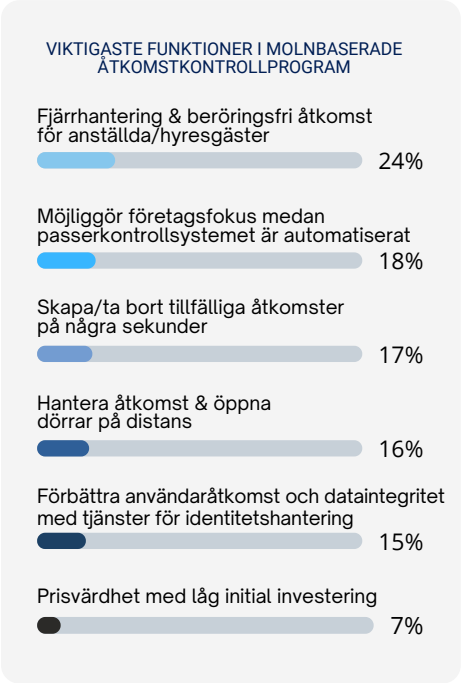
Molnet är viktigt för centraliserad säkerhet. När den digitala transformationen har fortsatt att modernisera alla aspekter av verksamheten har fördelarna med molnbaserad åtkomstkontroll blivit mer uppenbar, särskilt de lägre totala ägandekostnaderna för lösningen.

Dessutom möjliggör molnbaserade åtkomstlösningar enklare integration med andra molnapplikationer. Ökad enkel integration gör att lösningarna kan bli effektivare snabbare, från och med dag ett.

Som tidigare nämnts har 40 % av de tillfrågade centraliserat sina fysiska säkerhetssystem i molnet, upp från 35 % i förra årets undersökning. Och 57 % av de tillfrågade säger att molnbaserad åtkomstkontroll skulle förbättra deras säkerhet.







Undersökningen borrade också in era specifika aspekter av molnbaserad åtkomstkontroll. På frågan om vad som var de mest värdefulla delarna av en molnbaserad lösning för åtkomstkontroll, noterade respondenterna fjärrhantering och mobil/beröringsfri åtkomst för anställda och hyresgäster som toppval (23 %). Det näst mest värdefulla elementet (18 %) var förmågan för respondenterna att fokusera sin tid och ansträngning på sin verksamhet och överlåta drifttiden, mjukvaruuppdateringar och cybersäkerheten till sin molnbaserade leverantö. Det tredje mest värdefulla elementet som respondenterna citerade var förmågan att tilldela eller återkalla autentiseringsuppgifter och utfärda tillfällig åtkomst på sekunder (17 %).

Helt klart har fördelarna med molnbaserad åtkomstkontroll haft en verklig och materiell inverkan på säkerheten och fördelarna står i kontrast till lokala lösningar som inte kan hanteras på distans, leverera datainsikter eller ge effektivitetsförbättringar.

40 %

Har centraliserat sina fysiska säkerhetssystem i molnet

57 %

Tänker att molnbaserad åtkomstkontroll skulle förbättra deras säkerhet

DAGENS STÖRSTA UTMANINGAR

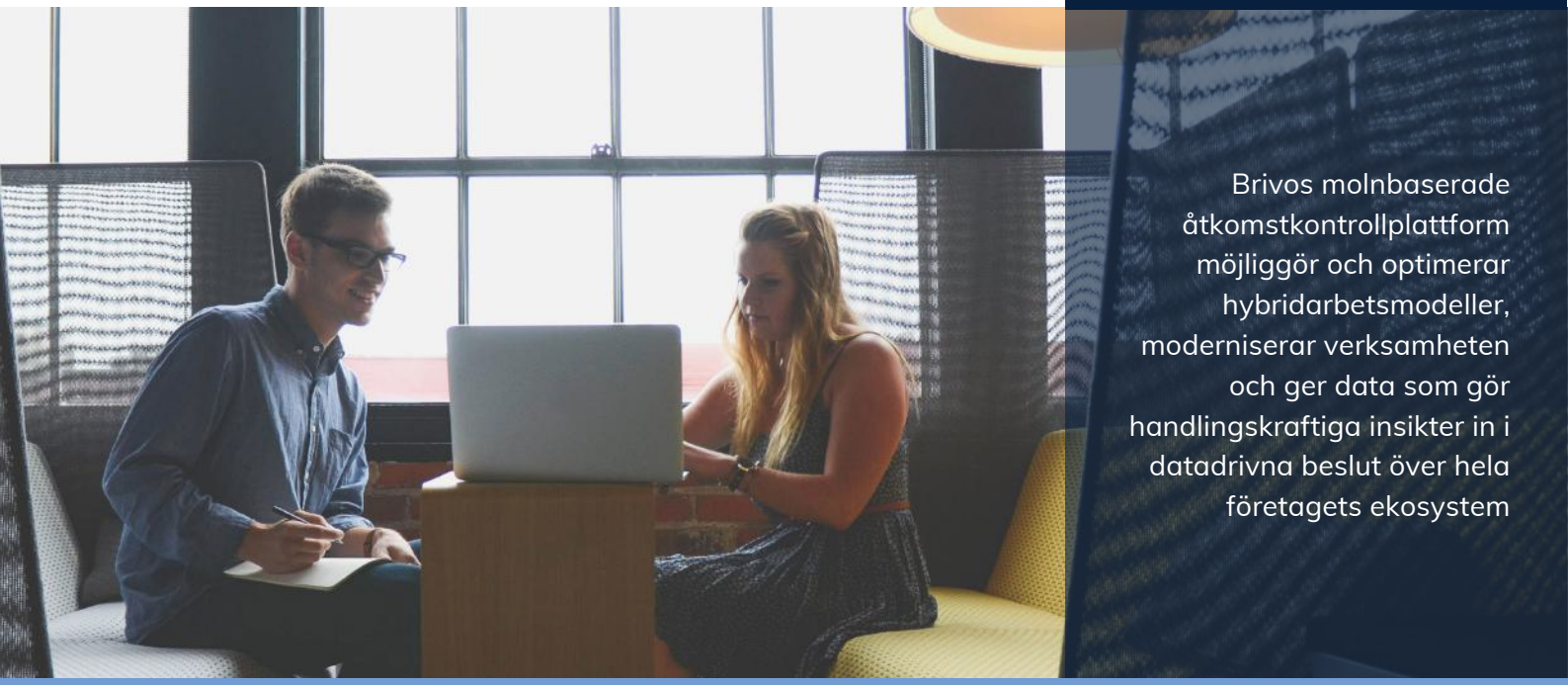
Undersökningspopulationen ombads välja sina tre vanligaste fysiska säkerhetsutmaningar. Respondenterna valde oftast fysiska säkerhetsintrång (39 %), chefsköp för säkerhetsprioriteringar (35 %) och personalbrist (32 %), vilket speglar förra årets största utmaningar. Nära efter de tre bästa finns förebyggande av förlust/stöld (29 %), personalutbildning (29 %) och efterlevnad (26 %).

Brivos säkerhetssvit, byggd på en robust, molnbaserad åtkomstkontrollplattform, möjliggör och optimerar hybridarbetsmodeller, moderniserar verksamheten och ger data som omvandlar handlingsbara insikter till datadrivna beslut i hela företagets ekosystem. Brivos signaturprodukt, Brivo Access, interagerar smidigt med Brivo-sviten av säkerhets- produkter, inklusive besökshantering, smart hemautomation, beläggningsövervakning och mobilhantering. Den erbjuder också en öppen API som integreras med ett oändligt antal funktioner och applikationer, inklusive identitetshantering, hisskontroll, co-working samt hälsa och välmående.

Brivo-system genererar en mängd data som organisationer kan utnyttja. För en bredare vy av branschdata och för att få tillgång till praktiska insikter, vänd dig till Brivo-rapporter, artiklar, undersökningar, blogginlägg och annat innehåll. För djupare analyser, gå till www.brivo.com för att lära dig mer.

DAGENS TUFFASTE UTMANINGAR INOM FYSISKT SÄKERHETSANSVAR

-Respondenterna valde upp till tre utmaningar-

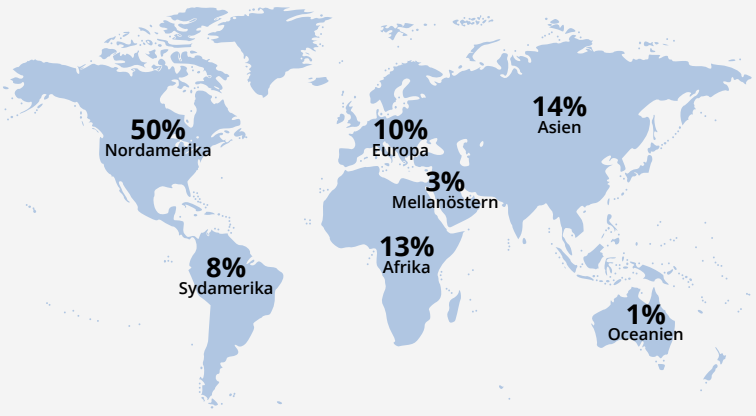


Brivos molnbaserade åtkomstkontrollplattform möjliggör och optimerar hybridarbetsmodeller, moderniserar verksamheten och ger data som gör handlingskraftiga insikter in i datadrivna beslut över hela företagets ekosystem

OM BRIVO

Simply Better Security

Geografisk fördelning av undersökningsrespondenterna



Brivo, Inc., skapade kategorin molnbaserad åtkomstkontroll och teknik för smarta utrymmen för över 20 år sedan och är fortfarande den globala ledaren för kommersiella fastigheter, flerfamiljsbostäder och stora distributionsföretag.

Företagets omfattande produktekosystem och öppna API förser företag med kraftfulla digitala verktyg för att öka säkerhetsautomatiseringen, höja anställdas och hyresgästers upplevelse och förbättra säkerheten för alla människor och tillgångar i samhället. Brivos plattform för åtkomst till byggnader är nu den digitala grunden för den största samlingen av kundanläggningar i världen, som upptar över 300 miljoner kvadratfot i 40 länder. Läs mer på www.brivo.com

Beräkna besparingar genom att flytta till molnet

beräkna din

Begär en konsultation

schemalägg det

Starta din säkerhetsuppgradering plan nu

uppgradera här

besök brivo.com

brivo
+31 20 88 80 980 | brivo.com

Copyright 2022 Brivo Systems LLC eller dess dotterbolag. Alla rättigheter förbehållna. Brivo och Brivo-logotyperna är registrerade varumärken eller varumärken som tillhör Brivo Systems LLC eller dess dotterbolag i USA och andra länder.Alla andra varumärken tillhör sina respektive ägare.