En guide till

Instant Privilege Access

Lär mer om Instant Privilege Access och vilka fördelar det ger i produktivitet och säkerhet

UPKEEPER

Innehållsförteckning

Instant Privilige Access

I detta whitepaper diskuterar vi en utmaning som många organisationer står inför; att behålla högsta säkerhet för sina klientdatorer samtidigt som man ger användare möjlighet att hantera sin dator själv.

Vi har funnit att medvetenheten om problemet är låg, och många organisationer har löst det genom att låta samtliga, eller allt för många, användare ha admin-rättigheter vilket öppnar för skadliga program och andra sårbarheter. Andra låser alla klientdatorer helt, vilket försämrar användarupplevelsen och belastar IT-supporten med rutinärenden.

Dagens lösningar, ofta kallade Privileged Access Management (“PAM”), kan vara komplexa och dyra att implementera, vilket hindrar IT-avdelningen och ledning från att ha kontroll.

Instant Priviliged Access (IPA) är en ny kategori av lösning som fokuserar på hantering av en användares egna admin-rättigheter på ett enkelt, kostnadseffektivt och säkert sätt.

Vi går igenom tekniska utmaningar med klientsäkerhet, scenarios och problem som behöver adresseras samt hur en IPA-lösning kan hantera detta.

Klientdatorer och deras användare är en av de största säkerhetsriskerna i ett IT system.

IT och datorsäkerhet är ett av de högst prioriterade områdena för alla företag och organisationer.

Användandet blir mer och mer personifierat, dvs. att man vill kunna anpassa sin programuppsättning och dator så att den passar just sitt arbetssätt och sin arbetsplats. Distansarbete ökar vilket gör att åtkomsten till användarnas datorer blir svårare.

Bolagen måste klara av dessa motsatta krav med en bra användarupplevelse och utan ökade kostnader för IT-supporten.

IPA

Instant Privilige Access (IPA) adresserar specifikt detta genom att ge användare rätt att själva göra förutbestämda förändringar utan fördröjning, även om förändringen tillfälligt kräver admin-rättigheter. Bolaget har kan styra vilka förändringar som är tillåtna och få full spårbarhet, utan att IT-avdelningen belastas.

Övergripande förståelse för klientdatorsäkerhet

Datorer som hanteras av en användare som är lokal-admin löper väsentligt större risk för intrång och skadlig kod och kräver mer underhåll, men har de mest nöjda användarna.

För att bättre förstå varför privilege access är viktigt i ett större säkerhetsperspektiv måste vi först förstå det aktuella hotet mot användarna av klientdatorer. Här kommer vi titta på de olika ytterligheterna när det kommer till hur klientdatorer är konfigurerade och anslutna samt visa deras olika för- och nackdelar sett ur ett säkerhetsperspektiv. Vi har även med produktivitet och användarnöjdhet.

I grafiken på nästa sida kan man se att de klientdatorer som inte är hanterade och nyttjas av lokala administratörer är de som är mest flexibla och när det fungerar så har de också en väldigt hög användarnöjdhet.

Studier visar också att datorer som kontinuerligt används av lokala administratörer löper mycket högre risk att infekteras av skadlig kod samtidigt som de över tid även kräver mer support och underhåll.

Scenario 1

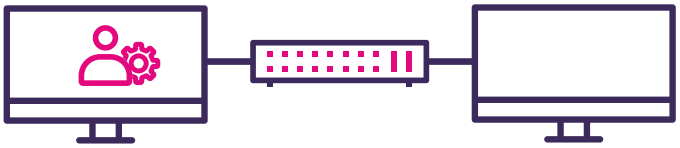
Forskning och styrning av enklare enheter

- Administratör, ej nätansluten
- Ingen extern access
- Hög säkerhetsnivå

Scenario 2

Datorer som hanterar andra enheter

- Administratör, slutet nät
- Begränsad exponering
- Hög säkerhetsnivå



Scenario 3

Kontorsdator som är vmanagerad

- Användare
- Hanterad och uppdaterad
- Medel säkerhetsnivå

Scenario 4

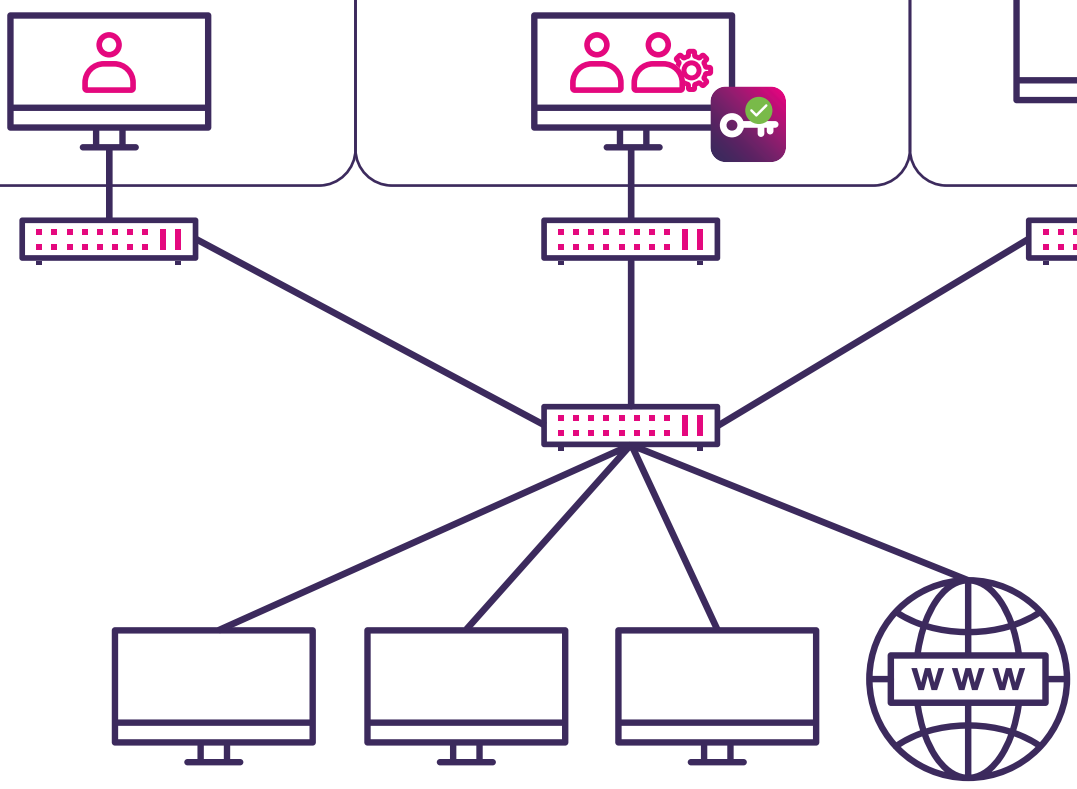
Kontorsdator som kan vara managerad

- Användare och admin vid behov
- Flexibel användning med kontroll
- Medel säkerhetsnivå

Scenario 5

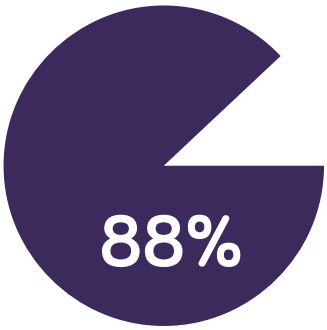
Hemmadator

- Administratör
- Flexibel användning
- Låg säkerhetsnivå



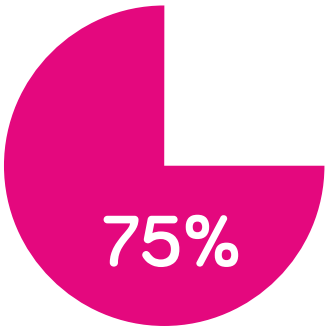
“I have multiple customers who have decreased the number of tickets to their service desk by a whopping 75% by getting rid of end-user admin rights.”

Sami Laiho, Windows OS & Security Expert, Senior Technical Fellow



Andel av tillfrågade organisationer som anser att insiderhot är en orsak till oro[1]

Antalet Microsoft-sårbarheter i kategorin “Elevation of Privilege” 2022 som nu står för mer än hälften av alla Microsoft-sårbarheter[2]



Andel av kritiska Microsoft-sårbarheter som kan mildras genom att ta bort admin-rättigheter[2]

1 ENISA Report Threat Lancscape 2020 | 2 Beyond Trust: Microsoft Vulnerabilities Report 2023

Att skapa helt säkra klientdatorer är inte omöjligt men är i de flesta fall kopplad till minskad produktivitet och användarnöjdhet.

Best Practice - ge användaren minsta möjliga rättighet

Best practice, ur ett säkerhetsperspektiv, säger att en användare skall ha så lite rättigheter som möjligt vid varje givet tillfälle. Men utan flexibilitet hämmas användarens produktivitet och användarupplevelse.

Vi är många som förespråkar att man alltid skall ge användare och applikationer så begränsade rättigheter som möjligt och bara till de resurser som skall nyttjas. Det innebär att användare och applikationer skall ha så låga rättigheter som möjligt till de resurser som de nyttjar i det kontinuerliga arbetsflödet.

Om en användare eller applikation från tid till annan har behov av utökade rättigheter till befintliga eller andra resurser så skall de enbart tilldelas tillfälligt och under kontrollerade former.

Att ge användare eller applikationer högre rättigheter eller tillgång till resurser som de ej har behov av skapar onödig risk både när det gäller säkerhet och misstag.

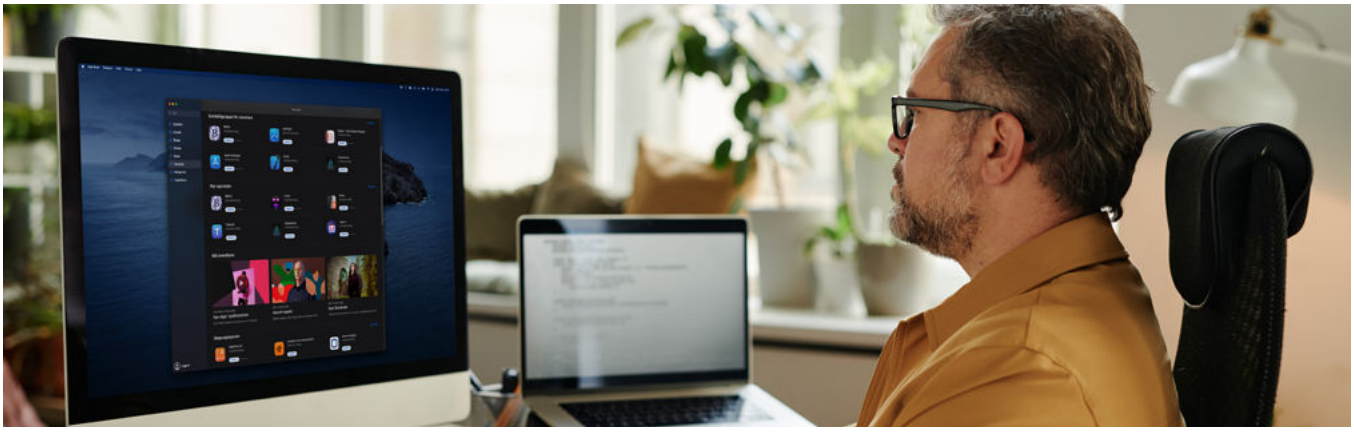
Erik - kunnig användare med för mycket rättigheter

Användare Erik har behov av några applikationer som bara han nyttjar och har tillgång till. Applikationerna är inte del av företagets standarduppsättning, men är viktiga för Eriks arbete. IT-avdelningen har inte kunskap om dessa och får inte heller notifieringar om uppdateringar etc.

För att det skall vara enkelt för Erik att underhålla applikationerna har man valt att låta Erik vara administratör på sin dator. Genom att Erik är administratör på

datorn kan han på egen hand underhålla applikationerna och IT-avdelningen behöver inte engageras.

Erik är kunnig. Men i och med att han är administratör innebär det även att han kan installera andra applikationer som han väljer själv, men också applikationer eller skript som han startar av misstag eller som levereras dolt via mejl eller webbsidor. Här börjar problemen.



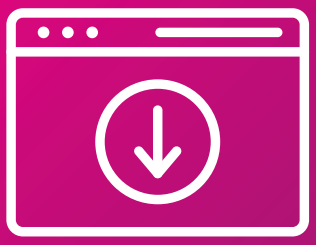
Att vara lokal administratör ger ökad frihet och flexibilitet för användaren men det skapar samtidigt en ökad exponering säkerhetsmässigt.

Exemplet ovan kan tyckas trivialt, men det är ett tydligt brott mot principen om minsta möjliga access och är alltför vanligt. För att ge användaren den flexibilitet som krävs låter alldeles för många organisationer alla eller många användare att ha förhöjda rättigheter permanent. Problemet är inte bara vad dessa användare kan göra, utan även det faktum att det inte finns spårbarhet på vad som installerats eller har hänt på datorn.

Att användaren inte är lokal administratör i det dagliga är det säkraste alternativet både för organisationen och den enskilda användaren. Är man lokal administratör i det dagliga arbetet så ökar risken för att man gör sin dator obrukbar. Av misstag eller via skadlig kod erhållen via mejl, webb eller andra yttre källor. Är man lokal administratör så ökar också risken att skadlig kod tar sig vidare in på andra enheter så som datorer, plattor, telefoner, servrar och funktioner som är kopplade till samma nätverk i organisationen.

Användarscenarios - vilka problem måste lösas?

För att vara effektiv måste en lösning som adresserar minsta möjliga rättighet kunna hantera flera olika aktiviteter, åtgärder och situationer. Det handlar både om vad användaren ska kunna göra, men också var eller i vilket användarscenario åtgärden ska kunna utföras.



Installation av applikation

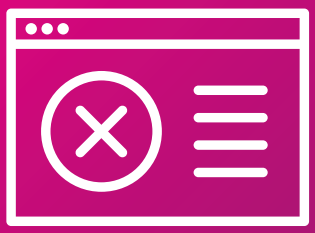
En användare som har behov av att installera en applikation som inte finns i organisationens hanterade applikationskatalog men är som är godkänd, måste i en managerad miljö vända sig till organisationens IT-funktion. De får i sin tur logga in lokalt eller på distans med förhöjda rättigheter för att installera applikationen. Detta kommer med en ledtid och användaren kommer behöva vänta på att få installationen genomförd. För personen från IT-funktionen som genomför förändringen kommer detta ta onödig tid då denna förmodligen inte kan själva applikationen och dess funktion, vilket kan skapa många frågor och i sämsta fall en obrukbar installation på grund av felkonfigurering.

Om användaren själv skulle kunna begära tillfälliga lokala administratörsrättigheter som är konfigurerade att endast godkänna installationen av den specifika applikationen från en specifik plats, så skulle installationen kunna genomföras på ett säkert sätt och eventuell konfigurering bli till användarens bästa.

Nätverksproblem

En användare som får problem med sin nätverkskonfiguration måste i en hanterad datormiljö alltid lämna datorn till organisationens IT-funktion som kan avhjälpa felet. Att lämna bort datorn bli ofta kostsamt både i produktionsbortfall och användarnöjdhet, men kan vara nödvändigt i vissa fall.

Om användaren skulle kunna begära lokala administratörsrättigheter och få guidning från IT-funktionen i organisationen så skulle man kunna minska produktionsbortfallet och frustrationen för användaren.



Felsökning

En användare som får problem med sin dator och kontaktar organisationens IT-funktion för hjälp har ofta inte rättighet att felsöka sin egen dator på den nivå som krävs. I vissa fall kan IT-avdelningen hjälpa remote, i andra fall inte.

Om användaren i det dagliga är en vanlig användare men kan begära tillfälliga lokala administratörsrättigheter som är fördefinierade av organisationens IT-funktion, så är riskerna för misstag och körning av skadlig kod minimal. Varje process som startas i administratörsläge måste bekräftas genom att användaren anger sina inloggningsuppgifter vilket kan vara användarnamn och lösenord, pinkod, ansiktsigenkänning eller någon annan inloggningsfunktion som bekräftar användaren. När användaren erhållit lokala administratörsrättigheter så kan denne på egen hand, eller med guidning av organisationens IT-funktion, felsöka datorn och förhoppningsvis lösa det uppkomna problemet.

Vad är Privilege Access Management?

PAM adresserar ofta problemet som sådant men inte alla användarscenarios. PAM-lösningar täcker också många andra aspekter vilket gör implementering och användande komplex och lösningarna blir dyra.

Privilege Access Management handlar om att man kan kontrollera och monitorera utökade rättigheter när det gäller användare, konton, processer, applikationer och system i hela IT-miljön. Syftet med Privilege Access Management är att man skall minska exponeringen rent säkerhetsmässigt för användaren och organisationen, men också följa händelserna så att det enbart nyttjas enligt vad man bestämt.

Att implementera Privilege Access Management system är i de allra flesta fall komplext, tidskrävande och dyrt. Det kan krävas månader av planering i en större organisation där många blir involverade för att förstå exakt vad som behöver hanteras under implementeringen. Då system ofta är omfattande och för den oinvigde relativt komplexa, krävs det ofta externa resurser som först måste sätta sig in i verksamheten innan de kan hjälpa till med det strategiska arbetet och sedan själva implementationen. Detta innebär att det inte bara är själva systemet som många gånger är dyrt utan det resulterar även i höga konsultkostnader som ofta överstiger själva systemkostnaden med råge.

I många fall nyttjas system i första hand för att tilldela och kontrollera förhöja rättigheter för användare och speciella konton. I dessa fall begär användaren förhöjda rättigheter för att kunna genomföra någon typ av förändring som kräver detta. Begäran hanteras sedan manuellt av personer eller automatiskt via ett fördefinierat regelverk.

Introduktion till Instant Privilege Access

Instant Privilige Access (“IPA”) adresserar specifikt behovet av att när det behövs kunna ge en användare temporärt förhöjda rättigheter på ett säkert, kontrollerat och automatiserat sätt. Då IPA fokuserar på just detta blir det en lösning som är enklare och mer kostnadseffektiv att implementera jämfört med exempelvis en PAM lösning.

Instant Privilege Access är en funktion där användare direkt efter begäran kan ges förhöjda rättigheter till en specifik enhet utifrån ett fördefinierat regelverk. När användaren fått rättigheterna kan de utföra åtgärder på enheten utifrån regelverket och allt som utförs loggas. Den förhöjda rättigheten återställs inom en definierad period. Processen kräver inte inblandning från t.ex. IT- avdelningen.

Instant Privilege Access är en delfunktion av Privilege Access Management där man fokuserar på säkerhet, enkelhet och användarnöjdhet. Funktionen skall kunna aktiveras oavsett var man befinner sig dvs. det skall fungera om man är på kontoret, i hemmet eller på resande fot. Den ska också fungera med eller utan access till lokalt nätverk eller internet. Förutom att man kan begära access oavsett vart man befinner sig så skall funktionen ge användaren direkt återkoppling huruvida man erhållit eller nekats access.

Detta innebär att en användare som begär rättigheter kommer få behörighet direkt utifrån det förbestämda regelverket och därmed kunna genomföra vad man har rätt till. Den direkta accessen främjar produktiviteten där användaren omgående kan genomföra den önskade uppgiften utan inblandning av andra resurser. När användaren genomfört sina ändringar så återkallas den förhöjda rättigheten och användaren för åter sina normala rättigheter.

Allt som användaren startar med sina förhöjda rättigheter skall bekräftas med någon form av validering, vilket kan vara användarnamn och lösenord, pinkod, ansiktsigenkänning eller någon annan inloggningsfunktion som bekräftar användaren. Det som genomförs med förhöjda rättigheter skall loggas separat så att åtgärderna kan övervakas och analyseras. Analys och förändrade behov kan leda till justerade rättigheter för enskilda användare eller hela organisationen och skall ske omedelbart vid förändring.

Med Instant Privilege Access så minskar man exponeringen rent säkerhetsmässigt då användaren aktivt måste starta förändringen och godkänna den genom att ange inloggningsinformation. Det faktum att användaren har förhöjda rättigheter under en begränsad tid ger också en minskad exponering.

upKeeper Instant Privilege Access

upKeeper IPA gör att en organisation kan ge utvalda användare eller grupper förutbestämda förhöjda rättigheter med full kontroll och spårbarhet som beskrivs ovan. Lösningen är lika enkel att implementera som en vanlig applikation och kräver inga förändringar av processer eller policys.

upKeeper Instant Privilege Access är en implementation av Instant Privilege Access där vi tagit fasta på kärnvärdena och fokuserat på säkerheten och användarbarheten. Med upKeeper Instant Privilege Access ger man användarna möjlighet att enkelt begära förhöjda rättigheter enligt ett fördefinerat regelverk som fungerar oavsett var användaren befinner sig och oberoende av uppkoppling eller inte.

När man som användare fått förhöjda rättigheter kan man genomföra godkända uppgifter som till exempel att installera en applikation eller ändra

ett registervärde. När man genomfört uppgiften så återkallas rättigheterna och användaren kan därmed inte genomföra fler förändringar med förhöjda rättigheter. Användaren kan åter begära förhöjda rättigheter om behovet skulle uppstå. Allt som användaren genomför med förhöjda rättigheter kommer loggas så att man kan följa det direkt eller analysera i efterhand.

Förutom de fördelar som upKeeper Instant Privilege Access ger ur ett säkerhetsperspektiv så finns det andra fördelar för både användarna och IT-supporten vilket gagnar hela organisationen.

För IT-supporten så ger funktionen en bättre kontroll och möjlighet till uppföljning. Man kan ge olika användargrupper eller enskilda användare olika möjligheter till förändringar baserat på behov. När behoven förändras kan man med enkelhet justera möjligheterna för användargruppen eller den enskilda användaren.

För användarna så ger funktionen möjligheten att kunna genomföra förändringar när de behöver dem, oavsett var de befinner sig. Funktionen aktiveras av användaren som också behöver verifiera sina inloggningsuppgifter via aktiverad inloggningsfunktion vilket kan vara lösenord, kort, pin kod, fingeravtryck eller ansiktsigenkänning. Detta förfarande gör att användaren kan känna sig säker på att det är bara funktioner den aktivt startar som körs med förhöjda rättigheter.

För organisationen ger funktionen en minskad belastning på IT-supporten som kan ta sig an andra uppgifter och användarna kan göra mer när det passar dem. Över tid kommer man se att produktiviteten ökar, vilket kan kopplas till nöjdare medarbetare inom IT-supporten och användargruppen som blir mer flexibla och tryggare.

1. Användaren begär admin-rättigheter genom upKeeper IPA

2. IPA ger användren rättigheter enligt fördefinierad policy

3. Användaren gör ändringar och tasks som loggas av IPA

4. Admin-rättigheterna löper ut efter en fördefinierad tid eller antal åtgärder

5. Användaren har inte längre admin-rättigheter

Att implememententera upKeeper Instant Privlege Access

Att rulla ut traditionella Privilege Access Management (PAM) system kan vara tids- och resurskrävande i större organisationer då de kräver noggrann planering och omfattande konfigurering.

Att rulla ut upKeeper Instant Privilege Access går lika snabbt och enkelt som att installera en vanlig applikation.

1. Skapa ett användarkonto i portalen för upKeeper Instant Privilege Access.
2. Skapa en initial konfiguration av vem som skall ha vilka rättigheter.
3. Ladda ner klientapplikationen.
4. Rulla ut klienten via ett klienthanteringssystem så som upKeeper Manager, Microsoft Intune, Microsoft System Center Configuration Manager eller liknade.
5. Följ upp användning och gör nödvändig justering.

Införandeprocessen är enkel och tar oftast ett par timmar från registrering till utrullning men uppdatering eller skapande av säkerhetspolicy kan ta längre tid beroende på organisation.

Vill du veta mer?

Vill du veta mer om upKeeper Instant Privilige Access?

Mer information

Kontakta mig

Om oss

upKeeper är skapat för IT-tjänsteleverantörer och organisationer med en egen IT-funktion. Sedan 2008 har vi levererat system för klienthantering och även specifika lösningar inom garanterad återställning, hantering av admin-rättigheter och energibesparing för datorer. Vi ger användarna mer frihet och ökad produktivitet samtidigt som ni behåller kontrollen och får möjligheten att snabbt komma tillbaka efter en attack. Fler än 100 000 klienter hanteras idag av våra lösningar.

upKeeper Solutions AB
Tvistevägen 48
907 36 Umeå
www.upkeeper.se
Växel 090-349 33 90