White Paper

# Säkra slutpunkter – ett kritiskt verksamhetsmål

Sponsrad av: Apple

Tom Mainelli Michael Suby
September 2023

## OPINIONSARTIKEL AV IDC

Vad är det som håller IT-beslutsfattare vakna om nätterna? Säkerhet. Det är för att smarta IT-beslutsfattare vet att hela företaget kan äventyras genast om det uppstår fel med säkerheten, oavsett hur välskött företaget är eller hur populär dess produkt eller tjänst är.

Och världen blir tyvärr inte säkrare. Företagsspionage, skurkstater, organiserad brottslighet och till och med vanliga tjuvar har uppgraderat sig när det gäller teknik. För att ligga steget före illasinnade aktörer måste IT-avdelningen hålla ögonen öppna och alltid vara villiga att anamma nya leverantörer och tekniker för att skydda sina anställda, kunder och data.

Listan över säkerhetsutmaningar som IT-avdelningen står inför är lång och omfattar allt från slutpunkter (datorer) till datacenter, nätverken som ansluter allt och programvaran som kör allt. I den här artikeln fokuserar vi på vikten av att säkra slutpunkten. Säkerheten i de andra domänerna spelar trots allt inte så stor roll om slutpunkten inte är säker.

En av de viktigaste utmaningarna med att säkra slutpunkten är att en säker slutpunkt traditionellt sett innebär kompromisser för slutanvändarens upplevelse, med låsta enheter som är svåra att använda. Och då hittar den andra primära svagheten i alla säkerhetssystem – användaren – ofta sätt att kringgå säkerheten för att få jobbet gjort. När säkerheten blir en friktionspunkt för användarna tjänar den inte längre sitt syfte.

Tekniska framsteg har i allt större utsträckning gjort det möjligt att bibehålla både en högkvalitativ användarupplevelse och säkerhet. Framsteg inom identifiering av skadlig programvara, dataskydd, autentisering och sammansmältningen mellan maskinvara och programvara innebär att dagens slutpunkter inte behöver offra produktivitet för ökad säkerhet.

## METOD

IDC genomförde en onlineundersökning av IT-beslutsfattare i USA och Kanada (n = 513) i juli 2023 och frågade om deras synpunkter om säkerhet i stort och vikten av att säkra datorslutpunkter specifikt. Respondenterna representerar ett antal företag med 500 eller fler anställda från en rad olika branscher. Dessa IT-beslutsfattare stöder olika operativsystem, bland annat Microsoft Windows, Apple macOS och Google ChromeOS. De antingen väljer, köper eller driftsätter säkerhetsprogram för sitt företag eller är chef för personerna som gör det.

## LÄGESÖVERSIKT

Säkerhet är en kritisk fråga för ledningen. Framåtsträvande företag förstår att bra säkerhet inte är något som är ”bra att ha”, utan snarare ett krav för ett sunt och blomstrande företag som bedriver sin verksamhet i ett hotlandskap som ständigt förändras och drivs av koordinerade illasinnade aktörer med gott om pengar.

Över 50 % av företag världen över har upplevt en ransomware-attack som störde verksamheten under de senaste 12 månaderna, enligt IDC:s undersökning Future Enterprise Resiliency and Spending (FERS) från mars 2023 av IT-beslutsfattare i företag med 500 eller fler anställda. Över en tredjedel av den gruppen sa att attacken störde verksamheten i en vecka eller mer. Trots att större företag utan tvekan har mer robusta säkerhetsprotokoll är de långt ifrån immuna mot sådana attacker. Faktum är att den högsta procentandelen av störningar som orsakats av ransomware påverkade företag i kategorierna 1 000–2 499 anställda (71 %), 2 500–4 999 anställda (72 %) och 5 000–9 999 anställda (70 %). Med andra ord är inget företag immunt mot sådana attacker, oavsett hur stort det är.

Samma undersökning pekar ut slutpunkter som den huvudsakliga startpunkten för ransomware-attacker. De första angreppspunkterna är surf på webben (21 %), flyttbara medier (18 %), e-postbilaga (17 %), leveranskedja (17 %), webbadress i ett e-postmeddelande (14 %) och insideråtkomst (8 %).

Den ihållande övergången till fler anställda som arbetar under hybrid- och distansformer har gjort ransomware och andra säkerhetsrisker allt svårare för IT-avdelningen att hantera. I IDC:s undersökning om slutpunktssäkerhet från december 2022 framkom det att i över 97 % av organisationerna arbetar en del av de anställda på distans. Även om denna siffra förväntas minska något under de kommande tolv månaderna kommer den att förbli mycket hög under överskådlig framtid.

I och med att företag brottas med de ihållande utmaningarna som ingår i en stor distansarbetsstyrka så är det fler som implementerar nollförtroendestrategier. Fokusområden för bästa metoder omfattar att upprätta en grund av säkerhetskontroller, avancerat skydd för slutpunktssäkerhet, enhetsattestering (för att säkerställa att enheter som ansluter till nätverket är legitima) och kraftfull användarautentisering.

När man tar med allt ovan i beräkningarna är det inte förvånande att den stora majoriteten av respondenterna i vår undersökning valde övergripande förbättring av datasäkerhet och att säkerställa att datorer är säkra som sina främsta IT-prioriteringar, vilket återspeglas i bild 1.

Det är värt att påpeka att i bilden nedan var den tredje viktigaste frågan för IT-avdelningen att förbättra de anställdas produktivitet med hjälp av bättre enheter. När vi bad respondenterna att välja de tre viktigaste frågorna valdes alternativet om bättre enheter oftast. Det ger IT-avdelningen ett klart och tydligt budskap: Säkerheten är viktig, men det får inte vara på bekostnad av medarbetarnas produktivitet, och de bästa enheterna kombinerar hög säkerhet med nöjda slutanvändare vars arbete inte hindras av säkerheten.

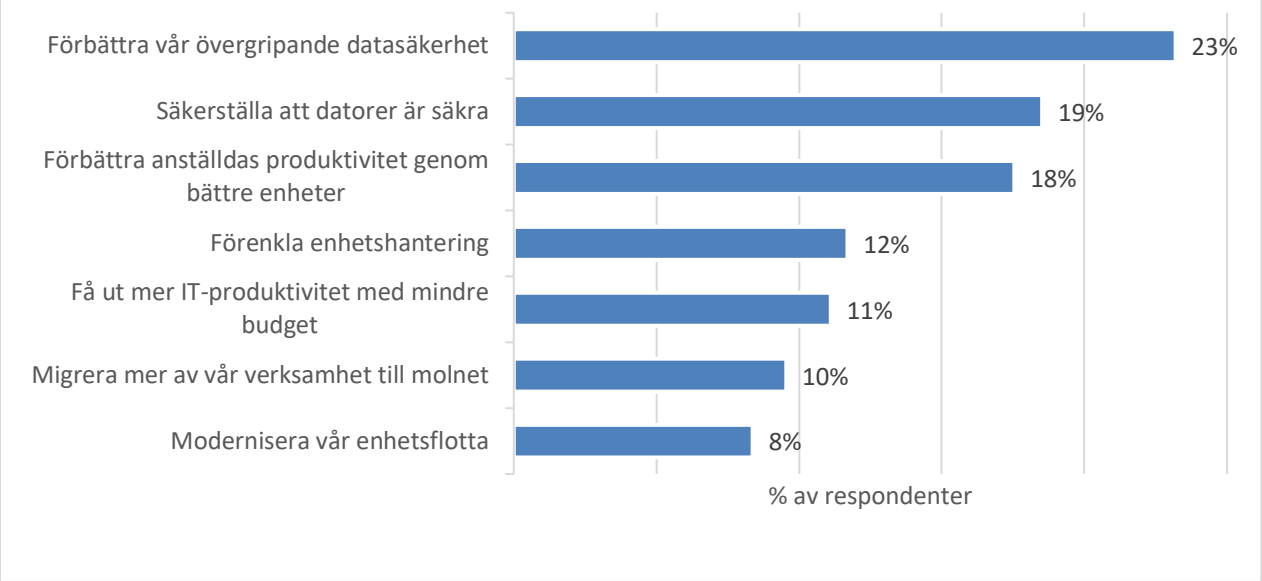
När vi frågade IT-beslutsfattare vad deras främsta beslutsfaktor är när det gäller deras nästa datorleverantör så hamnade säkerhet på första plats, före prestanda, stöd för befintliga program och integration med befintlig IT-infrastruktur. Det kanske mest anmärkningsvärda är att alternativet om specifikationer hamnade nästan längst ner.

Se bild 1 för IT-avdelningens främsta prioriteringar. Se bild 2 för det viktigaste att ha i åtanke vid val av datorleverantör.

## BILD 1

### Det viktigaste för IT-avdelningen: Data- och slutpunktssäkerhet

*Fråga: Vilka av följande IT-frågor är viktiga prioriteringar för ditt företag idag?*



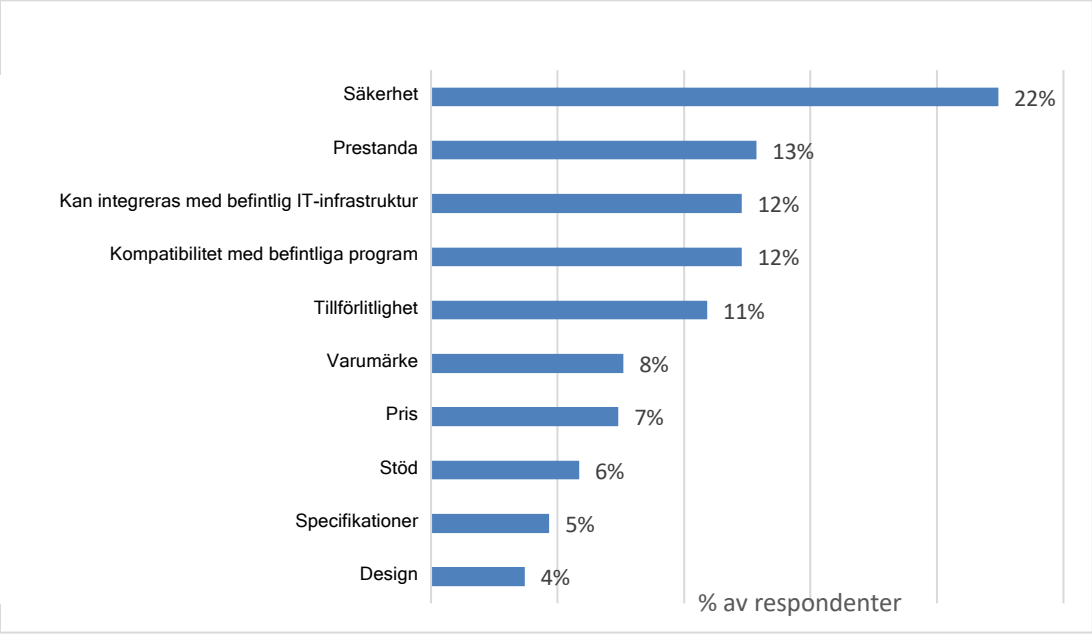

Källa: IDC:s undersökning om säkra slutpunkter, n = 513

Observera: Data omfattar de som rankas högst upp på listan (nr 1-rankning)

## BILD 2

### De viktigaste faktorerna vid val av datorleverantör

*Fråga: Vilka är de viktigaste avgörande faktorerna när du väljer en dator för ditt företag?*




Källa: IDC:s undersökning om säkra slutpunkter, n = 513

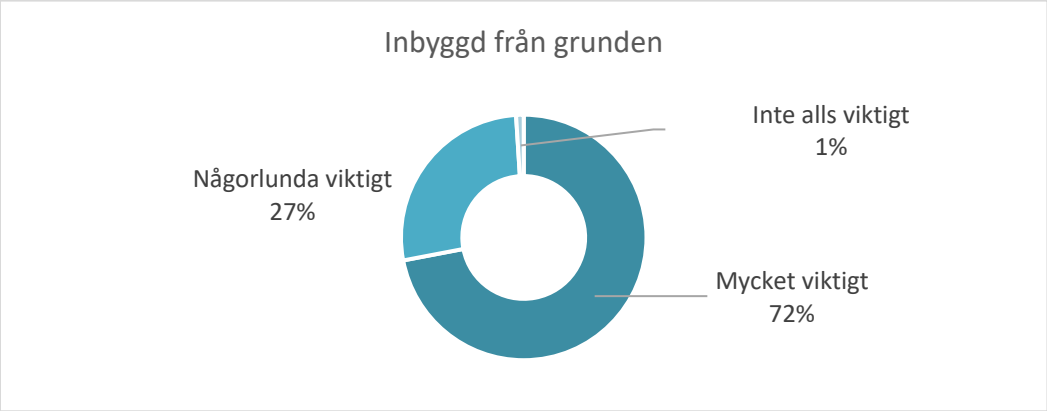
Observera: Data omfattar de som rankas högst upp på listan (nr 1-rankning)

Två koncept som tilltalade respondenterna i hög grad var inbyggd säkerhet och integrerat dataskydd. På frågan ”Hur viktigt anser du att det är att ha inbyggd säkerhet i en dator från grunden – inklusive maskinvaran, den inbyggda programvaran och operativsystemet – för att skydda den från dagens och morgondagens hot?” var responsen överväldigande positiv – 72 % sa att det var mycket viktigt, och 27 % sa att det var någorlunda viktigt. Bara 1 % sa att det inte var viktigt alls. Vid närmare anblick är det viktigt att notera att bland IT-beslutsfattare på organisationer inom hälso- och sjukvård och ekonomi var procentandelen som sa att det var mycket viktigt ännu högre (84 % respektive 75 %). Konceptet integrerat dataskydd hamnade också högt upp. Vi frågade ”Hur viktigt anser du att det är att ha datakrypteringsfunktioner integrerade i datorns maskinvara?” 71 % sa att det var mycket viktigt, 29 % sa att det var någorlunda viktigt och 0 % sa att det var oviktigt.  Mer information om inbyggd säkerhet och integrerad datakryptering finns i bild 3.

## BILD 3

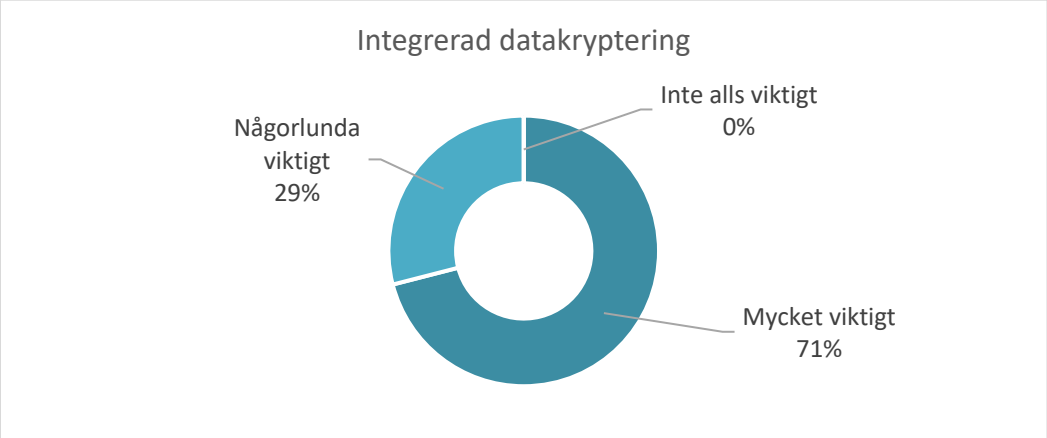
### Vikten av inbyggd säkerhet och integrerad datakryptering

*Fråga: "Hur viktigt anser du att det är att ha inbyggd säkerhet i en dator från grunden - inklusive maskinvaran, den inbyggda programvaran och operativsystemet - för att skydda den från dagens och morgondagens hot?"*




Källa: IDC:s undersökning om säkra slutpunkter, n = 513

*Fråga: "Hur viktigt anser du att det är att ha datakrypteringsfunktioner integrerade i datorns maskinvara?"*




Källa: IDC:s undersökning om säkra slutpunkter, n = 513

Maskinvara med inbyggd säkerhet från grunden är viktigt och integrerad datakryptering är ett avgörande krav, men säkerhetsexperter vet att den svagaste länken i en säkerhetskedja vanligtvis är slutanvändarna själva. Därför är användarautentisering så viktigt, och det är även anledningen till att teknikleverantörer har arbetat hårt för att utveckla autentisering som funktion. Tyvärr är det här ett område där vår undersökning visar att många organisationer har hamnat på efterkälken.

De goda nyheterna är att 68 % av de tillfrågade sa att deras företag kräver komplexa lösenord, och 63 % sa att de använder tvåfaktorsautentisering. De dåliga nyheterna är att endast 23 % använder teknik för enkel inloggning (SSO), och endast 20 % använder biometrisk säkerhet (t.ex. finger- eller ansiktsidentifiering). Det är värt att notera att bland våra respondenter sa 56 % att biometrisk autentisering var mycket säkrare än lösenord, 35 % sa att den var lite säkrare, 9 % sa att den var lika säker och ingen (0 %) sa att den var mindre säker.

En framträdande autentiseringsteknik som har lanserats nyligen är inloggningsnycklar. En inloggningsnyckel är en form av digital autentisering där ett par uppsättningar information används för att ge en mycket säkrare lösning än ett lösenord. Eftersom den här tekniken är ny sa bara 14 % att deras företag använder den, men smarta IT-beslutsfattare bör titta närmare på tekniken redan i dag. Mer information om användning av användarautentisering finns i bild 4.

## BILD 4

### Metoder för användarautentisering

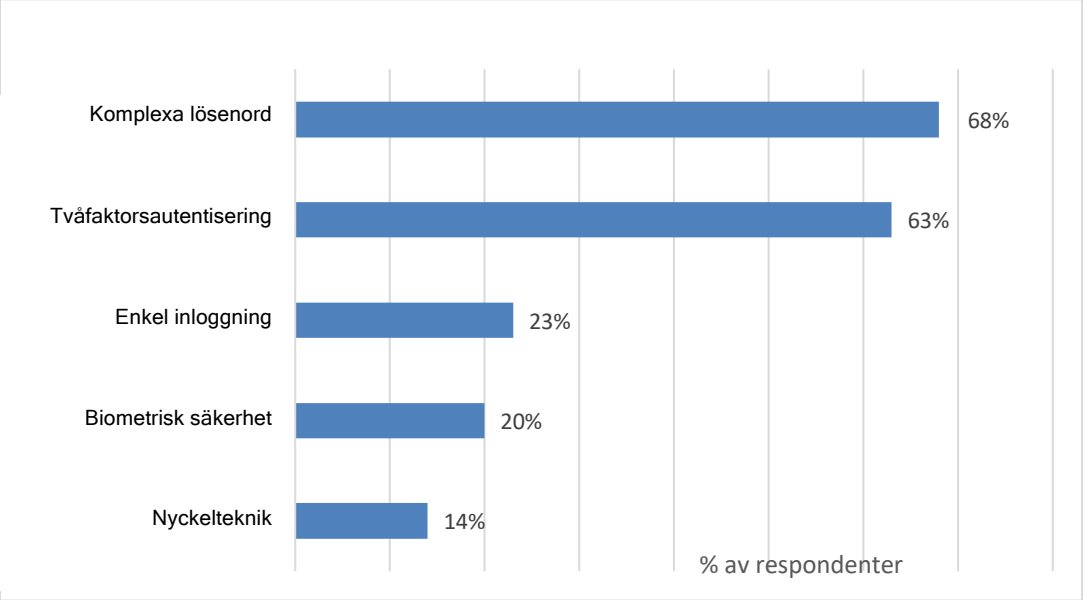
*Fråga 1. Kräver ditt företag att anställda använder komplexa lösenord för att logga in på sin dator?*

*Fråga 2. Driftsätter ditt företag datorer med stöd för biometriska säkerhetsåtgärder, t.ex. fingerskanning?*

*Fråga 3. Har ditt företag börjat undersöka fördelarna med att använda nyckelteknik?*

*Fråga 4. Kräver ditt företag tvåfaktorsautentisering?*

*Fråga 5. Använder ditt företag funktioner för enkel inloggning (SSO)? (J/N)*




Källa: IDC:s undersökning om säkra slutpunkter, n = 513

Data anger procentandel som säger ”ja”

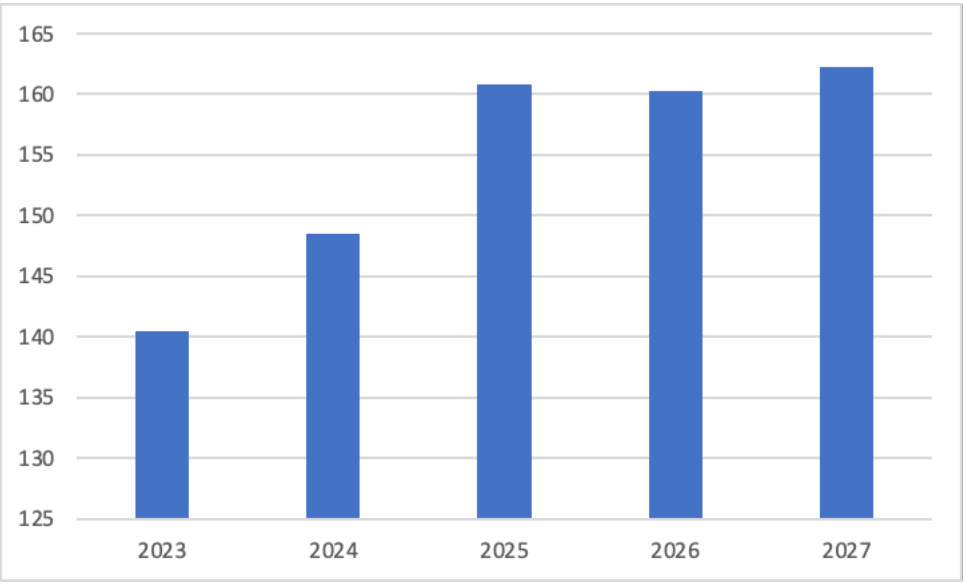
En chockerande hög procentandel av respondenterna har inte ens implementerat grundläggande autentiseringsprotokoll i form av komplexa lösenord (32 %) eller tvåfaktorsautentisering (37 %). **En eftersträvansvärd bästa metod** är att implementera en konsekvent autentiseringsform i hela organisationen. När du har etablerat den här grunden kan du börja överväga SSO-funktioner i kombination med ett starkt huvudprotokoll för autentisering. Efter nästa maskinvaruuppdatering kan du slutligen titta närmare på datorer som kan stödja de högsta autentiseringsnivåerna: biometrisk säkerhet och nyckelteknik.  Aktivering av biometri och inloggningsnycklar innebär en framtid där

anställda snabbt och säkert kan logga in på sina datorer och därifrån omedelbart till sina appar och webbplatser.

Det är där, vid nästa maskinvaruuppdatering, som vi avslutar det här avsnittet. Många företag har en uppsättning av gamla datorer som behöver bytas ut. Även om din organisation köpte ett stort antal nya slutpunkter så sent som 2020 är dessa datorer snart fyra år gamla. Under den tiden har maskinvarusäkerheten fortsatt att utvecklas för att hålla jämna steg med hoten. Kanske lika viktigt är att de flesta av dessa produkter levererades före den utbredda övergången till distans- och hybridarbete, vilket innebär att många saknar kameror, mikrofoner och högtalare av hög kvalitet som krävs för att anställda ska kunna använda de program för onlinemöten och samarbete som nu har blivit väsentliga. IDC:s Personal Computing Device Tracker förutspår nu tillväxt inom denna kategori de kommande åren, efter flera år av avtagande leveranser. Observera: Kommersiella enheter avser enheter som köps av icke-konsumentenheter. För IDC:s prognos för konsumentdatorer/kommersiella datorer, se bild 5.

## BILD 5

### Global prognos för kommersiella datorer




Källa: IDC PCD Tracker, augusti 2023

Företag bör kontinuerligt utvärdera sina anställdas datorbehov för att förbli konkurrenskraftiga på marknaden och attrahera och behålla topptalanger. En gång i tiden var IT-avdelningen tvungen att göra svåra avvägningar mellan säkerhet och användarupplevelsen, men nu kan rätt leverantör hjälpa till med att hitta en lösning utan kompromisser. Slutligen är **en annan bästa metod att ha i åtanke** att tillämpa åtkomstprinciper med nollförtroende för nästa maskinvarudriftsättning. Den här strategin förutsätter att när en enhet försöker komma åt en företagsresurs ska den inte vara betrodd förrän den har verifierats. Inom nollförtroende används tekniker och processer för att intyga enhetens säkerhetstillstånd (helst ända från maskinvaran och upp till kritiska IT- och säkerhetsprogram), anslutande nätverk (t.ex. offentligt wifi kontra privat nätverk) och användaridentitet.

## Att överväga Mac i företaget

Fler IT-avdelningar stöder Mac-datorer idag, och i vår undersökning hittade vi en viktig anledning till det. Av respondenterna, som har flera olika operativsystem i sin datorbas, uppgav 76 % att de tror att Mac är säkrare än andra datorer. Uppfattningen om att Mac-datorer är säkrare (47 %) var den främsta anledningen till att skaffa fler under de kommande 12 månaderna, tätt åtföljt av enkelhet i driftsättning och hantering (36 %).

Apple fokuserar på att ge en fantastisk användarupplevelse samtidigt som de höjer säkerheten genom att bygga in säkerhet i både chippen och programvaran. Ett exempel på detta är Apples Touch ID, en inbyggd biometrisk säkerhetsfunktion. Apple-chippen har Secure Enclave som krypterar och skyddar lösenkoden som används för att skydda Touch ID-data.

**Apple-kundfokus**

”En av de viktigaste funktionerna i Apples produkter är att integritet och säkerhet faktiskt är inbyggt i själva produkten. Det är inte bara ett tillägg i efterhand, och det uppskattar vi väldigt mycket.” – Linda Jojo, Vice VD och kundchef, United Airlines

Mac-datorer är utrustade med säker start och signerad systemvolym för att hantera riskerna med komprometterade operativsystem och startsekvenser. Säker start säkerställer att endast den kryptografiskt certifierade versionen av macOS körs igång vid uppstart, och signerad systemvolym skyddar operativsystemets integritet under körning. Föråldrad programvara utgör också en cyberrisk som Apple minimerar genom att automatisera och skydda den heltäckande distributionen och installationen av programvaruuppdateringar.

Bra programvara från tredje part är avgörande för medarbetarnas produktivitet, men den programvaran måste också vara fri från skadlig kod. Apple har en mångbottnad metod för att förhindra skadlig kod. Apples App Store i Mac skannar varje app efter skadlig kod. Eftersom programvara på Mac-datorer också kan hämtas från webben kräver Apple att utvecklarna skickar in sina program till Apples notarietjänst, som även skannar efter skadlig kod. Apples Gatekeeper, som ingår i macOS, kontrollerar avseende notarisering och förhindrar att en osignerad app körs. XProtect – Apples verktyg mot skadlig kod – blockerar och raderar dessutom all känd skadlig programvara.

Data är en av organisationens mest värdefulla tillgångar och måste därför skyddas. Kombinationen av maskinvarubaserad FileVault-kryptering, Apple-stödda VPN-protokoll och heltäckande kryptering i Apple-tjänster (t.ex. iMessage och iCloud) säkerställer att data skyddas vid vila, under transport och under användning.

Social manipulation är ett annat verktyg i hotaktörernas välfyllda verktygslåda som slutanvändare behöver vara uppmärksamma på och försvara sig mot. Det är ett stort ansvar, men Apple kan hjälpa till med Safaris varningar för bedrägliga webbplatser. Apples stöd för inloggningsnycklar underlättar företagens modernisering av autentiseringsmetoder – just inloggningsuppgifter är något som hotaktörer ofta stjäl – utan att offra en bra upplevelse för slutanvändaren.

God säkerhet hänger ihop med stabil enhetshantering. Apple erbjuder därför en rad olika funktioner för enhetshantering, inklusive inbyggda hanteringsramverk med hantering av mobila enheter (MDM, mobile device management). Apple Business Manager erbjuder beröringsfri driftsättning och länkar till MDM-lösningar, medan API:er för slutpunktssäkerhet för Mac gör det möjligt för utvecklare att skapa lösningar för att övervaka, analysera och reagera på säkerhetshot. Apple erbjuder även identitetsintegreringar med ett inbyggt ramverk för enkel inloggning som fungerar med moderna identitetsleverantörer.

Slutligen tillhandahåller Apple dessa säkerhetsfunktioner, inklusive både stora och små programvaruuppdateringar, med macOS utan extra kostnad för företagskunder och konsumenter.

## UTMANINGAR/MÖJLIGHETER

Trots en hotmiljö som ständigt utvecklas pressas IT-avdelningen att göra mer med mindre: mindre pengar, mindre IT-personal och färre resurser. Förutom att hantera de pågående säkerhetsriskerna som alla företag står inför har många IT-organisationer även fått i uppdrag att på ett mätbart sätt förbättra anställdas produktivitet och upplevelse genom maskinvaran, programvaran och tjänsterna de driftsätter. Att lyckas med båda uppgifterna – att förbättra säkerheten och medarbetarnas produktivitet och upplevelse – kan verka omöjligt. Men det är också en viktig möjlighet för IT. Det är en möjlighet att utvärdera maskinvaran, programvaran och tjänsterna de köper, leverantörerna som de köper från och hur de distribueras till en allt mer hybrid arbetsstyrka. Det är dessutom dags att räkna om på modeller för total ägandekostnad (TCO) för att bättre återspegla hur företag köper och använder teknik idag.

## SLUTSATS

Säkerhet är och kommer att fortsätta att vara en huvudfråga för IT-avdelningen. I en tid av begränsade IT-budgetar och större maskinvaruuppdateringar i antågande är det klokt att utvärdera vilka leverantörer du ska lägga dina pengar på framöver. Överväg att implementera bästa praxis kring autentisering och beröringsfri driftsättning, och köp maskinvara som gör dessa övergångar möjliga. Prioritera inte säkerheten framför produktivitet och användarupplevelsen när det finns leverantörer som erbjuder datorer med inbyggd säkerhet och datakryptering som tillhandahåller både säkerhet och en positiv upplevelse för slutanvändarna.

## Om IDC

International Data Corporation (IDC) är den främsta globala leverantören av marknadsinformation, rådgivningstjänster och evenemang för marknaderna för informationsteknik, telekommunikation och konsumentteknik. IDC hjälper IT-proffs, företagsledare och investeringsgrupper att fatta faktabaserade beslut om teknikinköp och affärsstrategier. Fler än 1 100 IDC-analytiker tillhandahåller global, regional och lokal expertis om teknik- och branschmöjligheter och trender i över 110 länder världen över. I 50 år har IDC tillhandahållit strategiska insikter som hjälper våra kunder att uppnå sina viktigaste affärsmål. IDC är ett dotterbolag till IDG, världens ledande företag inom media, forskning och evenemang som rör teknik.

## Globalt huvudkontor

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

---