

Ett affärscase för IT-konsolidering



Innehålls- förteckning

01

IT-spridningen är utom kontroll
→

02

Befria IT-teamet från
osammanhängande lösningar
→

03

Styrkan i enhetlighet
→

04

Säker AI-användning
→

05

En enhetlig plattform
→

06

Bli en föregångare med
IT-konsolidering
→

Möjligheterna med IT-konsolidering

Den här e-boken riktar sig till IT-ledare som vill slippa kaoset och skapa harmoni i IT-infrastruktur, hantering och bland medarbetare. Lär dig att förbättra prestandan, minska komplexiteten och kostnaderna, öka effektiviteten, stärka säkerheten och förbereda organisationen för AI genom att konsolidera till en enhetlig plattform.

01

IT-spridningen är utom kontroll

När det kommer till hanteringen av digitala ekosystem kan det kännas som att enhetlighet är utom räckhåll. **Att uppfylla en organisations föränderliga krav på produktivitet, säkerhet och AI-beredskap innebär ofta att man får pussla ihop lösningar, ett verktyg i taget.** Även om man lyckas hålla systemet igång, leder det också till att man skapar en komplex IT-miljö som är osammanhängande, tidskrävande att hantera och kostsam att underhålla.

IT-team kan snabbt bli överväldigade av den komplexa och ofta dyra verktygsstacken för slutpunktshantering, identitets- och åtkomsthantering, meddelanden, e-post och produktivitet – listan kan göras lång. Varje åtskilt verktyg innebär ofta olika leverantörer med särskilda krav och isolerade miljöer. Inte undra på att det känns som om budgetar och resurser måste räcka allt längre.

Komplexiteten skapar utmaningar för hela organisationen. Produktiviteten blir lidande när medarbetarna tvingas tillbringa arbetsdagen med att navigera flera olika inloggningar och kämpa för att dela information mellan osammanhängande verktyg. Om de behöver komma åt resurser från olika enheter och platser försvårar den fragmenterade slutpunktshantering för IT-team att upprätthålla säkerheten. Det är dags att rensa upp bland IT-verktygen och förenkla hanteringen.

Antalet specialiserade IT-verktyg och leverantörer fortsätter att växa – och det snabbt.



Sluta betala komplexitetsskatt

Varje inköp av en ny programvarulicens följer samma mönster: ny lösning, nytt kostnadsställe, nytt lager av komplexitet. IT-ledare tvingas göra mycket på en begränsad budget, och dessutom ska de på något sätt hitta resurser för att främja nya AI-initiativ. För att hålla kontroll på budgeten måste många IT-ledare ständigt utvärdera infrastrukturen och leta dubblerade och oanvända licenser. Under 2024 letade IT-ledare besparingar på följande sätt:

83 % minskade utgifterna på oanvänd programvara²

82 % förhandlade fram bättre avtal **med sina leverantörer**²

79 % köpte billigare licensalternativ²

De här strategierna kan leda till vissa besparingar, men det finns en hake. Det växande lapptäcket av appar skapar en "komplexitetsskatt". Värdefull tid och viktiga resurser går åt att granska verktyg och ta bort inaktiva funktioner, samtidigt som de ska hantera säkerhet och åtkomst för osammanhängande lösningar. I stället för att fokusera på arbete som verkligen gör skillnad slösar IT-teamen tid på att granska licenser, förhandla med leverantörer och vända på varenda krona – samtidigt som de underhåller de befintliga lösningarna var för sig. Sådana tidskrävande uppgifter stjälar fokus från mer meningsfullt arbete.

Trots den här typen av besparingsåtgärder kryper komplexitetskostnaden upp igen.

Den enda hållbara lösningen är att ompröva organisationens teknikstrategi. Att konsolidera till en enhetlig plattform minskar komplexiteten och gör det möjligt för IT-team att fokusera på att omvandla verksamheten i stället.

15 %

av alla organisationer har betalat mer än 5 miljoner USD för **att granska sina programvaruleverantörer** under de senaste tre åren²

61 %

av all IT-personal som hanterar digitala tillgångar menar att de **fortfarande inte har full insyn i vilka IT-tillgångar** som påverkar affärsresultaten²

02

Befria IT-teamet från osammanhängande lösningar

För organisationer med många olika tekniklösningar kan den dagliga IT-hanteringen vara en tuff utmaning. Varje engångslösning kräver sin expertis, och det tekniska ekosystemet kan likna en labyrint av osammanhängande verktyg.

IT-teamen blir överbelastade av alla arbetsuppgifter för hantering, underhåll, integrering och support. Varje specialiserat verktyg kräver direkthantering, så flera olika IT-specialister med särskild kompetens behövs för att kunna hålla systemen i drift. Redan nu rapporterar **64 procent** av alla IT-ledare om svårigheter att rekrytera på grund av bristen på nödvändig kompetens eller erfarenhet.³ Det gör det svårare att anställa, utbilda och upprätthålla expertis inom ett team.



03

Styrkan i enhetlighet

Det finns ett bättre sätt att hantera IT-miljön. Genom att konsolidera till en enhetlig lösning kan du minska överbelastningen och skapa ett starkt, flexibelt och fokuserat IT-team. Det gör att du kan:

Effektivisera hanteringen av leverantörsavtal, underhåll och drift.

Förbättra produktiviteten genom att påskynda support- och begärandehantering.

Proaktivt skydda din IT-miljö tack vare enhetlig insyn och hantering.

Det handlar inte bara om att effektivisera systemen. Det handlar om att möjliggöra det viktigaste: Att ge ditt team de bästa förutsättningarna att forma organisationens framtid.

Minska den digitala friktionen

Tekniken ska röja hinder ur vägen, inte skapa nya. Som IT-ledare vet du att **osammanhängande produktivitetens verktyg kan påverka hela organisationen.**

62 procent av alla anställda uppger att de lägger ner för mycket tid på att informationssökning under arbetsdagen.⁵ Den genomsnittliga medarbetaren tillbringar nu **57 procent** av arbetstiden på möten, e-postmeddelanden och chattar, så det är inte så konstigt att **68 procent** menar att de inte får tillräckligt med oavbruten fokustid.⁵

Osammanhängande punktlösningar skapar friktion i dagliga arbetsflöden på nästan omärkbara sätt, men frustrationen ökar snabbt. Flera inloggningar, isolerat arbete, utspridd information och system som inte samarbetar – varje friktionspunkt påverkar kreativiteten och innovationen på ett negativt sätt.

Genom att konsolidera till en plattform kan du minska antalet hinder och skapa utrymme för den värdefulla kreativiteten. Föreställ dig din organisation omvandlas genom konsolidering: Medarbetarna använder en enda enhetlig, säker portal för att komma åt de verktyg och resurser de behöver. Informationen flödar fritt och samarbetet sker naturligt.

När friktionen försvinner återfår människor sin kapacitet att utföra mer meningsfullt arbete. Det handlar inte bara om att undanröja hindren – det handlar om att skapa en miljö där tekniken förstärker människans förmåga.



Centralisera säkerhetsarbetet

Cyberhotbilden är mer komplex än någonsin. De skadliga aktörerna har fler resurser, är mer sofistikerade och har nya tillvägagångssätt som utmanar även de bäst förberedda säkerhetsteam. När säkerhetshoten blir mer sofistikerade blir det svårare att hänga med. **Åttio procent** av alla organisationer har angreppsvägar som exponerar viktiga tillgångar.⁶ **Åttiotvå procent** av alla IT-säkerhetsledare har någon gång blivit överrumplade av en säkerhetsbrist som undgått en kontrollmekanism de trodde fanns.⁷

Organisationer spenderar nu **65 procent** av sina säkerhetsbudgetar på tredjepartsprodukter, och endast **35 procent** går till internt arbete.⁸

Vad är det som skapar den här obalansen? Storföretag har ofta tillgång ett brett spektrum av verktyg för att säkerställa att de har den bästa lösningen för varje enskild uppgift, även när det innebär fler appar att hantera. Det här tillvägagångssättet kan leda till ökade utgifter och en ökad komplexitet.

600 milj. cyberbrottsangrepp inträffade år 2024 – per dag

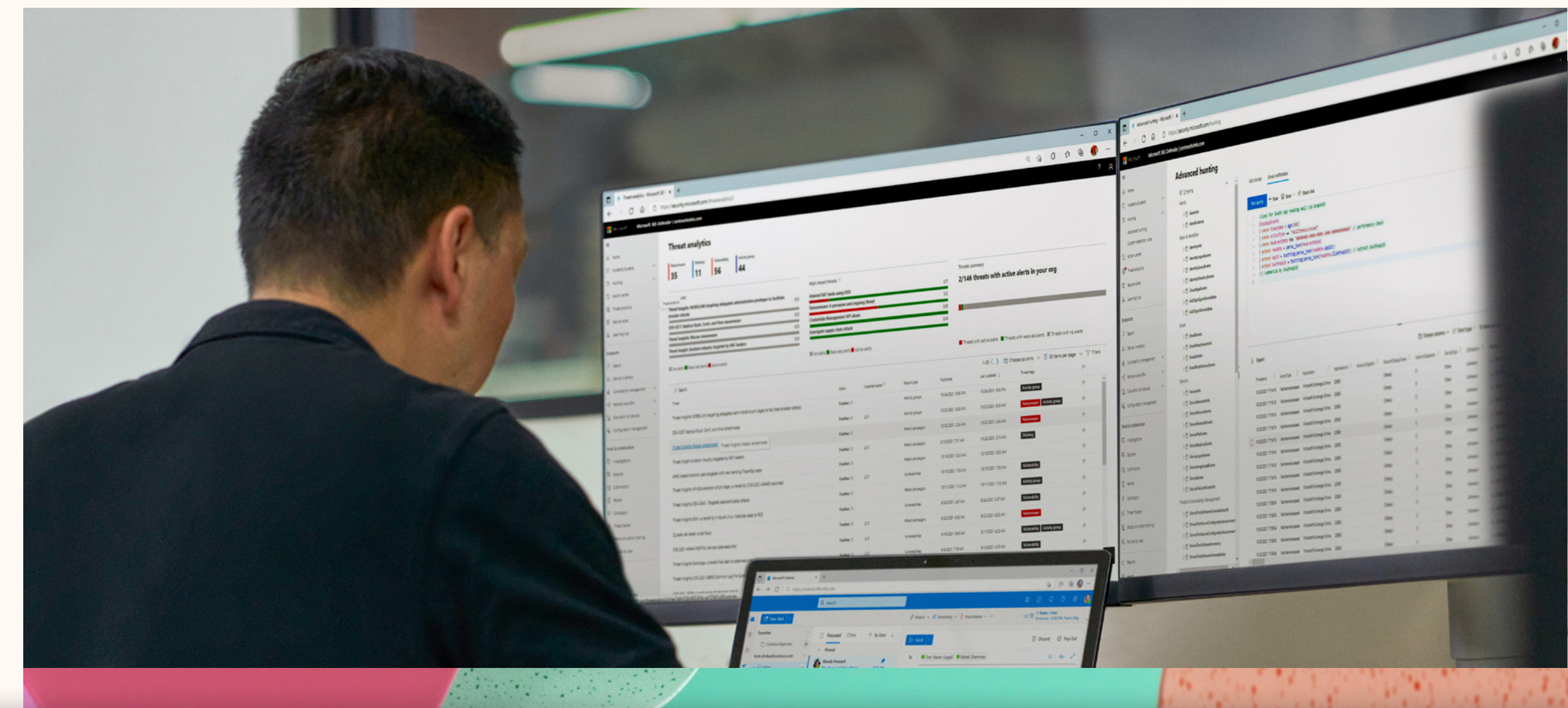
2,75 ggr fler instanser av utpressningrelaterade angrepp utförda av människor⁶

Som svar på det växande hotet köper IT-säkerhetsteam in allt fler lösningar.

19 % Den tvååriga genomsnittliga ökningen av antalet säkerhetsverktyg som storföretagen använder sig av

Att köpa in fler säkerhetsverktyg kan kännas som ett bra sätt att förbättra organisationens skydd. Men att ständigt jaga nya lösningar kan faktiskt göra din organisation mer sårbar. En komplex IT-miljö med många inbördes beroenden är svårare att förstå, hantera och skydda. Ett överflöd av verktyg hindrar dig från att få en tydlig, företagsomfattande bild av teknikstacken. Det skapar också en större attackyta med fler "sidodörrar" in i företagets IT-system.

Genom att konsolidera säkerhetsarbetet på en och samma heltäckande plattform gör du komplexitet till klarhet. Du får en tydlig överblick över hela din digitala egendom. Ett starkt säkerhetsläge går inte att skapa genom att köpa in allt fler olika verktyg. Det blir till när du skapar rätt grund med en enhetlig plattform.



04

Säker AI-användning

IT-medarbetare vill gärna använda AI-teknik till att lätta deras arbetsbörda.

75 % av alla anställda **använder redan AI** i arbetet⁹

78 % av alla AI-användare **tar med sig egna AI-verktyg** till jobbet⁹

Medarbetarna väntar inte på att företagens säkerhetsprotokoll ska hinna ikapp. Och när det blir allt populärare att ta med sig egna AI-verktyg kan organisationer hamna på efterkälken. Endast **24 procent** av alla initiativ för generativ AI innefattar robusta säkerhetsåtgärder.¹⁰

Om organisationer inte skapar förutsättningarna för säker AI-användning åtgärdar medarbetarna bristen på produktivitet med hjälp av skugg-AI: osanktionerade verktyg som finns utanför organisationens system och kontroll.

Förekomsten av skugg-AI innebär två stora utmaningar:

Ingen tillsyn

Skugg-AI medför för allvarliga risker. Vad hindrar en medarbetare från att kopiera och klistra in känslig information i sitt personliga AI-verktyg? Varje interaktion med ett okontrollerat AI-verktyg blir ett nytt säkerhetshot. Organisationens data kommer sannolikt att läcka ut eller användas för att träna en extern modell.

Begränsad användbarhet

79 procent av alla anställda vill använda AI till analytiska uppgifter,⁵ men ett AI-verktyg är bara så användbart som den information det har åtkomst till. Segmenterade, isolerade AI-verktyg producerar ofta ofullständiga svar. Det är därför som egna AI-verktyg ofta bara är av begränsad nytta för personalen.





Organisationer står nu vid ett vägsval: att låta fragmenterad AI leda till möjliga säkerhetsbrister, eller att ta kontroll och införa en enhetlig plattform som är AI-beredd. Som IT-ledare har du en viktig strategisk möjlighet att vägleda din organisation i det här kritiska skedet. Frigör kraften i AI för hela organisationen, med en programsvit som sammanför produktivtetsappar med säkerhets- och efterlevnadsfunktioner – och som är designad att sömlöst integrera med nya AI-funktioner.

Med en konsoliderad plattform kan du effektivt distribuera rätt verktyg för att minska risken med AI-användning och skydda dina data. Att konsolidera gör det också lättare att leverera och hantera en sömlös, säker anslutning mellan organisationens AI-lösning och egna data, resurser och arbetsflöden. Det gör att din AI-lösning kan producera de exakta, användbara insikterna som medarbetarna behöver för att kunna fokusera på jobb som verkligen gör skillnad.

En enhetlig plattform

Microsoft 365 E3 är en enhetlig plattform som förenklar IT-hanteringen, förbättrar organisationens produktivitet med hjälp av sammanhängande upplevelser, skyddar verktyg och slutpunkter och sömlöst integrerar med AI.

Fördelarna med konsolidering med Microsoft 365 E3

Minska IT-kostnaderna

Välj en heltäckande lösning som förenklar molnhanteringen och samlar leverantörerna för att minska de totala utgifterna och förbättra ROI.

Skydda organisationen

Skydda åtkomsten till data, appar och resurser med en enhetlig lösning för hotskydd, stark multifaktorautentisering, policyer för villkorsstyrd åtkomst och kontinuerlig tillgänglighetskontroll.

Inför generativ AI på ett säkert sätt

Genom att skapa en säker grund med en heltäckande plattform som garanterar datasekretess och säkerhet blir din organisation redo att införa AI med Microsoft 365 Copilot.

Slipp IT-komplexitet

Centralisera hanteringen av appar, slutpunkter och identiteter och minska antalet punktlösningar för produktivitet – och kontrollera åtkomst och användning utan att störa organisationens arbetsflöde.

Genom att konsolidera IT-ekosystemet med Microsoft 365 E3 väljer du ett säkrare och mer produktivt sätt att arbeta. Den heltäckande plattformen gör ditt IT-team och hela organisationen beredda att möta vad som än kommer härnäst.

06

Bli en föregångare med IT-konsolidering

Dagens IT-spridning är inte längre hållbar. Att konsolidera det digitala ekosystemet är inte bara en smart strategi – det är ett avgörande steg om du ska kunna minska kostnaderna, förenkla hanteringen, öka produktiviteten och stärka säkerheten i din organisation. Genom att ena verktyg och processer ger du organisationen möjlighet att jobba mer effektivt, förnya i snabbare takt och tryggt anamma AI.



Kom i gång

Källor:

¹ "The state of observability in 2024" Dynatrace, 2024.
<https://www.dynatrace.com/info/reports/state-of-observability-2024/>

² "2024 State of ITAM Report", Flexera, 2024.
<https://info.flexera.com/ITAM-REPORT-State-of-IT-Asset-Management>

³ "Challenges in recruiting employees in the IT industry worldwide 2023", Statista, 5 december 2023.
<https://www.statista.com/statistics/1425097/recruitment-challenges-in-the-tech-industry-worldwide/>

⁴ "Is IT Complexity Standing in the Way of Your Organization's Growth?", Harvard Business Review, 9 december 2022.
<https://hbr.org/sponsored/2022/12/is-it-complexity-standing-in-the-way-of-your-organizations-growth>

⁵ "Kommer AI att göra arbetet?", Microsofts årliga index för arbetstrender, 9 maj 2023.
<https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>

⁶ "Microsofts digitalförsvarsrapport 2024", Microsoft Security, 2024.
<https://www.microsoft.com/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

⁷ "2022 Security Leaders Peer Report", Panaseer, 2022.
<https://panaseer.com/resources/reports/2022-security-leaders-peer-report>

⁸ "The cybersecurity provider's next opportunity: Making AI safer", McKinsey & Company, 14 november 2024.
<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer>

⁹ "AI på arbetet är här. Det är nu det svåra jobbet börjar", Microsofts årliga index för arbetstrender, 8 maj 2024.
<https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

¹⁰ "Cost of a Data Breach Report 2024", IBM, 2024.
<https://www.ibm.com/reports/data-breach>

¹¹ "Datasäkerhet som grund för säkert införande av AI", Microsoft Security, 2024.
<https://clouddamcdnprodep.azureedge.net/gdc/gdckHueRY/original>

© 2025 Microsoft Corporation. Med ensamrätt. Det här dokumentet tillhandahålls i befintligt skick. Den information och de åsikter som uttrycks i dokumentet, inklusive webbadresser och hänvisningar till andra webbplatser, kan ändras utan förvarning. Risker för att använda dessa åvilar dig. Det här dokumentet ger dig inga juridiska rättigheter till någon immateriell egendom i någon Microsoft-produkt. Du får kopiera och använda detta dokument för interna referensändamål.