



MICROSOFT 365 PRODUKTFÖRDELAR

Microsoft 365 Säkerhets- jämförelse

Microsoft 365 produktfördelar

Microsoft 365 Business Premium är Microsofts mest attraktiva erbjudande för små och medelstora företag (SME) som vill ha en integrerad lösning som sammanför produktiviteten hos Microsoft 365 med avancerad säkerhet och enhetshantering.

Denna tabell visar hur mycket säkrare ditt företag och dina användare kan vara med Microsoft 365 Business Premium jämfört med Microsoft 365 Business Standard och Office 365 E3.

Symbolförklaring



Inte inkluderat



Delvis inkluderat



Inkluderat

Aktivera fjärråtkomst och skydda identiteter

Få säker åtkomst till affärsapplikationer oavsett var du arbetar.

Produktfördel	Relevans...	Microsoft komponent	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Office 365 E3
Se till att bara önskade personer har tillgång till ditt system genom att konfigurera policies som inaktiverar åtkomst från osäkra platser och enheter.	En brandvägg ger inte längre tillräckligt skydd, när data finns i molnet och anställda arbetar från olika platser och enheter.	Conditional Acces			
Använd multifaktorautentisering för att skydda ditt system och din data mot obehörig åtkomst , när ett lösenord är förlorat eller stulet	Lösenord kan lätt komprometteras. Genom att kräva fler typer av godkännande för att bevisa din identitet när du loggar in på en applikation ser du till att dina konton är upp till 99,9% mindre benägna att äventyras	Multi-Factor Authentication (1)			
Ge anställda fjärrskrivbordsåtkomst från valfri enhet, samtidigt som du upprätthåller central kontroll och säkerhet.	Stöder en mobil arbetskraft som kan fungera från alla enheter och platser medan du får samma avancerade säkerhet, som Azure erbjuder	Windows Virtual Desktop			
Ge anställda, som arbetar från externa platser, säker tillgång till kritiska on-premapplikationer eller affärsapplikationer , utan att behöva tillåta bred tillgång till företagets internet.	Det är billigare än traditionella fjärråtkomstlösningar som VPN, fungerar på flera enheter och du kan styra vilka applikationer som ska vara tillgängliga till skillnad från att ge tillgång till hela nätverket.	Azure AD Application Proxy			







(1) M365 Business Premium innehåller flera funktioner för multifaktorautentisering och tillhandahåller en bättre användarupplevelse. Du kan till exempel välja att inte aktivera MFA för användare som är på kontor, men be om godkännande om de får tillgång till dina data och system från andra platser eller arbetar från en osäker enhet:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing>

Försvara dig mot cyberhot och skydda affärsdata










Kontrollera vem som har tillgång till din företagsinformation




Produktfördel	Relevans...	Microsoft komponent	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Office 365 E3
Undvik falska och skadliga webbplatser genom att skanna länkar i realtid i e-post och dokument	Bara under 2019 blockerade Microsoft över 13 miljarder skadliga och misstänkta e-postmeddelanden	Microsoft Defender for Office 365	☆	★	☆
Skydd mot sofistikerad skadlig kod genom avancerad analys av bilagor i e-post.	Över 90% av skadlig programvara levereras via e-post.	Microsoft Defender for Office 365	☆	★	☆
Aktivera policyer mot nätfiske som använder maskininlärning och imitationsidentifiering för att ge skydd mot avancerade attacker.	Ca 90% av alla cyberattacker börjar med ett e-postmeddelande. Phishing uppstår när individer eller organisationer får ett bedrägligt e-postmeddelande som uppmuntrar dem att klicka på en länk som ger cyberbrottslingar tillgång till en enhet eller till personlig information.	Microsoft Defender for Office 365	☆	★	☆
Tillämpa skydd mot skadlig kod på alla Windows 10-enheter och skydda filer i viktiga systemmappar mot förändringar gjorda av ransomware.	Enligt Myndigheten för Samhällsskydd och Beredskap ökade hot från riktade ransomware-attacker mot svenska företag.	Windows Exploit Guard Enforcement	☆	★	☆
Använd automatisk detektion för att förhindra att känslig information som t ex personnummer eller kreditkortsnummer läcker till oönskade personer.	Nästan hälften av dataintrången beror på skadliga eller kriminella attacker, medan 27% är ett resultat av handhavandefel . Med Data Loss Prevention kan du undvika oavsiktlig delning av känslig information.	Microsoft Data Loss Prevention	☆	★	★

Kryptera känsliga e-postmeddelanden så att anställda kan kommunicera säkert med kunder eller andra utanför företaget. Ser till att bara den avsedda mottagaren kan läsa meddelandet.	E-post är ett sårbart medium, särskilt när e-postmeddelanden skickas över osäkra eller offentliga WiFi-nätverk. Även mejl, inklusive din inloggningsinformation, som skickas i ett säkert företagsnätverk kan fångas upp av externa användare.	Office 365 Message Encryption			
Bestäm vem som har tillgång till affärsinformation genom att använda begränsningar som t ex "Kopiera inte" och "Skicka inte fram" i e-post och dokument.	Nästan alla företag och organisationer har konfidentiell eller känslig data som inte ska vidarebeordras och falla i fel händer.	Office 365 Message Encryption			

Hantera enheter enkelt och säkert

Behåll kontrollen över telefoner, surfplattor och datorer som har åtkomst till dina företagsdata.

Produktfördel	Relevans...	Microsoft komponent	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Office 365 E3
Skydda affärsdata på iOS- och Android-enheter. Kräver till exempel att användare anger en PIN-kod eller ett fingeravtryck för att få tillgång till affärsdata och krypterad data på mobila enheter.	Personligt ägda, okrypterade enheter som har tillgång till företagets system är en säkerhetsrisk, när anställda arbetar från externa platser.	Intune			
Se till att affärsdokument, mejl och annan data bara kan lagras och förvaras i godkända mobila Office-appar, inte i obehöriga och personliga appar och webbplatser.	Personliga appar är inte nödvändigtvis säkra. Hög risk för sårbarheter finns hos 38% av mobilapplikationer för iOS och i 43% av Android-applikationer.	Intune			
Ta bort affärsdata från förlorade eller stulna enheter utan att påverka den personliga informationen.	Skyddar dina företagsdata från obehöriga användares åtkomst och säkerställer också att du kan ta bort data på anställdas egna enheter när de är inte längre är anslutna till företaget.	Intune			

<p>Tillämpa BitLocker-kryptering och automatisk installation av viktiga Windows-uppdateringar via förenklade kontroller.</p>	<p>BitLocker skyddar filer och data mot obehöriga användares åtkomst genom kryptering av hårddisk.</p>	<p>Bitlocker</p>			
<p>Sätt igång medarbetare snabbt och kostnadseffektivt med nya Windowsenheter som använder molnbaserad förberedelse och förkonfiguration av nya datorer och bärbara datorer.</p>	<p>Eliminerar behovet av traditionell imageutrollning och enheterna kan skickas direkt från tillverkare till slutanvändare utan att behöva gå via it avdelningen först.</p>	<p>Windows Autopilot</p>	