Pakalpojuma "Kiberdrošība uzņēmumiem" kopsavilkums

Bitdefender

Galvenās funkcijas

Aizsardzības risinājums, kas bloķē ļaunatūru, izspiedējprogrammas un uzrauga aizdomīgu uzvedību datoros.

- Rīka licenču lietošanas noteikumi: šeit.
- Privātuma atrunas: šeit.

Funkcionālie parametri

PC: Bitdefender XEDR darbojas uz darbstacijām ar operētājsistēmu Windows 7 SP1 vai jaunāku versiju, tostarp Windows 8.1, Windows 10 un Windows 11.

Mac: Bitdefender XEDR ir pieejams macOS vidē, sākot no Mac OS X 10.12 (Sierra) un jaunākām versijām.

Linux: Bitdefender XEDR darbojas uz izplatītākajām Linux distribūcijām, tostarp Ubuntu, Debian, CentOS un RHEL, sākot no versijām 6.x/16.04 un jaunākām.

Pilna funkcionalitāte, tai skaitā uzvedības uzraudzība, incidentu vizualizācija un reakcijas darbības, ir pieejama tikai tad, ja ierīce ir pilnībā atjaunināta un atbilst Bitdefender drošības komponentu prasībām.

Pakalpojuma ietvaros vienam lietotājam tiek apkalpota viena ierīce.

Checkpoint (Harmony Email & Collaboration)

Galvenās funkcijas

E-pasta un mākoņplatformu drošības risinājums, kas novērš pikšķerēšanu, ļaunprogrammatūru un datu noplūdi.

- Rīka licenču lietošanas noteikumi: šeit.
- Privātuma atrunas: šeit.

Funkcionālie parametri

Piemērojams tikai Microsoft Exchange Online (Microsoft Office 365) vai Google Workspace mākoņvidēs uzturētajiem e-pastiem. Nav paredzēts lokālo e-pastu serveru apkalpošanai.

Viena licence ietver vienu individuālā lietotāja pastkastes apkalpošanu. Koplietotām pastkastēm un adresātu grupām netiek noteikta papildu maksa.

Dropsuite

Galvenās funkcijas

Automātiska Microsoft 365 datu rezerves kopēšana un atjaunošana, lai pasargātu e-pastus un dokumentus. Nodrošina piekļuves datu un lietotāju identitāšu rezerves kopijas un arhivēšanu atbilstībai un drošībai.

- Rīka licenču lietošanas noteikumi: šeit.
- Privātuma atrunas: šeit.

Funkcionālie parametri

Viena licence ietver vienu individuālā lietotāja apkalpošanu. Koplietotām pastkastēm un adresātu grupām netiek noteikta papildu maksa.

Klientiem, kuri vēlas izmantot neierobežotu krātuvi, ir jāiekļauj vismaz 80% no saviem Microsoft 365 vai Google Workspace licencētajiem lietotājiem. Ja klients nevar nodrošināt vismaz 80% lietotāju pievienošanu, kopējais konta glabāšanas apjoms tiek noteikts 100 GB par katru samaksātu lietotāja licenci.

Risinājums nodrošina datu rezerves kopēšanas un arhivēšanas atbalstu šādām platformām: Microsoft Office 365, Google Workspace (iepriekš G Suite), Gmail, IMAP/POP3, Hosted Exchange, Open-Xchange un Microsoft Entra Active Directory.

Datu uzglabāšanas termiņš – pēc noklusējuma viens gads (ar iespēju noteikt ilgāku laiku). E-pastiem datu dublēšana tiek veikta vismaz 12 reizes dienā, SharePoint un Teams – trīs reizes dienā, citām aplikācijām – vismaz vienu reizi dienā.

Commvault

Galvenās funkcijas

Risinājums, kas veido darbastaciju failu un datu rezerves kopijas, nodrošinot ātru atjaunošanu pēc incidentiem vai bojājumiem.

- Rīka licenču lietošanas noteikumi: šeit.
- Privātuma atrunas: šeit.

Funkcionālie parametri

Pakalpojuma ietvaros vienam lietotājam tiek apkalpotas 1–3 ierīces.

Datu uzglabāšanas termiņš – viens gads. Datu dublēšana tiek veikta vienu reizi četrās stundās vai pie pirmās iespējas, kad dators ir tiešsaites režīmā. Ja dators ilgāk par sešiem mēnešiem ir bezsaites režīmā, jaunu datu dublēšana vairs netiek veikta.

PC: Windows (no 7), macOS (Sierra–Mojave), Linux (Ubuntu, Debian, CentOS, RHEL, Fedora, SLES u.c.).

Dublēšanas pārklājums – lokālie faili, dati un mapes, lietotāja uzstādījumi. Netiek atjaunotas programmatūras vai sistēmas.

Usecure

Galvenās funkcijas

Darbinieku kiberdrošības apmācību platforma ar e-kursiem un pikšķerēšanas simulācijām, lai mazinātu cilvēciskos riskus.

- Rīka licenču lietošanas noteikumi: šeit.
- Privātuma atrunas: šeit.

Funkcionālie parametri

Ierobežota pieejamība latviešu valodā e-apmācību moduļiem.

Pakalpojuma "Kiberdrošība uzņēmumiem" saturs

Pakalpojuma saturs	Abonementa veids	
	Bāze	Kodols
Lietotāju tehniskais atbalsts (lietotāju izmaiņas, darbības traucējumu novēršana u.c.)*	✓	✓
Drošības konfigurāciju pielāgošana	✓	✓
Antivīrusa aizsardzība	✓	✓
Aizsardzība pret izspiedējprogrammatūru (ransomware)	✓	✓
Proaktīva apdraudējumu un anomāliju uzraudzība darbstacijās (EDR)	✓	✓
Reakcija uz apdraudējumiem, novēršanas darbības	✓	✓
E-pastu aizsardzība pret pikšķerēšanu un ļaunatūru	✓	✓
Darba vides aplikāciju un e-pastu datu rezerves kopēšana mākonī (Microsoft 365/Google Workspace backup)	✓	✓
E-pastu aizsardzība pret nejaušu sensitīvas informācijas izsūtīšanu (DLP)	x	✓
Pikšķerēšanas simulācijas darbiniekiem reizi ceturksnī	x	✓
Kiberhigiēnas e-apmācības darbiniekiem (e-kursi)	x	✓
Darbstacijas (datora) failu rezerves kopēšana mākonī (back up)	x	✓
Microsoft 365 lietotāju un grupu datu rezerves kopēšana (Entra ID backup)	x	✓
E-pastu arhivēšana (neizdzēšami, automātiski)	x	✓
Iespēja attālināti dzēst datus no pazaudēta vai nozagta datora	x	✓
Ikmēneša vai ikceturkšņa drošības atskaite par veiktajiem darbiem/novērstajiem apdraudējumiem	x	✓

* Reakcijas laiks uz pieteikumu – 2 stundu laikā (darbdienās plkst. 8.00–20.00). Tehnisko atbalstu nodrošina LMT sadarbībā ar SIA "Egate".