

Cybersecurity for Businesses: Service Summary

Bitdefender

Main functions

A security solution designed to block malware and ransomware, while also monitoring suspicious activity on computers.

- Terms of use for tool licences available [here](#).
- Privacy statements available [here](#).

Functional parameters

PC: Bitdefender XEDR is compatible with workstations running Windows 7 SP1 or later versions, including Windows 8.1, Windows 10, and Windows 11.

Mac: Bitdefender XEDR supports macOS environments from Mac OS X 10.12 (Sierra) and later versions.

Linux: Bitdefender XEDR supports most common Linux distributions, including Ubuntu, Debian, CentOS, and RHEL, from version 6.x/16.04 upwards.

Full functionality, such as activity monitoring, incident visualisation, and response actions, is only available if the device is fully updated and meets the requirements of Bitdefender security components.

The service covers one device per user.

Checkpoint (Harmony E-mail & Collaboration)

Main functions

An e-mail and cloud security solution designed to prevent phishing, malware, and data leaks.

- Terms of use for tool licences available [here](#).
- Privacy statements available [here](#).

Functional parameters

Limited to e-mails hosted on Microsoft Exchange Online (Microsoft Office 365) or Google Workspace cloud environments. Not intended for local e-mail servers.

One licence covers one individual user mailbox. No additional fees are charged for shared mailboxes and recipient groups.

Dropsuite

Main functions

Automatic backup and recovery of Microsoft 365 data to protect e-mails and documents. This includes backup and archiving of access data and user identities for compliance and security purposes.

- Terms of use for tool licences available [here](#).
- Privacy statements available [here](#).

Functional parameters

One licence includes one individual user service. No additional fees are charged for shared mailboxes and recipient groups.

For unlimited storage, customers are required to include at least 80% of their Microsoft 365 or Google Workspace licensed users. If a customer cannot include at least 80% of users, the total account storage is limited to 100 GB per paid user licence.

The solution offers data backup and archiving support for the following platforms: Microsoft Office 365, Google Workspace (formerly G Suite), Gmail, IMAP/POP3, Hosted Exchange, Open-Xchange, and Microsoft Entra Active Directory.

Data retention period: one year by default (with extension options).

E-mail data is backed up at least 12 times a day, for SharePoint and Teams three times a day, and for other apps at least once a day.

Commvault

Main functions

A solution designed to backup workstation files and data, ensuring fast recovery after incidents or damage.

- Terms of use for tool licences available [here](#).
- Privacy statements available [here](#).

Functional parameters

The service covers 1–3 devices per user.

Data retention period: one year. Data is backed up once every four hours or at the earliest opportunity when the computer comes online. New data is not backed up if the computer has been offline for over six months.

PC: Windows (from 7), macOS (Sierra–Mojave), Linux (Ubuntu, Debian, CentOS, RHEL, Fedora, SLES, etc.).

Backup coverage includes local files, data and folders, as well as user settings. No software or system / bare metal backups.

Usecure

Main functions

A cybersecurity training platform for staff, offering e-learning courses and phishing simulations to minimise human-related risks.

- Terms of use for tool licences available [here](#).
- Privacy statements available [here](#).

Functional parameters

Limited availability of e-training modules in Latvian.

Cybersecurity for Businesses: Content

Content of the service	Type of subscription	
	Base	Core
User technical support (user count adjustments, elimination of malfunctions, etc.)*	✓	✓
Adjustment of security configurations	✓	✓
Antivirus protection	✓	✓
Protection against ransomware	✓	✓
Proactive monitoring of threats and anomalies in workstations (EDR)	✓	✓
Threat response, preventive actions	✓	✓
Protection of e-mails from phishing and malware	✓	✓
Cloud-based backup of workspace apps and e-mails (Microsoft 365/Google Workspace backup)	✓	✓
E-mail protection against accidental leakage of sensitive information (DLP)	x	✓
Quarterly phishing simulations for employees	x	✓
Regular cyber hygiene trainings for employees (e-learning courses)	x	✓
Cloud-based workstation (computer files and folders) backup	x	✓
Backup of Microsoft 365 user and group data (Entra ID backup)	x	✓
E-mail archiving (immutable, automatic)	x	✓
Remote data deletion option for lost or stolen computers	x	✓
Monthly or quarterly security reports on completed tasks/mitigated threats	x	✓

* Support response time: within 2 hours (Monday through Friday, 8 AM to 8 PM).
Technical support is provided by LMT in cooperation with SIA "Egate".